December 2021 · Christina Rupp & Dr. Sven Herpig

Germany's Cybersecurity Architecture

Translation of the 7th German Edition

(October 2021)

Supported by the Data Science Unit:
Anna Semenova & Pegah Maham

Stiftung Neue Verantwortung

Think Tank at the Intersection of Technology and Society

Table of Contents

1. Background and Methodology

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 transpired since then: Cybersecurity has become a core part of German security and defense 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 2016 strategy[3], nor the recently updated 2021 strategy[4], 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[5] in November 2020 within the framework of its National Cyber Security Pact. 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[6]. In this respect, this publication therefore seeks to make a contribution within the framework of Stiftung Neue Verantwortung's policy work on cybersecurity[7]. 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.

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, Cyber-Sicherheitsstrategie für Deutschland 2021.
5 Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland.
6 Julia Schuetze, Warum dem Staat IT-Sicherheitsexpert:innen fehlen.
7 Stiftung Neue Verantwortung, International Cybersecurity Policy.

A country's cybersecurity architecture includes all actors – government agencies, platforms, organizations, etc. – that are part of the ecosystem according to the national definition of cybersecurity (policy). In this publication, we only list the governmental part of the cybersecurity architecture, that means all governmental and directly related actors.

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.

Within the current version, the level of the United Nations has been added. Moreover, necessary adjustments, updates, and additions have been made on the other levels. Other international actors, 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 regarding additional information not included in these pages. Please contact Christina Rupp with suggestions for changes or additions. Corrections to the current version are published on the corresponding website in the form of a "bug tracker".

This document will be periodically updated in order to account for the latest developments and any additional enhancements to Germany's cybersecurity architecture. The next update will be published in March/April 2022.

This publication is a translation that is based on the current 7th edition of the German versions. The earlier editions in German (and 6th in English) 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	German / English
7th edition	10/2021	Sven Herpig	Christina Rupp	German / English *Supported by the Data Science Unit: Anna Semenova & Pegah Maham*

CYBERSECURITY ARCHITECTURE OF GERMANY

UN
EUROPEAN UNION
FEDERAL LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
NATO

UNSC UNGA ECOSOC
GGE OEWG
UNDESA UNOCT UNODC UNODA UNIDIR UNDP UNCTAD ITU
IGF UNGIS DTN UN OICT UNITAR UNICRI
UNISSIG UNICC

EAD Council ER EK NAC
EUMC INTCEN PSK EVA GD CONNECT GD DIGIT GD HOME GD JRC GD RTD JCU Europol ENISA Eurojust CEPOL eu-LISA EDSB CDC SC CDMB C3B MC
EUMS INT ESVK EU Hybrid Fusion Cell CMPD HWPCI ECCC CERT-EU ERCC ECSO EC3 ISG C3M ISG CHT EA Hybrid CoE JISD ESCD NCIA ACO ACT
PESCO NIS Cooperation Group Horizon 2020 TGG ECCG OLAF EUCTF ICTAC ECTEG MeliCERTes CSIRTs Netzwerk EJN EJCN EJTN NCISG NCI Academy NCIRC NCSC CyOC NS-O CCDCOE
CIDCC CyCLONe NIS Platform EU CyberNet SOG-IS EGC group Gruppe der Interessenträger für die Cybersicherheitszertifizierung SKI-Kontaktgruppe cPPP ENISA AG TF-CSIRT EUISS

Cyber-SR IT-Rat
BMG AA BMVI BMI BMJV BMVg BKAmt BMBF BMWi BMZ BMF
BAMAD BAAINBw BPol BBK BND Bw BfDI BNetzA ZKA BaFin ITZBund BDBOS BKartA
DAkkS SprinD BWI CIHBw Cyberagentur BAKS UniBw SWP DsiN TISiM GIZ vzbv
Forschungsrahmenprogramm zum auf IT-Sicherheit „Digital. Sicher. Souverän." Nationaler Pakt Cybersicherheit Cyber Security Cluster Bonn gematik G4C UP KRITIS Initiative Wirtschaftsschutz GMLZ CODE Kompetenz- und Forschungszentren für IT-Sicherheit Initiative IT-Sicherheit in der Wirtschaft Nationaler CERT-Verbund ITSMIG Bündnis für Cybersicherheit
KdoCIR ZITiS BKA BfV
BSI
Cyber-Reserve KdoStratAufkl KdoITBw GLZ CIR LZ BSOC CERT-Bund ACS CSN Cyber-AZ

Dataport CERT Nord VCV IT-PLR IMK FITKO Sicherheitskooperation Cybercrime
BW BY BE BB HB HH HE MV NI NW RP SL SN ST SH TH
IM BW StMD SenInnDS MIK Senator:in für Finanzen SK [HH] HMdIS MEID MV MI IM NRW MASTD SK [SL] SK [SN] Ministerium der Finanzen Sachsen-Anhalt MELUND SH TFM
CSBW StMFH CIO [BE] CIO [BB] CIO [HB] CIO [HH] Hessisches Ministerium für Digitale Strategie und Entwicklung CIO [MV] CIO [NI] MWIDE NRW CIO [RP] Ministerium für Finanzen und Europa CIO [SN] CIO [ST] CIO [SH] CIO [TH]
CIO [BW] StMI CISO [BE] CISO [BB] CISO [HB] CISO [HH] Hessen3C CISO [MV] CISO [NI] CIO [NW] CISO [RP] CIO [SL] CISO [SN] CISO [ST] CISO [SH] CISO [TH]
CISO [BW] LSI LfV [BE] LfV [BB] LfV [HB] LfV [HH] CIO [HE] LfV [MV] LfV [NI] CISO [NW] LfV [RP] CISO [SL] LfV [SN] LfV [ST] LfV [SH] LfV [TH]
LfV [BW] CIO [BY] ITDZ Berlin ZIT-BB ZAC [HB] ZAC [HH] CISO [HE] DVZ M-V IT.N LfV [NW] LDI [RP] LfV [SL] SID ZAC [ST] ZAC [SH] TLRZ
BITBW CISO [BY] Berlin-CERT CERT-Brandenburg LfDI [HB] HmbBfDI LfV [HE] CERT M-V N-CERT IT.NRW CERT-rlp IT-DLZ [SL] SAX.CERT LfD [ST] ULD Thüringen CERT
CERT BWL LfV [BY] CDC-Lv ZAC [BB] HZD ZAC [MV] ZAC [NI] CERT NRW ZAC [RP] ZAC [SL] ZAC [SN] 4C ITVSH ZAC [TH]
ZAC [BW] IT-DLZ [BY] ZAC [BE] LDA CERT [HE] LfDI [MV] LfD [NI] ZAC [NW] LfDI [RP] LfDI [SL] Sächs.DSDG TLfDI
LfDI [BW] Bayern-CERT BlnBDI RIO-Ausschuss ZAC [HE] EMERGE IoT Cybersicherheitsbündnis LDI [NW] LZC Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken AG IS
Cyberwehr ZAC [BY] Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin CCC HBDI Netzwerweis.de Digitalagentur Niedersachsen DIGITAL SICHER NRW SN4C
IT-Rat Baden-Württemberg BayLfD IT-Rat Brandenburg ZIT Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock Cybercrime-Kompetenzzentrum ZCS
SITiF BW Cyberabwehr Bayern Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datenkriminalität Cottbus Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen
Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität CAZ ZAC NRW
ZCB
Kompetenzzentrum Cybercrime
ZD.B

Kommunalgremium IT-PLR
KGSt KSV Vitako IT-SiBe-Forum

Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel

Version: October 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 one's are being deliberately used throughout this publication 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.

Within the following list, own translations of actors are listed with quotation marks. Institutions written in italics are either still in the planning process or are currently in development.

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
4C	"Cybercrime Competence Center"	Cybercrime Competence Center
AA	Federal Foreign Office	Auswärtiges Amt
ACO	Allied Command Operations	
ACS	"Alliance for Cybersecurity"	Allianz für Cyber-Sicherheit
ACT	Allied Command Transformation	
AG IS	"Information Security Working Group"	Arbeitsgruppe Informationssicherheit
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

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
BAMAD	Federal Office for Military Counter-Intelligence	Bundesamt für den Militärischen Abschirmdienst
Bayern-CERT	Computer Emergency Response Team Bavaria	Computer Emergency Response Team Bayern
BayLfD	"Bavarian State Commissioner for Data Protection"	Bayerische:r Landesbeauftrag-te:r für den Datenschutz
BBK	Federal Office of Civil Protection and Disaster Assistance	Bundesamt für Bevölkerungs-schutz und Katastrophenhilfe
BDBOS	Federal Agency for Public Safety Digital Radio	Bundesanstalt für den Digital-funk der Behörden und Organisa-tionen mit Sicherheitsaufgaben
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 Informationsfreiheit
BfV	Domestic Intelligence Service of the Federal Republic of Germany	Bundesamt für Verfassungsschutz
BITBW	State Authority IT Baden-Württemberg	Landesoberbehörde IT Baden-Württemberg
BKA	Federal Criminal Police Office	Bundeskriminalamt
BKAmt	Federal Chancellery	Bundeskanzleramt
BKartA	Federal Cartel Office	Bundeskartellamt
BlnBDI	"State Commissioner for Data Protection and Freedom of Information Berlin"	Berliner Beauftragte:r für Datenschutz und Informationsfreiheit
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

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
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
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
BSOC	"Federal Security Operations Center"	Bundes Security Operations Center
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"	Cyber-Allianz-Zentrum
CCC	Cyber-Competence-Center	Cyber-Competence-Center
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence	

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
CDC	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 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	"CERT North"	CERT Nord
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-Brandenburg	Computer Emergency Response Team Brandenburg	Computer Emergency Response Team Brandenburg
CERT-Bund	Computer Emergency Response Team for Federal Agencies	Computer Emergency Response Team der Bundesverwaltung
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
CIDCC	*Cyber and Information Domain Coordination Centre*	
CIHBw	Cyber Innovation Hub of the German Armed Forces	Cyber Innovation Hub der Bundeswehr

