April 2021 · Rebecca Beigel & Dr. Sven Herpig
Supported by Christina Rupp

Germany's Cybersecurity Architecture

Translation of the 6th German Edition

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Table of Contens

1. Background

The foundation of Germany's cybersecurity architecture dates back to 1986. It was in this year that the organization preceding the "Bundesamt für Sicherheit in der Informationstechnik" (Federal Office for Information Security, BSI, official translation), known as the "Zentralstelle für das Chiffrierwesen" (Central Office for Encryption, ZfCh, own translation), set up a working party to deal with questions of security amid the rapid development of ICT technology[1]. On January 1, 1991, the BSI began its work as an offshoot of the "Bundesnachrichtendienst" (Federal Intelligence Service, BND, official translation). In particular following the publication of the Cyber Security Strategy for Germany 2011, Germany's national security architecture caught the public's attention[2].

Much has happened since then: Cybersecurity has become a core part of German security and defence policy, which has led to the emergence of new national and international players in the field as well as the development of links between them. Nevertheless, neither the 2011 strategy, nor the updated 2016 strategy[3], contain an overview of the increasingly complex architecture of German authorities' tasks and competencies in cyberspace, albeit visualized or otherwise. For the first time, the "Bundesministerium des Innern, für Bau und Heimat" (Federal Ministry of the Interior, Building and Community, BMI, official translation) has presented a list of cybersecurity actors and initiatives from state, civil society, academia and industry as an online compendium in November 2020 within the framework of its National Cyber Security Pact[4]. We hope that our publication series, in existence since 2018, has contributed to the BMI's decision to take this step.

A structured policy approach is indispensable for effectively and efficiently positioning Germany within the realm of cyberspace, especially when considering limited resources[5]. In this respect, this publication therefore seeks to make a contribution within the framework of Stiftung Neue Verantwortung's policy work on cybersecurity[6]. Hence, this publication provides a visualization of Germany's national cyber security architecture, a list of abbreviations and actors, as well as an explanation of the relationships between individual actors. In the current edition of this publication, municipal and NATO actors have been included as two new levels. Moreover, updates, adjustments and new actors have been made and added at EU, federal and federal state levels.

1 Federal Office for Information Security, Jahresbericht 2003.
2 Federal Ministry of the Interior, Cyber-Sicherheitsstrategie für Deutschland 2011.
3 Federal Ministry of the Interior, Cyber-Sicherheitsstrategie für Deutschland 2016.
4 Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland.
5 Julia Schuetze, Warum dem Staat IT-Sicherheitsexpert:innen fehlen.
6 Stiftung Neue Verantwortung, International Cybersecurity Policy.

Identified connections in the visualization represent different aspects of a given relationship, ranging from the deployment of employees within the respective organization to members of the advisory board, financial grants or legal and professional supervision. Other international actors such as the United Nations (UN), mere legislative and judicial actors at all levels as well as actors in the private sector, academia and civil society are not yet accounted for.

This publication is based almost exclusively on open-source information. For this reason, we are grateful for any tips based on open-source information regarding additional information not included in these pages. Please contact Christina Rupp with suggestions for changes or additions. This document will be periodically updated in order to account for the latest developments of Germany's cybersecurity architecture.

Within the next edition (to be published in fall 2021) we would like to provide an overview of the evolution of described cybersecurity architecture and employ new opportunities for visualization.

This publication is a translation that is based on the current 6th edition of the German version. The earlier editions in German can be retrieved accordingly:

Edition	Date	Co-Author	Co-Author	Publication
1st Edition	07/2018	Sven Herpig	Tabea Breternitz	Link
2nd Edition	04/2019	Sven Herpig	Clara Bredenbrock	Link
3rd Edition	11/2019	Sven Herpig	Kira Messing	Link
4th Edition	03/2020	Sven Herpig	Rebecca Beigel	Link
5th Edition	10/2020	Sven Herpig	Rebecca Beigel	Link
6th Edition	04/2021	Sven Herpig	Christina Rupp	Current version

CYBERSECURITY ARCHITECTURE OF GERMANY

EUROPEAN UNION

NATO

FEDERAL LEVEL

FEDERAL STATE LEVEL

LOCAL LEVEL

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

Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel

Version: April 2021

3. Actors and Abbreviations

For reference, this list contains all abbreviations and terms used within our visualization. Explanations for all actors mentioned can be found at the respective levels (in alphabetical order). In cases of existing German and English official abbreviations for an actor, the former ones are being deliberately used throughout this publication in order to ensure comprehensibility and consistency with the visualization. Accordingly, the respective headers of the actor explanations are structured as follows, either a) German title (English title, abbreviation, own/official translation), or b) English title alone.

It should be noted that not all of them can be found in the visualization, as some of them are perceived to be integrated in the portrayal of other actors (example: CERT-Bund in BSI). Within the following list, own translations of actors are underlined. Institutions written in *italics are either still in the planning process or are currently in development*.

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
4C	Cybercrime Competence Center – Saxony-Anhalt	Cybercrime Competence Center – Sachsen-Anhalt
AA	German Federal Foreign Office	Auswärtiges Amt
ACO	Allied Command Operations	
ACS	Alliance for Cybersecurity	Allianz für Cyber-Sicherheit
ACT	Allied Command Transformation	
BAAINBw	Federal Office of Bundeswehr Equipment, Information Technology, and In-Service Support	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
BaFin	Federal Financial Supervisory Authority	Bundesanstalt für Finanzdienstleistungsaufsicht
BAKS	Federal Academy for Security Policy	Bundesakademie für Sicherheitspolitik
BAMAD	Federal Office for Military Counter-Intelligence	Bundesamt für den Militärischen Abschirmdienst
Bayern CERT	Computer Emergency Response Team Bayern	Computer Emergency Response Team Bayern

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
BBK	Federal Office of Civil Protection and Disaster Assistance	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BDBOS	German Federal Agency for Public Safety Digital Radio	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
BeLVIS	Chief Information Security Officer of the State Administration Mecklenburg-Western Pomerania	Beauftragte:r für Informationssicherheit Mecklenburg-Vorpommern
Berlin-CERT	Computer Emergency Response Team Berlin	Computer Emergency Response Team Berlin
BfDI	Federal Commissioner for Data Protection and Freedom of Information	Bundesbeauftragte:r für den Datenschutz und die Informationssicherheit
BfIS	Chief Information Security Officer of the State Administration Saxony	Beauftragte:r für Informationssicherheit Sachsen
BfV	Domestic Intelligence Service of the Federal Republic of Germany	Bundesamt für Verfassungsschutz
BKA	Federal Criminal Police Office	Bundeskriminalamt
BKAmt	Federal Chancellery	Bundeskanzleramt
BKartA	Federal Cartel Office	Bundeskartellamt
BMBF	Federal Ministry of Education and Research	Bundesministerium für Bildung und Forschung
BMF	Federal Ministry of Finance	Bundesministerium für Finanzen
BMG	Federal Ministry of Health	Bundesministerium für Gesundheit
BMI	Federal Ministry of the Interior, Building and Community	Bundesministerium des Innern, für Bau und Heimat
BMJV	Federal Ministry of Justice and Consumer Protection	Bundesministerium der Justiz und für Verbraucherschutz
BMVg	Federal Ministry of Defence	Bundesministerium der Verteidigung
BMVI	Federal Ministry of Transport and Digital Infrastructure	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Federal Ministry for Economic Affairs and Energy	Bundesministerium für Wirtschaft und Energie

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
BMZ	Federal Ministry for Economic Cooperation and Development	Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
BND	Foreign Intelligence Service of Germany	Bundesnachrichtendienst
BNetzA	Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BPol	Federal Police	Bundespolizei
BSI	Federal Office for Information Security	Bundesamt für Sicherheit in der Informationstechnik
Bündnis für Cybersicherheit	Coalition for Cyber Security	Bündnis für Cybersicherheit
Bw	German Armed Forces	Bundeswehr
BWI	National IT Systems House GmbH	Bundesweite IT-Systemhaus GmbH
C3B	NATO Consultation, Control and Command Board	
CAZ	Cyber-Alliance Centre – Bavaria	Cyber-Allianz-Zentrum – Bayern
CCC	Cyber-Competence-Center – Brandenburg	Cyber-Competence-Center – Brandenburg
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence	
CDC	NATO Cyber Defence Committee	
CDC-Lv	Cyber Defense Center of the Berlin State Administration	Cyber Defense Center der Landesverwaltung Berlin
CDMB	NATO Cyber Defence Management Board	
CEPOL	The European Union Agency for Law Enforcement Training	Europäische Polizeiakademie
CERT BWL	Computer Emergency Response Team Baden-Wuerttemberg	Computer Emergency Response Team Baden-Württemberg
CERT Brandenburg	Computer Emergency Response Team Brandenburg	Computer Emergency Response Team Brandenburg

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
CERT Hessen	Computer Emergency Response Team Hesse	Computer Emergency Response Team Hessen
CERT M-V	Computer Emergency Response Team Mecklenburg-Western Pomerania	Computer Emergency Response Team Mecklenburg-Vorpommern
CERT Nord	Computer Emergency Response Team Schleswig-Holstein, Hamburg, Bremen and Saxony-Anhalt	Computer Emergency Response Team Schleswig-Holstein, Hamburg, Bremen and Sachsen-Anhalt
CERT NRW	Computer Emergency Response Team North Rhine Westphalia	Computer Emergency Response Team Nordrhein-Westfalen
CERT Saarland	Computer Emergency Response Team Saarland	Computer Emergency Response Team Saarland
CERT-Bund	Computer Emergency Response Team for Federal Agencies	Computer Emergency Response Team des Bundes
CERT-EU	Computer Emergency Response Team of the European Commission	Computer Emergency Response Team der Europäischen Kommission
CERT-rlp	Computer Emergency Response Team Rhineland-Palatinate	Computer Emergency Response Team Rheinland-Pfalz
CERT-Verbund	National CERT Network	Nationaler Verbund von Computer Emergency Response Teams
CIDCC	Cyber and Information Domain Coordination Centre	
CIHBw	Cyber Innovation Hub	Cyber Innovation Hub
CIR	Cyber and Information Domain Service	Organisationsbereich Cyber- und Informationsraum der Bundeswehr
CISO-rlp	Chief Information Security Officer of the State Administration Rhineland-Palatinate	Informationssicherheitsbeauftragte:r der Landesverwaltung Rheinland-Pfalz
CMPD	Crisis Management and Planning Directorate	Direktion Krisenbewältigung und Planung
CODE	Cyber Defence Research Institute	Forschungsinstitut Cyber Defence
Council	Council of the European Union	Rat der Europäischen Union

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
cPPP	Contractual Public-Private Partnership on Cybersecurity	
CSIRTs Netzwerk	Computer Security Incident Response Teams Network	Computer Security Incident Response Teams Netzwerk
Cyber Security Cluster Bonn	Cyber Security Cluster Bonn e. V.	Cyber Security Cluster Bonn e. V.
Cyberabwehr Bayern	Cyber Defence – Bavaria	Cyberabwehr – Bayern
Cyberagentur	Agency for Innovation in Cybersecurity	Agentur für Innovation in der Cybersicherheit GmbH
Cyber-AZ	National Cyber Defence Centre	Nationales Cyber-Abwehrzentrum
Cybercrime-Kompetenzzentrum	Cybercrime Competency Center – North Rhine-Westphalia	Cybercrime-Kompetenzzentrum – Nordrhein-Westfalen
Cyber-Reserve	Military Cyber Reserve	Cyber-Reserve
Cyber-SR	National Cyber Security Council	Nationaler Cyber-Sicherheitsrat
Cyberwehr	Cyber Defence – Baden-Wuerttemberg	Cyberwehr – Baden-Württemberg
CyCLONe	Cyber Crisis Liaison Organisation Network	
CyOC	NATO Cyberspace Operations Centre	
DAkkS	German National Accreditation Body	Deutsche Akkreditierungsstelle
Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken	Cybercrime Department of the Public Prosecutor's Office of Saarbrücken	Cybercrime Department of the Public Prosecutor's Office of Saarbrücken
Dezernat Cybercrime des Landeskriminalamtes Mecklenburg-Vorpommern	Cybercrime Department of the Mecklenburg-Western Pomerania State Office of Criminal Investigation	Dezernat Cybercrime des Landeskriminalamtes Mecklenburg-Vorpommern
Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz	Cybercrime Department of the Rhineland-Palatinate State Office of Criminal Investigation	Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
Dezernat Cybercrime des Landeskriminalamtes Thüringen	Cybercrime Department of the Thuringia State Office of Criminal Investigation	Dezernat Cybercrime des Landeskriminalamtes Thüringen
Dezernat LPP 222	Department LPP 222 Cybercrime – Saarland	Dezernat LPP 222 Cybercrime – Saarland
DsiN	Germany Secure on the Internet e. V.	Deutschland sicher im Netz e. V.
EA	European co-operation for Accreditation	Europäische Kooperation für Akkreditierung
EAD	European External Action Service	Europäischer Auswärtiger Dienst
EC3	European Cybercrime Center	Europäisches Zentrum zur Bekämpfung der Cyber-Kriminalität
ECCC	European Cybersecurity Industrial, Technology and Research Competence Centre	Europäisches Zentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit
ECCG	The European Cybersecurity Certification Group	Europäische Gruppe für die Cybersicherheitszertifizierung
ECSO	European Cyber Security Organisation	
ECTEG	European Cybercrime Training and Education Group	
EDSB	European Data Protection Supervisor	Europäische:r Datenschutzbeauftragte:r
EGC group	European Government CERTs group	
EJCN	European Judicial Cybercrime Network	
EJN	European Judicial Network	
EJTN	European Judicial Training Network	
EK	European Commission	Europäische Kommission
EMERGE IoT	EMERGE IoT – Mecklenburg-Western Pomerania	EMERGE IoT – Mecklenburg-Vorpommern
ENISA	European Union Agency for Cybersecurity	Agentur der Europäischen Union für Cybersicherheit

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
ENISA AG	ENISA Advisory Group	ENISA-Beratungsgruppe
ER	European Council	Europäischer Rat
ERCC	Emergency Response Coordination Centre	Zentrum für die Koordination von Notfallmaßnahmen
ESCD	Emerging Security Challenges Division	
ESVK	European Security and Defence College	Europäisches Sicherheits- und Verteidigungskolleg
EU Hybrid Fusion Cell	EU Hybrid Fusion Cell	EU-Analyseeinheit für hybride Bedrohungen
EUCTF	European Union Cybercrime Task Force	
EUISS	European Union Institute for Security Studies	Institut der Europäischen Union für Sicherheitsstudien
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice	Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht
EUMC	European Union Military Committee	Militärausschuss der Europäischen Union
EUMS INT	Intelligence Directorate of the European Union Military Staff	Intelligence Directorate des EU-Militärstabs
Eurojust	European Union Agency for Criminal Justice Cooperation	Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen
Europol	European Police Office	Europäisches Polizeiamt
EVA	European Defence Agency	Europäische Verteidigungsagentur
FITKO	Federal IT Cooperation	Föderale IT-Kooperation
G4C	G4C German Competence Centre against Cyber Crime e. V.	G4C German Competence Centre against Cyber Crime e. V.

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
GD CONNECT	Directorate-General for Communications Networks, Content and Technologies	Generaldirektion Kommunikationsnetze, Inhalte und Technologien
GD DIGIT	Directorate-General for Informatics	Generaldirektion Informatik
GD HOME	Directorate-General for Migration and Home Affairs	Generaldirektion Migration und Inneres
GD JRC	Directorate-General Joint Research Centre	Gemeinsame Forschungsstelle
GD RTD	Directorate-General for Research and Innovation	Generaldirektion Forschung und Innovation
gematik	gematik	gematik
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH
GLZ CIR	Situation Center Cyber and Information Domain Service	Gemeinsames Lagezentrum Cyber und Informationsraum
GMLZ	Joint Information and Situation Centre of the Federal Government and the Federal States	Gemeinsames Melde- und Lagezentrum
Gruppe der Interessen-träger für die Cybersicher-heitszertifizierung	Stakeholder Cybersecurity Certification Group	Gruppe der Interessenträger für die Cybersicherheitszertifizierung
Hessen3C	Hessen Cyber Competence Center	Hessen Cyber Competence Centre
Horizon 2020	Horizon 2020	
HWP	Horizontal Working Party on Cyber Issues	
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats	
IMK	Conference of Interior Ministers	Innenministerkonferenz
Initiative IT-Sicherheit in der Wirtschaft	Initiative IT Security in the Economy	Initiative IT-Sicherheit in der Wirtschaft

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
Initiative Wirtschaftsschutz	Initiative for Economic Protection	Initiative Wirtschaftsschutz
InSiBe	Chief Information Security Officer of the State Administration Hamburg	Informationssicherheitsbeauf-tragte:r Hamburg
INTCEN	EU Intelligence Analysis Centre	Zentrum für Informationsgewinnung und -analyse
ISG C3M	Inter-Service Group "Community Capacity in Crisis Management"	Inter-Service Group "Community Capacity in Crisis Management"
ISG CHT	Inter-Service Group "Countering Hybrid Threats"	Inter-Service Group "Countering Hybrid Threats"
IT-PLR	IT Planning Council	IT-Planungsrat
IT-Rat	IT Council	IT-Rat
IT-SiBe-Forum	Forum of Municipal IT Security Officers	IT-SiBe-Forum
ITSMIG	IT Security made in Germany	IT Security made in Germany
ITZBund	Federal Information Technology Centre	Informationstechnikzentrum Bund
JISD	Joint Intelligence and Security Division	
KdoCIR	Cyber- and Information Domain Commando	Kommando Cyber- und Informationsraum
KdoITBw	Information Technology Command	Kommando Informationstechnik
KdoStratAufkl	Strategic Reconnaissance Command	Kommando Strategische Aufklärung
KGSt	Municipal Joint Office for Administrative Management	Kommunale Gemeinschaftsstelle für Verwaltungsmanagement
Kommunalgremium IT-PLR	Municipial Committee of the IT Planning Council	Kommunalgremium des IT-Planungsrates
Kompetenz- und Forschungszentren für IT-Sicherheit	Competence and research centers for IT security	Kompetenz- und Forschungszentren für IT-Sicherheit
Kompetenzzentrum Cybercrime	Cybercrime Competency Center – Bavaria	Kompetenzzentrum Cybercrime – Bayern

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
Kooperationsgruppe unter der NIS-Richtlinie	NIS Cooperation Group	Kooperationsgruppe unter der NIS-Richtlinie
Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen	Coordination Office for Cyber Security North Rhine-Westphalia	Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen
KSV	Central Municipal Associations	Kommunale Spitzenverbände
Landes-InfSiBe	Chief Information Security Officer of the State Administration Berlin	Landesbeauftragte:r für Informationssicherheit Berlin
Länder-CERTs	Computer Emergency Response Teams of the Federal States	Computer Emergency Response Teams der Bundesländer
Länder-CIO	State Commissioner for Information Technology	Landesbeauftragte:r für Informationstechnologie
Länder-CISO	Chief Information Security Officer of the State Administration	Informationssicherheitsbeauftragte:r der Landesverwaltung
LfV	State Offices for the Protection of the Constitution	Landesbehörden für Verfassungsschutz
LKA 54	Special Commissioner's Office for Cybercrime – Hamburg	Fachkommissariat Cybercrime – Hamburg
LSI	State Office for Information Security of Bavaria	Landesamt für Sicherheit in der Informationstechnik Bayern
LZ	National IT Situation Centre	Nationales IT-Lagezentrum
MC	NATO Military Committee	NATO-Militärausschuss
MeliCERTes	MeliCERTes	
NAC	North Atlantic Council	Nordatlantikrat
Nationaler Pakt Cybersicherheit	National Cybersecurity Pact	Nationaler Pakt Cybersicherheit
N CERT	Computer Emergency Response Team Lower Saxony	Computer Emergency Response Team Niedersachsen
NCI Academy	NCI Academy	
NCIA	NATO Communications and Information Agency	

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
NCIRC	NATO Computer Incident Response Capability	
NCSC	NATO Cyber Security Centre	
Netzverweis.de	Netzverweis.de – Mecklenburg-Western Pomerania	Netzverweis.de – Mecklenburg-Vorpommern
NIS Platform	NIS Public-Private Platform	
NS-O	NATO School Oberammergau	
OLAF	European Anti-Fraud Office	Europäisches Amt für Betrugsbekämpfung
PESCO	Permanent Structured Cooperation	Ständige Strukturierte Zusammenarbeit
PSK	Political and Security Committee	Politisches und Sicherheitspolitisches Komitee
SAX.CERT	Computer Emergency Response Team Saxony	Computer Emergency Response Team Sachsen
SC	NATO Security Committee	
Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock	Special Prosecutor for Combatting Information and Communication Crimes of Rostock	Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock
Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus	Special Public Prosecutor's Office to Combat Computer and Data Network Crime of Cottbus	Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus
Sicherheitskooperation Cybercrime	Security Cooperation Cybercrime	Sicherheitskooperation Cybercrime
SKI-Kontaktgruppe	CIP Contact Group	Kontaktgruppe zum Schutz Kritischer Infrastrukturen
SN4C	Cyber Crime Competence Center Saxony	Cyber Crime Competence Center Sachsen
SOG-IS	Senior Officials Group Information Systems Security	

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin	Special Department for the Fight against Cybercrime of Berlin's Public Prosecutor's Office	Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin
SprinD	Agency for Springboard Innovation	Agentur für Sprunginnovationen
SWP	German Institute for International and Security Affairs	Stiftung Wissenschaft und Politik
TF-CSIRT	Reference Incident Classification Taxonomy Task Force	
TGG	Taxonomy Governance Group	
Thüringen CERT	Computer Emergency Response Team Thuringia	Computer Emergency Response Team Thüringen
TISiM	Transfer Office "IT Security for Small and Medium-sized Enterprises"	Transferstelle IT-Sicherheit im Mittelstand
UniBw	Universities of the German Federal Armed Forces	Universitäten der Bundeswehr
UP KRITIS	Public-Private Partnership for Critical Infrastructure Protection	Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen
VCV	Administrative CERT-Group	Verwaltungs-CERT-Verbund
Vitako	Federal Working Group of Municipal IT Service Providers	Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V.
vzbv	Federation of German Consumer Organisations	Bundesverband der Verbraucherzentralen und Verbraucherverbände e. V.
ZAC (Bundesland)	Central Contact Points for Cybercrime of the Police Forces of the Federal States for the Economy	Zentrale Ansprechstellen Cybercrime der Polizeien der Länder für die Wirtschaft
ZAC NRW	Central and Contact Office Cybercrime North Rhine-Westphalia	Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen
ZCB	Central Office Cybercrime Bavaria	Zentralstelle Cybercrime Bayern
ZCS	Central Office Cybercrime Saxony	Zentralstelle Cybercrime Sachsen

Abbreviations/ Terms Used in Visualization	Official English Title/ Own Translation	Official German Title
Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität	Central Office for the Fight against Information and Communication Crime – Baden-Wuerttemberg	Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität – Baden-Württemberg
ZIT	Central Office for Combating Internet and Computer Crime – Hesse	Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität – Hessen
ZITiS	Central Office for Information Technology in the Security Sector	Zentrale Stelle für Informationstechnik im Sicherheitsbereich
ZKA	Customs Investigation Bureau	Zollkriminalamt

4. Explanation: Actors at EU level

Agentur der Europäischen Union für Cybersicherheit (European Union Agency for Cybersecurity, ENISA, official translation)
ENISA is an EU agency that assists the European Commission in cybersecurity matters. With regard to its consulting role, ENISA is contributing to EU cyber policy development, supporting cyber capacity building, participating in knowledge exchange with relevant stakeholders and is raising awareness for cybersecurity. ENISA also aims to improve cooperation within the EU, to promote greater coherence between sectoral initiatives by way of the NIS Directive, and to establish exchanges of information and analysis centers in critical sectors. It is also a hub for knowledge and information in the cybersecurity community. In order to improve the EU's resilience to cybersecurity threats and to find early solutions and strategies to challenges arising from new technologies, ENISA also aims to bring together different stakeholders with the goal of foresight. As a result of the Cybersecurity Act, it is tasked with using "European cybersecurity certification schemes" as the basis for certifying products, processes and services to support the Digital Single Market. ENISA coordinates Member States' measures to prevent and defend against cyberattacks. Annually, ENISA publishes a threat landscape report (ENISA Threat Landscape) which identifies and assesses threats from cyberspace.

ENISA works with both relevant Member State authorities and at EU level – in particular with Computer Security Incident Response Teams, the CERT-EU, EC3 and INTCEN – to develop situation-specific awareness and to support policy decisions with regard to hazard monitoring, effective cooperation, and responses to large-scale, cross-border incidents. At German level, ENISA cooperates with the BSI/CERT-Bund. Recently, ENISA underwent a name change from "European Network and Information Security Agency" to "European Union Agency for Cybersecurity". The abbreviation of the original name remained the same after the process[7].

Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (European Union Agency for Criminal Justice Cooperation, Eurojust, official translation)
With regard to internal security, the EU places particular emphasis on organized crime, terrorism, cybercrime and human trafficking. Eurojust plays an important role in combating these threats on an operational level. By promoting information ex-

7 European Commission, Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.
European Commission, State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyber-attacks.
European Court of Auditors, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
European Union Agency for Cybersecurity, About ENISA.
European Union Agency for Cybersecurity, ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.
Federal Office for Information Security, BSI Magazin 2019/1.
Federal Office for Information Security, Cyber-Sicherheit: Nationale und Internationale Zusammenarbeit.

change, connecting ongoing investigations, developing criminal law strategies and enabling joint action, Eurojust is responsible for coordinating case investigations.

To enhance the investigative capabilities of Member States' law enforcement agencies in the field of cybercrime as well as their general understanding of cybercrime and the investigative options available to their law enforcement agencies and judiciaries, Eurojust works with the EC3's specialized advisory groups, networks of heads of cybercrime units and prosecutors specializing in cybercrime. Relations between Eurojust, relevant national authorities, the EJN, Europol, OLAF and INTCEN should be fostered[8].

Computer Emergency Response Team der Europäischen Kommission (Computer Emergency Response Team of the European Commission, CERT-EU, official translation)
CERT-EU is an IT emergency response team directly linked to the European Commission. It supports all EU institutions, bodies and agencies. Its tasks range from raising awareness for prevention purposes through advisories and white papers, to cyber threat reconnaissance and incident response through support and coordination, for example, by evaluating, validating and verifying available information. In addition, CERT-EU monitors potential vulnerabilities and takes action to strengthen the technical infrastructure of the EU institutions through "ethical hacking techniques" and penetration testing.

CERT-EU is comprised of experts from central EU institutions (inter alia European Commission and General Secretariat of the European Council). It works closely with other CERTs of Member States and is a member of the CSIRTs network. Recently, a structured cooperation between CERT-EU and ENISA has been agreed. In the past, CERT-EU and the NATO Computer Incident Response Capability (NCIRC) have concluded a technical agreement of cooperation[9].