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
CIO [Federal State]	State Commissioner for Information Technology	Landesbeauftragte:r für Informationstechnologie
CIR	Cyber and Information Domain Service	Organisationsbereich Cyber- und Informationsraum
CISO [Federal State]	Chief Information Security Officer of the State Administration	Informationssicherheitsbeauftragte:r
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
cPPP	Contractual Public Private Partnership on Cybersecurity	
CSBW	*"Cybersecurity Agency Baden-Wuerttemberg"*	*Cybersicherheitsagentur Baden-Württemberg*
CSIRTs Netzwerk	Computer Security Incident Response Teams Network	Computer Security Incident Response Teams Netzwerk
CSN	"Cyber Security Network"	Cyber-Sicherheitsnetzwerk
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
Cyber-AZ	National Cyber Defence Centre	Nationales Cyber-Abwehrzentrum
Cybercrime-Kompetenzzentrum	"Cybercrime Competency Center"	Cybercrime-Kompetenzzentrum
Cyber-Reserve	"Military Cyber Reserve"	Cyber-Reserve
Cybersicherheitsbündnis	"Cybersecurity Alliance"	Cybersicherheitsbündnis
Cyber-SR	National Cyber Security Council	Nationaler Cyber-Sicherheitsrat
Cyberwehr	"Cyber Defence"	Cyberwehr
CyCLONe	Cyber Crisis Liaison Organisation Network	

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
CyOC	NATO Cyberspace Operations Centre	
DAkkS	German National Accreditation Body	Deutsche Akkreditierungsstelle
Dataport	Dataport	Dataport
Senator:in für Finanzen	"Finance Senator of the Free Hanseatic City of Bremen"	Der:die Senator:in für Finanzen Bremen
Dezernat Cybercrime der Staats-anwaltschaft Saarbrücken	"Cybercrime Department of the Public Prosecutor's Office of Saarbrücken"	Dezernat Cybercrime der Staats-anwaltschaft Saarbrücken
DIGITAL.SICHER.NRW	"Competence Center for Cybersecurity in the Economy"	Kompetenzzentrum für Cybersicherheit in der Wirtschaft
Digitalagentur Niedersachsen	"Digital Agency Lower Saxony"	Digitalagentur Niedersachsen
DsiN	"Germany Secure on the Internet e. V."	Deutschland sicher im Netz e.V.
DTN	United Nations Digital and Technology Network	
DVZ M-V	"Service Provider for the State Administration of Mecklen-burg-Western Pomerania"	DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern
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 Be-kämpfung 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
ECOSOC	United Nations Economic and Social Council	Wirtschafts- und Sozialrat der Vereinten Nationen

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
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	EMERGE IoT
ENISA	European Union Agency for Cybersecurity	Agentur der Europäischen Union für Cybersicherheit
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 CyberNet	EU Cyber Capacity Building Network	
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

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
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
Forschungsrahmenprogramm zur IT-Sicherheit "Digital. Sicher. Souverän."	"Research Framework Program on IT Security 'Digital. Secure. Sovereign.'"	Forschungsrahmenprogramm zur IT-Sicherheit "Digital. Sicher. Souverän."
G4C	German Competence Centre against Cyber Crime	German Competence Centre against Cyber Crime
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

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
GGE	Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security	
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH	Deutsche Gesellschaft für Internationale Zusammenarbeit
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 Interessenträger für die Cybersicherheitszertifizierung	Stakeholder Cybersecurity Certification Group	Gruppe der Interessenträger für die Cybersicherheitszertifizierung
HBDI	"State Commissioner for Data Protection and Freedom of Information Hesse"	Hessische:r Beauftragte:r für Datenschutz und Informationsfreiheit
Hessen3C	Hessen Cyber Competence Center	Hessen Cyber Competence Center
Hessisches Ministerium für Digitale Strategie und Entwicklung	"State Ministry for Digital Strategy and Development"	Hessisches Ministerium für Digitale Strategie und Entwicklung
HmbBfDI	"State Commissioner for Data Protection and Freedom of Information of the Free and Hanseatic City of Hamburg"	Hamburgische:r Beauftragte:r für Datenschutz und Informationsfreiheit der Freien und Hansestadt Hamburg
HMdIS	"State Ministry of the Interior and Sports"	Hessisches Ministerium des Innern und für Sport
Horizon 2020	Horizon 2020	
HWPCI	Horizontal Working Party on Cyber Issues	
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats	
HZD	"Hessian Central Office for Data Processing"	Hessische Zentrale für Datenverarbeitung
ICTAC	ICT Advisory Committee of the EU Agencies	

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
IGF	Internet Governance Forum	
IM BW	"Ministry of the Interior, Digitalization and Migration Baden-Wuerttemberg"	Ministerium des Inneren, für Digitalisierung und Migration Baden-Württemberg
IM NRW	"Ministry of the Interior of North Rhine-Westphalia"	Ministerium des Innern des Landes Nordrhein-Westfalen
IMK	Conference of Interior Ministers	Innenministerkonferenz
Initiative IT-Sicherheit in der Wirtschaft	"Initiative IT Security in the Economy"	Initiative IT-Sicherheit in der Wirtschaft
Initiative Wirtschaftsschutz	"Initiative for Economic Protection"	Initiative Wirtschaftsschutz
INTCEN	EU Intelligence Analysis Centre	Zentrum für Informations-gewinnung und -analyse
ISG C3M	Inter-Service Group "Community Capacity in Crisis-Management"	
ISG CHT	Inter-Service Group "Countering Hybrid Threats"	
IT.N	"IT Lower Saxony"	IT.Niedersachsen
IT.NRW	"State Office Information and Technology North Rhine-Westphalia"	Landesbetrieb Information und Technik Nordrhein-Westfalen
IT-DLZ [BY]	"IT Service Center of the Free State of Bavaria"	IT-Dienstleistungszentrum des Freistaats Bayern
IT-DLZ [SL]	"State Office for IT Services Saarland"	Landesamt für IT-Dienstleistungen Saarland
ITDZ Berlin	"IT Service Center Berlin"	IT-Dienstleistungszentrum Berlin
IT-PLR	IT Planning Council	IT-Planungsrat
IT-Rat	"IT Council"	IT-Rat
IT-Rat Baden-Württemberg	"IT Council Baden-Wuerttemberg"	IT-Rat Baden-Württemberg

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
IT-Rat Brandenburg	"IT Council Brandenburg"	IT-Rat Brandenburg
IT-SiBe-Forum	"Forum of Municipal IT Security Officers"	IT-SiBe-Forum
ITSMIG	IT Security made in Germany	IT Security made in Germany
ITU	International Telecommunication Union	Internationale Fernmeldeunion
ITVSH	"IT Network Schleswig-Holstein"	IT-Verbund Schleswig-Holstein
ITZBund	Federal Information Technology Centre	Informationstechnikzentrum Bund
JCU	*Joint Cyber Unit*	
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
Kompetenzzentrum Cybercrime	"Cybercrime Competency Center"	Kompetenzzentrum Cybercrime
Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen	"Coordination Office for Cyber Security North Rhine-Westphalia"	Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen
KSV	"Central Municipal Associations"	Kommunale Spitzenverbände
LDA	"State Commissioner for Data Protection and for the Right to Inspect Files Brandenburg"	Landesbeauftragte:r für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
LDI [NW]	"State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia"	Landesbeauftragte:r für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
LDI [RP]	"State Office Data and Information"	Landesbetrieb Daten und Information
LfD [Federal State]	"State Commissioner for Data Protection"	Landesbeauftragte:r für den Datenschutz
LfDI [Federal State]	"State Commissioner for Data Protection and Freedom of Information"	Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit Baden-Württemberg
LfV [Bundesland]	State Offices for the Protection of the Constitution	Landesbehörde für Verfassungs-schutz Brandenburg
LSI	"State Office for Information Security of Bavaria"	Landesamt für Sicherheit in der Informationstechnik Bayern
LZ	"National IT Situation Centre"	Nationales IT-Lagezentrum
LZC	"Central State Office for Cybercrime"	Landeszentralstelle Cybercrime
MASTD	"Ministry of Labor, Social Affairs, Transformation and Digitalization"	Ministerium für Arbeit, Soziales, Transformation und Digitalisierung
MC	NATO Military Committee	NATO-Militärausschuss
MEID MV	"State Ministry of Energy, Infrastructure and Digitalization of Mecklenburg-Western Pomerania"	Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern
MeliCERTes	MeliCERTes	
MELUND SH	"Ministry of Energy, Agriculture, the Environment, Nature and Digitalization"	Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung Schleswig-Holstein
MI	"State Ministry of the Interior and Sport of Lower Saxony"	Niedersächsisches Ministerium für Inneres und Sport
MIK	"Brandenburg Ministry of the Interior and Municipal Affairs"	Ministerium des Innern und für Kommunales Brandenburg
Ministerium der Finanzen Sachsen-Anhalt	"Ministry of Finance Saxony-Anhalt"	Ministerium der Finanzen Sachsen-Anhalt

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
Ministerium für Finanzen und Europa	"Ministry of Finance and Europe of Saarland"	Ministerium für Finanzen und Europa Saarland
MWIDE NRW	"Ministry of Economy, Innovation, Digitization and Energy of North Rhine-Westphalia"	Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
NAC	North Atlantic Council	Nordatlantikrat
Nationaler CERT-Verbund	"National Cybersecurity Pact"	Nationaler CERT-Verbund
N-CERT	Computer Emergency Response Team Lower Saxony	Computer Emergency Response Team Niedersachsen
NCI Academy	NCI Academy	
NCIA	NATO Communications and Information Agency	
NCIRC	NATO Computer Incident Response Capability	
NCISG	NATO Communication and Information Systems Group	
NCSC	NATO Cyber Security Centre	
Netzverweis.de	Netzverweis.de	Netzverweis.de
NIS Cooperation Group	NIS Cooperation Group	Kooperationsgruppe unter der NIS-Richtlinie
NIS Platform	NIS Public-Private Platform	
NPCS	National Cybersecurity Pact	Nationaler Pakt Cybersicherheit
NS-O	NATO School Oberammergau	
OEWG	Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security	
OLAF	European Anti-Fraud Office	Europäisches Amt für Betrugsbekämpfung
PESCO	Permanent Structured Cooperation	Ständige Strukturierte Zusammenarbeit

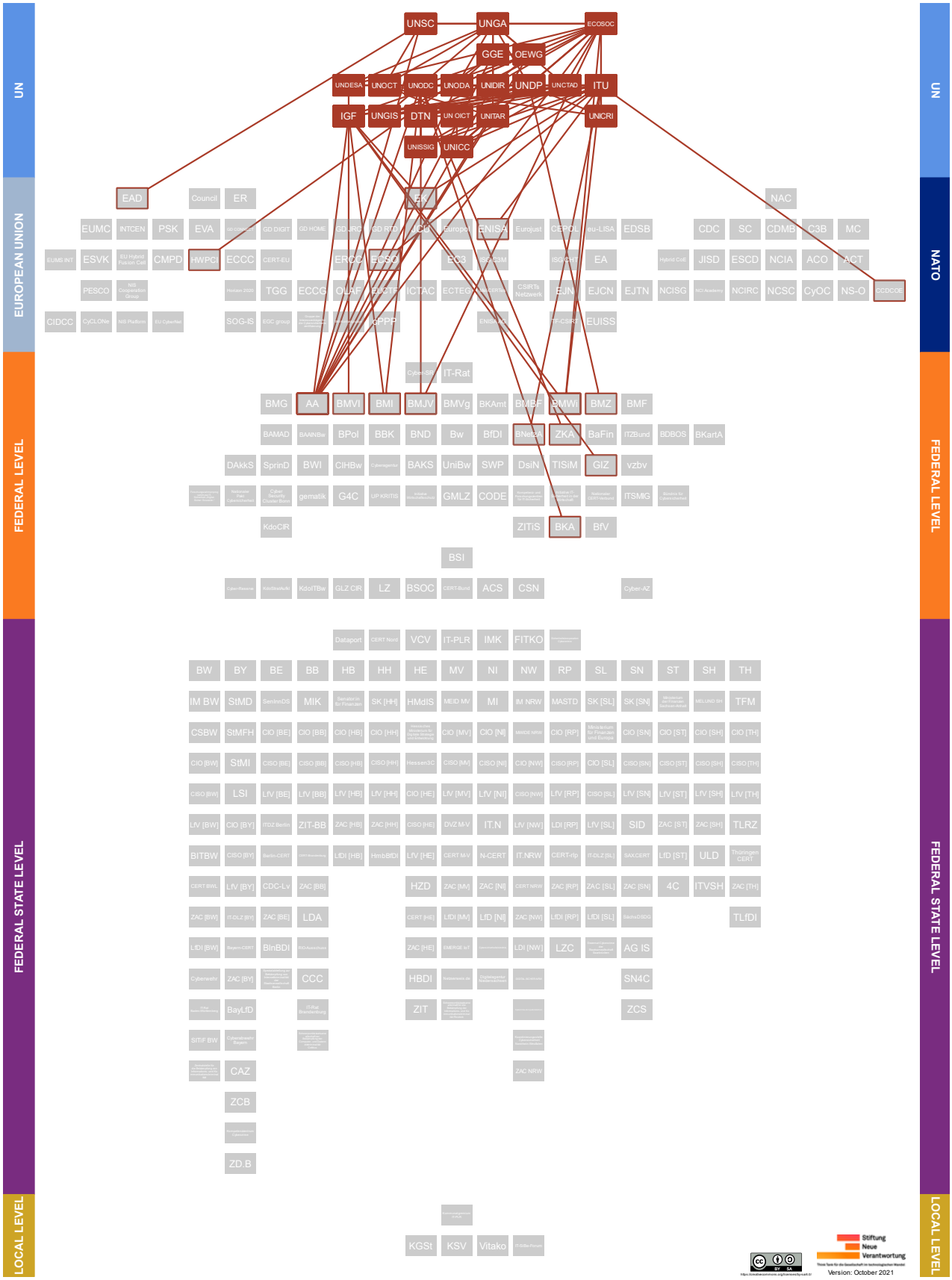
Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
PSK	Political and Security Committee	Politisches und Sicherheitspolitisches Komitee
RIO-Ausschuss	"Committee of Departmental Information Officers"	Ausschuss der Ressort Information Officer
SächsDSDG	"State Commissioner for Data Protection Saxony"	Sächsische:r Datenschutzbeauftragte:r
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
SenInnDS	"Senate Department for the Interior and Sport"	Senatsverwaltung für Inneres und Sport Berlin
Sicherheitskooperation Cybercrime	"Security Cooperation Cybercrime"	Sicherheitskooperation Cybercrime
SID	"State Enterprise Saxon Information Technology Services"	Staatsbetrieb Sächsische Informatik Dienste
SITiF BW	"IT Security Center of the Financial Administration Baden-Württemberg"	Sicherheitszentrum IT der Finanzverwaltung Baden-Württemberg
SK [Federal State]	"State Chancellery"	Staatskanzlei
SK [HH]	"Senate Chancellery Hamburg"	Senatskanzlei Hamburg
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 Visualisation	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	Federal Agency for Disruptive Innovation	Agentur für Sprunginnovationen
StMFH	"Bavarian State Ministry of Finance and Home Affairs"	Bayerisches Staatsministerium der Finanzen und für Heimat
StMI	"Bavarian State Ministry of the Interior, for Sport and Integration"	Bayerisches Staatsministerium des Innern, für Sport und Integration
SWP	German Institute for International and Security Affairs	Stiftung Wissenschaft und Politik
TF-CSIRT	Reference Incident Classification Taxonomy Task Force	Reference Incident Classification Taxonomy Task Force
TFM	"State Ministry of Finance of Thuringia"	Thüringisches Finanzministerium
TGG	Taxonomy Governance Group	Taxonomy Governance Group
ThüringenCERT	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
TLfDI	"State Commissioner for Data Protection and Freedom of Information Thuringia"	Thüringische:r Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit
TLRZ	"Thuringian State Computer Center"	Thüringer Landesrechenzentrum
ULD	"Independent State Center for Data Protection Schleswig-Holstein"	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UN OICT	United Nations Office of Information and Communications Technology	

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
UNCTAD	United Nations Conference on Trade and Development	Konferenz der Vereinten Nationen für Handel und Entwicklung
UNDESA	United Nations Department of Economic and Social Affairs	Hauptabteilung Wirtschaftliche und Soziale Angelegenheiten der Vereinten Nationen
UNDP	United Nations Development Programme	Entwicklungsprogramm der Vereinten Nationen
UNGA	United Nations General Assembly	UN-Generalversammlung
UNGIS	United Nations Group on the Information Society	
UniBw	Universities of the German Federal Armed Forces	Universitäten der Bundeswehr
UNICC	United Nations International Computing Centre	
UNICRI	United Nations Interregional Crime and Justice Research Institute	UN-Institut für interregionale Kriminalitäts- und Justizforschung
UNIDIR	United Nations Institute for Disarmament Research	UN-Institut für Abrüstungsforschung
UNISSIG	United Nations Information Security Special Interest Group	
UNITAR	United Nations Institute for Training and Research	Ausbildungs- und Forschungs-institut der Vereinten Nationen
UNOCT	United Nations Office of Counter-Terrorism	
UNODA	United Nations Office for Disarmament Affairs	Büro der Vereinten Nationen für Abrüstungsfragen
UNODC	United Nations Office on Drugs and Crime	Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung
UNSC	United Nations Security Council	UN-Sicherheitsrat

Abbreviations/Terms Used in Visualisation	Official English Title/Own Translation	Official German Title
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
vzbv	Federation of German Consumer Organisations	Bundesverband der Verbraucherzentralen und Verbraucherverbände
ZAC [Federal State]	"Central Contact Points for Cybercrime of the Police Forces of the Federal States for the Economy"	Zentrale Ansprechstelle Cybercrime 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
ZD.B	"Center for Digitization Bavaria"	Zentrum Digitalisierung.Bayern
Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität	"Central Office for the Fight against Information and Communication Crime"	Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität
ZIT	"Central Office for Combating Internet and Computer Crime"	Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität
ZIT-BB	"Brandenburg IT Service Provider"	Brandenburgischer IT-Dienstleister
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 UN level



Ausbildungs- und Forschungsinstitut der Vereinten Nationen (United Nations Institute for Training and Research, UNITAR, official translation)
As a UN training and research institution, UNITAR provides training opportunities to improve global and national decision-making processes and actions towards building a better future and implementing the 2030 Agenda. UNITAR's activities are aimed at institutions and individuals from both the public and private sectors. UNITAR also offers training and educational programs in the field of cyber security. These deal with, among other things, warfare in cyberspace and international humanitarian law, cyber operations and human rights, or digital diplomacy. Together with other organizations, UNITAR hosts a "Cyber Policy and United Nations Negotiations Fellowship" for women from around the world.

UNITAR is a joint research and training institution of the UNGA and the ECOSOC within the UN system. UNITAR uses UNICC services and is a signatory to the UN Global Counter-Terrorism Coordination Compact coordinated by UNOCT. Germany is represented on UNITAR's Board of Trustees by its Ambassador (AA) to the UN in Geneva[8].

Büro der Vereinten Nationen für Abrüstungsfragen (United Nations Office for Disarmament Affairs, UNODA, official translation)
UNODA supports global as well as regional measures and efforts that contribute to controlled disarmament, particularly of weapons of mass destruction. These include, for example, the provision of objective information, confidence-building initiatives in military affairs, or addressing the humanitarian impact of new weapons technologies. In the area of cybersecurity, UNODA inter alia offers a free online course on cyber diplomacy and has published a commentary on voluntary norms for responsible state behavior in the use of ICT. Together with the Cybersecurity Tech Accord, UNODA has launched a competition (Apps 4 Digital Peace) to encourage the development of applications capable of increasing stability in cyberspace and reducing potential for conflict and malicious user behavior.

UNODA is part of the UN Secretariat and among other things supports the work of UNGA and DISEC on issues related to disarmament in terms of content and organization. UNODA has provided the secretariat for the GGE's and has also supported the OEWG organizationally. It offers financial support to UNIDIR and is a signatory to the UN Global Counter-Terrorism Coordination Compact coordinated by UNOCT. The AA supports selected UNODA projects and trust funds financially[9].