Contractual Public-Private Partnership on Cybersecurity (cPPP)
The European Commission and the European Cybersecurity Organisation signed a cPPP as part of the EU's cybersecurity strategy. In order to establish innovative and trustworthy European solutions, the cPPP aims to promote cooperation between public and private actors in the early stages of research and innovation. These solu-

8 Eurojust, Casework at Eurojust.
Eurojust, Eurojust Decision.
European Commission, Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.
Federal Office for Information Security, Avalanche-Botnetz: BSI weitet Schutzmaßnahmen aus. (Website deleted)

9 CERT-EU, About Us.
CERT-EU, RFC 2350.
ENISA, ENISA and CERT-EU sign Agreement to start their Structured Cooperation.
European Commission, European Commission Fact Sheet: Questions and Answers: Directive on Security and Information systems, the first EU-wide legislation on cybersecurity.
European Commission, NATO and CERT-EU discuss cyber threats ahead of EU elections.
European Court of Auditors, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.

tions are meant to consider fundamental rights, in particular the right to privacy. They are additionally meant to promote the cybersecurity industry. As part of the Horizon 2020 program, the EU will invest up to 450 million euros[10].

Computer Security Incident Response Teams Netzwerk (Computer Security Incident Response Teams Network, CSIRTs Network, official translation)
The CSIRTs Network was established as part of the NIS Directive and aims to contribute to existing, trusted operational cooperation between Member States. It provides a forum for cooperation and for development of a coordinated response to cross-border cybersecurity incidents.

The CSIRTs Network consists of appointed representatives of Member States' CSIRTs as well as the CERT-EU. Germany is represented by its CERT-Bund. The European Commission participates as an observer. ENISA appoints the secretariat, promotes cooperation between CSIRTs and, where necessary, offers active support for the coordination of incidents[11].

Cyber Crisis Liaison Organisation Network (CyCLONe)
In 2020, the Cyber Crisis Liaison Organisation Network (CyCLONe) was created as an operational contribution to the recommendations of the European Commission for a coordinated reaction to large, transnational cybersecurity incidents and crises (Blueprint). As a forum, CyCLONe should contribute to realizing consultations on reactionary national strategies through strengthened cooperation mechanisms and better information flows between actors at the technical (CSIRTs) and the political levels. Coordinated impact assessments on expected or observed consequences of a crisis should furthermore be made accessible to political decision-makers at national and EU level, respectively. CyCLONe is currently not yet operational, and EU Member States can participate on a voluntary basis.

The idea for such a network, supported by the European Commission, stems from a working group of the NIS Cooperation Group led by France and Italy; ENISA acts as the secretariat of the network. In the near future, insights, especially from cybersecurity exercises (Blue OLEx for example), are supposed to feed into the work of the network[12].

10 ECSO, About the cPPP.
11 CSIRTs Network, CSIRTs Network Members.
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.
12 European Commission, Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.
European Union Agency for Cybersecurity, Blue OLEx 2020: the European Union Member States launch the Cyber Crisis Liaison Organisation Network (CyCLONe).
Federal Ministry of the Interior, BMI und BSI beteiligen sich an Cyberkrisenübung Blue OLEx 2020.
Vertretung der Europäischen Kommission in Deutschland, EU-Staaten testen ihre Zusammenarbeit im Falle von Cyber-Angriffen.

Cyber and Information Domain Coordination Centre (CIDCC)
The initiative for a Cyber and Information Domain Coordination Centre (CIDCC) was introduced by Germany as a project within the framework of the Permanent Structured Cooperation (PESCO). In addition to Germany, which assumed the role of coordinator through its KdoCIR, the Netherlands, Hungary and Spain are also participating in the development of the CIDCC. In the long term, the CIDCC should serve as a permanent, multinational military element, in which situational pictures from cyber and information space are compared and evaluated. Moreover, their information can be introduced in the planning and management of EU operations and missions. The CIDCC is slated to be fully operational by 2026. Until then, it is to be equipped with the capabilities to be able to organize and implement operations in the cyber and information space itself. Until the planned move of the CIDCC to Brussels in 2023, it will be located within the KdoCIR.

The KdoCIR coordinated with the European Union Military Staff (EUMS) as well as the European Defence Agency (EVA) in its conceptualization of the CIDCC[13].

Direktion Krisenbewältigung und Planung (Crisis Management and Planning Directorate, CMPD, official translation)
The CMPD is responsible for integrated civilian-military planning within the European External Action Service, thereby contributing to the implementation of the EU's Common Security and Defence Policy. The aim of such strategic planning is to identify possible courses of action for the EU and to serve as the foundation for the Council's decision-making in international crisis situations.

These options are summarized in the so-called Crisis Management Concepts and are then presented to EU ministers. They constitute the basis for operational planning and mission execution[14].

ENISA-Beratungsgruppe (ENISA Advisory Group, ENISA AG, official translation)
The ENISA AG was established with the Cybersecurity Act. It is comprised of recognized experts representing relevant stakeholders from the IT sector and small and medium-sized enterprises, as well as operators of "essential services", consumer groups and other competent authorities. Members of the AG serve a term of 2.5 years.

Experts in the European Commission and from Member States can attend meetings and participate in the work of the AG. The Executive Director of ENISA can invite rep-

13 German Armed Forces, Europäisches Verteidigungsprojekt für Cybersicherheit – Das Cyber and Information Domain Coordination Centre.
Federal Ministry of Defence, Cyber and Information Domain Coordination Centre (CIDCCC).
PESCO, Cyber and Information Domain Coordination Center (CIDCC).
14 European Union External Action Service, The Crisis Management and Planning Directorate (CMPD). (Website deleted)

resentatives of other entities to participate in meetings. The AG advises ENISA in the performance of its tasks, in particular when the Executive Director prepares a proposal for ENISA's annual work program. It also provides advice on how communication with relevant stakeholders can be improved with regard to the annual work program[15].

EU-Analyseeinheit für hybride Bedrohungen (EU Hybrid Fusion Cell, official translation)

The EU Hybrid Fusion Cell focuses on the analysis of external aspects of hybrid threats. It is housed within the EU Intelligence and Situation Centre (EU INTCEN) of the European External Action Service. The Cell is meant to collect, analyze and share classified and public information – specifically those related to indicators and alerts of hybrid threats – from various actors within the European External Action Service, the European Commission and Member States. Through such analyses, the Cell should heighten awareness of security risks and support political decision making among actors at national and EU level. The Cell also has a network of national contact points for the defense against hybrid threats, which meets twice per year in order to inter alia exchange best practices, strengthen resilience and formulate counterinitiatives to hybrid threats.

The Cell works closely with the Intelligence Directorate of the EUMS and, especially for information about cyber threats, with the CERT-EU. Quarterly reports of the EU Hybrid Fusion Cell are routinely sent to both Inter-Service Groups CHT and C3M. Structured working relationships and information exchanges exist with the NATO Hybrid Analysis Branch within the JISD and the NATO CCDCOE[16].

Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, eu-LISA, official translation)

eu-LISA is managing integrated, large-scale IT systems, which ensure the internal security of the Schengen Area. They allow the exchange of visa data between Schen-

15 European Parliament and Council of the European 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 Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".
European Commission, FAQ: Joint Framework on countering hybrid threats.
European Commission, Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats.
European Commission, Gemeinsamer Rahmen für die Abwehr hybrider Bedrohungen -eine Antwort der Europäischen Union.
EU-NATO, Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017.
OSW, Towards greater resilience: NATO and the EU on hybrid threats.

gen Area countries as well as the determination of responsibility amongst EU countries in the examination of a particular asylum application. Furthermore, it tests new technologies to help create a more modern, effective and secure border management system in the EU.

eu-LISA works closely with Member States as well as the EDSB, Frontex, the Council of the EU, the EK, ENISA, Eurojust and Europol on the EU level[17].

Europäische Gruppe für die Cybersicherheitszertifizierung (The European Cybersecurity Certification Group, ECCG, official translation)
The EGGC, an expert group comprised of representatives from Member States, contributes to the development of certification schemes by ENISA. Specific schemes are developed for different types of products and services, which include, for example, the period of validity of security certificates. Furthermore, the European Cybersecurity Certification Group assists the Commission in establishing a European work program for cybersecurity certification schemes. The work program is meant to function as a strategic document to aid the industry in preparing for future certification requirements at an early stage.

The group cooperates with the Stakeholder Cybersecurity Certification Group. In order to respond to rapid developments in the technology field, the group can, alongside the European Commission, request that ENISA develops new possible certification schemes not yet included in the work program[18].

Europäische Kommission (European Commission, EK, official translation)
The European Commission plays both a strategic and organizational role in EU cybersecurity architecture. It is responsible for capacity building and fostering cooperation in cybersecurity, for strengthening the EU's position in the field, and for promoting the integration of cybersecurity into other EU policy areas. The European Commission has its own early warning system (ARGUS), which includes an internal communication network and a specific coordination procedure. In the event of a major, EU-wide crisis affecting cyberspace, coordination efforts are handled through ARGUS.

A number of directorates-general work in the field of cybersecurity, including CONNECT, DIGIT, HOME, JRC and RTD. The CERT-EU and the ERCC (ERCC through GD

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

18 European Commission, The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification.
European Parliament and Council of the European 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).

ECHO) are affiliated with the European Commission as well. In the past, the EC, together with the European Council, has reached two memoranda of understanding on enhanced NATO-EU cooperation, including in the area of cybersecurity and defense, with the NATO Secretary General[19].

Europäische Kooperation für Akkreditierung (European co-operation for Accreditation, EA, official translation)
The EA is an amalgamation of European accreditation agencies and is responsible for the coordination of accreditation in Europe. It is a non-profit organization and is comprised of 50 nationally recognized accrediting agencies. EA aims to contribute to a harmonization of accreditation procedures. As a result, it is also responsible for the accreditation of IT-security products.

The EA was officially designated by the European Commission. As a result, the European Commission has a seat on its Supervisory Board. The DAkkS is a member of the EA and represents German interests[20].

Europäische Polizeiakademie (The European Union Agency for Law Enforcement Training, CEPOL, official translation)
CEPOL is an EU agency responsible for the development, implementation and coordination of training for law enforcement officials. It brings together a network of training institutes for law enforcement officers in Member States and supports them in providing training on law enforcement cooperation, security priorities and information exchange. The CEPOL Cybercrime Academy was inaugurated in Budapest as an additional part of the training portfolio. It is designed to train up to 100 participants simultaneously.

CEPOL trainings are held in cooperation with the European Commission, EC3, EJTN, Eurojust, the EUCTF, the ECTEG and Interpol[21].

19 Commission of the European Communities, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Bestimmungen der Kommission zum allgemeinen Frühwarnsystem „ARGUS".
Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".
European Commission, Anhang zur Empfehlung der Kommission über die koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.
European Court of Auditors, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
EU-NATO, Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization.

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

21 CEPOL, About us.
CEPOL, CEPOL Cybercrime Academy Inaugurated.
Email exchange with CEPOL representatives in August 2019.

Europäische Verteidigungsagentur (European Defence Agency, EVA, official translation)
The European Defence Agency supports all EU Member States (except Denmark) in the development of their defense capabilities through European cooperation. One of EVA's objectives is the development of cyber defense capabilities. It supports EU Member States in the development of their own defensive capabilities and cyber defense constitutes one of its four core programs.

Together with the EAD, EVA jointly manages all secretarial functions for the Permanent Structured Cooperation (PESCO). EVA signed a Memorandum of Understanding with ENISA, the EC3, and CERT-EU with the goal of developing a cooperation framework for the organizations. The Chief Executive of the EVA meets regularly with the SACT as well as Assistant SECGEN's of NATO. The EVA Steering Board is also briefed regularly by the latter[22].

Europäischer Auswärtiger Dienst (European External Action Service, EAD, official translation)
The European External Action Service is a leader in the field of conflict prevention, cyber diplomacy and strategic communication. The EAD maintains a Crisis Response System (CRS) for coordinating responses to crises and emergencies. It is used whenever events (potentially) concern the security interests of the EU or its Member States. The EAD is managed by the High Representative of the European Union for Foreign Affairs and Security Policy, who is responsible for both the EU's Common Foreign and Security Policy and the EU's Common Security and Defence Policy, while simultaneously acting as Vice President of the European Commission. This aims at ensuring coherent policymaking in the fields of security and cybersecurity policy.

The EAD hosts EUMS INT, INTCEN, the EU Hybrid Fusion Cell and the CMPD. Furthermore, EAD representatives chair the PSK. The High Representative regularly exchanges views with the NATO Secretary General and also occasionally participates in NAC meetings at the level of defense ministers[23].

22 European Court of Auditors, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
European Defence Agency, Four EU cybersecurity organisations enhance cooperation.
European Defence Agency, Our current priorities.
European External Action Service, Permanent Structured Cooperation – PESCO.
European Union, Europäische Verteidigungsagentur (EVA).
EU-NATO, Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017.

23 Annegret Bendiek, Gemeinsame Außen- und Sicherheitspolitik: von der Transformation zur Resilienz.
Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".
European Council/ Council of the European Union, Politisches und Sicherheitspolitisches Komitee (PSK).
European Union External Action Service, High Representative/Vice President.
European Union External Action Service, The Crisis Management and Planning Directorate (CMPD). (Website deleted)
EU-NATO, Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.
IMPETUS, An Integral Element of the EU Comprehensive Approach.

Europäische:r Datenschutzbeauftragte:r (European Data Protection Supervisor, EDSB, official translation)
The European Data Protection Supervisor undertakes its role within the European Union. He or she, and the supervisory authority supporting his or her duties, are responsible for ensuring the supervision of and adherence to principles of data protection when processing personal data going through the EU's many institutions. Safeguarding the protection of privacy includes, for example, conducting investigations or processing any submitted complaints. Furthermore, the EDSB observes and evaluates possible implications for data protection that arise through new technological developments. The EDSB is appointed for a term of five years and works together with national data protection authorities within EU Member States. In the past, the EDSB also took a stance on inter alia the EU's cybersecurity strategy as well as other proposals, recommendations and communications of the European Commission from a data-privacy law perspective.

The EDSB can, on request, advise the European Commission and the Council of the EU. The Council of the EU is involved in the appointment of the EDSB. The EDSB assumes a supervisory role over Europol and Eurojust. At German level, contact and exchange exists with the BfDI[24].

Europäischer Rat (European Council, ER, official translation)
The European Council is responsible for determining the "political objectives and priorities" of the EU. To this respect, it can adopt conclusions on specific topics and occasions and has adopted a Strategic Agenda for the EU for the years of 2019-2024. In its first main priority, "Protecting citizens and freedoms", the necessity of protecting against malicious cyber activities, hybrid threats and disinformation is stressed.

The European Council is composed of heads of state and government from all EU Member States as well as the Presidents of the European Commission and the European Council (both without voting rights). It meets at least twice every six months. Meetings of foreign policy importance also include the High Representative of the EU[25].

Europäisches Amt für Betrugsbekämpfung (European Anti-Fraud Office, OLAF, official translation)
OLAF is responsible for investigating allegations of fraud against the EU budget, corruption and serious misconduct within the EU institutions. These investigations may

24 European Data Protection Supervisor, Über den EDSB.
European Data Protection Supervisor, EDPS formal comments in response to the 'Cybersecurity Package' adopted by the Commission.
European Data Protection Supervisor, Häufig gestellte Fragen.
Federal Commissioner for Data Protection and Freedom of Information, Stellungnahme zu überarbeiteten Standarddatenschutzklauseln.
25 European Council, A New Strategic Agenda 2019 – 2024.
European Council, Der Europäische Rat.

result in the initiation of criminal proceedings, financial recoveries or other disciplinary action. OLAF may become involved with issues of cyber and IT security either as part of its operational self-protection or as a component within an investigated offense.

OLAF reports to the EC but is independent in the execution of its mandate. It regularly reports to the Council of the EU's Working Group on Fraud Prevention[26].

Europäisches Polizeiamt (European Police Office, Europol, official translation)
Europol is the law enforcement agency of the European Union and supports both the European Commission as well as EU Member States in the prosecution of cybercrime, terrorism and organized crime. It also works with non-EU Member States and international organizations.

In the field of cybercrime, Europol bolsters law enforcement efforts, particularly through the European Cybercrime Centre (EC3). Europol works together closely with the BKA. The BKA serves as a Europol National Unit and therefore Europol's German point of contact[27].

Europäisches Sicherheits- und Verteidigungskolleg (European Security and Defence College, ESVK, official translation)
The civil and military personnel of EU institutions and EU Member States are trained at the European Security and Defence College within the areas of the Common Foreign and Security Policy and the Common Security and Defence Policy. Training and courses on cybersecurity and cyber defense comprise one of the six focus areas on offer at the ESVK. A Cyber Education, Training, Evaluation and Exercise Platform (ETEE) was established at the ESVK to this end.

The ESVK is institutionally housed within the EAD. It was established through a decision of the Council of the EU. It retains close cooperation and exchange with ENISA, Europol, CEPOL, ECTEG, CERT-EU, as well as the Hybrid CoE and the NATO CCDCOE. The ESVK draws on a broad network of EU-wide training institutions for its training exercises. At German level, the AA, BAKS and the BMVg participate in this network[28].

26 European Anti-Fraud Office, About Us.
European Anti-Fraud Office, Cooperation with EU institutions.
27 Federal Criminal Police, Europol.
Europol, About Europol.
Europol, European Cybercrime Centre – EC3.
28 ESDC, EAB.Cyber.
ESDC, Education & Training.
ESDC, Institutes.
ESDC, Who We Are.

Europäisches Zentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (European Cybersecurity Industrial, Technology and Research Competence Centre, ECCC, official translation)

In December 2020, EU Member States voted in favor of the Romanian capital Bucharest as location of the new ECCC. The ECCC is meant to promote European autonomy in cybersecurity and the competitiveness of the European cybersecurity industry, in addition to strengthening the Digital Single Market. The ECCC, whose existence is initially planned until 2029, is intended to bundle existing funds for cybersecurity within the European Union and investments in a targeted manner (Horizon Europe and Digital Europe funding programs) and to coordinate research projects in the EU in the field of cybersecurity. Outside of these functions, the ECCC is furthermore meant to develop and coordinate the National Coordination Centres Network and the Cybersecurity Competence Community.

The ECCC is based on a proposal by the EC and is intended to complement the tasks of ENISA[29].

Europäisches Zentrum zur Bekämpfung der Cyber-Kriminalität (European Cybercrime Center, EC3, official translation)

Europol's European Centre for Cybercrime Prevention (EC3) strengthens law enforcement authorities' ability to react to cybercrime within the EU. The EC3 focuses on three areas in combating cybercrime: forensics, strategy and operations. It annually publishes the Internet Organised Crime Threat Assessment (IOCTA), a strategic report outlining its key findings as well as emerging threats and developments in cybercrime. Furthermore, EC3 houses the Joint Cybercrime Action Taskforce (J-CAT), which is tasked with facilitating information-driven and coordinated action against key cybercriminal threats through cross-border investigations and operations by its partners.

At European level, EC3's partners are the CERT-EU, CEPOL, Eurojust, ENISA, the European Commission, and ECTEG. In cooperation with the CERT-EU, EC3 also provides forensic analysis and other technical information for the CSIRTs network[30].

29 Council of the European Union, Bukarest (Rumänien) wird Sitz des neuen Europäischen Kompetenzzentrums für Cybersicherheit.
Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.
European Commission, European Cybersecurity Industrial, Technology and Research Competence Centre.
Council of the European Union, New Cybersecurity Competence Centre and network: informal agreement with the European Parliament.
European Commission, European Cybersecurity Industrial, Technology and Research Competence Centre.
European Council, EU to pool and network its cybersecurity expertise – Council agrees its position on cybersecurity centres.
Netzpolitik, Neues EU-Kompetenzzentrum für Cybersicherheit bleibt umstritten.

30 European Court of Auditors, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
Europol, Cybercrime.
Europol, European Cybercrime Center – EC3.
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.

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)
The Hybrid CoE aims to support the capabilities of participating nations in building up resilience and developing strategies to combat hybrid threats. In practice, this occurs by way of research, conducting workshops and conferences, and through the exchange of best practices between various stakeholders within three Communities of Interest (COI). The COI group focusing on strategy and defence is coordinated by Germany.

The idea of establishing the Hybrid CoE was supported by the Council of the EU and the NAC. Together with the JRC of the European Commission, the Hybrid CoE introduced at the end of 2020 a conceptual framework for hybrid threats. In the past, the Hybrid CoE and the European Defence Agency agreed to cooperate together to contribute to the implementation of priorities outlined in the Capability Development Plan of the EU. Germany is among the nine founding nations of the Hybrid CoE[31].

European Cybercrime Training and Education Group (ECTEG)
The ECTEG consists of law enforcement authorities of EU and European Economic Area (EEA) Member States, as well as representatives of international institutions, the scientific community, private industry and relevant experts. Its objective is to prepare global law enforcement for cybercrime incidents.

ECTEG was funded by the European Commission. ECTEG works closely with EC3 and CEPOL to harmonize cybercrime training across national borders, enable the exchange of knowledge and promote the standardization of methods for training programs. Germany's "Polizeiakademie Hessen" (Police Academy Hesse, own translation) and the "Hochschule Albstadt-Sigmaringen" (Albstadt-Sigmaringen University, official translation) are also involved as members[32].

European Cyber Security Organisation (ECSO)
The ECSO was established in Belgium as a self-financed non-profit organization. ECSO connects European actors in EU Member States active in the field of cybersecurity, such as research centers, companies, end-users and Member States of the European Economic Area, as well as countries associated with Horizon 2020. Among ECSO's objectives are developing a competitive European ecosystem, strengthening protection of the European Digital Single Market with trusted cybersecurity solutions and contributing to the digital autonomy of the European Union.

31 European Centre of Excellence for Countering Hybrid Threats, About Us.
European Commission, The JRC proposes a new framework to raise awareness and resilience against hybrid threats.
European Commission, Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats.
32 ECTEG, European Cybercrime Training and Education Group.
ECTEG, Members.

ECSO is a contractual partner of the European Commission. In this function, it is responsible for the implementation of the contractual Public-Private Partnership for cybersecurity (cPPP). It furthermore maintains close working relations with representatives from GD CONNECT, GD RTD, GD JRC, GD DIGIT and the EAD. At the invitation of the respective Council Presidency, ECSO is regularly invited to report on the current status of its work to the Horizontal Working Party on Cyber Issues. There is also continuous cooperation with ENISA, Europol and EVA, among others[33].

European Government CERTs group (EGC group)
The EGC group is an informal association of governmental CERTs in Europe. Its members work together in the field of incident response by building on mutual trust and similarities in their competency areas. It also identifies areas for joint research and development as well as knowledge in specialized areas for the purpose of common usage. Moreover, the EGC group is concerned with facilitating the exchange of information and technology with respect to vulnerabilities, among others. The group, that convenes three times annually, has a technical focus rather than a policymaking focus.

The EU is represented by CERT-EU and Germany by the CERT-Bund. In addition, there is close cooperation with ENISA[34].

European Judicial Network (EJN)
The European Judicial Network was created at the behest of the Council of the European Union as a network of national contact points to facilitate judicial cooperation in criminal matters, especially those which combat forms of serious crime. In this respect, the EJN organizes training events, provides information and is instrumental in establishing contact between responsible authorities.

The secretariat of the EJN is located within Eurojust and is involved in a cooperation with the European Judicial Cybercrime Network[35].

European Judicial Cybercrime Network (EJCN)
The EJCN's objective is to foster connections between practitioners specializing in the challenges posed by cybercrime, "cyber-enabled crime", and investigations in cyberspace. Furthermore, it aims to increase the efficiency of investigations and prosecutions.

33 ECS, About ECSO.
34 EGC Group, Contact.
EGC Group, European Government CERTs (EGC) group.
Federal Office for Information Security, Europäische CERTs in Bonn. (Website deleted)
35 European Judicial Network, About EJN.
European Judicial Network, Network Atlas.

Eurojust participates in the EJCN board and organizes regular EJCN meetings. It also consults the EJCN on policy development and other stakeholder activities to ensure a lively exchange between Eurojust's expertise in the field of international legal cooperation and the operational and subject-matter expertise of EJCN member[36].

European Judicial Training Network (EJTN)
The EJTN offers a platform for training and knowledge exchange for the European judiciary.

In the field of cybersecurity, EJTN works with CEPOL on those training sessions it provides[37].

European Union Cybercrime Task Force (EUCTF)
The EUCTF was jointly set up by Europol, the European Commission and Member States. It is a trust-based network that meets every six months.

Its members are Member States' National Cybercrime Units and representatives of Europol, the European Commission and Eurojust. In their meetings, CEPOL, Eurojust, GD Home and EUCTF identify, discuss and prioritize challenges and actions in the fight against cybercrime[38].

Gemeinsame Forschungsstelle (Directorate-General Joint Research Centre, GD JRC, official translation)
The Joint Research Centre is subordinate to the European Commission and is financed by Horizon 2020. The JRC provides scientific findings as well as innovative instruments throughout the entire political cycle to national and EU authorities. In doing so, it seeks to anticipate emerging challenges and point out the impact of different political decisions. One of the ten scientific areas researched at the JRC is "Information Society", which is broken down into 16 research areas which include, for example, cybersecurity and the digital internal market.

Together with the Hybrid CoE, the Joint Research Centre introduced a conceptual framework on hybrid threats in 2020[39].

Generaldirektion Forschung und Innovation (Directorate-General for Research and Innovation, GD RTD, official translation)
The Directorate-General for Research and Innovation of the European Commission is responsible for the European Union's research and innovation policy and seeks

36 Eurojust, European Judicial Cybercrime Network.
37 Email exchange with CEPOL representatives in August 2019.
EJTN, About us.
38 Europol, EUCTF.
39 EU Science Hub, Information Society.
EU Science Hub, JRC in brief.
EU Science Hub, Organisation.
EU Science Hub, Research Topics.

to support and strengthen science, technology and innovation according to the priorities of the European Commission. In this respect, it analyzes, for example, the national research and innovation policies of EU Member States in order to increase their effectiveness and efficiency. If necessary, it also makes country-specific recommendations.

Moreover, the GD RTD is responsible for managing funding programs, such as Horizon 2020. In fulfilling its duties, GD RTD works together closely with inter alia GD CONNECT, GD HOME and GD JRC[40].

Generaldirektion Informatik (Directorate-General for Informatics, GD DIGIT, official translation)
GD DIGIT is in charge of the IT security of the European Commission's systems. It is furthermore responsible for maintaining an IT operation that supports other Commission departments and EU institutions in their day-to-day work and for improving cooperation between Member States' relevant administrative bodies.

Together with the Director of GD CONNECT, the Director of GD DIGIT represents the European Commission in the Management and Executive Board of ENISA[41].

Generaldirektion Kommunikationsnetze, Inhalte und Technologien (Directorate-General for Communications Networks, Content and Technologies, GD CONNECT, official translation)
GD CONNECT is responsible for further developing the Digital Single Market, and thus also for developing the potential of European leadership in network and IT security.

GD CONNECT has "parent-GD responsibility" for ENISA, meaning it assumes representation at directorate-general level of the CERT-EU Board and contributes to responses to cyber incidents at this level. GD CONNECT is responsible for all strategic aspects of research and innovation activities related to ICT within the framework of Horizon 2020. Close working relationships exist with GD RTD. The proposal for the establishment of the ECCC by the European Commission was prepared by GD CONNECT[42].

40 European Commission, Strategic Plan 2016-2020: Directorate-General for Research and Innovation.
41 European Commission, Annual Activity Report: DG CONNECT.
European Commission, Informatics.
European Court of Auditors, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
42 European Commission, Annual Activity Report: DG CONNECT.
European Commission, Communication Networks, Content and Technology.
European Commission, Strategic Plan 2016-2020: Directorate-General for Communications Networks, Content and Technology.

Generaldirektion Migration und Inneres (Directorate-General for Migration and Home Affairs, GD HOME, official translation)
GD HOME works on matters of migration, asylum and internal security. The latter includes the fight against organized crime and terrorism, as well as police cooperation, organization of the EU's external borders and cybercrime. To combat cybercrime, GD HOME works with EU Member States to ensure the full implementation of existing EU legislation and is responsible for adapting it to current developments. The Strategic Analysis and Response Center (STAR), part of GD HOME, provides information and assessments, especially risk analyses, to support the formulation of policies, crisis management, situational awareness and communications.

These are exchanged with European Commission Services, the EAD and other relevant agencies (particularly Europol and Frontex). Close working relationships exist with eu-LISA, Europol and CEPOL, among others[43].

Gruppe der Interessenträger für die Cybersicherheitszertifizierung (Stakeholder Cybersecurity Certification Group, official translation)
Upon the entry into force of the Cybersecurity Act, a stakeholder group for cybersecurity authorization was established to ease ENISA's and the European Commission's access to stakeholders. The group is comprised of representatives of European Commission stakeholders – digital service providers or national accreditation bodies, for example – on the recommendation of ENISA.

The Stakeholder Cybersecurity Certification Group is tasked with advising the European Commission (within the context of the EU framework for cybersecurity certification), as well as the development of the rolling work program listed in Art. 47. Upon request, the group can advise ENISA on issues connected to their duties regarding markets, certification and standardization. It is jointly chaired by representatives of the European Commission and ENISA. The secretariat is managed by ENISA[44].

Horizon 2020
Horizon 2020 is a European Commission program that has made available nearly 80 billion euro for research and innovation initiatives over the course of seven years. As such, it is the financial instrument of the Innovation Union initiative and aims to strengthen Europe's competitiveness. Horizon 2020 can also support projects in the field of cybersecurity.

43 Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".European Commission, Policies.
European Commission, Strategic Plan 2016–2020: DG Migration and Home Affairs.

44 European Parliament and Council of the European 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).

A coordinating office as well as an initial information center are available to interested parties through the BMBF. GD RTD is responsible for the overall management of Horizon 2020, while GD CONNECT is responsible for the strategic design of ICT-related research activities[45].

Horizontal Working Party on Cyber Issues (HWP)
The HWP coordinates the Council's work on cyber policy and related legislative activities. The tasks and objectives of the HWP also include harmonizing and unifying approaches on cyber policy issues, improving information sharing on cyber issues between EU Member States, and setting EU cyber priorities and strategic objectives within the EU. It is involved in legislative as well as executive processes.

The HWP works with the European Commission, EAD, Europol, Eurojust, EVA and ENISA, and is also in close cooperation with other working groups. Germany participates in the HWP through representatives of the BMI, which is in charge, and the AA[46].

Institut der Europäischen Union für Sicherheitsstudien (European Union Institute for Security Studies, EUISS, official translation)
EUISS works on research and policy analyses within the area of the Common Security and Defence Policy (CSDP) and, in this respect, seeks to contribute to decision-making. EUISS regularly publishes works on questions of foreign, security and defense policy, and organizes events and carries out communications work in these areas. Its topic portfolio includes cybersecurity, cyber diplomacy and cyber capacity building.

EUISS was established by the European Council and works together with a number of institutions, including the European Commission, the European Parliament and the European External Action Service, as well as with the respective governments of EU Member States[47].

Intelligence Directorate des EU-Militärstabs (Intelligence Directorate of the European Union Military Staff, EUMS INT, official translation)
The Intelligence Directorate of the EU Military Staff consists mainly of national experts from EU Member States and is organizationally attached to the EAD. Based on

45 European Commission, Security.
European Commission, What Is Horizon 2020?.
Federal Ministry of Education and Research, Netzwerk der Nationalen Kontaktstellen.
46 European Council, Horizontal Working Party on Cyber Issues (HWP).
The Council of the European Union, Establishment of a Horizontal Working Group on Cyber Issues.
Federal Office for Information Security, Cyber-Sicherheit in Europa gestalten. (Website deleted)
47 EUR-Lex, Document 32001E0554.
EUR-Lex, Institut der Europäischen Union für Sicherheitsstudien.
European Union, Institut der Europäischen Union für Sicherheitsstudien (EUISS).
European Union Institute for Security Studies, Cyber.

classified information from EU Member States or EU deployment areas, it provides situational military analyses and evaluations for the decision-making process and the planning of civil and military operations under the Common Foreign and Security Policy (CFSP).

EUMS INT works closely with the civilian situation center INTCEN, formalized as Single Intelligence Analysis Capacity (SIAC), as well as the EU Hybrid Fusion Cell. SIAC functions as a center generating strategic information, early warnings and comprehensive analyses, which are made available to EU bodies and decision-makers from EU Member States. EUMS INT (partly together with INTCEN) also makes its products available to BMVg, AA, BND, Eurocorps and the German Military Representative to the European Union[48].

Inter-Service Group "Community Capacity in Crisis-Management" (ISG C3M)
ISG C3M is a network which regularly brings together all European Commission services and EU agencies involved in crisis management in order to raise awareness, create synergies and exchange information. The group acts as a nexus point for contact with all operational crisis and situation centers.

The EAD takes part in ISG C3M[49].

Inter-Service Group "Countering Hybrid Threats" (ISG CHT)
ISG CHT ensures a comprehensive approach to hybrid threats and monitors the progress of activities foreseen in JOIN (2016)18. The group meets quarterly.

ISG CHT is chaired by representatives of the EAD and by the European Commission at Directorate-General or Deputy Secretary-General level. It receives quarterly reports from the EU Hybrid Fusion Cell[50].

Kontaktgruppe zum Schutz Kritischer Infrastrukturen (CIP Contact Group, SKI-Kontaktgruppe, official translation)
The SKI-Kontaktgruppe is responsible for strategic coordination and cooperation within the realm of the European Programme for Critical Infrastructure Protection (EPCIP), which assesses European critical infrastructures and identifies whether better protections are needed. The SKI-Kontaktgruppe also provides Member States

48 German Bundestag (Drucksache 19/489), Antwort der Bundesregierung auf die Kleine Anfrage: Pläne der Europäischen Kommission für eine geheimdienstliche „Europäische Aufklärungseinheit".
European Parliament, Parlamentarische Anfragen: Antwort von Frau Catherine Ashton – Hohe Vertreterin/Vizepräsidentin im Namen der Kommission.
Pia Seyfried, Red Herring & Black Swan: Five Eyes for Europe.
Raphael Bossong, Die nachrichtendienstlichen Schnittstellen der EU-Sicherheitspolitik.

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

50 Ibid.
Kristine Berzina et al., European Policy Blueprint for Countering Authoritarian Interference In Democracies: Annex A. European Efforts To Counter Disinformation.

with support in the protection of their national critical infrastructure.

The SKI-Kontaktgruppe brings together Member States' CIP Points of Contact under the chairmanship of the European Commission. Each EU Member State sends a CIP Point of Contact, who coordinates all CIP topics with other Member States, the European Commission and the Council of the EU[51].

Kooperationsgruppe unter der NIS-Richtlinie (NIS Cooperation Group, official translation)
The Directive on Security of Network and Information Systems (NIS Directive) set up a cooperation group that is chaired by the Presidency of the Council of the European Union. The regularly convening group consists of representatives of Member States, the European Commission (acting as the secretariat) and ENISA. It operates on a system of biennial work programs. The EU Member States designate a national contact point for this purpose. The group acts on the basis of consensus and can set up subgroups to work on specific questions related to its work. Its objective is to support the work of Member States to implement the NIS Directive uniformly by facilitating strategic cooperation and the exchange of information between Member States. For this purpose, the group develops non-binding guidelines for EU Member States and also supports them in capacity building.

Operationally, the group is supported by its subordinate CSIRTs network, for whose activities the group provides strategic guidance. ENISA supports the group by inter alia identifying best practices in the implementation of the NIS Directive or in strengthening the designated cybersecurity incident reporting process within the EU by developing thresholds, templates and tools. The Blue OLEx cybersecurity exercise (German participation by BMI and BSI) and the Cyber Crisis Liasion Organization Network (CyCLONe) originated in initiatives by members of the NIS Cooperation Group[52].

MeliCERTes
MeliCERTes is a cybersecurity core service platform for Computer Emergency Response Teams in the EU. It aims to strengthen operational cooperation and the exchange of information between teams and focuses on facilitating cross-border cooperation, enabled by the trustworthy exchange of data between ad-hoc Groups of CERTS. The current version of MeliCERTes works with open-source tools developed

51 Commission of the European Communities, Communication from the Commission on a European Programme for Critical Infrastructure Protection.
52 European Commission, European Commission Fact Sheet: Questions and Answers: Directive on Security and Information systems, the first EU-wide legislation on cybersecurity.
European Commission, NIS Cooperation Group.
European Union Agency for Cybersecurity, NIS Directive.

and maintained by the teams which allow for the implementation of any function performed by the CERTs, from incident management to hazard analysis.

ENISA is responsible for implementing and providing central aspects of the MeliCERTes facility[53].

Militärausschuss der Europäischen Union (European Union Military Committee, EUMC, official translation)
The European Union Military Committee is responsible for leading all military activities within the European Union (for example, CSDP missions) and acts in an advisory capacity to the Political and Security Committee on defense issues and recommendations. The EUMC consists of EU Member States' Chiefs of Defence (CHOD's), who are then represented by their military delegates.

In addition to its advisory duties for the PSK, the EUMC produces the military guidelines for the European Union Military Staff (EUMS), which is in turn responsible for the operational implementation of the CSDP. The Chairman of the EUMC (CEUMC) is appointed by the Council of the European Union and takes part in meetings of the PSK and the NATO Military Committee. Regular meetings occur between the EUMC and the NATO MC. Furthermore, the CEUMC participates in meetings of the Council of the EU when topics of defense relevance are discussed[54].

NIS Public-Private Platform (NIS Platform)
The NIS Platform was announced in the EU Cybersecurity Strategy in 2013. Its objective is to improve the resilience of those networks and information systems that underpin the services of private companies and public administration. Furthermore, it is supporting implementing measures laid out in the NIS Directive in order to enable a high level of network and information security and identify best practices.

The findings of the NIS Platform informed the European Commission's recommendations on cybersecurity in the past[55].

Politisches und Sicherheitspolitisches Komitee (Political and Security Committee, PSK, official translation)
The PSK is responsible for the EU's Common Foreign and Security Policy (CFSP). It is comprised of Member States' ambassadors in Brussels or representatives of

53 European Commission, A call for tender to advance MeliCERTes, the facility used by the CSIRTs in the EU to cooperate and exchange information.
European Commission, Tools and capacity building for better cyberspace monitoring, analysis and threat detection for Lithuania and EU.
54 Amtsblatt der Europäischen Gemeinschaften, Beschluss des Rates vom 22. Januar 2001 zur Einsetzung des Militärausschusses der Europäischen Union.
European External Action Service, European Union Military Committee (EUMC).
55 ENISA, NIS Platform.

Member States' foreign ministries. It normally meets twice a week but gathers more frequently when necessary. The PSK monitors international situation developments and is responsible for the political control and strategic management of crisis management operations. It is furthermore involved in the decision-making process of all cyber-related diplomatic actions.

The PSK is chaired by representatives of the European External Action Service. It can voice recommendations on strategic concepts and political options towards the Council of the EU. The PSK meets regularly with the NAC and also receives periodic briefings from the NATO Secretary General (or deputy) and the SACTEUR[56].

Rat der Europäischen Union (Council of the European Union, Council, official translation)

The EU Member States are responsible for their own cybersecurity. Even so, they coordinate at EU level in the Council of the European Union (often just referred to as 'Council' in order to differentiate from the European Council). The Council, which meets at the level of the ministers responsible for their policy area at national level, convenes in ten thematic configurations – such as Foreign Affairs (FAC), Justice and Home Affairs, or Economic and Financial Affairs. The presidency of the Council rotates biannually among EU Member States. The Council is involved in the EU legislative process and can also adopt acts of EU legislation itself. In addition, the Council is responsible for implementing the EU's Common Foreign and Security Policy on the basis of the decisions and guidelines adopted by the European Council. In the event of an EU-wide crisis in the area of cybersecurity, the Council takes over coordination on EU level through the Integrated Political Crisis Response (IPCR). Within this framework, it can resort to the informal round table, which can consist of representatives of the European Commission, the European External Action Service, EU agencies and affected Member States, as well as relevant experts and cabinet members of the President of the European Council. Moreover, the Council has established a number of bodies for coordination and information exchange, as well as the preparation of ministerial meetings, to which inter alia the Horizontal Working Group on Cyber Issues (HWP) or the Standing Committee on Operational Cooperation on Internal Security (COSI) belong. The latter is intended to strengthen operational measures related to the internal security of the EU such as law enforcement and border control.

The Council may instruct the European Commission to negotiate international agreements with their conclusion being subject to a decision of the Council based on an EC proposal. The High Representative of the EU for Foreign Affairs and Security Policy

56 European Council/Council of the European Union, Politisches und Sicherheitspolitisches Komitee (PSK).
European Court of Auditors, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
European Parliament, Understanding EU-NATO cooperation: Theory and practice.

chairs the FAC. The Committee includes senior officials from the interior and justice ministries of all EU Member States, representatives of the European Commission and the EAD. Representatives of Europol, Eurojust, Frontex, CEPOL or other relevant bodies can be invited as observers[57].

Reference Incident Classification Taxonomy Task Force (TF-CSIRT)
The TF-CSIRT aims to create and administer a reference document in order to develop mechanisms for updates and versioning and organize personal meetings of stakeholders.

TF-CSIRT includes members of the European CSIRTs, including the CERT-Bund and the Common Taxonomy Governance Group i.e., representatives of ENISA and EC3[58].

Senior Officials Group Information Systems Security (SOG-IS)
SOG-IS is an association of government organizations and agencies of the EU and the European Free Trade Association, which coordinates the standardization of protection profiles (based on common criteria) and certification policies between European certification authorities. It also develops protection profiles whenever the European Commission adopts a directive that must be transposed into national IT-security laws.

Germany's affiliate member is the BSI[59].

Ständige Strukturierte Zusammenarbeit (Permanent Structured Cooperation, PESCO, official translation)
PESCO was established as a cooperation framework to increase cooperation efforts within the Common Security and Defence Policy (CSDP). Dedicated PESCO projects aim to strengthen EU capabilities and interoperability through the development of cyber-defense capabilities.

The EAD (incl. EUMS) and the EVA form the PESCO Secretariat. The CIDCC was creat-

57 Council of the European Union, Cyberangriffe: EU plant Gegenmaßnahmen, inklusive Sanktionen.
Council of the European Union, Der Rat der Europäischen Union.
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, EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018).
Council of the European Union, Ständiger Ausschuss für die operative Zusammenarbeit im Bereich der Inneren Sicherheit (COSI).
Council of the European Union, The EU Integrated Political Crisis Response – IPCR – Arrangements.
European Council/Council of the European Union, Horizontal Working Party on Cyber Issues (HWP).
European Commission, Anhang zur Empfehlung der Kommission über die koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.
European Court of Auditors, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
European Union, Rat der Europäischen Union.

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

59 SOGIS, Introduction.

ed in the framework of PESCO project packages[60].

Taxonomy Governance Group (TGG)
The TGG is responsible for maintaining and updating the document "Common Taxonomy for Law Enforcement and The National Network of CSIRTs", which provides a common taxonomy for classifying criminal incidents. The TGG meets annually for a regular group meeting.

In doing so, it aims to facilitate cooperation between international law enforcement agencies, CSIRTs and prosecutors' offices, as well as strengthen preventative measures and investigative capabilities. ENISA, EC3/Europol, the EUCTF, CERT-EU as well as selected CSIRTs take part in the working group via respective subject matter experts[61].

Zentrum für die Koordination von Notfallmaßnahmen (Emergency Response Coordination Centre, ERCC, official translation)
The ERCC of the European Commission, housed within the Directorate-General for European Civil Protection and Humanitarian Aid Operations (GD ECHO), supports and coordinates various activities in the areas of prevention, preparedness and response.

ERCC functions as both the Commission's central crisis management agency and as the central EU's IPCR 24/7 contact point[62].

Zentrum für Informationsgewinnung und -analyse (EU Intelligence Analysis Centre, INTCEN, official translation)
INTCEN (earlier: EU Situation Centre (EU SITCEN)) is a civil analysis unit of the European External Action Service, which processes prepared materials (finished intelligence) from Member States. Unlike national intelligence services in EU Member States, INTCEN, which reports directly to the High Representative for Foreign Affairs and Security Policy, therefore has no independent operational intelligence-gathering capabilities. In addition, by taking into consideration other, publicly accessible information – such as reports from European delegations or EU satellite centers' intelligence assessments – it produces situational strategic assessments, special reports and derives options for action from them. It forms a component of the

60 EEAS, Ständige Strukturierte Zusammenarbeit – SSZ.
PESCO, About PESCO.
PESCO, PESCO Secretariat.
Council of the European Union, EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018).
61 Europol, Common Taxonomy for Law Enforcement and The National Network of CSIRTs.
Rossella Mattioli und Yonas Leguesse, Reference Incident Classification Taxonomy Task Force Update.
62 Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".

EAD's crisis management structures alongside the Military Intelligence Directorate of EU Military Staff (EUMS INT) and the Crisis Management and Planning Directorate (CMPD). In addition to the EU Hybrid Fusion Cell, INTCEN also houses the EU Situation Room (SITROOM), which provides the necessary operational capacity for the European External Action Service's immediate and effective response to crisis situations. It is the permanent civil-military authority on standby, providing round-the-clock global monitoring and situational assessment.

Among German authorities, the BND and BfV contribute reports and personnel to INTCEN. INTCEN reports go to BKAmt, BND, AA, BMVg, BAMAD, BMI and BfV, as well as to other institutions, depending on the topic. INTCEN products can also be made available to other EU institutions operating within the CFSP, the Common Security and Defence Policy or counterterrorism. Together with the EUMS INT, INTCEN forms the SIAC. Together with Europol, INTCEN proactively produces a threat analysis every six months, which it submits to COSI[63].

63 Council of the European Union, Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.
Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".
German Bundestag (Drucksache 19/489): Antwort der Bundesregierung auf die Kleine Anfrage: Pläne der Europäischen Kommission für eine geheimdienstliche „Europäische Aufklärungseinheit".
European External Action Service, EU INTCEN Factsheet.
Matthias Monroy, Europäisches Geheimdienstzentrum vor neuen Aufgaben.
Matthias Monroy, How European secret services organize themselves in "groups" and "clubs".
Raphael Bossong, Die nachrichtendienstlichen Schnittstellen der EU-Sicherheitspolitik.

5. Explanation: Actors at NATO level

Allied Command Operations (ACO)

Within NATO's military command structure, which consists of the Allied Command Operations (ACO) together with the Allied Command Transformation (ACT), the ACO is responsible for the planning and execution of all NATO operations. Moreover, it advises the political and military leadership of NATO in military questions. Under the leadership of the Supreme Allied Commander Europe (SACEUR), the ACO, headquartered at the Supreme Allied Powers Europe (SHAPE) in Mons, Belgium, commands various commandos at the operational and tactical levels geographically dispersed across the NATO alliance. In addition to units for air, land and sea, three further commandos for special operations, logistics and cyberoperations round out NATO's six tactical commandos. In the military realm, ACO is responsible for the strategic design of cyber defense.

This strategic design is supported at the tactical level through situation pictures provided by the NCIA. The CyOC is subordinate to the ACO Deputy Chief of Staff (DCOS) for Cyberspace. Together with the SECGEN, SACEUR has taken part in NATO briefings to the PSK[64].

Allied Command Transformation (ACT)

Compared to the operational focus of the ACO, the Allied Command Transformation is responsible for education, training and exercises within NATO's military command structure. It also contributes to capability development for the interoperability and future viability of the alliance. ACT is subordinate to the Supreme Allied Commander Transformation (SACT). Within the ACT, the Capability Development Directorate is responsible for cyber defense and cybersecurity. Here, exercises in cyberspace are prepared, such as the yearly NATO Cyber Coalition Exercise, among others.

The Bundeswehr takes part in the NATO Cyber Coalition Exercise, which is carried out with the support of the NATO Military Committee. ENISA is represented in a visiting role. NATO Centres of Excellence (CoE), such as the CCDCOE, are accredited through the ACT. ACT can commission the CCDCOE to take over certain duties. At the behest of ACT, the CCDCOE is currently taking over the function of Education and Training Department Head (E&T DH) for areas relating to cyber, and thus coordinates education in this area, for example, at the NS-O, which falls within ACT's mandate. The SACT and the Chief Executive of the EVA hold regular meetings[65].

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

65 Allied Command Transformation, Who We Are.
NATO, Cyber defence.

Cyber Defence Committee (CDC)
The CDC is a committee subordinate to the North Atlantic Council responsible for managing cyber defense within NATO. The CDC, which meets at expert level, oversees and steers NATO's efforts and activities within the realm of cyber defense.

The Cyber Defence Management Board (CDMB) has a reporting obligation to the CDC. In the case of a severe cybersecurity incident, the CDC can refer the situation to the North Atlantic Council for further consideration. The German representative in the CDC receives a coordinated instruction from the AA, BMI and BMVg, the BSI is involved in an advisory capacity during the instruction process[66].

Emerging Security Challenges Division (ESCD)
The Emerging Security Challenges Division is organizationally located within the NATO International Staff (IS). The ESCD is tasked with inter alia strengthening NATO's ability to anticipate and combat new challenges, and developing political solutions to defend the alliance against such challenges. For this purpose, it evaluates, for example, potential crises and their resulting consequences for NATO from a strategic perspective, and maintains topic-specific dialogues with organizations and actors, both within and outside of NATO. The ESCD is led by an Assistant Secretary General (ASG) for Emerging Security Challenges. It is also responsible for the NATO Science for Peace and Security Programme (SPS) as well as the Strategic Analysis Capability. In addition to departments for innovation, data policy, counterterrorism, hybrid challenges and energy security, the ESCD oversees a designated department for cyber defense. As a civil counterpart for engagement from a military perspective within SHAPE (ACO), the ESCD coordinates efforts to protect NATO networks against cyberattacks, supports alliance partners in strengthening their resilience and cultivates political cyber defense collaborations and partnerships. Furthermore, the ESCD commands a Cyber Threat Assessment Cell (CTAC), which monitors topics and developments relating to cybersecurity.

The ESCD was established based on the decision of the NAC. The ESCD leads the NATO Cyber Defence Management Board. Its Cyber Threat Assessment Cell operates in close consultation with the CyOC. The ESCD has held meetings with representatives of the EAD for discussions on cyber defense. The joint agreement on the designation of the BSI as National Cyber Defence Authority (NCDA) vis-à-vis NATO was concluded from the NATO side by the ESCD[67].

66 Jeffrey L. Caton, NATO Cyberspace Capability: A Strategic and Operational Evolution.
NATO, Cyber defence.
NATO CCDCOE, North Atlantic Treaty Organization.

67 NATO Emerging Security Challenges Division, Science for Peace and Security (SPS) Programme.
NATO HQ, ESCD.
NATO International Staff, Vacancy Notification: Cyber Threat Analyst, Cyber Threat Assessment Cell.
NATO, NATO, European Union experts review cyber defence cooperation.

Joint Intelligence and Security Division (JISD)

The Joint Intelligence and Security Division within the NATO IS is tasked with contributing to decision-making at the highest political level through increased situational awareness and the collection of a wide array of intelligence resources. For example, a unit for the analysis of hybrid threats (Hybrid Analysis Branch) is located within the JISD for this express purpose.

Products of the JISD are primarily made available to decision-makers within the NAC and the MC. JISD exchanges information with both ACT and ACO; especially close cooperation exists with the ACO in the communication of warnings. Beyond NATO, the JISD furthermore cooperates and regularly exchanges information with the EU Hybrid Fusion Cell. Both actors carry out parallel evaluations of the security landscape every year in order to contribute to a standardized consideration of the threat situation[68].

NATO Communications and Information Agency (NCIA)

The NATO Communications and Information Agency (NCIA) was founded after the fusion of seven former NATO organizations. The NCIA is responsible for the connectivity of the alliance as well as the procurement and protection of its communication and information infrastructures. Every year, the NCIA acquires new communications, computer systems, intelligence, surveillance and reconnaissance (C4ISR)-technologies, through which inter alia the interoperability of ICT systems is strengthened. The NCIA also supports NATO members and other partner states in the development of interoperable ICT capabilities. Those NATO Smart Defence Initiatives relating to cyber defense, such as the Smart Defence Multinational Cyber Defence Capability Development (MN CD2) or the Malware Information Sharing Platform (MISP), are organizationally located at the NCIA.

Both the NCSC and the NCI Academy are subordinate to the NCIA. The NCIRC also operates through the NCSC. The NCIA is in constant communication with the CyOC, to which it delivers status updates on NATO networks and on whose operational instructions it reacts to cybersecurity incidents. In a crisis scenario, ACO has the authority to prioritize the efforts and activities of the NCIA. Information exchanges occur between the CERT-EU and the NCIA, as do regular meetings at the working level[69].

68 Arndt Freytag von Loringhoven, A new era for NATO intelligence.
EU-NATO, Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017.
NATO, NATO's response to hybrid threats.
NATO, Structure.

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

NCI Academy

The establishment of the NCI Academy combined four previously separate NATO training institutions under the umbrella of the NCIA: NATO CIS School, Applications Training Facility The Hague, Air Command and Control Systems Training Centre, and SHAPE CIS Training Centre. The standardization of course catalogues through the NCI Academy is meant to allow for the best-possible training of participants in the fields of cybersecurity, leadership, information and C4ISR. Training at the NCI Academy is offered for NATO alliance members as well as non-member states. The NCIA aims to train up to 10,000 so-called "cyber defenders" for NATO and the EU between 2020 and 2027. To this end, the NCI Academy maintains partnerships with academia and the private sector.

Current course offerings at the NCI Academy were developed with support of the ACT. The CCDCOE assumes the E&T DH for the NCI Academy in the field of cyber[70].