8 GIP Digital Watch, United Nations Institute for Training and Research.
United Nations Institute for Training and Research, Cyber Policy and United Nations Negotiations Fellowship.
United Nations Institute for Training and Research, The Board of Trustees.
United Nations Institute for Training and Research, The Institute.

9 Cybersecurity Tech Accord, Cybersecurity Tech Accord announces new contest in partnership with the UN Office of Disarmament Affairs.
Federal Foreign Office, Jahresabrüstungsbericht 2020.
United Nations Office for Disarmament Affairs, About Us.
United Nations Office for Disarmament Affairs, Cyberdiplomacy.
United Nations Office for Disarmament Affairs, Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary.

Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (United Nations Office on Drugs and Crime, UNODC, official translation)
UNODC's mission is to combat threats based on transnational organized crime, corruption, terrorism as well as drug trafficking and use worldwide by providing practical assistance and promoting transnational action. In the context of fighting crime, UNODC is also committed to the fight against cybercrime. To this end, it aims to contribute to, among other things, awareness and capacity building, the development of national structures and criminal justice systems, and international cooperation. In implementing and operationalizing its projects, UNODC's commitment is supported by the "Global Programme on Cybercrime". In the past, UN Member States in Central America, North and East Africa, the Middle East, Southeast Asia, and the Pacific constituted geographic focal points of the program. The "Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime" (IEG), which has been meeting annually in recent years, is tasked with preparing a comprehensive study on cybercrime. Its findings are among other things intended to help examine the strengthening of existing or the establishment of new national, international, or other response options. In addition to the IEG, UNODC also acts as the secretariat of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. On its website, the UNODC also provides a "Cybercrime Repository" that contains databases on relevant legal cases, legislation, and lessons learned.

UNODC is part of the UN Secretariat and the CCPCJ of ECOSOC acts as its governing body. It also cooperates with the ITU in the area of cybercrime and is listed as a partner of ITU's GCI. UNODC participates in the DTN, UNGIS, and UNISSIG and is a signatory to the UN Global Counter-Terrorism Coordination Compact coordinated by UNOCT. The Ad Hoc Committee is a subsidiary body of UNGA. Representatives of the AA, the BKA, the BMI, the BMJV, and the ZKA have attended meetings of the IEG as part of the German delegations in various combinations. The BMJV has commented on a draft of the Comprehensive Study on Cybercrime on behalf of Germany. Germany

is one of the largest contributors to UNODC's budget, which is being financed – at least in part – from the budget of the AA[10].

Entwicklungsprogramm der Vereinten Nationen (United Nations Development Programme, UNDP, official translation)
UNDP works in 170 countries on sustainable development, democratic governance, peacebuilding, and resilience to climate and disasters. For example, UNDP helps countries build institutional capacity and develop policies with the overarching goal of contributing to reducing poverty and inequality. Upon request, UNDP also provides cybersecurity assistance to developing countries. This includes training and other services in risk assessment and mitigation, resilience, and policies, standards, and certification. In addition, UNDP can help build local capacity, skills, and procedures that become necessary in responding to cyber incidents. Together with FIRST, UNDP hosts an annual "Cybersecurity for Developing Nations" conference.

UNDP reports to the UNGA through the ECOSOC. A UNDP representative serves on the UNICRI Board of Trustees. UNDP participates in the DTN, UNGIS, and UNISSIG and is a signatory to the UN Global Counter-Terrorism Coordination Compact coordinated by UNOCT. It is one of the users of UNICC's Common Secure Threat Intelligence. Germany is a member of the UNDP Executive Board and the largest contributor to the UNDP budget, which originates from the budget of the BMZ[11].

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

11 Federal Foreign Office, ABC der Vereinten Nationen.
Federal Ministry of Finance, Bundeshaushaltsplan 2021 Einzelplan 23: Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung.
Paul Raines, UNDP Cybersecurity Assistance for Developing Nations.
United Nations Development Programme, About us.
United Nations Development Programme, Members of the Executive Board.
United Nations Development Programme, Top Contributions.
United Nations Development Programme, UNDP and FIRST to host third annual Cybersecurity for Developing Nations Conference.

Group of Governmental Experts on Advancing responsible State Behavior in Cyberspace in the Context of International Security (GGE)

The GGE's are temporary working groups of selected national governmental experts that discuss, among other things, the way international law applies to the use of ICT, norms for responsible state behavior in cyberspace, confidence-building measures, and capacity building. Over the years, the membership, which is made up equally of UN regional groups, has grown from 15 to 25 members. Since 2004, six GGE's have been convened, and four of them have agreed on a final report. In its 2013 report, the group affirmed the applicability of international law to cyberspace. The subsequent 2015 report established a set of 11 voluntary and non-binding norms to guide the behavior of states. These inter alia include respect for human rights and privacy, vulnerability reporting, refraining from operations on critical infrastructure, CERTs, and ICT misuse. Currently, there is no draft aiming at the establishment of a new GGE.

The establishment of the GGE's was mandated by the DISEC of the UNGA. The groups were substantially supported by UNODA, which has also provided their secretariat. In the past, representatives of UNIDIR have briefed the GGE's. The last GGE also held a regional consultation with EU Member States in the framework of the HWPCI. Germany has been part of all GGE's to date and has been represented by diplomats of the AA. A representative of the AA chaired the group in 2016/2017[12].

Hauptabteilung Wirtschaftliche und Soziale Angelegenheiten der Vereinten Nationen (United Nations Department of Economic and Social Affairs, UNDESA, official translation)

UNDESA is part of the UN Secretariat and works in the areas of analysis, capacity building, and standard-setting to support UN Member States in achieving their goals in economic, social, and environmental matters. It hosts a Department of Public Institutions and Digital Government (DPIDG) to which a Digital Government Branch (DGB) is subordinated. The head of UNDESA identifies policy and legal frameworks for privacy and cybersecurity as one of 10 key elements to sustainable and resilient recovery from the COVID-19 pandemic. Every two years, UNDESA publishes a study

12 Matthias Kettemann & Alexandra Paulus, Ein Update für das Internet. Reform der globalen digitalen Zusammenarbeit 2021.
United Nations General Assembly (A/70/174), Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.
United Nations Office for Disarmament Affairs, Advance Copy: Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security.
United Nations Office for Disarmament Affairs, Factsheet: Developments in the Field of Information and Telecommunications in the Context of International Security.
United Nations Office for Disarmament Affairs, Group of Governmental Experts.
United Nations Office for Disarmament Affairs, Joint Contribution: The future of discussions on ICTs and cyberspace at the UN.
United Nations Office for Disarmament Affairs, Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.
United Nations Office for Disarmament Affairs, The UN GGEs on ICTs and International Security.

and ranking on the state of e-government of all UN Member States. Therein, digital and cybersecurity laws are being employed as an indicator among many other aspects.

UNDESA is part of the UN Secretariat and supports deliberations to the UNGA and the ECOSOC bodies. A subordinate unit to the DGB provides the secretariat of the IGF. UNDESA cooperates with the ITU in cybersecurity matters and supports the development of the GCI. It is associated as an observer with the UN Global Counter-Terrorism Coordination Compact coordinated by UNOCT[13]*.*

Internationale Fernmeldeunion (International Telecommunication Union, ITU, official translation)
The ITU is a specialized agency of the UN responsible for information and communications technologies. Among other things, it develops technical standards for the ICT sector, on which the global telecommunications system and the majority of all Internet connections are based and mediates their international adoption. It also strives to remove barriers to the access and use of ICT worldwide, for example through technological knowledge transfer. In addition to states, the ITU also works with private-sector players. Cybersecurity constitutes one of ITU's thematic priorities. The ITU has published a guide for developing a national cybersecurity strategy. It maintains a corresponding repository of strategies that have already been adopted. In addition, ITU assists UN Member States in establishing Computer Incident Response Teams. Annually, the ITU organizes regional and a global cybersecurity exercise ("CyberDrill") aimed at building capacity, response capabilities, and regional cooperation. Periodically, the ITU issues a Global Cybersecurity Index (GCI), which measures country engagement in cybersecurity through legal, technical, and organizational indicators, as well as capacity development and cooperation.

The ITU is an autonomous UN specialized agency whose work is coordinated through ECOSOC and UNSCEB. UNCTAD and the CCDCOE participated as partners in the development of the national cybersecurity strategy guide. ITU's partners listed in the context of the GCI include UNDESA, UNODC, and ECSO. A cooperative agreement exists with the UNODC in the area of cybercrime, and ITU also works with UNDESA on other cybersecurity issues. Another cooperative agreement exists between the ITU and UNICRI to strengthen exchanges on best practices on cybersecurity, misuse of technology, and cybercrime. UNOCT's UNCCT is participating in CyberDrill. ITU par-

13 Division for Public Institutions and Digital Government, Digital Government.
Division for Public Institutions and Digital Government, Organisational Chart.
Elliott Harris, Ten Key Elements for Accelerating Digital Transformation for Sustainable and Resilient Recovery from COVID-19.
GIP Digital Watch, United Nations Department of Economic and Social Affairs.
United Nations Department of Economic and Social Affairs, UN E-Government Surveys.

ticipates in the DTN, the UNGIS, and the UNISSIG. ITU can participate in meetings of the MAG of the IGF and draws on services, including the Common Secure Threat Intelligence, from UNICC. Together with the EK, the ITU collaborates on the harmonization of ICT policies within ACP countries. With ENISA, the ITU among other things exchanges information on best practices and draws on its expertise in the European context. The ITU lists the BMWi and the BNetzA as participating member state institutions from Germany[14].

Internet Governance Forum (IGF)

The annual Internet Governance Forum is a discussion and exchange platform for a wide range of stakeholders from government, business, and civil society to discuss the development and use of the Internet across sectors and interests. This should contribute to an exchange of information and common understanding between stakeholders, the identification of emerging issues, and the availability of the Internet in developing countries. The substantial program and schedule of the IGF is determined by a Multistakeholder Advisory Group (MAG) composed of representatives of national governments, as well as the private sector, civil society, scientific and technical stakeholders from all UN regional groups. In the framework of the IGF, also events and workshops on cybersecurity are held. In addition to the global IGF, there are also initiatives for regionally and nationally held IGFs (NRIs).