NATO Computer Incident Response Capability (NCIRC)

The NATO Computer Incident Response Capability, subordinate to the NCIA, has organizational command over a Technical (NCIRC TC) and Coordination Centre (NCIRC CC), which are both housed within SHAPE. Both are meant to protect and repel NATO networks on a technical level from all kinds of attacks around the clock. In this respect, the NCIRC TC is responsible for the prevention, recognition and processing of possible cybersecurity incidents or threats and relays case-specific information. Furthermore, the NCIRC TC commands so-called Rapid Reaction Teams (RRT) as a permanent standby element, which, if requested, can react within a maximum of 24 hours to attacks of national importance and contribute to systems restoration. For its part, the NCIRC CC is responsible for coordinating cyber defense activities within NATO, among NATO allies and with international organizations.

The NCIRC CC also supports the CDMB with personnel and maintains relationships to other international organizations such as the EU. The NCIRC TC and the CERT-EU cooperate in a technical capacity in order to better information exchange and share best practices. Further cooperation exists at the working level between the NCIRC TC and the CERT-Bw. Requests to deploy RRT's must be granted by the CDMB for alliance states and by the NAC for non-NATO states. Experts of the RRT's participate in the cybersecurity exercises Cyber Coalition Exercise as well as Locked Shields[71].

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

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

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited multinational competency center for cybersecurity headquartered in Tallinn, Estonia. While it is part of NATO's legal entity as a NATO-accredited center of excellence, it has to be noted however, that it does not constitute a part of the NATO Command Structure. The CCDCOE offers NATO, its alliance members and partners training and education in strategic, operative, technical and legal aspects of cyber defense. The organization of the yearly cybersecurity exercise Locked Shields falls under the auspices of this principal function. CCDCOE also conducts its own research into these four aforementioned dimensions. These research findings (for example, INCYDER or the Cyber Defence Library) are made available to the greater public. In 2020, the CCDCOE initiated a five-year process to produce a Tallinn Manual 3.0, an update of the current manual (Tallinn Manual 2.0). Every year, the CCDCOE also organizes the International Conference on Cyber Conflict (CyCon), which brings together representatives from politics, industry and academia for interdisciplinary discussions.

On the part of NATO, ACT handles the accreditation of the CCDCOE, which can also instruct the CCDCOE to perform certain tasks. At the moment, ACT has tasked the CCDCOE with assuming the Department Head for Cyber Defence Operations Education and Training (E&T DH) and coordinating all training initiatives of NATO in the realm of cyber defense. To fulfill its mandate, the CCDCOE maintains working relationships with, for example, the NS-0, the NCI Academy, the EVA, the ESVK and the CODE at the University of the Bundeswehr München. Germany, as one of the seven founding nations of CCDCOE, currently holds the position of Deputy Director and participates in Locked Shield through representatives of the Bw and the BMVg[72].

NATO Consultation, Control and Command Board (C3B)

The NATO Consultation, Control and Command Board (C3B) advises and acts on behalf of the North Atlantic Council in the fields of consultancy, control and command (C3), which primarily includes, for example, information exchange, interoperability, surveillance and reconnaissance. With regard to cybersecurity, it is the primary body within NATO for discussions focusing on the implementation of cyber defense from a technical standpoint. The C3B meets twice a year to set its strategic priorities. The C3B comes together regularly in Permanent Session, composed of national representatives of the C3 (NC3REPs), in order to review the achievement of strategic goals. It also has many specialized subcommittees at its disposal, such as the Information Assurance and Cyber Defence Capability Panel. The C3B is supported in its work through the NATO Headquarters C3 Staff (NHQC3S), a joint unit of the International Military Staff and the International Staff.

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

Apart from national and Military Committee representatives, ACT and ACO also participate in the C3B. For Germany's part, this function is led by the BMVg. The BMVg and the BSI are represented in the subordinate Information Assurance and Cyber Defence Capability Panel[73]*.*

NATO Cyber Defence Management Board (CDMB)

In the NATO Cyber Defence Management Board, all cyber defense activities within the civilian and military organizational structure of NATO are coordinated through strategic planning. Moreover, the CDMB can finalize Memoranda of Understanding with NATO alliance members, for example, in order to better the exchange of information between both levels.

The CDMB is chaired by the ESCD and is required to report to the CDC. It consists of the representatives of all NATO actors with a mandate in the realm of cyber defense, including ACO, ACT and NCIA, for example[74]*.*

NATO Cyber Security Centre (NCSC)

The NATO Cyber Security Centre (NCSC) within the NCIA is responsible for the entire so-called "Cyber Security Service Line" and contributes to preventing, recognizing and reacting to cybersecurity incidents. Furthermore, a Cyber Security Collaboration Hub was created for better connectivity, information procurement and education between the national CERT's of NATO alliance members. The NATO Industry Cyber Partnership (NCIP) between internal NATO actors, national CERT's and industry representatives also exists under the umbrella of the NCSC. The NICP aims to improve cyber defense within the NATO supply chain, strengthen quick information pathways and exchange during cyber threats, and generally promote best practices.

The NCIRC is subordinate to the NCSC. Exchange of information and close working relationships exist with the CyOC, which are also promoted through their common location within SHAPE[75]*.*

NATO Cyberspace Operations Centre (CyOC)

The establishment of the NATO Cyberspace Operations Center is slated for completion by 2023, at which time it should be fully operational. The CyOC aims to support all NATO activities in cyberspace at both strategic and operational level through the development of situational awareness and position recognition, for example, within the context of coordinating NATO operations. For coordination purposes, CyOC shall have liaison elements with ACO regional commandos, among others.

73 NATO, Consultation, Command and Control Board (C3B).
NATO, Cyber defence.
74 Jeffrey L. Caton, NATO Cyberspace Capability: A Strategic and Operational Evolution.
NATO, Cyber defence.
75 NCIA, Securing the Cloud.
NCIA, What We Do: NATO's Cybersecurity Centre.
NICP, Objectives and Principles.

To foster situational awareness, the CyOC is reliant on alliance members' intelligence information and is supported in fulfilling its duties inter alia through the CTAC of the ESCD in NATO HQ as well as the NCIRC. CyOC is subordinate to the DCOS Cyberspace within the ACO and is located at SHAPE in Belgium[76].

NATO-Militärausschuss (NATO Military Committee, MC, official translation)
As NATO's highest military body, the NATO Military Committee compliments decision-making at the highest level. As a nexus point, it is responsible for the operational implementation of political decisions in military directives, supports the preparation of overall strategic concepts of the alliance, and can make recommendations for measures for the best-possible defense of the alliance. In the recent past, the MC also discussed, for example, cyberattacks and election interference. Every year, the MC carries out a strengths and capability assessment of countries threatening NATO interests. The MC meets at least once a week at the level of nationally deployed military representatives as representatives of their Chiefs of Defence. The latter convene three times per year in the MC format.

The MC is responsible for advising the NAC in military policy issues. The Strategic Commanders of the ACT and the ACO receive their directions through the MC. Germany is represented in the MC through representatives of the Bw. The MC regularly meets with its EU counterpart, the EUMC[77].

NATO School Oberammergau (NS-O)
As one of the NATO training institutions within the NATO Command Structure, the NATO School in Oberammergau, equally financed by Germany and the USA, offers training units and courses with an operational and technical focus. Within the realm of cybersecurity and cyber defense, the NS-O seeks to strengthen the capabilities of NATO alliance members and partner nations, and protect critical communications and information infrastructure against attacks. In this respect, the NS-O inter alia established a Cyber Security Certificate Programme together with the Naval Postgraduate School (NPS).

Training and education at the NS-O in the field of cybersecurity and cyber defense is coordinated through the CCDCOE[78].

76 Don Lewis, What is NATO Really Doing in Cyberspace?.
BrigGen Sandor Vass, Cyberspace Operations Centre: A Capability User Perspective.
Robin Emmott, NATO cyber command to be fully operational in 2023.
77 Europäisches Parlament, Understanding EU-NATO cooperation: Theory and practice.
NATO, Military Committee.
U.S. Department of Defence, NATO Military Committee Gets Virtual Check on Alliance Missions.
78 NATO School, NATO School Oberammergau – Naval Postgraduate School Cyber Security Professional Programme Closure in Morocco.
NATO School, Organization.

NATO Security Committee (SC)
The Security Committee deals with issues of security policy and develops recommendations for NATO security policy. In this respect, it plays an advisory role vis-à-vis the North Atlantic Council. Furthermore, the adoption of standards and guidelines inter alia in the realm of information security fall within its remit. The SC meets in varying formations, such as the SC in CIS Security Format (SC (CISS)), for example.

For Germany, the BMI is in charge of the SC. The BSI serves an advisory role and represents Germany within the SC (CISS). A reporting obligation to the NAC exists for the SC, which it must fulfil at least once per year. Referrals to the SC may be initiated by the NAC, NATO allies, the MC, or the C3B. Furthermore, representatives of the C3B as well as the ACO and the ACT are present at meetings of the SC. Further NATO bodies and actors are incorporated, if the occasion warrants their participation[79].

Nordatlantikrat (North Atlantic Council, NAC, official translation)
The North Atlantic Council, already provided for in the 1949 North Atlantic Treaty, consists of representatives of NATO alliance members. Representatives meet at least once a week at ambassador level, as well as every six months at the level of the ministers of foreign affairs and defense. The NAC meets roughly every two years as a summit of heads of state and government (Brussels Summit). The NAC is the primary political decision-making body within NATO. In the case of a severe cybersecurity incident or attack, the NAC would make a decision regarding a uniform NATO reaction and possibly trigger the mutual defense clause to account for crisis management according to Article 5 of the North Atlantic Treaty. The NAC makes its decisions following the principle of unanimity. Moreover, the NAC is able to submit joint statements, thus condemning specific behavior, for example.

At ambassador level, Germany is represented in the NAC by the Permanent Representative to NATO (AA). The NAC is chaired by the NATO Secretary General. The CDC is directly subordinate to the NAC and supports its work as a subcommittee. From a hierarchical perspective, the CDC is below the CDMB, followed in turn by the NCIRC. The NAC and the PSK of the EU regularly meet for formal and informal meetings. In the past, the High Representative of the Union for Foreign Affairs and Security Policy (or a representative from the EAD) has regularly participated in meetings of the NAC at the level of the defense ministers[80].

79 NATO, Security Committee (SC).
80 Center for European Policy Analysis, Moving Toward NATO Deterrence for the Cyber Domain.
NATO, North Atlantic Council.
NATO, Statement by the North Atlantic Council concerning malicious cyber activities.
Permanent Mission of the Federal Republic of Germany to NATO, Botschafter König.

6. Explanation: Actors at Federal Level

Agentur für Innovation in der Cybersicherheit (Agency for Innovation in Cybersecurity, Cyberagentur, own translation)
After an interim phase in Halle (Saale), the Cyberagentur will be moved to a long-term facility at Leipzig-Halle airport. The formation process of the Cyberagentur was completed in August 2020 and first commissions are said to have been made by the end of 2020. The task of the Cyberagentur is to identify innovations and to award contracts for the development of concrete potential solutions. In particular, ambitious research projects with high innovation potential in the field of cybersecurity as well as related key technologies for meeting state needs regarding internal and external security should be supported. Within this context, the Cyberagentur does not pursue its own research, development and innovations, but rather coordinates the needs of security agencies and improves cooperation between federal authorities, academia and the private sector. The work of the Cyberagentur is governed by parliamentary control mechanisms and conditions.

BMI and BMVg are jointly responsible for the Cyberagentur. Together with SprinD, the Cyberagentur constitutes an ecosystem that identifies, promotes and develops promising ideas and innovations. Both emerged as initiatives within the German government's "High-Tech Strategy 2025". In order to avoid redundancies, there is close coordination of work programs between the two agencies, through mutual commissioning on inter-agency issues, for example. The Cyberagentur also exchanges information with ZITiS, CIHBw and CODE. The Supervisory Board of the Cyberagentur consists of members and representatives of the BMI, BMVg, BMF as well as staff councils of the Bw's procurement offices, and academia[81].

Agentur für Sprunginnovationen (Agency for Springboard Innovation, SprinD, official translation)
SprinD, located in Leipzig, serves as a state instrument for innovation development. It supports research ideas deemed suitable as innovations, as well as affiliate companies that promote potential innovations and create new jobs. Generally speaking, the agency is open to research ideas from all subject areas. It is intended to launch innovations that are radically new with regard to applied technologies and have a high potential for market-changing impact, albeit through new products, services or value chains. One billion euros have been made available to the agency for its first ten years of work.

81 Andre Meister und Anna Biselli, Bundesrechnungshof bezweifelt Sinn der neuen Cyberagentur.
Federal Ministry of the Interior, Building and Community, Cyberagentur des Bundes nach Halle/Saale und Leipzig.
Federal Ministry of the Interior, Building and Community, Startschuss für die Cyberagentur.
Federal Ministry of Defence, Technologiesouveränität erlangen – die neue Cyberagentur.
German Bundestag (Drucksache 19/22958), Antwort der Bundesregierung auf die Kleine Anfrage: Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur).
Federal Government, Agentur für Innovation in der Cybersicherheit. (Website deleted)
Lina Rusch, Cyberagentur kommt – mit strengen Auflagen.

SprinD was founded jointly by the BMBF and the BMWi. Its Supervisory Board consists of representatives of the BMF, BMBF and BMWi as well as members from academia and politics. SprinD coordinates its tasks with the Cyberagentur[82].

Allianz für Cyber-Sicherheit (Alliance for Cybersecurity, ACS, own translation)
The ACS offers confidential exchange between its members and the BSI on cyber threats, protective measures and incident management. Members also receive information on how to develop their cybersecurity expertise. Any institution headquartered in Germany can become a member.

The ACS is a public-private partnership between the BSI, BITKOM and the private sector, as well as other public authorities, research institutions and academia. Its Advisory Board includes representatives from the BMI and BSI. ACS participants include inter alia the BBK, BaFin, BKartA, BKA, BMVI, BMWi, BWehr, an institute of the UniBw Munich as well as Vitako[83].

Auswärtiges Amt (German Federal Foreign Office, AA, official translation)
Within the framework of cyber foreign policy, the AA is committed to international cybersecurity, universal human rights in the digital realm and the utilization of economic opportunities offered through digitalization. To realize this mandate, the "Koordinierungsstab für Cyber-Außenpolitik" (International Cyber Policy Coordination Staff, KS-CA, official translation) was established within the AA, which operates under the purview of an Ambassador for Cyber Foreign Policy (CA-B). It has established cyber foreign policy responsibilities at selected missions abroad, which are inter alia tasked with reporting to headquarters in Berlin.

The AA is represented in the Cyber-SR. It alternates with the BMVg in managing the BAKS[84].

Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (Federal Office of Bundeswehr Equipment, Information Technology, and In-Service Support, BAAINBw, official translation)
The main task of the BAAINBw is to outfit the German military with both technical equipment and IT systems. These systems are mostly being commissioned and

82 Federal Ministry of Defence, Technologiesouveränität erlangen – die neue Cyberagentur.
Federal Ministry of Education and Research, Agentur für Sprunginnovationen.
Federal Ministry of Education and Research, Bundesregierung setzt Gründungskommission für die Agentur für Sprunginnovationen ein.
Federal Ministry for Economic Affairs and Energy, Aufsichtsrat der Agentur für Sprunginnovationen SprinD tritt zur konstituierenden Sitzung zusammen.
Deutschlandfunk, „Um Erfolg zu haben, müssen wir uns das Scheitern trauen".
Lina Rusch, Potsdam oder Leipzig? Karliczek vertraut auf SprinD-Gründungsdirektor bei Standortfrage.
Tagesschau, Die Suche nach dem nächsten großen Ding.
83 Federal Office for Information Security, Allianz für Cyber-Sicherheit – Über uns.
Federal Office for Information Security, Beirat der Allianz für Cyber-Sicherheit.
Federal Office for Information Security, Teilnehmerliste der Allianz für Cyber-Sicherheit.
84 Federal Foreign Office, Cyber-Außenpolitik.
Federal Foreign Office, Einrichtung einer Zuständigkeit für Cyber-Außenpolitik.

not developed independently. Through its role as project and utilization manager of the systems acquired and operated, it shares the responsibility for providing the Bw with the best possible protection against cyberattacks.

The BAAINBw falls under the purview of the BMVg. It provides the Bw with IT as well as digitized weapon systems and is responsible for the management of the BWI[85].

Bundesakademie für Sicherheitspolitik (Federal Academy for Security Policy, BAKS, official translation)
BAKS is a training institution for security policy of the Federal Government. It deals with security policy challenges in the digital age in different event formats, such as the "Berliner Forum zur Cyber-Sicherheit" (Berlin Forum on Cybersecurity, own translation).

BAKS falls under the purview of the BMVg. The BMVg and the AA take turns nominating the academy's president and vice president. The BAKS Board of Trustees is chaired by the Federal Chancellor and includes representatives of all ministries represented on the Federal Security Council (AA, BMVg, BMF, BMJV, BMWi, BMZ and the BKAmt). Representatives of the GIZ, the Bw, the BMI and the UniBw serve as members of the BAKS Advisory Board[86].

Bundesanstalt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority, BaFin, official translation)
The task of BaFin is to ensure a functioning and stable financial system of integrity in Germany. In the field of economic crime, BaFin recognizes an increasing risk of cybercrime for insurers, financial service providers and banks.

In the event of a cyber intrusion or attack, a close exchange of information with the BSI is taking place. BaFin falls under the purview of the BMF and is represented in the Cyber-AZ[87].

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Federal Office of Civil Protection and Disaster Assistance, BBK, official translation)
The BBK assumes functions in the overall concept of Germany's national security architecture. Within this framework, it increasingly concerns itself with the risk of cyberattacks on the nation's critical infrastructure.

85 Federal Office of Bundeswehr Equipment, Information Technology, and In-Service Support, Das BAAINBw.
86 Federal Academy for Security Policy, Cyber-Realität zwischen Freiheit und Sicherheit.
Federal Academy for Security Policy, Der Beirat.
Federal Academy for Security Policy, Das Kuratorium, der Bundessicherheitsrat.
87 Federal Financial Supervisory Authority, Aufgaben & Geschichte der BaFin.
Federal Financial Supervisory Authority, BaFinPerspektiven. Ausgabe 1 2020: Cybersicherheit.

The BBK is represented in the Cyber-AZ and its staff is responsible for the "Gemeinsame Melde- und Lagezentrum von Bund und Ländern" (Joint Information and Situation Centre of the Federal Government and the Federal States, GMLZ, official translation). The BBK falls under the purview of the BMI and is represented in UP KRITIS and the ACS[88].

Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (German Federal Agency for Public Safety Digital Radio, BDBOS, official translation)

BDBOS is responsible for the "Digitalfunk BOS" (BOS Digital Radio Network, official translation) and the networks of the Federal Government. The former ensures a digital radio network as a means of communication for all authorities and organizations with security tasks in the federal and federal state governments. With respect to the latter, the "Informationsverbund Berlin-Bonn" (Berlin-Bonn Information Network, IVBB, own translation) and the "Informationsverbund der Bundesverwaltung/Bundesverwaltungsnetz" (Federal Administration Information Network, IVBV, own translation) among others, were merged to form a uniform network infrastructure. In the long term, this current structure, together with the "Bund-Länder-Kommunen-Verbindungsnetz" (Federal-Länder-Municipal Interconnection Network, NdB-VN, own translation) is to be consolidated into the "Informationsverbund der öffentlichen Verwaltung" (Information Network of Public Administration, IVÖV, own translation).

BDBOS falls under the purview of the BMI and the BfIT assumes the chairmanship of the BDBOS Administrative Board. To safeguard the networks of the Federal Government, BDBOS works closely together with the BSI. The BOS Digital Radio Network is inter alia available to the BPol, BKA, ZKA, BBK, BfV and LfV[89].

Bundesamt für den Militärischen Abschirmdienst (Federal Office for Military Counter-Intelligence, BAMAD, official translation)

BAMAD is a federal agency that serves as the nation's military intelligence service. BAMAD is the third and smallest German intelligence service, alongside the BND and the BfV. It is tasked with defending against extremism and terrorism, as well as combating (cyber) espionage and sabotage in the Bw. In this context, BAMAD's "cyber shielding" encompasses all operational, reactive and preventive measures taken by BAMAD to counter intelligence and security-threatening activities or extremist/terrorist efforts in cyber and information space.

88 Federal Office of Civil Protection and Disaster Assistance, Gemeinsames Melde- und Lagezentrum von Bund und Ländern.

89 German Federal Agency for Public Safety Digital Radio, Chronik.
German Federal Agency foar Public Safety Digital Radio, Die Bundesanstalt.
German Federal Agency for Public Safety Digital Radio, Netze des Bundes.
German Federal Agency for Public Safety Digital Radio, Netze des Bundes – Zukunftsweisende Kooperation vereinbart.
German Federal Agency for Public Safety Digital Radio, Nutzergruppen.
Federal Government, Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme.

BAMAD falls under the purview of the BMVg and is represented in the Cyber-AZ[90].

Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, BSI, official translation)
The BSI is responsible for strengthening the security of the Federal Government's information technology and ensuring the protection of government networks. In order to be able to take immediate remedial action in the event of a cyber incident of outstanding importance, the BSI has Mobile Incident Response Teams (MIRT) at its disposal which can be dispatched to federal administration as well as companies in charge of critical infrastructure. For the federal administration, the BSI acts as the central reporting point for IT security. As an authority with technical expertise, it also promotes information security and cybersecurity in administrative duties, the economy and society through numerous activities, partnerships and initiatives. At the request of federal states, the BSI can advise and support them on IT security issues. Similar services ranging from information and consulting to technical support and the provision of technical protection measures are also available to German municipalities, if desired. In order to establish better networks on a regional level, the BSI has built liaison offices throughout Germany in Berlin (responsible for Berlin and Brandenburg), Hamburg (responsible for the northern region: Hamburg, Bremen, Lower Saxony, Schleswig-Holstein, Saxony-Anhalt and Mecklenburg-Western Pomerania), Wiesbaden (responsible for the Rhine-Main region: Hesse, Saarland and Rhineland-Palatinate), Bonn (responsible for the western region: North Rhine-Westphalia), and Stuttgart (responsible for the southern region: Baden-Wuerttemberg and Bavaria). The BSI's second site in Freital is in charge of the liaison office's work in the eastern region (Thuringia and Saxony). A third BSI site in Saarbrücken, primarily focusing on AI, is currently being established. Annually, the BSI publishes a "Lagebericht zur IT-Sicherheit in Deutschland" (Situation report on German IT security, own translation).

The BSI falls under the purview of the BMI and is involved in UP KRITIS. Among others, it hosts the Cyber-AZ, ACS, LZ, CERT-Bund and the Bürger-CERT. In addition to the federal and state administrations, all federal state CERTs organized in the VCV receive occasion-related cybersecurity alerts from the BSI. Together with the ITZBund, the BSI has established a "Lenkungskreis Informationsfreiheit" (Steering Committee for Information Security, own translation). Moreover, the BSI has agreed on a cooperation agreement with the vzbv, which, among other areas, deals with digital consumer protection. The BSI is represented in the DsiN advisory board and cooperates with the G4C. It cooperates furthermore with ENISA, is a member of SOG-IS and is also

90 Federal Office for Military Counter-Intelligence, Über uns.
Federal Office for Military Counter-Intelligence, Aufgaben und Befugnisse.
Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: Militärischer Abschirmdienst (MAD).

represented in NATO bodies (CDC, C3B and SC) or involved in corresponding national processes of instruction. The BSI has been designated by Germany as the national NATO Cyber Defence Authority (NCDA)[91].

Bundesamt für Verfassungsschutz (Domestic Intelligence Service of the Federal Republic of Germany, BfV, official translation)
The BfV investigates how new technologies allow extremists, terrorists, or foreign intelligence services, for example, to spy in Germany, spread disinformation or sabotage computer systems. It seeks to defend public and private institutions against cyberattacks and illuminate their origins. Annually, the BfV publishes a "Verfassungsschutzbericht" (Report on the protection of the constitution, own translation), which inter alia also provides information on the status quo of the threat of cyber attacks and any respective incidents in Germany. The BfV also publishes publicly accessible so-called 'Cyber-Briefs' in irregular intervals which are providing information on specific threats.

The BfV falls under the purview of the BMI. Occasion-related classified reports ('Cyber-Spezial') are sent by the BfV to the BMI, BKAmt, and AA. It is represented in the Cyber-AZ as well as the "Initiative Wirtschaftsschutz'" and relies on the expertise of ZITiS. In addition, the BfV's cyber defense unit exchanges information with its counterparts in the "Landesbehörden für Verfassungsschutz" (State Offices for the Protection of the Constitution, LfV, official translation), if existent[92].

Bundesbeauftragte:r für den Datenschutz und die Informationsfreiheit (Federal Commissioner for Data Protection and Freedom of Information, BfDI, official translation)
The BfDI provides advice on and monitors the processing of data and information generated by federal public and non-public agencies. It is politically independent in the performance of its duties and is subject to parliamentary control only by the Bundestag.

91 Federal Office for Information Security, Auftrag.
Federal Office for Information Security, Bundesgesetzblatt Teil I Nr. 54, Jahrgang 2009, Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes.
Federal Office for Information Security, Themen.
Federal Office for Information Security, Vorfallsunterstützung.
Federal Office for Information Security, Zweitstandort der Bundesbehörde BSI entsteht in Freital. (Website deleted)
Federal Government, Besserer Schutz vor Cyber-Angriffen.
German Bundestag (Drucksache19/3398), Antwort der Bundesregierung auf die Kleine Anfrage: Nationale und internationale Kooperationen des Bundesamtes für die Sicherheit in der Informationstechnik.
Background Conversations, 2019.
Fabienne Tegeler, Angebote des BSI für Kommunen.
Lina Rusch, BSI bekommt KI-Ableger in Saarbrücken.

92 Domestic Intelligence Service of the Federal Republic of Germany, Cyberangriffe.
Domestic Intelligence Service of the Federal Republic of Germany, Welche Ziele verfolgen ausländische Nachrichtendienste?. (Website deleted)
German Bundestag (Drucksache 19/2645), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.

BfDI and BSI are cooperating. Further contacts between the BfDI and the EDSB exist. The BfDI is represented in the advisory board of DsiN[93].

Bundeskanzleramt (Federal Chancellery, BKAmt, official translation)
The BKAmt supports the Federal Chancellor in his or her substantial work. To fulfill this duty, it maintains close contact to federal ministries through so-called "Spiegelreferate" (mirror departments, own translation). It comes into contact with cybersecurity topics inter alia through its service and technical supervision of the BND and its financing of SWP. The office of the "Bundesbeauftragte:r für Digitalisierung" (Federal Government Commissioner for Digitalization, official translation) is institutionally located in the BKAmt.

The BKAmt is represented in the Cyber-SR. The BND is subordinate to the BKAmt. Institutional contributions to the SWP are paid from its budget[94].

Bundeskartellamt (Federal Cartel Office, BKartA, official translation)
The BKartA is responsible for protecting competition within the German economy. As part of its investigation of digital markets, its mandate also includes the protection of consumer rights, for example, with regard to personal data processing. In the past, the BKartA has initiated sector inquiries inter alia on messenger services and the authenticity of user ratings on the Internet.

The BKartA falls under the purview of the BMWi. BKartA and BSI cooperate in the area of digital consumer protection. It is also a member of the ACS[95].

Bundeskriminalamt (Federal Criminal Police Office, BKA, official translation)
As the central office of the German police, the BKA has expanded the national fight against crime into cyberspace. It solves crimes in cyberspace, investigates and tries them in order to prevent cybercrime. In this respect, the BKA is attributed a distinct law enforcement competence in cases of cyber crime affecting federal authorities or institutions, Germany's internal or external security, or to the detriment of critical infrastructures. To this end, it has established a new "Cybercrime" department (CC), in which competencies are concentrated to track cybercrime. For this purpose, the BKA can inter alia conduct source telecommunication surveillance as well as on-

93 Federal Commissioner for Data Protection and Freedom of Information, Aufgaben.
Federal Commissioner for Data Protection and Freedom of Information, Eurojust und Europäische Staatsanwaltschaft.
Federal Commissioner for Data Protection and Freedom of Information, Geschäftsverteilungsplan.
Federal Commissioner for Data Protection and Freedom of Information, 28. Tätigkeitsbericht zum Datenschutz 2019.
94 Federal Chancellery, Chef des Bundeskanzleramtes.
95 Federal Cartel Office, Bundeskartellamt und BSI: Partner im Dienst der Verbraucherinnen und Verbraucher.
Federal Cartel Office, Bundeskartellamt leitet Sektoruntersuchung zu Messenger-Diensten ein.
Federal Cartel Office, Gefälschte und manipulierte Nutzerbewertungen beim Online-Kauf – Bundeskartellamt zeigt Hintergründe und Lösungsansätze.

line visitations, for which it is also using surveillance software. In addition, the BKA has a 24/7 standby at its disposal in order to combat cybercrime. Annually, the BKA publishes a federal situation report on cybercrime. In addition to cybercrime, the BKA also investigates cyber espionage within its "Staatsschutz" (State Security, ST, official translation) division.

The BKA is part of the BMI. It is represented in the Cyber-AZ, as well as in G4C and the "Initiative Wirtschaftsschutz". It is on the DsiN advisory board and relies on the expertise of ZITiS. The BKA is the German point of contact for Europol and serves as a National Unit[96]*.*

Bundesministerium der Justiz und für Verbraucherschutz (Federal Ministry of Justice and Consumer Protection, BMJV, official translation)
The BMJV is first and foremost a legislative ministry which supports other federal ministries in their legislative ambitions. Within the Federal Government, it is responsible for economic consumer policy. In this respect, it deals with issues such as the protection of citizens and online merchants from cybercrime or online bullying.

The BMJV is represented in the Cyber-SR[97]*.*

Bundesministerium der Verteidigung (Federal Ministry of Defence, BMVg, official translation)
Within the Federal Government, the Federal Ministry of Defense is the department in charge of military defense and thus also for Germany's defense in cyberspace. In addition, it is responsible for ensuring cybersecurity within networks and data centers of the Bundeswehr. Within the ministry, the Chief Information Security Officer of the defense portfolio (CISO Ressort) within the "Abteilung Cyber- und Informationstechnik" (Department of Cyber and Information Technology, own translation) is responsible for matters of cyber defense.

The BMVg is represented in the Cyber-SR. The Bw is subordinate to the BMVg, while the BAKS also falls under its purview. The Cyberagentur has been set up under joint leadership of the BMVg and BMI. For its work in cyberspace, the BMVg relies on na-

96 Federal Criminal Police Office, Europol.
Federal Criminal Police Office, Straftaten im Internet.
Federal Criminal Police Office, Quellen-TKÜ und Online-Durchsuchung.
Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: Bundeskriminalamt.
Datensicherheit.de, BKA: Bundeskriminalamt baut Cybercrimebekämpfung aus.
German Bundestag (Drucksache 19/2645), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.

97 Federal Ministry of Justice and Consumer Protection, Aufgaben und Organisation.
Federal Ministry of Justice and Consumer Protection, Schutz von Bürgern und Onlinehandel vor Cyberkriminalität. (Website deleted)
Federal Ministry of Justice and Consumer Protection, Wir dürfen Cybermobbing nicht ignorieren. (Website deleted)

tional and international cooperation and partnerships, such as those with the Cyber Innovation Hub or the NATO CCDCOE[98]*.*

Bundesministerium des Innern, für Bau und Heimat (Federal Ministry of the Interior, Building and Community, BMI, official translation)
Among other duties, the BMI is responsible for civil security in cyberspace. Its "Abteilung Cyber- und Informationssicherheit" (Department for Cyber and Information Security, CI, own translation) is responsible for the cybersecurity of the federal government's ICT systems, the development of Germany's "Cybersicherheitsstrategie für Deutschland" (Cyber Security Strategy for Germany, own translation), which forms the government's interdepartmental strategic framework, as well as the preparation of further legislation. The BMI coordinates the implementation of the cybersecurity strategy through the "Bundesbeauftragter für Informationstechnik" (Federal Government Commissioner for Information Technology, BfIT, official translation), who also chairs the Cyber-SR.

The BMI is represented in the Cyber-SR. BPol, BKA, BSI, BfV, BDBOS and BBK all fall within its purview. ZITiS was founded following a BMI decree. The BMI is represented in the initiatives UP KRITIS, DsiN (Advisory Board) and the ACS. The Cyberagentur is to be established under joint leadership of BMI and the BMVg[99]*.*

Bundesministerium für Bildung und Forschung (Federal Ministry of Education and Research, BMBF, official translation)
As part of the Digital Agenda, the BMBF finances three competency centers for IT security research. With CISPA (Saarbrücken), ATHENE (Darmstadt) and KASTEL (Karlsruhe), Germany aims to bolster its research capacity in the field of cybersecurity. In addition, the BMBF has inter alia launched the research program "Selbstbestimmt und sicher in der digitalen Welt" (Self-determined and secure in the digital world, own translation) to promote multi-sectoral cybersecurity research as well as the initiative "StartUpSecure" to support company formations in the field of IT security.

The BMBF is represented in the Cyber-SR and supports the competency centers for IT Security[100]*.*

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

99 Federal Ministry of the Interior, Building and Community, Cyber-Sicherheitsstrategie für Deutschland.
Federal Ministry of the Interior, Building and Community, IT & Cybersicherheit.
Federal Ministry of the Interior, Building and Community, Unsere Abteilungen und ihre Aufgaben.
Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland Ein neuer Zusammenhalt für unser Land 2018.

100 Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: Forschungsrahmenprogramm „Selbstbestimmt und sicher in der digitalen Welt" und StartUpSecure.
Fraunhofer SIT, Institutsgeschichte.
Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.

Bundesministerium für Finanzen (Federal Ministry of Finance, BMF, official translation)
The BMF is primarily responsible for tax policy, budgetary matters and European fiscal policy. Together with national and international partners, it develops, inter alia, minimum standards for cybersecurity in the financial services industry.

The BMF is represented in the Cyber-SR. The ZKA is subordinate to it. It is also responsible for the legal and technical supervision of BaFin. The BMF and BMZ are shareholders of the GIZ[101].

Bundesministerium für Gesundheit (Federal Ministry of Health, BMG, official translation)
The BMG is responsible first and foremost for the performance of the statutory health insurance and nursing care insurance systems. The "E-Health-Gesetz" (E-Health Act, official translation) is meant to establish a digital infrastructure with the highest safety standards for the German health care system.

The BMG has commissioned gematik with the development of an electronic data transmission infrastructure, which is the prerequisite for secure interconnection of the health care system[102].

Bundesministerium für Verkehr und digitale Infrastruktur (Federal Ministry of Transport and Digital Infrastructure, BMVI, official translation)
The BMVI is responsible for transportation infrastructure, planning and security as well as digital infrastructure. Because these duties also result in it having responsibility for civil emergency preparedness and emergency response, the BMVI also develops crisis scenarios with regard to possible cyberattacks on digital infrastructure.

The BMVI is represented in the Cyber-SR[103].

Bundesministerium für Wirtschaft und Energie (Federal Ministry for Economic Affairs and Energy, BMWi, official translation)
The BMWi is dedicated to enabling secure and trustworthy IT access in order for the economy, society and the state to benefit from digitalization in the best way possible. It is particularly committed to the IT security of Industry 4.0.

The BMWi is represented in the Cyber-SR. It has launched the "Initiative IT-Sicherheit in der Wirtschaft". It is represented on the Advisory Board of DsiN, and the BNetzA

101 Federal Ministry of Finance, Grundelemente zur Cyber-Sicherheit.
Federal Ministry of Finance, Themen.
102 Federal Ministry of Health, Aufgaben und Organisation.
Federal Ministry of Health, E-Health-Gesetz.
103 Federal Ministry of Transport and Digital Infrastructure, Krisenmanagement.

also falls under its purview[104].

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (Federal Ministry for Economic Cooperation and Development, BMZ, official translation)
The BMZ is responsible for the developmental partnerships of the Federal Government. BMZ also develops secure IT solutions for partner countries and supports cyber capacity building through on-site educational programs.

BMZ is the most important client of GIZ and is one of its two shareholders, alongside the BMF[105].

Bundesnachrichtendienst (Foreign Intelligence Service of Germany, BND, official translation)
The BND is the foreign intelligence service of the Federal Republic of Germany and acts on behalf of the Federal Government. It makes a record of attacks abroad that could lead to cyber espionage or sabotage in Germany and warns any affected actors within national territory so that defense mechanisms can be triggered. This part of its work is also known under the acronym SSCD (SIGINT Support to Cyber Defence).

The BND falls under the purview of the BKAmt. Informations are exchanged and mutual obligations to provide information exist between BND, BfV and BAMAD. It is involved in "Initiative Wirtschaftsschutz" and is represented in the Cyber-AZ. Its staff is trained at the UniBw München, among others[106].

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways, BNetzA, official translation)
The BNetzA is primarily responsible for regulatory and competition issues in the electricity, gas, telecommunications, postal and railway sectors. With the importance of cybersecurity increasing in these areas, the BNetzA also deals with IT security requirements in relevant sectors.

The BNetzA falls under the purview of the BMWi. Together with the BSI it has published the "IT-Sicherheitskatalog" (Catalogue of IT Security Requirements, official

104 Federal Ministry for Economic Affairs and Energy, IT-Sicherheit.
Federal Ministry for Economic Affairs and Energy, IT-Sicherheit für die Industrie 4.0.
105 Federal Ministry for Economic Cooperation and Development and Development, Glossar – Digitalisierung und nachhaltige Entwicklung.
Federal Ministry for Economic Cooperation and Development and Development, Grundsatzfrage: Warum brauchen wir Entwicklungspolitik?.
106 Foreign Intelligence Service of Germany, Cybersicherheit.
Foreign Intelligence Service of Germany, Die Arbeit.
Heinz Fromm, Stellungnahme zur Vorbereitung der öffentlichen Anhörung am 17. Mai 2018 zum Thema „Föderale Sicherheitsarchitektur".
Kurt Graulich, Sicherheitsrecht des Bundes – Recht der Nachrichtendienste in Deutschland.

translation), the implementation of which is mandatory for all gas and electricity network providers[107].

Bundesverband der Verbraucherzentralen und Verbraucherverbände (Federation of German Consumer Organisations, vzbv, official translation)
The vzbv is the umbrella organization of Germany's 16 consumer centers and their 25 corresponding member associations. It coordinates their work and also represents consumer interests as an independent body in both politics and industry. Another task of the vzbv is to compile current market developments for consumers. The vzbv's headquarters is in Berlin, with one team based in Brussels. The vzbv's activities include digital communication and services, such as the protection of privacy in digital space, net neutrality and copyright law.

As much as 97% of the core work of the vzbv is financed by the BMJV. The vzbv and the BSI have a general agreement regarding their cooperation[108].

Bundespolizei (Federal Police, BPol, official translation)
The BPol is responsible for tasks in the field of border protection, aviation security, railway security and crime prevention. With illegal activities on the internet or aided by information technologies on the rise, BPol also increasingly combats cybercrime. It operates its own Computer Emergency Response Team (CERT BPol) to protect its facilities as well as information and communication technologies.

BPol falls under the purview of the BMI. It is represented in the Cyber-AZ and relies on the expertise of ZITiS. The ZAC is housed within federal and state governments' police forces. The CERT BPol is a guest of the CERT network[109].

Bundeswehr (German Armed Forces, Bw, official translation)
The Bw is responsible for the national defense and that of its allies, among other duties. In addition to Army, Air Force and Navy, the German Armed Forces also disposes the "Streitktäftebasis" (Joint Support Service, SKB, official translation), the "Zentraler Sanitätsdienst" (Joint Medical Service, ZSan), as well as the "Cyber- und Informationsraum" (Cyber and Information Domain Service, CIR, official translation) as military organizational units (MilOrgBer). The latter is responsible for the holistic defense of the cyber and information domain. It is led by KdoCIR, which inter alia includes KdoITBw and KdoStratAufkl.

107 Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways, Aufgaben und Struktur.
Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways, IT-Sicherheit im Energiesektor.
108 Federal Ministry of Justice and Consumer Protection, Verbraucherzentralen.
Federal Office for Information Security, BSI und Verbraucherzentrale stärken digitalen Verbraucherschutz.
Federation of German Consumer Organisations, Häufige Fragen (FAQ).
Federation of German Consumer Organisations, Über Uns.
109 Federal Police, Startseite.
Federal Police kompakt, 04/2015.
German Bundestag (Drucksache18/13555), Antwort der Bundesregierung auf die Kleine Anfrage: Aktuelle Situation und Ausrichtung der Bundespolizei.
Background Conversations, 2019.

The Bw falls under the purview of the BMVg. It trains part of its staff at the UniBw and is represented in the Cyber-AZ and various national and international CERT networks[110].

Bundesweite IT-Systemhaus GmbH (National IT Systems House GmbH, BWI, own translation)
The BWI is a firm of the Federal Government, an IT service provider of the Bw and a government IT service center. The main focus of its work constitutes the operation and modernization of the Bw's information and communication technologies as well as support in the areas of logistics and administration. The BWI is also responsible for the software management and IT security of any IT infrastructures it operates. The security specifications of the Bundeswehr apply to the networks and systems operated by BWI for the Bw, and the Bundeswehr Cyber Security Operations Center (CSOCBw) monitors these together with the CERT of the BWI. The BWI and the Bw have signed an agreement with the objective of closer cooperation, which should enable former soldiers to be integrated into and to work for BWI.

BWI GmbH is a state-owned company and IT system house for Bw and the Federal Government[111].

Bündnis für Cybersicherheit (Coalition for Cyber Security, own translation)
Together with associations, companies and federal authorities, the "Bündnis für Cybersicherheit" aims to enhance cooperation between the state and industry. The objective is to establish better networks in both sectors to ensure more effective cybersecurity, especially in an international context. As a forum between federal authorities and business representatives, the "Bündnis für Cybersicherheit" shall foster the exchange of information on international cybersecurity issues. The alliance also aims to strengthen Germany's digital sovereignty as a business location; joint projects, for example, aim to decrease high dependencies on foreign technologies.

The "Bündnis für Cybersicherheit"is based on an agreement between the BMI and the "Bundesverband der deutschen Industrie" (Federation of German Industries, BDI, official translation)[112].

Computer Emergency Response Team der Bundesverwaltung (Computer Emergency Response Team for federal agencies, CERT-Bund, official translation)
CERT-Bund is an emergency team and contact point for all federal authorities in the event of a security-relevant IT incident. It also makes preventive and, if necessary,

110 German Armed Forces, Auftrag und Aufgaben der Bundeswehr.
German Armed Forces, Das Kommando Cyber- und Informationsraum.
111 Federal Ministry of Defence, Auf engere Kooperation geeinigt: Bundeswehr und BWI GmbH.
Bundesweite IT-Systemhaus GmbH, Unternehmensbroschüre.
112 Federal Ministry of the Interior, Building and Community, Industrie und BMI etablieren Bündnis für Cybersicherheit.

reactive recommendations for action. Furthermore, it points out vulnerabilities, proposes measures for their adjustment and is available 24 hours a day.

In addition to the CERT-Bund, the BSI also maintains a "Bürger-CERT" (Citizen-CERT, own translation) which is essentially a warning and information service for private individuals allowing them to access information about current security gaps free of charge and in an objective manner.

The CERT-Bund is part of the BSI and cooperates with federal state-level CERTs within the framework of the VCV and CERT network. At the European level, CERT-Bund cooperates with the EGC Group as well as ENISA[113].

Cyber Innovation Hub (CIHBw)
The CIHBw of the Bw offers its employees, in cooperation with startups, a platform to research and further develop innovative technologies, the goal being to guarantee the competitiveness of the Bw in the fields of cyber and IT. This connection between the Bw and startups is meant to realize ideas more rapidly and to ensure better implementation of modern technologies. Within the CIHBw, soldiers work together with civilians, especially on the development of disruptive technologies for the Bw.

The CIHBw has its own department within the BWI and therefore exists within an administration with a clear line of command. In order to avoid redundancies, CIHBw exchanges information with the Cyberagentur[114].

Cyber-Reserve (Military Cyber Reserve, own translation)
At the same time when the CIR Domain was established as an organizational unit within the Bundeswehr, it was also decided to set-up a military 'Cyber-Reserve'. Its development is supported by a "Reservistenarbeitsgemeinschaft" (reservist working group, RAG, own translation) within the "Verband der Reservisten der Deutschen Bundeswehr" (Reservist Association of Deutsche Bundeswehr, VdRBw, official translation). Different to other reserve units, the cyber reserve is meant to explicitly recruit civilian personnel and executives with IT expertise in addition to former Bundeswehr soldiers. Pooling these diverse backgrounds shall enable joint exercises between cyber specialists from authorities, society and economy for the purpose of cyber defense, promoting a transfer of knowledge and educating cyber experts.

113 Federal Office for Information Security, CERT-Bund.
Federal Office for Information Security, Nationale und internationale Zusammenarbeit.
CERT-Bund, Über CERT-Bund.
114 Federal Ministry of Defence, Cyber Innovation Hub.
Federal Government, Regierungspressekonferenz vom 2. Dezember 2019.
MDR Sachsen-Anhalt, Der Chef der Cyberagentur in Halle.
Matthias Punz, BMVg: Führung springt beim Cyber Innovation Hub ab.
Sebastian Christ, Wehrbeauftragter kritisiert Umwandlung des Cyber Innovation Hub.

The 'Cyber-Reserve' supports the Bundeswehr in the performance of its tasks, in particular KdoCIR[115].

Cyber Security Cluster Bonn e. V.

The Cyber Security Cluster Bonn e. V. is an association of different institutions active within the context of cybersecurity. The cluster's geographical focus is the Bonn region, due in part to the resident BSI and KdoCIR. The aim is to harness their thematic and geographical proximity to one another in order to intensify cooperation, attract skilled workers and work together on concrete projects within the field of cybersecurity. In addition to government agencies, stakeholders from the private sector and academia are also members of the cluster. Moreover, the cluster has appointed a "Weisenrat" (Expert Council, own translation) – made up of representatives from scientific institutions – which is intended to make a further contribution to immunizing society against cyber attacks.

The BSI, KdoCIR of the Bw and the BfDI are members of the Advisory Board of the Cyber Security Clusters Bonn e. V.[116].

Deutsche Akkreditierungsstelle (German National Accreditation Body, DAkkS, own translation)

The DAkkS is Germany's national accreditation body. It is tasked with the accreditation of conformity assessment bodies, such as laboratories, inspection and certification agencies. In particular within its "Sektorkomitee Informationstechnik/Informationssicherheit" (sector committee information technology/information security, SK IT-IS, own translation) and its subcommittees, the DAkkS also carries out accreditation procedures within the realms of cybersecurity and IT security.

The Federal Republic of Germany (represented by the BMWi), the federal states of Bavaria, Hamburg and North Rhine-Westphalia are shareholders of the DAkkS. In addition to members from industry and representatives of the federal states, the DAkkS Supervisory Board also includes representatives of the BMWi and BSI. The DAkkS is a member of the EA[117].

115 Federal Ministry of Defence, Cyber-Reserve: Bundeswehr öffnet sich für IT-Community.
Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: RAG Cyber des VdRBw.
German Armed Forces, Reservist im Cyber- und Informationsraum.
Reservistenverband, Die Cyber-Reserve geht neue Wege.

116 Cyber Security Cluster Bonn, Über uns.
Cyber Security Cluster Bonn, Weisenrat für Cyber-Sicherheit.
Email exchange with representatives of the Cyber Security Cluster Bonn e. V. in November 2019.

117 Deutsche Akkreditierungsstelle, Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443.
Deutsche Akkreditierungsstelle, Aufsichtsrat.
Deutsche Akkreditierungsstelle, Profil.
Deutsche Akkreditierungsstelle, Sektorkomitee Informationstechnik / Informationssicherheit (SK IT-IS).
Deutsche Akkreditierungsstelle, Welche Aufgabe hat die DAkkS?.

Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH, GIZ, official translation)
The GIZ aids the Federal Government in realizing its goals for cooperation in international development. It supports the advancement of information and communication technologies and is planning to include cybersecurity as an element of traditional development cooperation in the future.

The BMZ and BMF are shareholders of GIZ[118].

Deutschland sicher im Netz e. V. (Germany Secure on the Internet e. V., DsiN, own translation)
DsiN was founded to provide comprehensive information on IT security to both the greater population and small and medium-sized businesses. In cooperation with its members and partners, DsiN runs various initiatives and projects to provide concrete assistance for IT security.

The BMI, BMWi, BSI, BKA and BfDI are represented on the DsiN advisory board. The Federal Minister of the Interior assumes patronage over the DsiN. DsiN cooperates with "Initiative IT-Sicherheit in der Wirtschaft"[119].

Forschungsinstitut Cyber Defence (Cyber Defence Research Institute, CODE, own translation)
CODE at the UniBw München was founded by the BMVg with the goal of developing technical innovations for the Bw and the Federal Government to protect data, software and systems. For this purpose, CODE has established three research clusters, that are dealing with cyber defense; smart data, AI and machine learning as well as quantum technology. Furthermore, this interdisciplinary, independent research institute is linked to the scientific training and education at the UniBwM.

As part of the UniBw, Bw personnel are also becoming scientifically trained at CODE[120].

Föderale IT-Kooperation (Federal IT Cooperation, FITKO, own translation)
FITKO coordinates various levels of the digital transformation within the administration of the "IT-Planungsrat" (IT Planning Council, IT-PLR, official translation) and improves its legal and political-strategic controllability. The agency was formally founded in January 2020 and is based in Frankfurt am Main. With regard to its digitalization projects, FITKO operates with a budget of up to 180 million euros within the framework of the "Onlinezugangsgesetz" (Online Access Act, OZG, own translation).

118 German Agency for International Cooperation, Bundesregierung.
German Agency for International Cooperation, Startseite.
Background Conversations, 2018.
119 Deutschland sicher im Netz, Presse.
120 Universität der Bundeswehr München, Forschungsinstitut CODE.
Universität der Bundeswehr München, Forschungsinstitut CODE. Unsere Mission.
Universität der Bundeswehr München, Beirat des Forschungsinstituts CODE.

FITKO is an operational substructure of the "IT-Planungsrat". A municipal committee of the IT Planning Council was established in 2020 under the chairmanship of FITKO[121].

gematik
gematik GmbH is a competence center and service company for the German health care system. For its secure networking and digitalization, gematik provides the telematic infrastructure guaranteeing the exchange of data between actors and institutions of the health care system. In this regard, gematik is particularly responsible for specifying and authorizing the services and components of both telematic infrastructure and its operational coordination. Besides telematic infrastructure, gematik is also responsible for the electronic health card, which serves as the exclusive proof of health insurance in Germany.

gematik is supported by various shareholders. The BMG, for example, holds 51% of shares. Its Advisory Board includes, among others, a representative of the BfDI, as well as the BSI and the BMWi[122].

Gemeinsames Lagezentrum Cyber- und Informationsraum (Situation Center Cyber and Information Domain Service, GLZ CIR, own translation)
GLZ CIR is part of the KdoCIR and serves as the analysis center of situational overviews for the CIR. It is tasked with bundling information and situational overviews from varying sources about those aspects of cyberspace relevant to the military, and then summarizing and working through courses of action. To this effect, it uses its own IT system, which employs an array of processes, such as artificial intelligence.

The GLZ CIR was established at the time the KdoCIR was set up; the BWI supported the Bw in the establishment of the IT system of the GLZ CIR. Situational analyses within the CIR are provided to the BMVg and the Cyber-AZ, among others[123].

Gemeinsames Melde- und Lagezentrum (Joint Information and Situation Centre of the Federal Government and the Federal States, GMLZ, official translation)
GMLZ is responsible for providing a consistent situational overview of civil protections to the Federal Government, the federal states and their competent authorities.

121 Lina Rusch, Digitaler Staat: Agenturen in den Startlöchern.
IT-Planungsrat, FITKO. (Website deleted)
Matthias Punz, Rechtlicher Rahmen für FITKO-Start steht.
122 Federal Ministry of Health, E-Health-Gesetz.
Gematik, Die elektronische Gesundheitskarte.
Gematik, Telematikinfrastruktur.
Gematik, Themen.
Gematik, Über uns.
123 Federal Ministry of Defence, Lagezentrum Cyber- und Informationsraum im Pilotbetrieb.
BWI, Von Big Data bis KI – Bundeswehr und BWI starten zweite Ausbaustufe des Gemeinsamen Lagezentrums CIR.
German Bundestag (Drucksache 19/2645), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.

To do so, it constantly tracks and evaluates relevant events at home and abroad and reports them in daily reports or precise status reports.

The BBK is represented in the GMLZ. Partners of the GMLZ include BPol, BKA and the EK. If necessary, the GMLZ forwards activation requests for EU disaster and crisis management to the ERCC[124].

G4C German Competence Centre against Cyber Crime e. V. (G4C German Competence Centre against Cyber Crime e. V., G4C, official translation)
G4C is an association that brings together different actors in a strategic alliance to combat cybercrime. They develop appropriate protective measures by way of a daily exchange of information between official cooperation partners and members.

The G4C cooperates with the BKA and the BSI[125].

Informationstechnikzentrum Bund (Federal Information Technology Centre, ITZBund, own translation)
ITZBund is the official IT service provider of the Federal Government's administration. It was founded from three predecessor authorities as part of an overall strategy to consolidate and bundle the Federal Government's IT capacities.

The ITZBund falls under the purview of the BMF. In August 2020, the ITZBund established together with the BSI a "Lenkungskreis Informationssicherheit" (Steering Committee for Information Security, own translation) to create closer cooperation between both institutions. The BfDI regularly reviews the data and information processing of the ITZBund[126].

Initiative IT-Sicherheit in der Wirtschaft (Initiative IT Security in the Economy, own translation)
The "Initiative IT-Sicherheit in der Wirtschaft" is an initiative of the BMWi for small and medium-sized businesses. It bundles together a large number of activities to increase their level of IT security. The initiative is advised by a steering committee on the implementation of its projects.