UNDESA provides the secretariat of the IGF. The IGF Secretariat has participated in the OEWG deliberations by submitting a position paper. The MAG currently includes a representative of the GIZ. In addition, representatives of the BMWi, the EK, the ITU, and UNCTAD may participate in MAG meetings. The German government is one of the largest contributors to the IGF Trust Fund, which is paid – at least in part – from the budget of the BMWi. The EK is an institutional partner of the European Dialogue on Internet Governance (EuroDIG), which takes place at the European level. Representa-

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

tives of the AA, BMI, BMVI, and BMWi are represented on the Steering Committee of the German IGF (IGF-D)[15].

Konferenz der Vereinten Nationen für Handel und Entwicklung (United Nations Conference on Trade and Development, UNCTAD, official translation)
UNCTAD supports developing countries at the national, regional and global levels, inter alia through analysis and technical assistance, in diversifying their economies, reducing financial volatility, and accessing digital technologies in order to embed them successfully and equitably in the international trade and economic system as well as promoting sustainable development in their respective countries. UNCTAD maintains a "Global Cyberlaw Tracker" which collects adopted and pending national legislation in the area of cybercrime, e-transactions, data protection and privacy, and consumer protection from all UNCTAD Member States.

UNCTAD reports to the UNGA and ECOSOC. UNCTAD participates in the DTN, UNGIS, and UNISSIG. UNCTAD may participate in meetings of the IGF's MAG. It makes use of services provided by the UNICC. UNCTAD participated as a partner in the guide issued by ITU on the development of a national cybersecurity strategy[16].

Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG)
Similar to the mandate of the GGE, the OEWG is a UN forum in which representatives of UN Member States discuss, among other things, international law, norms, capacity building, and confidence-building measures relating to ICT developments with possible implications for international security. All UN Member States can participate in the OEWG. In addition, other stakeholders, such as representatives of NGOs, academia, or businesses, are invited to apply to participate in intersessional meetings. The first OEWG adopted a consensus report in March 2021. Statements

15 European Dialogue on Internet Governance, About.
Federal Ministry of Finance, Bundeshaushaltsplan 2021 Einzelplan 09: Bundesministerium für Wirtschaft und Energie.
Internet Governance Forum, About IGF FAQs.
Internet Governance Forum, About the Internet Governance Forum.
Internet Governance Forum, Cyber.
Internet Governance Forum, Donors to the IGF Trust Fund.
Internet Governance Forum, MAG 2021 Members.
Internet Governance Forum, National IGF Initiatives.
Internet Governance Forum, Regional IGF Initiatives.
Internet Governance Forum Germany, Über uns.

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

and comments on draft reports by some UN Member States can be retrieved on the OEWG website or via UN Web TV. In December 2020, it was decided to establish a new OEWG for the years 2021-2025, which started its activities after the conclusion of the first OEWG.

The two OEWG's were established by resolutions of the UNGA. The IGF Secretariat participated in the OEWG deliberations by submitting a position paper. The UNODA managed applications for participation from other stakeholders. UNIDIR supports the work of the OEWG. Germany participated in meetings of the OEWG through representatives of the AA[17]*.*

Wirtschafts- und Sozialrat der Vereinten Nationen (United Nations Economic and Social Council, ECOSOC, official translation)

As one of the central UN bodies, ECOSOC is entrusted with international affairs in economic, social, cultural, educational, health, and related matters. Several bodies, such as the United Nations Economic Commission for Europe (UNECE) and the Commission on Crime Prevention and Criminal Justice (CCPCJ), are subordinate to ECOSOC, which also deal with cybersecurity-related issues as part of their mandates. For example, within the UNECE, one of five regional UN economic commissions, a sectoral initiative on cybersecurity has been established in the framework of its Working Group 6, which deals with regulatory cooperation and standardization policy. This initiative aims to contribute to the reduction of trade barriers as well as the promotion of competition through increased convergence of national technical regulations and the establishment of a common regulatory framework. On the other hand, the CCPCJ is a political decision-making body in the field of crime prevention and criminal justice, which, in addition to a forum function for knowledge and experience exchange among its Member States, aims to improve (inter)national measures to combat crime. On the recommendation of the CCPCJ, the ECOSOC has for example adopted a resolution to promote technical assistance, capacity building to strengthen national measures, and international cooperation to combat cybercrime. The CCPCJ prepares the United Nations Congress on Crime Prevention and Criminal Justice (UNCPCJ), which also discusses cybercrime and takes place every five years.

17 GIP Digital Watch, UN GGE and OEWG.
Secretariat of the Internet Governance Forum, Submission to the "Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security".
United Nations, The United Nations System.
United Nations General Assembly (A/AC.290/2021/CRP.2), Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report.
United Nations General Assembly (A/AC.290/2021/INF.1), Opened-ended Working Group on developments in the field of information and telecommunications in the context of international security, Third substantive session (8–12 March 2021): List of Participants.
United Nations General Assembly (A/RES/75/240), Resolution adopted by the General Assembly on 31 December 2020: Developments in the field of information and telecommunications in the context of international security.
United Nations Office of Disarmament Affairs, Open-ended Working Group.
United Nations Regional Information Centre, Die Charta der Vereinten Nationen.

The members of the ECOSOC are elected by the UNGA. The ECOSOC can provide information to the UNSC and assist it when requested. The UNDP reports to the UNGA through the ECOSOC. In the UN system, UNIDIR is a joint research and training institution of the UNGA and the ECOSOC. UNDESA supports, among other things, deliberations of ECOSOC bodies. The CCPCJ acts as steering body of the UNODC and has decided in favor of the establishment of an IEG on Cybercrime. UNCTAD reports to the ECOSOC, among others. The UNECE uses services provided by UNICC and participates in the DTN as well as the UNGIS. Germany is a member of the ECOSOC (until 2023) and the CCPCJ (also until 2023). In the past, representatives of the AA and the BMJV have participated in meetings of the CCPCJ. A representative of the "Physikalisch-Technische Bundesanstalt" (Federal Physical-Technical Institute, own translation), which is part of the BMWi, chairs Working Group 6 of the UNECE[18].

UN-Generalversammlung (United Nations General Assembly, UNGA, official translation)

The UN General Assembly is the main political organ of the UN with all-encompassing competence whose resolutions – except in budgetary matters – have no legally binding effect. The UNGA meets in a plenary session during an annual session held in the fall. The UNGA also works via six subcommittees that deal, for example, with disarmament and international security (First Committee, DISEC), economic and financial issues (Second Committee, ECOFIN), or social, humanitarian, and cultural issues (Third Committee, SOCHUM). In the framework of the UNGA, cybersecurity was first addressed in the UN in the late 1990s, which resulted in the convening of the first GGE. In addition, the UN Secretary-General has since submitted an annual report to the UNGA on "Developments in the field of information and telecommunications in the context of international security."

The UNGA elects inter alia the non-permanent members of the UNSC and the members of the ECOSOC. It can make recommendations to the UNSC and bring situations that may threaten international security to its attention. Every two years, it determines the priorities of UNOCT. UNODA provides substantive and organizational support to the work of UNGA and DISEC on disarmament-related issues. UNCTAD reports to the

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

UNGA. The GGE's and OEWG's take place or have taken place within the framework of the DISEC. The Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, for which the UNODC serves as secretariat, is a subsidiary body of the UNGA. Both UNIDIR and UNITAR are joint research and training institutions of the UNGA and the ECOSOC within the UN system. Among other things, UNODA provides substantive and organizational support to the work of UNGA and DISEC on disarmament-related issues, and UNDESA can also support deliberations of UNGA bodies[19].

UN-Institut für Abrüstungsforschung (United Nations Institute for Disarmament Research, UNIDIR, official translation)
The independent UN Institute for Disarmament Research is engaged in research on disarmament and other relevant issues in the context of international security policy. To this end, it seeks to engage in dialogue with UN Member States, bring together representatives from different sectors, and contribute ideas and promote practical measures. In addition, it is also available in an advisory capacity for UN Member States, UN agencies, and other partners. The area of cyber security is covered by UNIDIR's Security and Technology Programme (SecTec), in which cyber stability constitutes one of the four focus themes. SecTec has created the Cyber Policy Portal, an online resource for insights into the cybersecurity landscape of all UN Member States and individual regional organizations. It also hosts regular workshops and an annual Cyber Stability Conference.

Within the UN system, UNIDIR is a joint research and training institution of UNGA and ECOSOC. UNIDIR has assisted both chairs of the GGE and OEWG in carrying out their responsibilities. It is a signatory to the UN Global Counter-Terrorism Coordination Compact coordinated by the UNOCT. Financial support for UNIDIR includes contributions from Germany, the EU, and UNODA. The AA has co-hosted a cyber-related event with UNIDIR as well as financially supported corresponding thematic UNIDIR conferences[20].

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

20 GIP Digital Watch, United Nations Institute for Disarmament Research.
United Nations Institute for Disarmament Research, Capturing Technology: Rethinking Arms Control. The Impact of Artificial Intelligence on Cyber Operations.
United Nations Institute for Disarmament Research, Our Funding.
United Nations Institute for Disarmament Research, UNIDIR Cyber Policy Portal.
United Nations Institute for Disarmament Research, The UN, Cyberspace and International Peace and Security.

UN-Institut für interregionale Kriminalitäts- und Justizforschung (United Nations Interregional Crime and Justice Research Institute, UNICRI, official translation)
UNICRI's mission is to support UN Member States and the international community in combating criminal threats that threaten peace and stability, respect for human rights, and sustainable development. Following its ambition of promoting national self-responsibility and institutional capacity, UNICRI aims to contribute to this end as a focal point to inter alia promote just criminal justice systems and compliance with international instruments and standards. UNICRI's priorities also include cybersecurity and the misuse of technology. In this respect, UNICRI's focus areas include organized crime, discrimination and racism in cyberspace, and cybersecurity in robotics, autonomous systems, and critical infrastructure. UNICRI has an Emerging Crimes Unit, which is among other things involved in a World Bank project to provide tools and capacity building to combat cybercrime for emerging economies.