Members of the steering committee include representatives of the BMWi, the BSI and the DsiN. The latter was established as part of the initiative[127].

124 Federal Ministry of the Interior, Building and Community, Das Gemeinsame Melde- und Lagezentrum von Bund und Ländern.
Deutsches Zentrum für Luft- und Raumfahrt, Katastrophen- und Krisenmanagement.
125 German Competence Centre against Cyber Crime e. V. (G4C), Über uns.
126 Informationstechnikzentrum Bund, ITZBund und BSI intensivieren Zusammenarbeit für mehr IT-Sicherheit.
Informationstechnikzentrum Bund, IT-Sicherheit.
Informationstechnikzentrum Bund, Über uns.
127 Federal Ministry for Economic Affairs and Energy, Erste Berufsschulen in Niedersachsen setzen auf Bottom-Up für mehr IT-Sicherheit im Mittelstand.
Federal Ministry for Economic Affairs and Energy, Steuerkreis.

Initiative Wirtschaftsschutz (Initiative for Economic Protection, own translation)
The "Initiative Wirtschaftsschutz" aims to protect the German economy from threats emanating from cyberspace. The initiative offers a comprehensive protection concept consisting of measures, recommendations for action and seminars as well as an information portal. The latter also provides information on cyber defense and cyber crime. Within the portal's user area, companies can access official security recommendations and contact them directly, if necessary.

On governmental level, the "Initiative Wirtschaftsschutz" works with the BND, BfV, BKA and the BSI. The BMI coordinates the cooperation of government agencies and trade associations[128].

Innenministerkonferenz (Conference of Interior Ministers, IMK, official translation)
The IMK enables regular transregional cooperation between the interior ministers and interior senators of Germany's federal states. The IMK established two bodies: a "Länderoffene Arbeitsgruppe Cybersicherheit" (Cybersecurity working group open to all federal states, LOAG/LAG Cybersecurity, own translation) and the "Arbeitsgruppe Kommunikationssicherheit" (Communication Security Working Group, KomSi, own translation), the latter of which was established for the police. These working parties are responsible, for example, for administrative duties in the areas of catastrophe prevention or cybercrime.

Through the participation of the Federal Minister of the Interior, the Conference of Ministers of the Interior is linked to the BMI. On a regular basis, the IMK receives reports from the Cyber-SR[129].

IT-Planungsrat (IT Planning Council, IT-PLR, official translation)
The "IT-Planungsrat" is the central body for federal and state coordination of IT. It coordinates cooperation between the Federal Government and the federal states on IT issues, makes decisions on non-subject specific and interdisciplinary IT interoperability and IT security standards, operates e-government projects, and plans and develops the grid in line with the "Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder" (Act on the Interconnection of the Federal and State Information Technology Networks, IT-NetzG, own translation). It is comprised of the "Bundesbeauftragter für Informationstechnik" (Federal Govern-

128 Domestic Intelligence Service of the Federal Republic of Germany, Initiative Wirtschaftsschutz.
Domestic Intelligence Service of the Federal Republic of Germany, Initiative Wirtschaftsschutz. Das Informationsportal.
129 Bundesrat, Innenministerkonferenz.
CISO der niedersächsischen Landesverwaltung, Cybersicherheit in der Landesverwaltung.
Secupedia, Nationales Cyber-Abwehrzentrum.
Email exchange with representatives of the BSI in February 2020.
Innenministerkonferenz, 213. Sitzung der Innenministerkonferenz.

ment Commissioner for Information Technology, official translation) and of representatives of each federal state responsible for information technology. Three representatives of municipalities and municipal associations, appointed by municipal umbrella organizations and the BfDI, can attend the meetings in an advisory capacity. Other persons, including the respective contact persons of specialized ministerial conferences, may also be called upon if the decisions of the "IT-Planungsrat" impact their fields of expertise. Federal and state governments (in alphabetical order) take annual turns as chair of the "IT-Planungsrat". A further part of the "IT-Planungsrat" is the "Arbeitsgruppe Informationssicherheit" (Working Party on Information Security, AG InfoSic, own translation), which is responsible for developing IT objectives for public administration as well as strategies for their implementation that adhere to established guidelines.

The BfDI as well as representatives of the Central Municipal Associations are advisory members. FITKO and a municipal committee are subordinate to the IT-PLR. The head of the BKAmt and its respective federal state counterparts take note of the activity report of the "IT-Planungsrat" each year and inform themselves about further developments in the National E-Government Strategy[130].

IT-Rat (IT Council, own translation)
The "IT-Rat" is a political-strategic body for general issues responsible for the digitization and IT management of the federal administration.

The "IT-Rat'' is chaired by the head of the BKAmt. Deputy chairpersons are the "Bundesbeauftragte:r für Digitalisierung" (Federal Government Commissioner for Digitalisation, official translation) and the BfIT[131].

IT Security made in Germany (ITSMIG)
The trust mark ITSMIG was jointly launched by the BMI, the BMWi and representatives of the German IT security industry and is being continued as the TeleTrusT working group ITSMIG. It aims to coordinate the collective public image of organized German IT security industry members and to improve their cooperation.

The BMI and the BMWi provided support in establishing ITSMIG. Both ministries are represented in the advisory board of the working group[132].

130 IT Planning Council, Aufgaben des IT-Planungsrats.
IT Planning Council, Besprechung des Chefs des Bundeskanzleramtes mit den Chefinnen und Chefs der Staats- und Senatskanzleien der Länder.
IT Planning Council, IT-Planungsrat.
IT Planning Council, Umsetzung Leitlinie InfoSic. (Website deleted)
IT Planning Council, Zusammensetzung des IT-Planungsrates.
131 Federal Government Commissioner for Information Technology, IT-Rat.
132 TeleTrust, IT Security made in Germany.

Kommando Cyber- und Informationsraum (Cyber- and Information Domain Commando, KdoCIR, own translation)
The KdoCIR leads the CIR. As commando of the CIR, KdoCIR manages the areas of cyber, IT, strategic reconnaissance, geographic information systems of the Bw and its operative communications. First and foremost, the commando is intended to structure the CIR and manage human resources. It is furthermore the official residence of the CIR inspector and its representative, who has overall responsibility for the information security of the Bw as Chief Information Security Officer (CISOBw). The "Zentrum für Cyber-Sicherheit der Bundeswehr" (Center for Cyber Security of the Bundeswehr, ZCSBw, own translation) with the Bundeswehr's Cyber Security Operations Center (CSOCBw) are subordinate to the CISOBw. The latter is home to the CERTBw and provides incident response teams in the event of an attack on the IT systems of the Bundeswehr. KdoCIR employs a total of about 13,500 soldiers and civilian employees. The KdoCIR is located in Bonn.

Among other organizations, the KdoStratAufkl and the KdoITBw fall within its purview. It is also home to the Bw's GLZ CIR. The CISOBw is located in the KdoCIR. It is represented in the Cyber-AZ as a permanent member and provides one of the deputy coordinators. The establishment of the CIDCC as a PESCO project was initiated by KdoCIR. KdoCIR is represented as an advisory board member in the Cyber Security Cluster Bonn. Activities of the Bundeswehr relating its Cyber-Reserve are managed by KdoCIR[133].

Kommando Informationstechnik (Information Technology Command, KdoITBw, own translation)
The KdoITBw is a specialized commando within the organizational area of the Joint Support Service (SKB) of the Bw that deals with the deployment of the Bw's IT services. The headquarters of the KdoITBw has been in Bonn since its founding. KdoITBw ensures the installation, operation and protection of central IT and communications elements during missions. The commando has six subordinate "Informationstechnik-Battalione" (Information Technology Battalions, own translation) and various departments, such as the "Betriebszentrum IT-System der Bundeswehr" (Bundeswehr IT System Operations Center, own translation).

KdoITBw is subordinate to the KdoCIR and falls under the purview of the Bw's CIR[134].

133 Federal Office for Information Security, BSI Magazin 2020/01: Mit Sicherheit.
Federal Ministry of Defence, FAQ: Cyber-Abwehr.
German Armed Forces, Auftrag des Organisationsbereichs CIR.
German Armed Forces, Kommando Cyber- und Informationsraum.
134 Bund, Kommando Informationstechnik der Bundeswehr (KdoITBw).
German Armed Forces, Kommando Informationstechnik der Bundeswehr.
German Armed Forces, Zentrum für Cyber-Sicherheit der Bundeswehr.
Bernd Kammermeier, Zentrum für Cyber-Sicherheit der Bundeswehr –Moderner Dienstleister für IT-Sicherheit.

Kommando Strategische Aufklärung (Strategic Reconnaissance Command, KdoStratAufkl, own translation)
The KdoStratAufkl serves the information needs of the Bw in the protection of its personnel in operational areas and for early crisis detection. For this purpose, the KdoStratAufkl conducts reconnaissance in defined areas. The mission areas of the command are divided into the following areas: "Satellitengestützte Abbildende Aufklärung" (Satellite-based Imaging Reconnaissance, own translation), "Fernmelde- und Elektronische Aufklärung" (Telecommunications and Electronic Reconnaissance, own translation), "Elektronischen Kampf" (Electronic Fight, own translation), and "Objektanalyse" (Object Analysis, own translation). Further, the command is working on developing capacities in the field of computer network operations. It leads various CIR departments, such as the "Zentrum Cyber-Operationen" (Center for Cyber Operations, ZCO, own translation) which bundles the planning, preparation, management, and implementation capabilities for military reconnaissance and cyberoperations. The command operates out of Gelsdorf (Grafschaft) in the federal state of Rhineland-Palatinate

KdoStratAufkl is subordinate to the KdoCIR of the Bw's CIR[135].

Nationaler CERT-Verbund (National CERT Network, own translation)
The CERT-Verbund is an amalgamation of German Security- and Computer Emergency Response Teams (CERTS) from corporations, academia and administrations which have organized themselves at both the federal and the federal state levels. Mutual information sharing and cooperation should contribute to a rapid joint response to cyberattacks.

Among others, the CERTBw, the BSI (with the CERT-Bund) as well as the CERT of the BWI are represented within the CERT-Verbund. Bayern-CERT, CERT Baden-Wuerttemberg, CERT-NRW and CERT-rlp are involved from the part of federal states[136].

Nationaler Cyber-Sicherheitsrat (National Cyber Security Council, Cyber-SR, official translation)
As a strategic advisor to the Federal Government, the Cyber-SR aims to identify requirements for long-term action as well as trends in cybersecurity to stimulate appropriate impulses. In accordance, the Cyber-SR, which meets three times a year, shall make proposals for the further development of national regulations for more cyber security and identify areas for public-private cooperation. The Cyber-SR is

135 Bund, Kommando Strategische Aufklärung (KdoStratAufkl).
Bund, Zentrum Cyberoperationen (ZCO).
German Armed Forces, Das Zentrum Cyber-Operationen.
German Armed Forces, Kommando Strategische Aufklärung.
136 Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: CERT-Verbund.
Deutscher CERT-Verbund, Überblick.

supported by a permanent scientific working group, which is advising the Council on strategic issues and developing recommendations for action. The scientific working group also regularly publishes impulse papers.

The BMI, BKAmt, AA, BMVg, BMWi, BMJV, BMF and BMBF, as well as representatives of the federal states of Lower-Saxony and Hesse, are represented in the Cyber-SR. It is chaired by the BfIT. In the past, representatives of ENISA, the BfV and the SWP have also been invited to special meetings of the Cyber-SR. In addition to scientific representatives, the scientific working group also includes a representative of the BSI. Besides the federal government, the Cyber-SR is also to provide impetus for the IMK[137].

Nationaler Pakt Cybersicherheit (National Cybersecurity Pact, own translation)
The "Nationaler Pakt Cybersicherheit" is an initiative of the BMI, which is intended to support the Paris Call for Trust and Security in Cyberspace as a German contribution. Its aim is to involve all groups relevant to society, manufacturers, suppliers and users, as well as public administration, in a national pact establishing joint responsibility for digital security. As part of the pact, key players in German cybersecurity were collected in an online compendium last year. In addition, the pact is meant to evaluate the approach with recommendations for action for the next legislative period. In public, the pact is represented by a "quadriga".

Those taking part in the pact are, among others the "Bündnis für Cybersicherheit" and the Cyberagentur. The "Quadriga" of the "Nationaler Pakt Cybersicherheit" further includes representatives of the BMI, the executive board of the vzbv as well as civil society[138].

Nationales Cyber-Abwehrzentrum (National Cyber Defence Centre, Cyber-AZ, official translation)
The Cyber-AZ is tasked with optimizing operational cooperation between government agencies with regard to various hazards in cyberspace and for coordinating the appropriate protective and defensive measures. For this purpose, all information about cyberattacks on IT infrastructure are collected in the Cyber-AZ, located within the BSI. Daily situation briefings as well as a weekly meeting dealing with "Koordi-

137 Federal Ministry of the Interior, Cyber-Sicherheitsstrategie für Deutschland 2016.
Federal Ministry of the Interior, Building and Community, Sondersitzung des Nationalen Cyber-Sicherheitsrates.
Federal Ministry of Defence, Cyber-Sicherheitsrat.
Der Beauftrage der Bundesregierung für Informationstechnik, Cyber-Sicherheitsrat.
Fraunhofer-Institut für Sichere Informationstechnologie, Beratung aus der Forschung. Wissenschaftliche Arbeitsgemeinschaft Nationale Cyber-Sicherheit.
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE, Impulspapiere der Wissenschaftlichen AG Nationale Cyber-Sicherheit.

138 Federal Ministry of the Interior, Building and Community, Nationaler Pakt Cybersicherheit.
Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: Nationaler Pakt Cybersicherheit.

nierte Fallbearbeitung" (coordinated case processing, own translation) take place. Its working groups "Operativer Informationsaustausch" (Operational Information Exchange, own translation) and "Nachrichtendienstliche Belange" (Nachrichtendienstliche Belange, own translation) meet monthly, while a working group dealing with Critical Infrastructures comes together every three months. The Cyber-AZ prepares a "Cyber-Lage" (cyber situation report, own translation) as required.

The Cyber-AZ is a cooperation platform between the BSI, BPol, BKA, BfV, BBK, BND, KdoCIR, BaFin and BAMAD. The ZKA is involved on an associated basis. It sends its annual report to the Cyber-SR. In addition to above-mentioned authorities, the ‚Cyber-Lage' is sent to the 16 LfVs as well as members of the VCV. The BKA provides the coordinator of the Cyber-AZ; the BfV and the KdoCIR of the Bw take over this duty in its stead. All participating public authorities are required to dispatch their own liaisons to the Cyber-AZ[139].

Nationales IT-Lagezentrum (National IT Situation Centre, LZ, own translation)
The LZ at the BSI is tasked with creating a 24-hour IT situational overview meant to quickly assess occurring IT security incidents for governmental agencies and commercial enterprises and, if necessary, to react. This is achieved through constant monitoring and evaluation of an array of sources that provide the most comprehensive overview possible of the IT security situation of the Federal Republic of Germany. The capacities and structures of the LZ also allow for its development into an IT crisis response center whenever necessary.

The LZ works closely with the GMLZ, CERT-Bund and Cyber-AZ. Its daily "Lagebericht IT-Sicherheit" (IT security status report, own translation) is inter alia being sent to UP KRITIS, the VCV as well as the ACS[140].

Organisationsbereich Cyber- und Informationsraum (Cyber and Information Domain Service, CIR, official translation)
The Bw's CIR is responsible for the military's cyber and information domains. It comprises the sixth military organizational area of the Bw and should be fully staffed by 2021, with 13,500 employees.

139 Background Conversations, 2019.
Federal Office for Information Security, Cyber-Abwehrzentrum.
Federal Office for Information Security, BSI Magazin 2020/01: Mit Sicherheit.
Federal Criminal Police Office, Cyber-Abwehrzentrum.
German Bundestag (Drucksache 19/3356), Antwort der Bundesregierung auf die Kleine Anfrage: Aufgaben und Ausstattung des Nationalen Cyber-Abwehrzentrums.
German Bundestag (Drucksache 19/2645), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.

140 Federal Office for Information Security, Immer im Einsatz: Ein Tag im nationalen IT-Lage- und Analysezentrum.
Federal Office for Information Security, Nationales IT-Lagezentrum.
German Bundestag (Drucksache 19/2645), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.

CIR is a part of the Bw and is led by the KdoCIR, to which the KdoITBw and the KdoStratAufkl are subordinate[141].

Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen (Public-Private Partnership for Critical Infrastructure Protection, UP KRITIS, own translation)
UP KRITIS is tasked with ensuring the supply of critical infrastructure. For this purpose, UP KRITIS serves as a public-private cooperation between public authorities, operators of critical infrastructures and their associations. Established working groups (along branches and thematic issues) are discussing topics related to IT and cybersecurity, develop common positions and offer network opportunities which all contribute to mutual exchange of information.

The BMI, BSI and BBK cooperate within the framework of UP KRITIS, which are also represented in the UP KRITIS Council[142].

Stiftung Wissenschaft und Politik (German Institute for International and Security Affairs, SWP, official translation)
The SWP is a politically independent organization that advises the German Bundestag, the Federal Government and international organizations on questions of foreign and security policy. Its research includes digitalization and cybersecurity issues.

The SWP receives its institutional funding from the BKAmt. The AA, BMBF, BMZ and EK are among the SWP's third-party donors. Its Foundation Board is composed by representatives from BKAmt, BMBF, BMZ, BMI, AA, BMF, BMWi and BMVg, for example[143].

Transferstelle IT-Sicherheit im Mittelstand (Transfer Office "IT Security for Small and Medium-sized Enterprises", TISiM, own translation)
The "Transferstelle IT-Sicherheit im Mittelstand" was established by the BMWi. It is meant to function as a point of contact for small and medium-sized businesses and vocational professions in matters of IT security. It answers questions about IT se-

141 German Armed Forces, Auftrag des Organisationsbereichs CIR.
142 Federal Office for Information Security, Geschäftsstelle UP KRITIS, UP KRITIS. Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland.
Federal Office for Information Security und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, UP KRITIS. Organisation.
Internetplattform zum Schutz Kritischer Infrastrukturen, UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen.
Internetplattform zum Schutz Kritischer Infrastrukturen, Zusammenarbeit im Rahmen des UP KRITIS.
143 German Institute for International and Security Affairs, Cyber-Sicherheit.
German Institute for International and Security Affairs, Cluster »Digitalisierung – Cyber – Internet«.
German Institute for International and Security Affairs, Organe der Stiftung.
German Institute for International and Security Affairs, Unterstützerinnen und Unterstützer.
German Institute for International and Security Affairs, Über uns.

curity with information, instruction manuals, concrete measures, action plans and best practices. Industry, academic and administrative experts stand at the ready for exactly this purpose. Thereby, it aims to increase the readiness to implement IT security measures. It is subsidized with around five million euros per year.

The TISiM is housed in the DsiN-Forum in Berlin. It operates through a consortium which is led by DsiN. It also exchanges information with sponsors within the framework of the ACS[144].

Universität der Bundeswehr (University of the German Federal Armed Forces, UniBw, official translation)
UniBw scientifically trains officers and officer cadets at its locations in Munich (UniBwM) and Hamburg (HSU/UniBw Hamburg). Among other courses, degree programs currently include computer science, cybersecurity, information technology, mathematical engineering and business informatics.

UniBw provides scientific training for Bw personnel and is home to CODE, an inter-faculty research center in Munich[145].

Verwaltungs-CERT-Verbund (Administrative CERT-Group, VCV, own translation)
The VCV is a platform for the mutual exchange of information between CERT-Bund on the federal level and the CERTs of the federal states. It aims to strengthen IT crisis prevention and response as well as to improve the IT security of public administration. To this end, all participating CERTs have committed themselves to a binding reporting procedure that provides for an immediate reporting channel in the event of IT security incidents.

The BSI, CERT-Bund, CERTs on federal state level, and LSI are involved in the VCV[146].

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Central Office for Information Technology in the Security Sector, ZITiS, official translation)
ZITiS develops, researches, supports and advises German security authorities in the following areas: digital forensics, telecommunications surveillance, crypto and big-data analysis. ZITiS also works on technical questions related to the fight against

144 Federal Ministry for Economic Affairs and Energy, Altmaier: „Wir stärken die Kompetenzen des Mittelstands im Bereich IT-Sicherheit".
Federal Ministry for Economic Affairs and Energy, Neue Transferstelle IT-Sicherheit bündelt Hilfestellungen bundesweit.
Deutschland sicher im Netz, Transferstelle.

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

146 Federal Office for Information Security, Cyber-Sicherheit und IT-Krisenmanagement – Angriffe auf Kritische Infrastrukturen. (Website deleted)
Niedersächsisches Computer Emergency Response Team N-CERT, 2016, Kooperation der CERTS im Verwaltungs-CERT-Verbund (VCV).

crime, as well as in emergency response and counterintelligence. For this purpose, it develops and tests technical tools and methods in the cyber domain but has no authority to intervene of its own. National and international projects with ZITiS involvement that are known to the public investigate the use of artificial intelligence for the early detection of crimes (KISTRA), examine digital forensics in the field of evidence analysis (DIGFORASP) or aim to develop a Europe-wide standard for the forensic examination of cell phones (FORMOBILE). In addition, ZITiS is participating in a project at the EU level to establish a network to combat hybrid threats more effectively (EU-HYBNET).

ZITiS was founded by the BMI, which is also responsible for its supervision. It provides its expertise to federal authorities with security tasks, including inter alia the BKA, BfV, BPol, BND, ZKA, and BAMAD. Its annual program is prepared jointly with the BKA, BfV and BPol and approved by the BMI. The BfDI has the right to inspect files to monitor compliance with data protection regulations. The BKA is involved in the research consortium of the KISTRA project. KISTRA is funded by the BMBF. Both EU-HYBNET and FORMOBILE are part of Horizon 2020. The Hybrid CoE oversees the coordination of the EU-HYBNET project and other project partners include GD JRC and UniBwM. It is located on the campus of the UniBw and is thus also in geographical proximity to CODE. Together with CODE, it also trains its own personnel in the field of "Cyber Network Capabilities". In 2021, one focus of ZITiS' work consists the establishment of a joint development center for the purpose of IT surveillance together with the BKA[147].

Zollkriminalamt (Customs Investigation Bureau, ZKA, official translation)
The ZKA is responsible for preventing and solving moderate as well as serious and organized customs-related crime. To this effect, ZKA coordinates investigations of the different "Zollfahndungsämter" (Customs Investigation Offices, own translation) and can also initiate its own investigations in special cases. This also extends to activities in cyberspace.

The ZKA is subordinate to the BMF, is represented in the Cyber-AZ and can – as a federal security authority – draw on services provided by ZITiS[148].

147 Andre Meister, Hacker-Behörde bekommt 66 Millionen Euro.
Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: Zentrale Stelle für Informationstechnik im Sicherheitsbereich.
EU-HYBNET, Project Partners.
Florian Flade, Mysterium ZITiS. Was macht eigentlich die „Hackerbehörde"?.
Central Office for Information Technology in the Security Sector, Aufgaben & Ziele.
Central Office for Information Technology in the Security Sector, Gesetzliche Grundlage, Aufsicht und Kontrolle.
Central Office for Information Technology in the Security Sector, Forschungsprojekte.

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

7. Explanation: Actors at Federal State Level

Computer Emergency Response Teams der Bundesländer (Computer Emergency Response Teams of the Federal States, Länder-CERTs, own translation)
The Länder-CERTs are the Computer Emergency Response Teams of the individual federal states, that are affiliated with different departments:

- The CERT BWL of Baden-Wuerttemberg is affiliated with the "IT-Baden-Württemberg" (IT-Baden-Wuerttemberg, BITBW, own translation).
- Bayern-CERT is located at LSI.
- The Berlin-CERT is operated by the "IT-Dienstleistungszentrum Berlin" (IT Service Center Berlin, ITDZ Berlin, own translation).
- CERT-Brandenburg is operated by the "Brandenburg IT-Dienstleister" (Brandenburg IT Service Provider, ZIT-BB, own translation).
- Together, the federal states of Bremen, Schleswig-Holstein, Hamburg and Saxony-Anhalt make up "CERT Nord" (CERT North, own translation).
- Upon the founding of HC3, the Hessian CERT was integrated into its cybersecurity jurisdiction and now performs all tasks of the CERT.
- The CERT M-V is operated by the "Datenverarbeitungszentrum Mecklenburg-Vorpommern" (Service Provider for the State Administration of Mecklenburg-Western Pomerania, DVZ M-V, official translation).
- The N-CERT of Lower Saxony is associated with the "Ministerium für Inneres und Sport" (State Ministry of the Interior and Sport of Lower Saxony, own translation).
- The CERT NRW is located at the "Landesbetrieb Information und Technik Nordrhein-Westfalen" (State Office for Information and Technology of North Rhine-Westphalia, own translation).
- The CERT-rlp is part of the "Landesbetrieb Daten und Information Rheinland-Pfalz" (State Office for Data and Information Rhineland-Palatinate, own translation).
- CERT Saarland is being prepared by CERT-rlp in line with an agreement between the federal states of Saarland and Rhineland-Palatinate.
- The SAX.CERT of Saxony is linked to the "Staatsbetrieb Sächsische Informatik Dienste" (Saxon Informatics Services, own translation).
- ThüringenCERT is operated by the "Thüringische Landesrechenzentrum" (Thuringian State Computing Center, own translation).

Within the framework of the VCV, the Federal Government and the federal states cooperate in establishing and operating the CERTs on federal state level. The CERTs of

the federal states cooperate with the CERT-Bund at the BSI[149].

Cyberabwehr – Bayern (Cyber Defence – Bavaria, own translation)
"Cyberabwehr Bayern" is an information and coordination platform established in January 2020 that guarantees close and quick exchange of information between government institutions in the field of cybersecurity. Relevant authorities responsible for cyber defense are informed about IT incidents by the "Cyberabwehr Bayern" in order to take appropriate measures. Apart from providing assistance in acute situations by means of recording, evaluating and passing on information on attacks against IT security infrastructure, the "Cyberabwehr Bayern" also provides an overview of the threat situation in cyberspace, in addition to a situational overview in Bavaria. At the same time, it serves as a point of contact for the Cyber-AZ and thus facilitates information exchange between Bavaria and the Federal Government. Another task is the crisis-proof expansion of digital radio, which is used, among other actors, by the Bavarian police and fire departments.

The "Cyberabwehr Bayern" is housed within the "Cyber-Allianz-Zentrum Bayern" (Cyber-Alliance Centre Bavaria, own translation) in the "Bayerisches Landesamt für Verfassungsschutz" (State Office for the Protection of the Constitution of Bavaria, own translation). The "Bayerisches Landeskriminalamt" (State Office of Criminal Investigation of Bavaria, own translation), the "Bayerische Landesamt für Sicherheit in der Informationstechnik" (State Office for Security in Information Technology of Bavaria, own translation), the "Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg" (Central Agency for Cybercrime in Bavaria at the General Public Prosecutor's Office Bamberg, own translation), the "Bayerische Landesamt für Datenschutzaufsicht" (State Office for Data Protection Supervision of Bavaria, own translation), the "Landesbeauftragte für den Datenschutz" (State Commissioner of Bavaria for Data Protection, own translation), and the "Cyber-Allianz-Zentrum Bayern" are all part of the "Cyberabwehr Bayern"[150].

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

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

Cyber-Allianz-Zentrum – Bayern (Cyber-Alliance Centre – Bavaria, CAZ, own translation)
The CAZ is part of the "Bayerisches Landesamt für Verfassungsschutz" (State Office for the Protection of the Constitution of Bavaria, own translation) and supports companies based in Bavaria, as well as local universities and operators of critical infrastructure, in the fields of prevention and defense against electronic attacks. The CAZ acts as the central governmental control and coordination office in Bavaria as well as a confidential point of contact for affected institutions. Following forensic analysis and intelligence assessment, it suggests a response with recommendations for action. It can also contact affected companies or institutions with (anonymized) information on the patterns of attacks. The CAZ was the first institutional pillar of the "Initiative Cybersicherheit Bayern" (Cybersecurity Initiative of Bavaria, own translation) of the "Bayerisches Staatsministerium des Innern, für Sport und Integration" (Bavarian Ministry of the Interior, for Sport and Integration, own translation)[151].

Cyber-Competence-Center – Brandenburg (Cyber-Competence-Center – Brandenburg, CCC, own translation)
The CCC Brandenburg was established as a new specialist unit in the "Landeskriminalamt Brandenburg" (State Office of Criminal Investigation of Brandenburg, own translation). It aims to pool all personnel and technical competencies to combat and investigate all types of crime on the internet. It assumes responsibility for preventive and repressive tasks and supports police department investigations and inspections related to the fight against cybercrime.

The ZAC for commercial enterprises and authorities was also established here[152]*.*

Cyber Crime Competence Center Sachsen (Cyber Crime Competence Center Saxony, SN4C, own translation)
The SN4C was established within the "Landeskriminalamt Sachsen" (State Office for Criminal Investigation of Saxony, own translation). It focuses on various types of criminality on the internet, such as illegal online transactions. It takes a holistic approach to its work, bringing together relevant specialists and thus making use of synergy effects. Its tasks also include the procurement of necessary hardware and software and keeping an eye on current technical developments.

The SN4C assumes the duties of a "Zentrale Ansprechstelle für die Wirtschaft" (Central Point of Contact for the Economy, own translation)[153]*.*

151 Bayerisches Landesamt für Verfassungsschutz, Cyber-Allianz-Zentrum Bayern (CAZ).
152 Polizei Brandenburg, Cyber-Competence-Center im Landeskriminalamt.
153 Sächsisches Staatsministerium des Innern, Cybercrime Competence Center Sachsen (SN4C).
Sächsisches Staatsministerium des Innern, Zentrale Ansprechstelle Cybercrime (ZAC) für Unternehmen, Behörden und Verbände des Freistaates Sachsen.

Cybercrime Competence Center – Sachsen-Anhalt (Cybercrime Competence Center – Saxony-Anhalt, 4C, own translation)
The 4C was established within the "Landeskriminalamt Sachsen-Anhalt" (State Office for Criminal Investigations of Saxony-Anhalt, own translation). It pools specialists from different departments in the field of cybercrime. Employees of the "Landeskriminalamt Sachsen-Anhalt" are supported by scientists for whom new jobs have been specially created. The 4C-Sachsen-Anhalt aims to deal with more complicated cases across the federal state and support police in simple fraud cases.

The center is also a "Zentrale Ansprechstelle für die Wirtschaft"[154].

Cybercrime-Kompetenzzentrum – Nordrhein-Westfalen (Cybercrime Competency Center – North Rhine-Westphalia, own translation)
In the past, the "Landeskriminalamt Nordrhein-Westfalen" (State Office of Criminal Investigation of North Rhine-Westphalia, own translation) established a "Cybercrime-Kompetenzzentrum", which houses investigative commissions for outstanding cases, computer forensics experts, telecommunications surveillance, evaluation, analysis and prevention, critical internet research and an evaluation center for child sexual exploitation.

The ZAC for the industry is also located here[155].

Cyber Defense Center der Landesverwaltung Berlin (Cyber Defense Center of the Berlin State Administration, CDC-Lv, own translation)
The Cyber Defense Center of the Berlin State Administration is located in the "IT-Dienstleistungszentrum" (IT Service Center Berlin, ITDZ Berlin, own translation). It consists of a Security Operation Center (SOC), the Berlin-CERT, an area for analysis and forensics, as well as one for IT security coordination and consulting. In addition to protecting the data of Berlin's citizens, the CDC-Lv is also responsible for detecting and defending against attacks on the Berlin state network.

The CDC-Lv reports via the Berlin-CERT to Berlin's State Commissioner for Information Security (CIO). At the working level, there is an exchange with the Berlin liaison office of the BSI[156].

154 Hallelife.de, Sachsen-Anhalt startet Kompetenzzentrum gegen Internetkriminalität.
155 Polizei Nordrhein-Westfalen Landeskriminalamt, Das Cybercrime-Kompetenzzentrum beim LKA NRW.
156 ITDZ Berlin, Innovationsmanagement im ITDZ Berlin.
Background Conversation, 2021.

Cyberwehr – Baden-Württemberg (Cyber Defence – Baden-Wuerttemberg, own translation)
The "Cyberwehr – Baden-Württemberg" is a contact and information center for small and medium-sized businesses as well as a cyberattack coordination center. It is currently in the pilot phase and exclusively deployed in the regions surrounding Karlsruhe, Rastatt and Baden-Baden; the long-term aim is nationwide development of regional first-response infrastructures for IT security incidents. The established hotline serves as a first point of contact and consistent emergency number in the event of a cyberattack; it normally takes several hours to speak to an affected company on the phone to provide an initial incident diagnosis. If desired, it also recommends experts who can aid in limiting damage. In contrast to the "Zentrale Anlaufstelle Cybercrime" (Central Contact Point Cybercrime, own translation), the "Cyberwehr – Baden-Württemberg" only takes action in the fields of defense and damage limitation if an incident occurs. The tasks of the "Zentrale Anlaufstelle Cybercrime," on the other hand, also cover preventive measures and prosecution in the event of a claim or an attempted attack. Through legal regulations, it has exclusive powers in the context of law enforcement in solving a case or in the prevention of further attacks.

The "Cyberwehr – Baden-Württemberg" works closely with the ZAC of the "Landesamt für Verfassungsschutz" (State Office for the Protection of the Constitution of Baden-Württemberg, own translation) in the field of cyberespionage, and the CERT BW, as well as the "Forschungszentrum Informatik am Karlsruher Institut für Technologie" (Research Center for Computer Science at the Karlsruhe Institute of Technology, own translation)[157].

Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken (Cybercrime Department of the Public Prosecutor's Office of Saarbrücken, own translation)
The "Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken" is supporting Saarland's "Justizministerium" (Ministry of Justice, official translation) in combating crime on the internet.

The department trains with the "Institut für Rechtsinformatik" (Institute for Legal Informatics, own translation) and the CISPA Helmholtz Center for Information Security[158].

157 Cyberwehr, Die Cyberwehr.
Staatsministerium Baden-Württemberg, Landesregierung initiiert „Cyberwehr Baden-Württemberg".
158 Juristisches Internetprojekt Saarbrücken, Neues Dezernat „Cybercrime" bei der Staatsanwaltschaft Saarbrücken.

Dezernat Cybercrime des Landeskriminalamtes Mecklenburg-Vorpommern (Cybercrime Department of the Mecklenburg-Western Pomerania State Office of Criminal Investigation, own translation)
Department 45 of the "Landeskriminalamt Mecklenburg-Vorpommern" (State Office of Criminal Investigation of Mecklenburg-Western Pomerania, own translation) cooperates with cybercrime specialists in investigating cases and also accommodates the ZAC of Mecklenburg-Western Pomerania.

It receives notifications via the platform netzverweis.de and pursues them. It also cooperates with the "Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock" (Special Prosecutor for Combatting Information and Communication Crimes of Rostock, own translation) and the BKA[159].

Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz (Cybercrime Department of the Rhineland-Palatinate State Office of Criminal Investigation, own translation)
Department 47 functions as a central department and also supports local authorities. It also deals with outstanding cybercrime investigations, in particular procedures piloting new investigative techniques that build upon precedent or those of special public interest, procedures with new technical and/or investigative tactics, as well as cases in the field of international, gang-related, or organized crime. The department also acts as the ZAC for commercial enterprises.

The LKA of Rhineland-Palatinate has been a member of the ACS[160].

Dezernat Cybercrime des Landeskriminalamtes Thüringen (Cybercrime Department of the Thuringia State Office of Criminal Investigation, own translation)
The "Dezernat Cybercrime des Landeskriminalamtes Thüringen" deals with fraud on the internet and investigations of child and adolescent sexual exploitation on the internet.

The department is also home to the ZAC Thuringia[161].

Dezernat LPP 222 Cybercrime – Saarland (Department LPP 222 Cybercrime – Saarland)
In the past, the "Saarländische Kriminalpolizei" (Criminal Police of the State of Saarland, own translation) established a specialized cybercrime department to deal

159 Landeskriminalamt Mecklenburg-Vorpommern, Cybercrime in M-V. Aktuelle Aspekte.
Landespolizei Mecklenburg-Vorpommern, LKA-MV: Internationaler Ermittlungserfolg gegen Kinderpornografieplattform im Darknet.
160 Polizei Rheinland-Pfalz, Aufgaben des Dezernates Cybercrime.
161 Heise Online, Cybercrime: Neue Herausforderungen für Thüringer LKA.
Ministerium für Inneres und Kommunales Thüringen, Internetkriminellen gemeinsam mit den Unternehmen das Handwerk legen.

with particularly serious cases – especially when the public sector is affected – with a very high potential for damage or high technical requirements.

The ZAC of Saarland is also located here[162].

EMERGE IoT – Mecklenburg-Vorpommern (EMERGE IoT – Mecklenburg-Western Pomerania, own translation)
EMERGE IoT is a cooperation project (supported by the Internal Security Fund of the European Union) dedicated to intelligence-gathering, prosecution and prevention of criminal offences related to the Internet of Things (IoT). The goal is to analyze the technical foundations of the IoT and develop tools to improve investigations into attack scenarios on the Internet of Things.

The LKA of Mecklenburg-Western Pomerania and the "Universität Rostock" (University of Rostock, official translation) are involved[163].

Fachkommissariat Cybercrime – Hamburg (Special Commissioner's Office for Cybercrime – Hamburg, LKA 54, own translation)
With LKA 54, the Hamburg police has created a department which pools the competencies of criminal investigators and computer scientists to combine technological and police knowledge.

The ZAC Hamburg is attached to the commission[164].

Hessen Cyber Competence Center (Hessen3C)
The Hessen3C is a competency center offering interdisciplinary collaborative and institutionalized cooperation between state authorities in the federal state of Hesse. It evolved from the "Kompetenzstelle Cybersicherheit'" (Cybersecurity Competency Center, own translation), an outpost of the "Hessisches Innenministerium" (Interior Ministry of the State of Hesse, own translation), which has been completely transformed into Hessen3C. Hessen3C aims to improve the security of Hessian IT, ward off cyber dangers, increase the effectiveness of the fight against cybercrime and find synergies. The Hessen3C serves as a point of contact around the clock for cybersecurity incidents in state and local government and those affecting SMEs.

Hessen3C exchanges information on cyber topics with the Hessian police and the "Hessischer Verfassungsschutz" (State Office for the Protection of the Constitution

162 sol.de, Saar-Kripo eröffnet neue „Cybercrime"-Dienststelle. (Website deleted)
163 Universität Rostock, Universität Rostock unterstützt das Landeskriminalamt Mecklenburg-Vorpommern in Sachen Cyber-Kriminalitätsbekämpfung.
164 Polizei Hamburg, Zentrale Ansprechstelle Cybercrime (ZAC).

of Hesse, own translation); together they create a situational overview. Employees of the Hessen3C are from the CERT Hesse, the police and the "Hessischer Verfassungsschutz"; this is how cross-organizational expertise and services in the field of cybersecurity are made available. Since its founding, the Hessen3C operates the CERT-Hessen and heads the IT crisis management of the state's public administration. Working relationships exist towards the VCV, the CERT-Bund as well as the other CERTs of the Federal States. As of March 2021, Hessen3C is also represented in the Cyber-AZ[165].

Informationssicherheitsbeauftragte:r der Landesverwaltung (Chief Information Security Officer of the State Administration, CISO, own translation)

- In Baden-Wuerttemberg, the Chief Information Security Officer (CISO) is appointed by the state's "Ministerium für Inneres, Digitalisierung und Migration" (Ministry of the Interior, Digitalization and Migration, own translation). The CISO is responsible for defining and updating information security guidelines for the state administration, *advising the state's CIO, and preparing an annual report on the implementation and effectiveness of IT security measures, which is submitted to the state CIO*[166].
- Bavaria's CISO is based in the "Bayerisches Staatsministerium der Finanzen und für Heimat" (Bavarian State Ministry of Finance and for Community, own translation). He or she is responsible for the technical supervision of the Bavarian CERT, the implementation of IT security measures within the Bavarian public administration and reports to the head of the ministerial "Abteilung VII für Digitalisierung, Breitband und Vermessung" (Department VII for Digitization, Broadband and Measurement, own translation)[167].
- Berlin's Chief Information Security Officer (Landes-InfSiBe) is directly attached to the "Staatssekretär:in für Informations- und Kommunikationstechnik in der Senatsverwaltung für Inneres und Sport Berlin" (State Secretary for Information and Communications Technologies in the Berlin Senate Administration for the Interior and Sport, own translation).
  In addition to performing tasks for the implementation and control of processes and standards in the area of information security, the Landes-InfSiBe disposes a direct right of presentation towards the State Secretary. For the realm of IT security, the Landes-InfSiBe oversees technical control of the ITDZ Berlin[168].

165 Bundesverwaltungsamt, Referentin/Referent (m/w/d) im Hessen CyberCompetenceCenter (Dieser Link läuft ggf. aus, bei Interesse kann eine Kopie bei den Autor:innen angefragt werden).
Hessisches Ministerium des Innern und für Sport, Der Bereich Cybersecurity im Hessen3C.
Hessisches Ministerium des Innern und für Sport, Hessen3C.
Email exchange with representatives of the Hessen Cyber Competence Center in November 2019.

166 Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg, Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit.

167 IT-Beauftragter der Bayerischen Staatsregierung, IT-Sicherheitsstrukturen in Bayern.
Landesamt für Sicherheit in der Informationstechnik Bayern, IT-Sicherheitskonferenz für niederbayerische Kommunen am 20.02.2019 in Deggendorf.

168 Senatsverwaltung für Inneres und Sport Berlin, Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin.

- In Brandenburg, a state-wide CISO is appointed by the "Abteilung 6 für Digitalisierung, E-Government und IT-Leitstelle" (Department 6 for Digitization, E-Government and IT Control Center, own translation) within the "Ministerium des Innern und für Kommunales des Landes Brandenburg" (Brandenburg Ministry of the Interior and Municipal Affairs, official translation). He or she is inter alia responsible for the coordination of the entire IT security management as well as the preparation of an annual IT security report.
  Depending on their severity, the CISO is being informed of any security incidents by the CERT Brandenburg[169].
- Bremen's CISO is organizationally located at the "Senator:in für Finanzen der Hansestadt Bremen (Finance Senator of the Free Hanseatic City of Bremen, official translation). Since a first submission in July 2020, the Bremen CISO is producing a non-public annual report on information security in the Bremen state administration which addresses problems, solutions and alternatives[170].
- The Chief Information Security Officer (InSiBe) of the Free Hanseatic City of Hamburg has been established within the "Amt für IT und Digitalisierung der Senatskanzlei Hamburg" (Office for IT and Digitalization of the Hamburg Senate Chancellery, own translation), *which is headed by the state's CIO*[171].
- In Hesse, the head of the "Abteilung VII für Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung" (Department VII for Cyber and IT Security, Administrative Digitization, own translation) of the "Ministerium des Innern und für Sport" (State Ministry of the Interior and Sports, own translation) also assumes the function of the state's CISO.
  A representative of the Hessen3C acts as his or her deputy[172].
- In Mecklenburg-Western Pomerania, the state's Information Security Officer (BeLVIS) is based in the state's "Ministerium für Inneres und Europa" (Ministry of the Interior and Europe, official translation).
  He or she reports to the state CIO and coordinates interdepartmental information security management. The BeLVIS is responsible for the CERT M-V and represents Mecklenburg-Western Pomerania in the VCV[173].
- The information security management of the state administration in Lower Saxony falls under the responsibility of the state's CISO, who is based in the "Ministerium für Inneres und Sport" (Ministry of the Interior and Sport, own translation)[174].

169 Brandenburgisches Vorschriftensystem, Leitlinie zur Gewährleistung der IT-Sicherheit in der Landesverwaltung Brandenburg.
170 CISO Bremen, Vorlage für die Sitzung des Senats am 14.7.2020. Jahresbericht zur Informationssicherheit in der bremischen Verwaltung.
171 Freie Hansestadt Hamburg, Rahmen-Sicherheitskonzept.
172 Ministerium des Innern und für Sport Hessen, Der zentrale Informationssicherheitsbeauftragte der Landesverwaltung. Hessischer Landtag (Drucksache 20/1520), Antwort auf Kleine Anfrage: Umsetzung Informationssicherheitsrichtlinie.
173 DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH, DVZ.info 02/14.
Ministerium für Inneres und Sport Mecklenburg-Vorpommern, Stellenausschreibung Beauftragte/Beauftragter der Landesverwaltung für Informationssicherheit.
174 Ministerium für Inneres und Sport Niedersachsen, Informationssicherheit.
Ministerium für Inneres und Sport, Informationssicherheit in Niedersachsen.

- The post of North Rhine-Westphalia's CISO is assumed by the Head of the "Referat II B 4, Informationssicherheit in der Landesverwaltung" (Division II B 4, Information Security in the State Administration, own translation) within the state's "Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie" (Ministry of Economic Affairs, Innovation, Digitalisation and Energy, official translation)[175].
- In Rhineland-Palatinate, the information security officer for the state administration (CISO-rlp) is based in "Referat 392, Ressortübergreifende Informationssicherheit" (Division 392, Interdepartmental Information Security, own translation) of "Abteilung 9, IT-Zentralstelle, Breitband" (Department 9, IT Central Office, Broadband, own translation) of the state's "Ministerium des Innern und für Sport" (Ministry of the Interior and Sports, own translation).
  He or she entertains close exchange with the BSI, CERT-rlp and the security authorities of the state[176].
- In the Saarland, the head of the "Stabsstelle Informationssicherheitsmanagement und IT-Recht" (Administrative Department for Information Security Management and IT Law, own translation) within the state's "Ministerium für Finanzen und Europa" (Ministry of Finance and Europe, own translation) also assumes the function as the state's CISO.
  He or she has a direct right of presentation towards the state's CIO, reports on risks and the status of implementation of IT security measures, and can recommend measures to mitigate these hazards, if necessary[177].
- Saxony's CISO (BfIS) is also the head of "Referat 45, Informations- und Cybersicherheit, Kritische Infrastrukturen" (Division 45, Information and Cyber Security, Critical Infrastructures) within the "Sächsische Staatskanzlei" (Saxon State Chancellery, official translation).
  He or she is appointed by the state CIO and has a direct right of first refusal. The BfIS is a member of the Arbeitsgruppe Informationssicherheit des IT-Planungsrates (Working Party on Information Security of the IT Planning Council, AG InfoSic, own translation), a state working group of the IMK, as well as the ACS and UP KRITIS[178].
- In addition to the state's CIO, the "Ministerium der Finanzen" (Ministry of Finance, official translation) in Saxony-Anhalt is also home to the state's Information Security Officer (InSiBe).
  He or she informs the CIO and is responsible for processes to implement and comply with information security standards[179].

175 Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie Nordrhein-Westfalen, Geschäftsverteilungsplan.
176 Ministerium der Justiz Rheinland-Pfalz, Leitlinie zur Informationssicherheit der Landesverwaltung des Landes-Rheinland-Pfalz.
Ministerium des Innern und für Sport Rheinland-Pfalz, Stellenausschreibung Referentin / Referenten (m/w/d) im Referat 392.
177 Ministerium für Finanzen und Europa Saarland, Stabstelle Informationssicherheit und IT-Recht.
178 Sächsische Staatskanzlei, Beauftragter für Informationssicherheit des Landes (BfIS).
179 Ministerium der Finanzen Sachsen-Anhalt, Organisationsplan.
Ministerium für Justiz und Gleichstellung Sachsen-Anhalt, Leitlinie zur Informationssicherheit in der unmittelbaren Landesverwaltung Sachsen-Anhalt.

- In Schleswig-Holstein, the state's CISO is located within the "Abteilung 3, Digitalisierung und Zentrales IT-Management der Landesregierung" (Department 3, Digitalization and central IT security management of the state's government, own translation) within the "Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung" (Ministry of Energy, Agriculture, the Environment, Nature and Digitalization, official translation). The CISO is responsible for interdepartmental information security management.
  He or she has the right of presentation towards the state's CIO and is also represented in the Arbeitsgruppe Informationssicherheit des IT-Planungsrates (Working Party on Information Security of the IT Planning Council, AG InfoSic, own translation) for Schleswig-Holstein[180].
- The Thuringian CISO is appointed by the "Thüringer Finanzministerium" (Thuringia Finance Ministry, official translation), which is responsible for e-government and interdepartmental issues, *and reports directly to the State CIO*[181].

Kompetenz- und Forschungszentren für IT-Sicherheit (Competence and research centers for IT security, own translation)

The three competency and research centers for IT security in Saarbrücken (CISPA), Darmstadt (ATHENE) and Karlsruhe (KASTEL) are part of the Digital Agenda of the BMBF. By establishing the three research centers, the Federal Government has expanded research and development into the field of cybersecurity and privacy protection. ATHENE, formerly CRISP, was recently transformed into the "Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE" (National Research Centre for Applied Cybersecurity ATHENE, official translation). Since the beginning of 2020, it has been part of the Fraunhofer-Gesellschaft at the two Darmstadt institutes SIT and IGD, with participation from the "Technische Universität Darmstadt" (Technical University of Darmstadt, official translation) and the "Hochschule Darmstadt" (Darmstadt University of Applied Sciences, official translation).

The three competency and research centers for IT security are funded by the BMBF[182].

Kompetenzzentrum Cybercrime – Bayern (Cybercrime Competency Center – Bavaria, own translation)

The "Kompetenzzentrum Cybercrime – Bayern" (Department 54) was established at the "Landeskriminalamt Bayern" (State Office of Criminal Investigation of Bavaria, own translation). One of its main tasks is to simulate crisis management with companies and authorities responsible for public order – especially during emergency

180 Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung Schleswig-Holstein, Bemerkungen 2017 des Landesrechnungshofs Schleswig-Holstein mit Bericht zur Landeshaushaltsrechnung 2015; Bericht und Beschlussempfehlung des Finanzausschusses vom 01.12.2017, Drucksache 19/364; hier: Aktuelle Nachberichterstattung zu unserem Bericht vom 29.04.2019.
181 Finanzministerium Thüringen, Informationssicherheitsleitlinie der Thüringer Landesverwaltung.
182 Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.

situations, such as a cyberattack. It also takes on cases of cybercrime which are of supra-regional significance and cannot be processed by local police services[183].

Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen (Coordination Office for Cyber Security North Rhine-Westphalia, own translation)
Plans for a "Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen" were adopted in August 2020 by the state's Cabinet. It is meant to serve as the central service point of the state government, housed within the new digital department of the "Innenministerium Nordrhein-Westfalen" (Interior Ministry of the State of North Rhine-Westphalia, own translation).

It will be tasked with bundling the state and its public administration's cybersecurity information and acting as an interface for the BSI. There may also be overlap in responsibilities with the "Verfassungsschutz" (State Office for the Protection of the Constitution of North Rhine-Westphalia, own translation) and the "Cybercrime-Kompetenzzentrum des Landeskriminalamts" (Cybercrime Competency Center – North Rhine-Westphalia, own translation) in the fields of cybersecurity and cyber defense. All in all, it is intended to heighten cybersecurity protections in North Rhine-Westphalia for society, industry and state institutions[184].

Landesamt für Sicherheit in der Informationstechnik Bayern (State Office for Information Security of Bavaria, LSI, own translation)
Since its founding, the LSI has been responsible for protecting Bavarian IT infrastructure. It is intended to provide advice to municipalities and citizens.

The LSI is a member of the VCV. It hosts the Bayern-CERT and cooperates with the BSI[185].

Landesbeauftragte:r für Informationstechnologie (State Commissioner for Information Technology, Länder-CIO, own translation)
The following federal states have appointed a "Landesbeauftragte:r für Informationstechnologie," a so-called CIO (Chief Information Officer, official translation) of the state:

- In Baden-Wuerttemberg, the "Landesbeauftrage für Informationssicherheit" (State Commissioner for Information Security, own translation) is responsible for the IT strategy of the state administration and the E-Government Strategy, among other things. The CIO also acts as Chief Digital Officer (CDO) of the state administration. The CIO is assigned to the "Innenministerium Baden-Württem-

183 Bayerische Staatsregierung, Cyber-Kompetenzzentrum im Landeskriminalamt.
184 Behörden Spiegel, Neue Koordinierungsstelle für Cyber-Sicherheit in NRW.
Ministerium des Inneren des Landes Nordrhein-Westfalen, Kabinett beschließt Einrichtung von Koordinierungsstelle für Cybersicherheit.
185 Landesamt für Sicherheit in der Informationstechnik Bayern, Startseite.

berg" (Interior Ministry of the State of Baden-Württemberg, own translation)[186].