Within the UN system, UNICRI is a research and training institution of the ECOSOC. UNICRI is governed by a Board of Trustees that includes, among others, an ex officio representative of the UNDP. A cooperation agreement exists between ITU and UNICRI to strengthen exchanges on best practices in the field of cybersecurity, misuse of technology, and cybercrime. Together with the UNCCT of the UNOCT, UNICRI has published a report on the malicious use of artificial intelligence for terrorist purposes[21].

UN-Sicherheitsrat (United Nations Security Council, UNSC, official translation)
Within the UN, the UN Security Council is conferred primary responsibility for maintaining international peace and security according to the UN Charter (Article 24). It is composed of five permanent members (China, France, Russia, the United Kingdom, and the United States of America) and ten non-permanent members, elected for a two-year term based on an equal geographical representation of the United Nations' Regional Groups. Over time, also cybersecurity has become a topic of formal and informal (so-called "Arria" meetings) Security Council meetings and debates. In the past, for example, cyber operations against critical infrastructure, conflict prevention, cyber resilience, and capacity building have been discussed in this context. The work of the UNSC is supported by a variety of subsidiary bodies and committees such as the United Nations Security Council Counter-Terrorism Committee (CTC), which in turn is assisted by the Counter-Terrorism Committee Executive Directorate (CTED). The CTC and CTED are also dedicated to combating the use of ICT for terrorist purposes, among other things.

21 United Nations Interregional Crime and Justice Research Institute, About UNICRI.
United Nations Interregional Crime and Justice Research Institute, Current and Past Activities.
United Nations Interregional Crime and Justice Research Institute, Cybersecurity and Technology Misuse.
United Nations Interregional Crime and Justice Research Institute, Governing Body.

Germany is regularly represented in the UNSC as a non-permanent member, most recently between 2019 and 2020. The non-permanent members of the UNSC are elected by the UNGA. The ECOSOC may provide information to the UNSC and assist it upon request. In the past, representatives of Germany's Permanent Mission to the United Nations in New York (AA) and the EAD's delegation of the European Union to the United Nations in New York have, among others, participated in debates on cybersecurity. Together with the UNOCT (and Interpol), the CTED has published a compendium of best practices on critical infrastructure protection[22].

United Nations Digital and Technology Network (DTN)

As an internal UN mechanism, the DTN's mission is to foster collaboration on topics related to digital and technology, as well as promoting coordinated and collective digitization within the UN system. Among other things, the DTN aims to facilitate spaces for exchanging lessons learned, current priorities, collaborations on joint projects and evaluation, and enabling the establishment of subgroups on specific topics and technologies. Among the DTN's topical interests in which it seeks progress are information security and cybersecurity. Meetings of the DTN, which are held twice a year, are usually attended by the Chief Information Officers (CIO) of the UN agencies represented in the UN System Chief Executives Board for Coordination (UNSCEB) who act as representatives of their organization. The DTN is supported by an informal external expert group that can provide advice and recommendations. Institutional predecessors of the DTN were the ICT Network (ICTN) and the Information Systems Coordination Committee (ISCC).

The head of the UN OICT assumes the role of DTN's co-chair. The DTN reports to the High-level Committee on Management (HLCM) of the UNSCEB. The DTN may accept, modify, or reject recommendations from the UNISSIG reporting to it. Participants in the DTN include the ITU, the UNCTAD, the UNDP, the UNECE (ECOSOC), and the UNODC[23].

United Nations Group on the Information Society (UNGIS)

As an interdepartmental association of 31 UN organizations, the UNGIS aims to support the implementation of the outcome documents of the two World Summits on

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

23 UN Systems Chief Executives Board for Coordination, Digital and Technology Network.
UN Systems Chief Executives Board for Coordination, Digital & Technology Network (DTN): Terms of Reference.
UN Systems Chief Executives Board for Coordination, 30th Meeting of the CEB ICT Network.

the Information Society in Geneva (2003) and Tunis (2005) by utilizing synergies and implementing coordinated measures. Both outcome documents refer, among other things, to the need for a "global culture of cybersecurity" as well as the combating and prosecution of cybercrime. UNGIS members are the UN agencies represented in the UNSCEB. This is intended to ensure, as part of the work of UNGIS, that ICT-related topics retain an important place on the UN agenda and that ICT is also included in the mandate of UNSCEB members in the context of development. UNGIS convenes annually for a high-level meeting. Other events and meetings also take place at the operational level.

Participants in UNGIS include the ITU, the UNCTAD, the UNDP, the UNECE (ECOSOC), and the UNODC[24].

United Nations Information Security Special Interest Group (UNISSIG)
As an internal UN mechanism, the UNISSIG has set itself the cooperation in the field of information security as a goal and strives to contribute to the improvement of information security within all member organizations. Specifically, the UNISSIG aims to minimize risks through continuous and collective assessments of the current threat situation and the establishment of a coordinated information security management for the UN system. UNISSIG meetings, held annually, are generally attended by the Chief Information Security Officers (CISO) of the UN organizations represented in the UNSCEB.

The UNISSIG was established by the DTN and reports to the Network. Participants in the UNISSIG include the ITU, the UNCTAD, the UNDP, and the UNODC[25].

United Nations International Computing Centre (UNICC)
As a specialized UN entity, UNICC provides other UN organizations – among other services – with network infrastructure, centralized digital services, and information security support. In the area of information security, this includes, for example, vulnerability management, penetration testing, phishing simulations, and the operation of a Threat Intelligence Network and Security Operation Center. UNICC also operates the Common Secure Threat Intelligence as part of its Common Secure Information Security Hub, through which information on cyber threats and related incidents can be shared via UNICC. For example, this can take place in an automated manner via a Malware Information Sharing Platform. Participating institutions come together for an annual meeting.

24 GIP Digital Watch, United Nations Group on the Information Society.
United Nations Digital Library, Declaration of Principles. Building the information society: A global challenge in the new millennium.
United Nations Digital Library, Tunis Agenda for the Information Society.
United Nations Group on the Information Society, About UNGIS.
United Nations Group on the Information Society, Members.

25 UN Systems Chief Executives Board for Coordination, HLCM ICT Network UN Information Security Special Interest Group (UNISSIG): Terms of Reference.
UN Systems Chief Executives Board for Coordination, Information Security Special Interest Group.

UNICC's customers and partners include ITU, UNCTAD, UNECE (ECOSOC), UNITAR, and the UN OICT. Common Secure Threat Intelligence users include the ITU, UNCTAD, and UNDP[26].

United Nations Office of Counter-Terrorism (UNOCT)

UNOCT's responsibilities include inter alia improving coordination and ensuring coherence among signatory institutions to the UN Global Counter-Terrorism Coordination Compact, as well as enhancing UN support for national counterterrorism capacity building. UNOCT is also home to the UN Counter-Terrorism Center (UNCCT), in which cybersecurity constitutes one of its programs and projects. In this area, the UNCCT aims to strengthen the capabilities of UN Member States and private organizations in curbing the misuse of ICT by terrorist actors, mitigating the threat of cyber operations by them on critical infrastructure, as well as contributing to the collection of digital evidence on social media in a manner that is compliant with human rights.

UNOCT is part of the UN Secretariat, and its priorities are determined every two years by UNGA as part of the review of the UN Global Counter-Terrorism Strategy. UNOCT inter alia works with the CTC as a subsidiary body of the UNSC. The UNCCT participates in ITU's cybersecurity exercise CyberDrill. In the past, the UNCCT has also organized a hackathon to combat digital terrorism with the UN OICT. Together with UNICRI, the UNCCT has released a report on the malicious use of artificial intelligence for terrorist purposes. Signatories of the UN Global Counter-Terrorism Coordination Compact include UNDP, UNICRI, UNIDIR, UNITAR, UNODA, UNODC, and UN OICT. UNDESA is associated with the Compact as an observer. The EU and Germany are among the top 10 contributors to UNOCT. Germany is a member of the Advisory Board of the UNCCT[27].

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

In the area of cybersecurity, the UN OICT has set itself the task of identifying cyber threats to the UN, preventing them, and contributing to their remediation when they

26 GIP Digital Watch, UN International Computing Centre.
United Nations International Computing Centre, Clients and Partner Organizations.
United Nations International Computing Centre, UNICC Facilitates UN Inter-Agency Collaboration with a Reputation for Cyber Excellence.
United Nations International Computing Centre, What We Do.

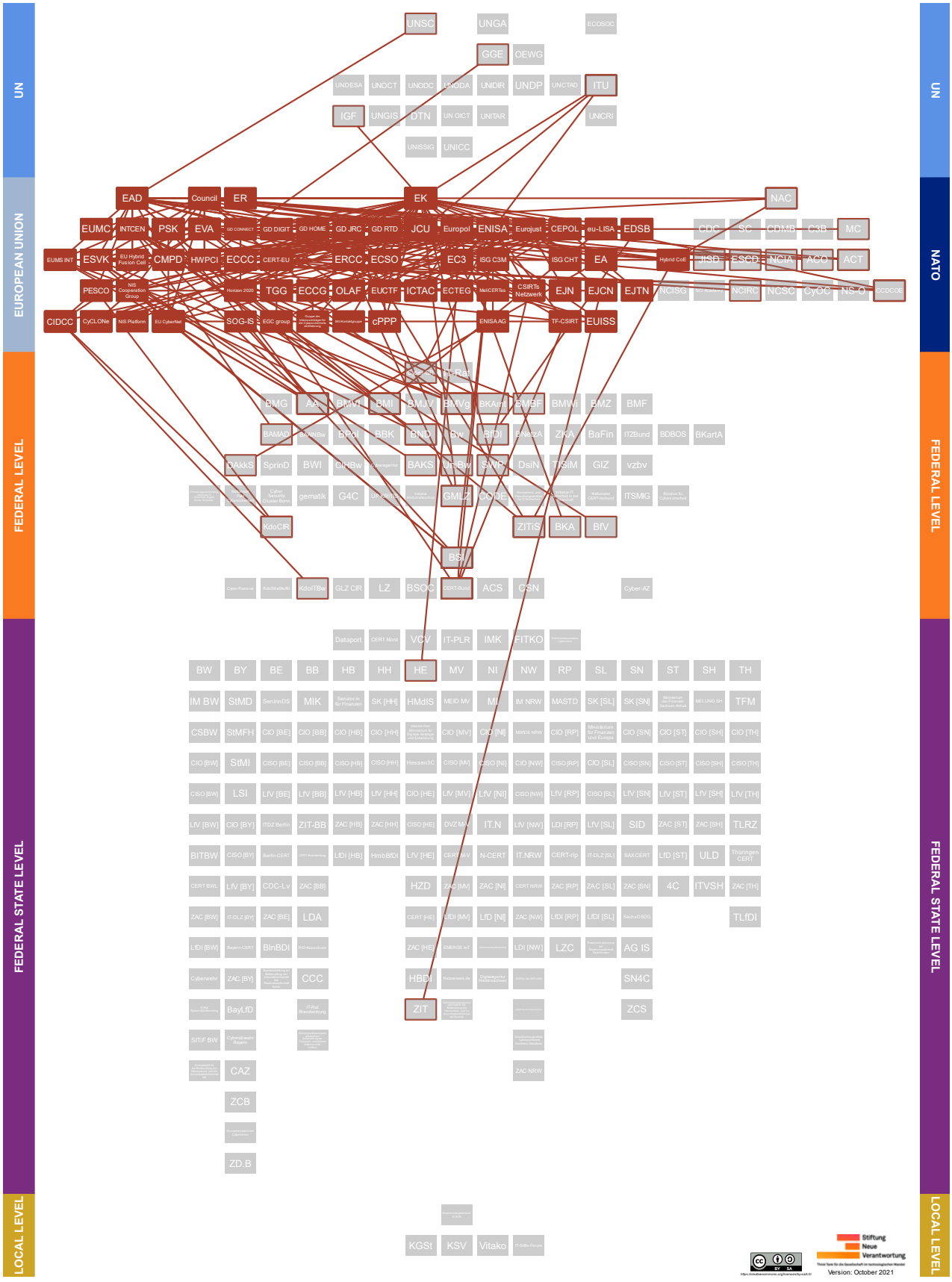
27 AIT Austrian Institute of Technology, United Nations Counter-Terrorism Centre führte Cybersecurity Innovation Challenge am AIT durch.
United Nations Interregional Crime and Justice Research Institute, Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes.
United Nations Office of Counter-Terrorism, About us.
United Nations Office of Counter-Terrorism, Advisory Board.
United Nations Office of Counter-Terrorism, Funding and donors.
United Nations Office of Counter-Terrorism, UN Global Counter-Terrorism Coordination Compact Entities.
United Nations Office of Counter-Terrorism. UN Counter-Terrorism Centre, Cybersecurity.
United Nations Office of Counter-Terrorism. UN Counter-Terrorism Centre, UNCCT-ITU Cyber Drill 2020 – Terrorist Threat Simulation Cyber Exercise.

occur as a focal point for partners within the UN. To this end, it has, for example, produced an information risk management and guidelines for the UN Secretariat, including an action plan. The UN OICT is home to the Digital Blue Helmets program (DBH), which – as a platform – is designed to contribute to rapid information sharing, cyber defense, increasing resilience, and coordinated deployment of protective measures in the event of a cybersecurity incident. It comprises specialized cybersecurity experts and maintains among other things a Global Cybersecurity Monitoring Centre in New York and regional Cybersecurity Monitoring Centres. In the long term, the DBH aims to contribute to mitigating the impact of zero-day vulnerabilities, promoting digital IDs, and further enhancing the UN's defense capabilities against external threats, among others.

The head of the UN OICT serves as co-chair of the DTN. In the past, UN OICT has organized a hackathon with UNOCT's UNCCT to combat digital terrorism. It is among the clients and partners of the UNICC[28].

28 Office of Information and Communications Technology, About OICT.
Office of Information and Communications Technology, Coordination.
Office of Information and Communications Technology, Cybersecurity.
Office of Information and Communications Technology, Digital Blue Helmets.

5. Explanation – Actors at EU level



Agentur der Europäischen Union für Cybersicherheit (European Union Agency for Cybersecurity, ENISA, official translation)

ENISA[29] is an EU agency that assists the European Commission in cybersecurity matters. Regarding its consulting role, ENISA is contributing to EU cyber policy development, supporting cyber capacity building, participating in knowledge exchange with relevant stakeholders, and raising awareness for cybersecurity. ENISA also aims to improve cooperation within the EU, promote greater coherence between sectoral initiatives by way of the NIS Directive, and 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 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 malicious cyber activities. Annually, ENISA publishes a threat landscape report (ENISA Threat Landscape) which identifies and assesses threats from cyberspace. In addition, ENISA organizes regular cybersecurity exercises of various formats, such as the biennial Cyber Europe Exercise together with EU Member States, the annual European Cybersecurity Challenge (ECSC), and the ICTAC Exercise.

GD CONNECT bears the "parent-DG responsibility" for ENISA and represents the EK in ENISA's Management and Executive Board together with GD DIGIT. ENISA works with both relevant Member State authorities and at EU level – in particular with national Computer Security Incident Response Teams, the CERT-EU, Europol's 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. It is involved in the ICTAC as well as the TGG and is foreseen as a participating institution of the JCU. A Memorandum of Understanding for cooperation and exchange in the field of cybersecurity was concluded between EVA, CERT-EU, EC3, and ENISA. ENISA and eu-LISA entered into a three-year joint cooperation plan in early 2021 to inter alia strengthen cooperation and exchange knowledge as well as expertise in the field of information security. Further cooperative working relationships exist with GD JRC, ECSO, ESVK, and the EGC group. Together with CERT-EU (and the ECDC), ENISA has set up the ICTAC Exercise. ENISA provides the secretariat of the CSIRTs network and CyCLONe. The ECCC is intended to complement ENISA's tasks and shall collaborate with ENISA to perform its functions. The HWPCI cooperates with

29 Recently, ENISA underwent a name change from the "European Network and Information Security Agency" to the "European Union Agency for Cybersecurity". The abbreviation of the original name remained the same after the process.

ENISA. ENISA supports the NIS Cooperation Group, inter alia, by identifying best practices in implementing the NIS Directive or strengthening the envisaged cybersecurity incident reporting process within the EU by developing thresholds, templates, and tools. The ENISA AG advises ENISA on, among other things, the implementation of its tasks. Upon request, also the Stakeholder Cybersecurity Certification Group may advise ENISA. It is responsible for the implementation and deployment of key aspects of the MeliCERTes facility. The ECCG, in addition to the EK, may request ENISA to develop new possible certification schemes. In a visiting capacity, the ENISA participates in the NATO Cyber Coalition Exercise organized by the ACT. Among other things, ENISA and the ITU exchange information on best practices. At the German level, ENISA cooperates with the BSI/CERT-Bund. In addition, representatives of the BSI are represented on the Management Board and the National Liaison Officers Network of ENISA[30].

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 exchange, connecting ongoing investigations, developing criminal law strategies, and enabling joint action, Eurojust is responsible for coordinating case investigations. This is intended to strengthen the investigative capabilities of Member States' law enforcement agencies in the area of cybercrime, the understanding of cybercrime, and the investigative options of both law enforcement and the judiciary. Eurojust regularly publishes reports, such as the annual Cybercrime Judicial Monitor, which provides an overview of legislation and case law at the EU and national level, or occasion-based reports on specific challenges and best practices.

30 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, Cybersecurity exercise boosts preparedness of EU Agencies to respond to cyber incidents.
European Union Agency for Cybersecurity, Cyber agencies assess future cooperation opportunities.
European Union Agency for Cybersecurity, ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.
European Union Agency for Cybersecurity, European Cyber Security Challenge 2020 – Event Date Change.
European Union Agency for Cybersecurity, EU Agency for Cybersecurity and Joint Research Centre discuss cooperation.
European Union Agency for Cybersecurity, List of ENISA Management Board Representatives and Alternates.
European Union Agency for Cybersecurity, List of National Liaison Officers (NLO).
European Union Agency for Cybersecurity, Second Staff Exchange between EU Cybersecurity Organisations.
Federal Office for Information Security, BSI Magazin 2019/1.
Federal Office for Information Security, Cyber-Sicherheit: Nationale und Internationale Zusammenarbeit.

Eurojust works with EC3's specialized advisory groups, networks of heads of cybercrime units, and prosecutors specializing in cybercrime. Relations between Eurojust, relevant national authorities, and third states should be fostered. Within Eurojust's organizational structure, Germany is represented as an EU Member State with a seat on its weekly convening "College". This is supported by an Executive Board with the participation of the EK. Partnership relations exist with the following EU institutions: Europol, EC3, CEPOL, eu-LISA, OLAF, and EJTN. It also cooperates with the HWPCI. Together with Europol, Eurojust has in the past published a report on common challenges in the fight against cybercrime. Eurojust is home to the EJN secretariat and is a member of the EUCTF. Eurojust is also represented on the Board of the EJCN and prepares its regular meetings. Eurojust can be invited as an observer to meetings of the COSI (Council of the EU). The EDSB has a supervisory role over Eurojust regarding the lawful processing of personal data[31].