- Bavaria has appointed a "Beauftragte für Informations- und Kommunikationstechnik der Bayerischen Staatsregierung" (Commissioner for Information and Communications Technologies of the Bavarian State Government, CIO Bayern, own translation). The CIO Bayern is responsible, for example, for the IT and E-Government Strategies and administrative digitization and represents Bavaria on the "IT-Planungsrat". The position is currently being filled by the "Bayerische Staatsministerin für Digitales" (Bavarian Minister of State for Digital Affairs, own translation)[187].
- In Berlin, the "Staatssekretärin für Informations- und Kommunikationstechnik in der Senatsverwaltung für Inneres und Sport Berlin" (State Secretary for Information and Communications Technologies in the Berlin Senate Administration for the Interior and Sport, own translation) assumes the position of the state's CIO and reports to the "Innensenator" (Interior Senator, own translation). She represents the state of Berlin on the "IT-Planungsrat"[188].
- The state of Brandenburg has appointed a Chief Process Innovation Officer who looks after the state's IT affairs. He is based in the "Innenministerium" (Interior Ministry of the State of Brandenburg, own translation)[189].
- In Bremen, the CIO position is located within the "Staatsrat des Finanzressorts" (State Council of Finances, own translation)[190].
- Hamburg has appointed a Chief Digital Officer who will head the "Amt für IT und Digitalisierung" (Office for IT and Digitalization, own translation)[191].
- The CIO of the state of Hesse is responsible for the state's information technology and e-government. The CIO is based in the "Hessisches Ministerium für Digitale Strategie und Entwicklung" (State Ministry for Digital Strategy and Development of Hesse, own translation) and represents Hesse on the "IT-Planungsrat"[192].
- In Mecklenburg-Western Pomerania, the position of CIO is held by the "Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern" (State Ministry of Energy, Infrastructure and Digitalization of Mecklenburg-Western Pomerania, own translation)[193].
- The CIO of Lower Saxony heads the "Stabsstelle Informationstechnik der Landesverwaltung des Ministeriums für Inneres und Sport" (Office for Information Technology of the State Administration of the State Ministry of the Interior and Sport of Lower Saxony, own translation). In addition to IT strategy and e-government, the CIO's tasks also include the modernization of administration[194].
- The CIO of North Rhine-Westphalia is based in the "Ministerium für Wirtschaft,

186 CIO Baden-Württemberg, Stefan Krebs.
187 Bayerisches Staatsministerium für Digitales, IT-Beauftragte der Bayerischen Staatsregierung.
188 CIO, Sabine Smentek wird CIO vom Land Berlin.
189 CIO, Die IT-Chefs der Bundesländer.
190 Freie Hansestadt Bremen, Staatsrat Dr. Martin Hagen.
191 Senatskanzlei Hamburg, Senatskanzlei Amt für IT und Digitalisierung.
192 Hessische Ministerin für Digitale Strategie und Entwicklung, CIO.
193 Regierung Mecklenburg-Vorpommern, Staatssekretärin Ina-Maria Ulbrich.
194 Niedersächsisches Ministerium für Inneres und Sport, Neuer CIO in Niedersachsen: Dr. Horst Baier ist IT-Bevollmächtigter der Landesregierung.

Innovation, Digitalisierung und Energie" (State Ministry of Economics, Innovation, Digitization and Energy of North Rhine-Westphalia, own translation). The CIO is responsible for IT management as well as standardization tasks and representing the state in the "IT-Planungsrat"[195].

- The CIO of Rhineland-Palatinate is responsible, among other things, for IT infrastructures, the basic and cross-sectional IT services of the state administration, the standardization agenda and coordinating IT deployment across departments[196].
- Saarland's CIO is called the "Bevollmächtigte des Saarlandes für Innovation und Strategie" (State Government Commissioner for Innovation and Strategy of Saarland, own translation)[197].
- Saxony's CIO leads the "Sächsische Staatskanzlei" (State Chancellery of Saxony, own translation) and is responsible for the "Stabsstelle Landesweite Organisationsplanung, Personalstrategie und Verwaltungsmodernisierung'" (Office for Statewide Organizational Planning, Personnel Strategy and Administrative Modernization of Saxony, own translation). It represents the state in the "IT-Planungsrat."[198].
- Currently, Saxony-Anhalt's "Finanzministerium" (State Ministry of Finance of Saxony-Anhalt, own translation) provides the state CIO, known as the "Beauftragte der Landesregierung für Informations- und Kommunikationstechnik" (State Government Commissioner for Information and Communication Technology of Saxony-Anhalt, own translation), who represents Saxony-Anhalt on the "IT-Planungsrat"[199].
- The CIO of Schleswig-Holstein is responsible for the state's central IT management and is associated with the "Staatskanzlei Schleswig-Holstein" (State Chancellery of Schleswig-Holstein, own translation)[200].
- The CIO of Thuringia is based in the state's "Finanzministerium" (State Ministry of Finance of Thuringia, own translation) and is responsible for the standardization of IT and e-government structures[201].

Landesbehörden für Verfassungsschutz (State Offices for the Protection of the Constitution, LfV, official translation)

- Within the "Landesamt für Verfassungsschutz Baden-Württemberg" (Baden-Württemberg State Office for the Protection of the Constitution, own translation), Department 4 is primarily concerned with cybersecurity-related fields of work. It is responsible for counterintelligence and cyber defense as well

195 Die Landesregierung Nordrhein-Westfalen, Prof. Andreas Meyer-Falcke neuer CIO.
196 Ministerium des Innern und für Sport Rheinland-Pfalz, Digitale Verwaltung Rheinland-Pfalz.
197 Staatskanzlei Saarland, Bevollmächtigter für Innovation und Strategie Chief Information Officer (CIO).
198 Sächsische Staatskanzlei, Staatssekretäre.
199 Sachsen-Anhalt, Der Beauftragte der Landesregierung für Informationstechnik (CIO).
200 Schleswig-Holstein, E-Government – Steuerung und Zusammenarbeit.
201 Freistaat Thüringen, CIO des Freistaats Thüringen.

as secret and sabotage protection[202].

- In Bavaria, Department 5 of the "Landesamt für Verfassungsschutz" (Bavarian State Office for the Protection of the Constitution, official translation) is inter alia responsible for economic protection and counterintelligence. The "Cyber-Allianz Zentrum Bayern" (Cyber-Alliance Centre Bavaria, CAZ, own translation) and its subordinate "Cyberabwehr Bayern" (Cyber Defence Bavaria, own translation) are also located there[203].
- Berlin's "Senatsverwaltung für Inneres und Sport" (Senate Administration for the Interior and Sport, own translation) houses the state's Office for the Protection of the Constitution (Department 2). Responsibilities for economic and secret protection (Department Wi/GSB) as well as counterintelligence (Department II D) are located there. In the past, the Senate Administration has transferred tasks of cyber defense to the BfV in the framework of an administrative agreement[204].
- In Brandenburg, the State Office for the Protection of the Constitution is located in the state's "Ministerium des Innern und für Kommunales" (Ministry of the Interior and for Municipal Affairs, official translation) (Department 5). Its fields of activity include counterintelligence and economic protection. In the latest "Verfassungsschutzbericht" (Report on the protection of the constitution, own translation) of Brandenburg references to inter alia current developments in so-called "cyber-extremism" have been made[205].
- The self-description of the "Bremer Landesamts für Verfassungsschutz" (Bremen State Office for the Protection of the Constitution, own translation) or its last report on the protection of the constitution include no reference to any responsibilities within the fields of economic protection or cyber defense[206].
- Department V3 of the "Landesamt für Verfassungsschutz Hamburg" (Hamburg State Office for the Protection of the Constitution, own translation) works inter alia on counterintelligence. Its subordinate unit V32 has competencies and tasks in the field of economic protection. The latest report on the protection of the constitution by Hamburg also refers to threats from cyber espionage, cyber sabotage and cyber attacks[207].
- Within the "Landesamt für Verfassungsschutz Hessen" (Hesse State Office for the Protection of the Constitution, own translation) Department 30 is in charge of counterintelligence and economic protection. In an effort to protect the economy,

202 Landesamt für Verfassungsschutz Baden-Württemberg, Aufbau und Organisation.
Landesamt für Verfassungsschutz Baden-Württemberg, Cyberspionage.
203 Landesamt für Verfassungsschutz Bayern, Organisation.
Landesamt für Verfassungsschutz Bayern, Spionageabwehr / Wirtschaftsschutz.
204 Senatsverwaltung für Inneres und Sport Berlin, Organigramm.
Senatsverwaltung für Inneres und Sport Berlin, Verfassungsschutzbericht 2019.
205 Ministerium des Innern und für Kommunales, Aufbau und Organisation.
Ministerium des Innern und für Kommunales Brandenburg, Wirtschaftsschutz.
Ministerium des Innern und für Kommunales, Verfassungsschutzbericht des Landes Brandenburg 2019.
206 Landesamt für Verfassungsschutz Bremen, Über Uns.
207 Landesamt für Verfassungsschutz Hamburg, Organigramm des Landesamtes für Verfassungsschutz.
Behörde für Inneres und Sport Freie Hansestadt Hamburg, Verfassungsschutzbericht 2019.

cyber espionage is listed as an explicit area of responsibility[208].

- In Mecklenburg-Western Pomerania, the State Office for the Protection of the Constitution is located in the "Ministerium für Inneres und Europa" (Ministry of the Interior and Europe, official translation). Counterintelligence and economic protection as its fields of work include threats from cyber attacks and industrial espionage[209].
- The Lower Saxony State Office for the Protection of the Constitution (Department 5) is located in its "Ministerium für Inneres und Sport" (Ministry of the Interior and Sport, own translation) and oversees inter alia economic protection and cyber defense (Department 55). With respect to economic protection, it is available to companies as a supporting point of contact with regard to the prevention of industrial espionage. Concerning the latter, it is inter alia collecting, gathering, analyzing and evaluating data in the context of IT-supported espionage and sabotage operations by foreign intelligence services[210].
- The "Ministerium des Innern des Landes Nordrhein-Westfalen" (Ministry of the Interior of the state of North Rhine-Westphalia, own translation) houses the state's Office for the Protection of the Constitution. Its Department 6 (Group 61) possesses, for example, responsibilities for a cyber center for analysis, prototyping and Internet reconnaissance (Unit 611) and works on counterintelligence, economic protection and cyber defense (Unit 613)[211].
- In Rhineland-Palatinate, the State Office for the Protection of the Constitution is institutionally located in the state's "Ministerium des Innern und für Sport" (Ministry of the Interior and Sports, own translation). Its areas of responsibility include espionage, cyber defense and economic protection[212].
- The "Ministerium für Inneres, Bauen und Sport des Saarlandes" (Saarland Ministry for Internal Affairs, Construction and Sport, official translation) is home to the State Office for the Protection of the Constitution. Its tasks include counterintelligence and economic protection. The latest Saarland report on the protection of the constitution refers to threats from cyber and electronic attacks[213].
- The "Sächsisches Landesamt für Verfassungsschutz" (Saxon State Office for the Protection of the Constitution, own translation) is institutionally attached to the local Ministry of the Interior. *Close working relationships exist with the BfV, its counterparts in all federal states, the BND, the BAMAD, the BSI and the Cyber-AZ*[214].

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

- In Saxony-Anhalt, the State Office for the Protection of the Constitution is located in its "Ministerium für Inneres und Sport" (Ministry of the Interior and Sports, own translation) (Department 4). Department 44 is responsible for counterintelligence and economic protection. According to the Saxony-Anhalt report on the protection of the constitution, counterintelligence also includes cyberattacks[215].
- The State Office for the Protection of the Constitution of Schleswig-Holstein is located in the "Ministerium für Inneres, ländliche Räume und Integration" (Ministry of the Interior, Rural Areas, Integration and Equality, official translation) (Department IV 7). Its fields of work include counterintelligence and economic protection. A different department (IV 76) also deals with digital work, IT, G10 and secret protection[216].
- In Thuringia, the State Office for the Protection of the Constitution is organizationally located within the "Ministerium für Inneres und Kommunales" (Thuringian Ministry of the Interior and Municipal Affairs, own translation). Department 54 oversees counterintelligence as an area of work, which also includes cyber defense and economic protection[217].

Netzverweis.de – Mecklenburg-Vorpommern (Netzverweis.de – Mecklenburg-Western Pomerania, own translation)

The website netzverweis.de is a joint initiative of the "Landeskriminalamtes Mecklenburg-Vormpommern" (State Office of Criminal Investigation of Mecklenburg-Western Pomerania, own translation) and the "DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH" (DVZ Data Processing Centre Mecklenburg-Western Pomerania GmbH, own translation) under the patronage of the "Ministerium für Inneres und Europa" (State Ministry for the Interior and Europe of Mecklenburg-Western Pomerania, own translation). It functions as an online reporting office through which citizens can provide authorities with anonymous tips on cybercrime. This information is then forwarded to the *LKA-Mecklenburg-Western Pomerania, where it is processed by specialists and investigated*[218].

Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock (Special Prosecutor for Combatting Information and Communication Crimes of Rostock, own translation)

With statewide jurisdiction, the "Staatsanwaltschaft Rostock" (Public Prosecutor's Office of Rostock, own translation) is concurrently the "Schwerpunktstaatsan-

215 Ministerium für Inneres und Sport Sachsen-Anhalt, Organisationsplan.
Ministerium für Inneres und Sport des Landes Sachsen-Anhalt, Verfassungsschutzbericht 2019.
216 Der Ministerpräsident des Landes Schleswig-Holstein, Spionageabwehr und Wirtschaftsschutz.
Ministerium für Inneres, ländliche Räume, Integration und Gleichstellung, Organisationsplan.
217 Ministerium für Inneres und Kommunales Thüringen, Organigramm.
Ministerium für Inneres und Kommunales Thüringen, Wirtschaftsspionage / Wirtschaftsschutz.
218 Netzverweis, Online-Meldestelle.
Regierung Mecklenburg-Vorpommern, Landesregierung.

waltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock," thus also covering the area of cybercrime[219].

Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus (Special Public Prosecutor's Office to Combat Computer and Data Network Crime of Cottbus, own translation)
The "Staatsanwaltschaft Cottbus" (Public Prosecutor's Office of Cottbus, own translation) operates as the state of Brandenburg's "Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität"[220].

Sicherheitskooperation Cybercrime (Security Cooperation Cybercrime, own translation)
"Sicherheitskooperation Cybercrime" is an initiative of the criminal investigation offices of six federal states (Baden-Württemberg, Hesse, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate, and Saxony) and Bitkom, which offers a platform for the police and the digital economy to counter the dangers of cybercrime together and to exchange knowledge and technical skills for this purpose[221].

Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin (Special Department for the Fight against Cybercrime of Berlin's Public Prosecutor's Office, own translation)
The "Staatsanwaltschaft Berlin" (Public Prosecutor's Office of Berlin, own translation) commands a special department for cybercrime. The main focus of the department is fraud of goods and trade credit in connection with online trading[222].

Zentrale Ansprechstellen Cybercrime der Polizeien der Länder für die Wirtschaft (Central Contact Points for Cybercrime of the Police Forces of the Federal States for the Economy, ZAC, own translation)
The ZAC makes itself available to companies seeking to either prevent or react to internet-related crimes. In each federal state, specifically trained police officers investigate in partnership with IT specialists.

At the federal state level, the ZAC is usually based at the LKA, and, where applicable, with respective cyber competency centers (see descriptions of the cyber competency centers). The ZAC at federal level is located at BPol[223].

219 Justiz Online in Mecklenburg-Vorpommern, Zuständigkeit.
220 Staatsanwaltschaft Cottbus, Schwerpunktstaatsanwaltschaft. (Website deleted)
221 Sicherheitskooperation Cybercrime, Aktivitäten.
Sicherheitskooperation Cybercrime, Die Kooperation.
222 Diana Nadeborn, Berliner Staatsanwaltschaft rüstet auf gegen Cyberkriminalität.
223 Bundeskriminalamt, Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft.
Der Polizeipräsident in Berlin, Zentrale Ansprechstelle Cybercrime für die Wirtschaft im LKA Berlin.

Zentralstelle Cybercrime Bayern (Central Office Cybercrime Bavaria, ZCB, own translation)
The ZCB, housed within the "Generalstaatsanwaltschaft Bamberg" (Chief Public Prosecutor's Office of Bamberg, own translation), is tasked with investigating cybercrime all over Bavaria. In coordination with the "Bayerisches Justizministerium" (State Ministry of Justice of Bavaria, own translation), the ZCB also works on non-procedural issues in the field of cybercrime.

To do so, it cooperates with the ZCOs of other federal states and is involved in specialist committees at home and abroad. It supports the Bavarian judiciary in its training activities in the area of cybercrime. It also cooperates with the responsible specialists of the Bavarian police, the BKA, and with international partners, in cases such as organized cybercrime proceedings. The ZCO Bavaria is a member of the ACS[224].

Zentralstelle Cybercrime Sachsen (Central Office Cybercrime Saxony, ZCS, own translation)
The ZCS, housed within the "Generalstaatsanwaltschaft Dresden" (Public Prosecutor General's Office of Dresden, own translation), is the judicial counterpart to the SN4C of the LKA-Sachsen. It focuses on the prosecution of internet-related crimes[225].

Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität – Baden-Württemberg (Central Office for the Fight against Information and Communication Crime – Baden-Württemberg, own translation)
The "Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität" tasks within the "Generalstaatsanwaltschaft Stuttgart" (Public Prosecutor General's Office of Stuttgart, own translation) consists in the monitoring of developments in the field of information and communication technologies and to inform the "Staatsanwaltschaft" (Public Prosecutor's Office, own translation). It also plans and carries out training sessions. The "Zentralstelle" examines new investigative tools in the field of information and communication technologies according to their usefulness in law enforcement.

It is also intended to facilitate cooperation with other departments involved in this field and cooperates with the BKA and the LKA Baden-Württemberg[226].

224 Federal Office for Information Security, Teilnehmerliste der Allianz für Cyber-Sicherheit. Generalstaatsanwaltschaft Bamberg, Zentralstelle Cybercrime Bayern (ZCB).
225 Staatsministerium der Justiz, Sächsisches Justizministerialblatt Nr. 5/2018. MDR Sachsen, Sachsen fehlen Polizisten fürs Netz. (Website deleted)
226 Ministerium der Justiz und für Europa Baden-Württemberg, Zentralstelle für die Bekämpfung von informations- und Kommunikationskriminalität eingerichtet. (Website deleted)

Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität – Hessen (Central Office for Combating Internet and Computer Crime – Hesse, ZIT, own translation)
The ZIT was established as a branch of the "Generalstaatsanwaltschaft Frankfurt (a.M.)" (Public Prosecutor General's Office of Frankfurt, own translation) in Gießen. It is the central operating office for particularly complex and extensive investigations into areas of child sexual exploitation and abuse on the internet, darknet crime and other cybercrime.

ZIT is the BKA's first point of contact for unresolved internet crimes with local jurisdiction in Germany and in mass proceedings against several suspects nationwide. It is also a founding member of the European Judicial Cybercrime Network[227].

Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (Central and Contact Office Cybercrime North Rhine-Westphalia, ZAC NRW, own translation)
ZAC NRW – not to be confused with North Rhine-Westphalia's "Zentrale Ansprechstelle Cybercrime der Polizei für Wirtschaftsunternehmen" (Central and Contact Office Cybercrime of the Police for Business and Industry, own translation), listed as ZAC Nordrhein-Westfalen in the visualization and located in the state's LKA – has been the "Staatsanwaltschaft Köln" (Public Prosecutor›s Office Cologne, own translation) responsible nationwide cybercrime unit of the judiciary. It is the largest judiciary cybercrime unit in the nation, responsible for conducting proceedings in high-profile cybercrime investigations, fulfilling the functions of a central contact point for cybercrime and participating in further training measures in the regional and national context.

The ZAC NRW is in close exchange with other central offices for cybercrime of the federal states, police authorities, commercial enterprises and the BSI[228].

227 Staatsanwaltschaften Hessen, Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT).
228 Justiz-ONLINE, Zentral- und Ansprechstelle Cybercrime (ZAC NRW).

8. Explanation – Actors at Local Level

Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V. (Federal Working Group of Municipal IT Service Providers, Vitako, own translation)
Vitako, located in Berlin, currently brings together 52 data centers, software and IT-service companies operating in over 10,000 municipalities in Germany. Vitako aims to bundle knowledge and know-how in order to aid its members with regard to the use of information technology in the public sector. Furthermore, as an association, Vitako represents the interests and perspectives of municipal IT service providers in political forums and committees on legal as well as technical-organization parameters. Within Vitako, members have joined together to form twelve specialist working groups for the purpose of exchanging information and developing guidelines for action and association positions. These groups discuss, for example, current developments within the field of e-government, IT security or standardization.

Vitako dispatches three representatives to the municipal committee of FITKO. Close working relationships exist with the central municipal associations, which are supported by Vitako through its know-how and its advocacy in questions of IT security. Vitako's recommendations are always made in coordination with the central municipal associations. Moreover, Vitako maintains a cooperation with the KGSt[229].

IT-SiBe-Forum (Forum for Municipal IT Security Officers, own translation)
As an internal, non-public forum of municipalities and states, the IT-SiBe-Forum is a platform open to all municipal IT security officers who, as contacts in municipal administrations and municipal institutions, are responsible for the implementation of IT security and the introduction of "IT-Grundschutz" (IT Baseline Protection, official translation) standards[230]. The IT-SiBe-Forum offers them opportunities to exchange information and experiences. The principles of the IT-SiBe-Forum include the preservation of municipal self-administration, mutual support and a bundling function for cross-level cooperation.

The IT-SiBe Forum also forms working groups of the central municipal associations with IT security practitioners from the municipal level. Most recently, the IT-SiBe-Forum was actively involved in the revision of the "IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung" (IT Baseline Protection Profile for Basic Protection of Municipal Administration, own translation) and the "Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen" (Handout for

229 Vitako, Gremien.
Vitako. Satzung.
Vitako, Verband.
Vitako, Verein.
230 It should be noted that not all municipalities in Germany have a municipal IT security officer and that the scope of their duties and responsibilities can vary greatly and be widely dispersed due to municipal heterogeneity.

the design of the information security guideline in municipal administrations, own translation)[231].

Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (Municipal Joint Office for Administrative Management, KGSt, own translation)
As a municipal association, KGSt supports its members – cities, counties, communities and other administrative organizations from the entirety of the DACH region – in all questions within the realm of municipal management. It also provides support in implementing administration modernization efforts. In practice, this includes providing more than 2,200 municipalities with information, recommendations for action, and individual consultations and seminars in the fields of municipal IT management, IT strategy and IT data security. The KGSt has also established an innovation circle "Digital and IT Management", in which some 30 municipal IT experts regularly meet to exchange experiences and, if necessary, draft position papers.

The KGSt maintains cooperation with the Central Municipal Associations and is represented in the municipal committee of FITKO by two representatives[232].

Kommunale Spitzenverbände (Central Municipal Associations, KSV, own translation)
As a collective term, Central Municipal Associations are comprised of voluntary inter-municipal associations and advocacy groups of German communities and states at federal-state level: the "Deutscher Städtetag" (Association of German Cities, own translation), the "Deutscher Städte- und Gemeindebund" (German Association of Towns and Municipalities, own translation), and the "Deutscher Landkreistag" (German Association of Rural Districts, own translation). Their work is coordinated within the "Bundesvereinigung der kommunalen Spitzenverbände" (Federal Organisation of Central Municipal Organisations, own translation), whose chairmanship rotates annually between the three associations. Together or as individual associations, municipal interest groups take a position on political decision-making processes or federal planning with municipal relevance and become involved in relevant legislative procedures, when appropriate. This also includes the topics of IT and cybersecurity. Representing the municipal policy interests of its members serves to promote municipal self-administration. In this context, it is furthermore a concern of the Central Municipal Associations, which are also organized at federal state level, to cultivate and facilitate the exchange of experiences and information between its members.

231 Heino Sauerbrey, Ziel und Zweck des Internetforums für IT-Sicherheitsbeauftragte der Länder und Kommunen.
IT-SiBe-Forum, Grundsätze.
IT-SiBe-Forum, Kurzinformation.
IT-SiBe-Forum, Meilensteine.
232 KGSt, Über Uns.
KGSt, IT-Strategie, IT-Steuerung und Informationssicherheit.
KGSt, Organisation, Digitales und IT.
KGSt, Innovationszirkel: Digitales und IT-Steuerung.

Together with the BSI, the Central Municipal Associations have developed a basic IT protection profile for municipalities. Furthermore, BVkom has issued recommendations for IT attacks on municipal administrations in collaboration with BKA and the BSI. Through the Central Municipal Associations and the IT-SiBe-Forum, the BSI has involved local governments in the modernization of basic IT protection. Together with Vitako, the KSV have published a handout on the design of information security guidelines in municipal administrations. The Central Municipal Associations can participate in the meetings of the IT Planning Council in an advisory capacity through a total of three (one each) designated representatives. The KSV are involved in the nomination of representatives for FITKO's municipal body and can, in theory, also act as such themselves. For example, the German Association of Towns and Municipalities comprises one of three representatives for towns and municipalities in the FITKO municipal body. On a purely representative basis, the German Association of Cities and the German Association of Rural Districts are also represented on behalf of the cities and counties. The German Association of Rural Districts is also a member of the ACS[233].

Kommunalgremium des IT-Planungsrates (Municipal Committee of the IT Planning Council, own translation)

A municipal committee of the IT Planning Council was established in 2020 under the chairmanship of FITKO. It is meant to perform functions in the area of municipal IT needs management, query municipal IT needs and establish a communication and information platform between FITKO and municipalities in the area of federal IT. As a result, the committee is also involved in the operational implementation of the "Onlinezugangsgesetz" (Online Access Act, OZG, own translation) to improve online access to administrative services. Hence, the Municipal Committee acts as an advisory body at the strategic level to the IT Planning Council and reports to it regularly through the FITKO. In addition to monthly virtual meetings, biannual face-to-face meetings are scheduled.

The municipal committee (14 members in total) comprises three representatives from each of the counties, cities and municipalities including their respective central municipal association, three representatives from Vitako and two representatives from the KGSt[234].

233 BSI, Empfehlungen bei IT-Angriffen auf kommunale Verwaltungen.
BSI, IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung.
Deutscher Landkreistag, Bundesvereinigung der kommunalen Spitzenverbände.
Deutscher Landkreistag, Der Verband.
Deutscher Städtetag, Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen.
DStGB, Wir über uns.
IT-Planungsrat, Zusammensetzung des IT-Planungsrats.
Schubert & Klein, Kommunale Spitzenverbände.

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

About Stiftung Neue Verantwortung

Stiftung Neue Verantwortung (SNV) is a non-profit think tank at the intersection of technology and society. At SNV's core is a methodology of collaborative development of policy proposals and analyses. SNV experts do not work alone – they develop and test ideas together with representatives from politics and public administration, technology companies, civil society and academia. Our experts work independently of interest groups and political parties. We guarantee our independence through diversified financing, comprised of contributions from different foundations, state and corporate actors.

About the Authors

Rebecca Beigel is a Project Manager for international cybersecurity policy at Stiftung Neue Verantwortung. Her work focuses on German cybersecurity policy and on cybersecurity exercises in country-specific contexts.

Dr. Sven Herpig is the Head for International Cybersecurity Policy. At SNV, Sven primarily deals with Germany's cybersecurity policy, government hacking (including the "Bundestrojaner") and IT vulnerability management, as well as election security in interconnected societies, attacks on machine-learning applications, and the European Union's resilience strategy.

Christina Rupp is a Project Assistant for International Cybersecurity Policy at Stiftung Neue Verantwortung. Her research interests lay in cyber diplomacy and cyber foreign policy, in particular international norms for responsible behavior in cyberspace.

Contact the Authors:

Rebecca Beigel
Project Manager International Cybersecurity Policy
rbeigel@stiftung-nv.de
+49 (0) 30 403 676 983

Dr. Sven Herpig
Head of International Cybersecurity Policy
sherpig@stiftung-nv.de
+49 (0) 30 81 45 03 78 91

Christina Rupp
Project Assistant International Cybersecurity Policy
crupp@stiftung-nv.de

Imprint

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

Translator and Editor:
Austin Davis