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 comprises experts from central EU institutions (inter alia the EK and General Secretariat of the Council of the EU). GD CONNECT is represented on the Board of the CERT-EU. The CERT-EU is foreseen as a participating organization of the JCU and is already part of the ICTAC. It works closely with other CERTs of Member States as well as the EU Hybrid Fusion Cell and is a member of the CSIRTs network. CERT-EU represents the EU in the EGC group. A Memorandum of Understanding for cooperation

31 Eurojust, Casework at Eurojust.
Eurojust, College.
Eurojust, Cybercrime.
Eurojust, Cybercrime Judicial Monitor: Issue 6 – May 2021.
Eurojust, Eurojust Decision.
Eurojust, EU partners.
Eurojust, Germany.
Eurojust, Overview Report. Challenges and best practices from Eurojust's casework in the area of cybercrime.
European Commission, Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.
Europol and Eurojust, Common challenges in combating cybercrime. As identified by Eurojust and Europol.
Federal Office for Information Security, Avalanche-Botnetz: BSI weitete Schutzmaßnahmen aus. (Website deleted)

and exchange in the field of cybersecurity was concluded between EVA, EC3, ENISA, and CERT-EU. Recently, a structured cooperation between CERT-EU and ENISA has been agreed upon. Further exchange and working relations exist with the ESVK. CERT-EU participates in the TGG. In the past, CERT-EU and the NCIRC have concluded a technical agreement of cooperation. In addition, CERT-EU exchanges information with NCIA and regularly convenes at operational level[32].

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 solutions 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. As a contractual partner of the EK, ECSO is responsible for the implementation of the cPPP[33].

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 the Member States. It provides a forum for cooperation and the development of a coordinated response to cross-border cybersecurity incidents.

The CSIRTs Network is subordinate to the NIS Cooperation Group and consists of appointed representatives of Member States' CSIRTs as well as the CERT-EU. Germany is represented by its CERT-Bund. The EK participates in the network as an observer. ENISA appoints the secretariat, promotes cooperation between CSIRTs, and, where necessary, offers active support for the coordination of incidents. EC3 and CERT-EU provide forensic analysis and other technical information to the network. The participation of the CSIRTs network in the JCU is envisaged[34].

32 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.
33 ECSO, About the cPPP.
34 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.

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 Cyber Crises Liaison Organisations (CyCLO) 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 the national and EU level, respectively. EU Member States can participate on a voluntary basis. CyCLONE's first cybersecurity exercise, CySOPEx, took place in May 2021, simulating a large-scale cross-border cyber crisis and testing the cyber crisis management of EU Member States. This exercise is expected to contribute, among other things, to the development of the standard operating procedures (SOP) foreseen in the Blueprint.

The idea for such a network, supported by the EK, stems from a task force of NIS Cooperation Group led by France and Italy; ENISA acts as the network's secretariat. In the near future, insights, especially from cybersecurity exercises (Blue OLEx, for example), are supposed to feed into the work of the network. CySOPex was carried out with the support of ENISA and the EC. Participation of CyCLONe in the JCU is envisaged[35].

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 developping 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 shall reach its initial operating capability by 2023 and is slated to be fully

35 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 Commission, Joint exercise to test cooperation and cyber resilience at EU level.
European Union Agency for Cybersecurity, Blue OLEx 2020: the European Union Member States launch the Cyber Crisis Liaison Organisation Network (CyCLONe).
European Union Agency for Cybersecurity, EU Member States test rapid Cyber Crisis Management.
Federal Ministry of the Interior, Building and Community, 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. (Website deleted)

operational by 2026. Until then, it is to be equipped with the capabilities 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 CIDCC Steering Committee includes representatives of the participating EU Member States of the EVA, the EUMS, and ENISA. It is currently chaired by the commander of the KdoITBw. The KdoCIR coordinated with the EUMS and the EVA in its conceptualization of the CIDCC[36].

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. Such strategic planning aims to identify possible courses of action for the EU and serve as the foundation for the European 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. The CMPD is located in the EAD[37].

ENISA-Beratungsgruppe (ENISA Advisory Group, ENISA AG, official translation)
The ENISA AG was established with the Cybersecurity Act. It comprises 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 representatives 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[38].

36 Dorothee Frank, Meilenstein für die europäische Cyberlage.
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).

37 European Union External Action Service, The Crisis Management and Planning Directorate (CMPD) (Website deleted).

38 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).

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 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 the 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 to inter alia exchange best practices, strengthen resilience and formulate counterinitiatives to hybrid threats.

The EU Hybrid Fusion Cell is institutionally located within the INTCEN in the EAD. The Cell works with EUMS INT 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[39].

EU Cyber Capacity Building Network (EU CyberNet)

EU CyberNet serves to support EU cyber capacity-building efforts by strengthening external EU projects and increasing the EU's capacity to provide technical assistance in the context of cybersecurity and cybercrime. In addition to its networking function, the EU CyberNet also aims to improve coordination amongst stakeholders and mobilize collective expertise. By 2023, the EU CyberNet aims to have established a network of at least 500 cybersecurity experts and at least 150 stakeholders, have created a technical platform to connect experts and stakeholders, providing training and support, and have become a knowledge hub for the external cyber engagement of the EU. The latter also envisages, among other things, the provision of strategic, technical, operational, and policy support to EU authorities, for example, through ad hoc advice. Regularly, EU CyberNet also organizes events on relevant cyber capacity-building topics and hosts an annual conference.

39 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.

The establishment of EU CyberNet was foreseen in documents of the Council of the EU and the EK. EU CyberNet is funded by the EK and implemented by the Estonian Information System Authority with the support of the AA as a member of the Board of Trustees. EU CyberNet has briefed the PSK on the implementation of the EU Cyber Security Strategy. CEPOL, ESVK, EUISS, and BSI are already members of the stakeholder community[40].

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 Schengen Area countries and 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.

The Agency cooperates closely with the Member States, and at EU level with the EDBS, the Council of the EU, the EK, CEPOL, Eurojust, and Europol and GD HOME. Eurojust and Europol are also represented on eu-LISA's Management Board and advisory groups. The ENISA and eu-LISA concluded a three-year joint cooperation plan at the beginning of 2021, under which inter alia cooperation and the exchange of knowledge and expertise in the field of information security are to be strengthened. Contacts on working-level have also been established with NATO CCDCOE. The BMI is represented by a representative on the Management Board of eu-LISA[41].

Europäische Gruppe für die Cybersicherheitszertifizierung (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, including, for example, the period of validity of security certificates. Furthermore, the European Cybersecurity Certification Group assists the Commission in establishing a European work

40 Council of the European Union, EU External Cyber Capacity Building Guidelines.
EU CyberNet, EU CyberNet.
EU CyberNet, Informal cybersecurity briefing to the Political and Security Committee.
EU CyberNet, Project Deliverables.
EU CyberNet, Team.
EU CyberNet, Stakeholder Community.

41 European Union, Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (eu-LISA).
European Union Agency for Cybersecurity, ENISA and eu-LISA – Cooperation for a More Digitally Resilient Europe.
eu-LISA, Declaration of Interest – Kai Schollendorf.
eu-LISA, EU Agencies.
eu-LISA, EU Institutions.

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, parallel to the European Commission, request that ENISA develops new possible certification schemes not yet included in the work program[42].

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, strengthening the EU's position in the field, and promoting the integration of cybersecurity into other EU policy areas. The European Commission has its own early warning system (ARGUS), including an internal communication network and a specific coordination procedure. In the event of a significant, EU-wide crisis affecting cyberspace, coordination efforts are handled through ARGUS.

Several Directorates-General work in the field of cybersecurity, including CONNECT, DIGIT, HOME, JRC and RTD. The CERT-EU, and the ERCC (ERCC through GD ECHO) are also affiliated with the European Commission. The Council of the EU may entrust the EK with the negotiation of international agreements, the conclusion of which is decided by the Council based on a proposal from the EK. OLAF is subordinate to the EK. The ECCC is based on a proposal of the EK, which is also, together with the EU Member States, represented by two representatives on the ECCC Governing Board. The EK chairs the CIP Contact Group and the Stakeholder Cybersecurity Certification Group (the latter jointly with ENISA). It is also represented on the Advisory Board of the EA. The eu-LISA, the EC3, the HWPCI, and the EUISS cooperate with the EK. The EK is involved in the development and implementation of CEPOL trainings. The ECCG is assisting the EK in establishing a European work program for cybersecurity certification schemes. Upon request, the EDSB may act in an advisory capacity for the EK. The EK participates in the CSIRTs network as an observer and is a member of the EUCTF. In the past, the EK has taken into account the results of the NIS Platform for its recommendations on cybersecurity. The establishment of the EU CyberNet has been foreseen, among others, in documents of the EK. ECSO is a contractual partner of the EK. The ITU cooperates with the EK in the context of harmonization of ICT policies within ACP countries. The EK may participate in meetings of the MAG of the IGF.

42 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).

In the past, the EK, 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. The EK is one of the partners of the GMLZ and is also among the third-party funders of the SWP[43]*.*

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 coordinating accreditation in Europe. It is a non-profit organization and is comprised of 50 nationally recognized accrediting agencies. The EA aims to contribute to 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[44]*.*

Europäische Polizeiakademie (European Union Agency for Law Enforcement Training, CEPOL, official translation)
CEPOL is an EU agency responsible for developing, implementing, and coordinating 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 and developed in cooperation with the European Commission, EC3, EJTN, Eurojust, the EUCTF, and ECTEG. Further exchange and working relations exist with the ESVK and GD HOME. CEPOL is also a member of the stakeholder community of EU CyberNet and is involved in the ICTAC. It may be invited as an observer to meetings of COSI (Council of the EU)[45]*.*

43 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.

44 European Accreditation, EA Advisory Board.
European Accreditation, Relations with European Commission. European Accreditation, Who are we?.
German National Accreditation Body, Europäischer Rechtsrahmen.

45 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 (all except Denmark are part of the EVA) in developing 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. Specifically, the EVA supports, among other things, the creation of a risk management model for cybersecurity in the context of military capability supply chains, the establishment of the Cyber Ranges Federation project, the development of specific capabilities for APT detection, and cyber situational awareness.

The EVA is subordinate to the Council of the EU, to which it reports and from which it receives its guidance. The High Representative of the EU for Foreign Affairs and Security Policy also assumes the role as EVA's head. The Steering Board of the EVA meets at the level of the Member States' defense ministers; for Germany, the Federal Minister of Defense (BMVg) is a member. Together with the EAD, EVA jointly manages all secretarial functions for the Permanent Structured Cooperation (PESCO). The EVA is represented in the Steering Board of the CIDCC and participates in the ICTAC. The EVA signed a Memorandum of Understanding with ENISA, the EC3, and CERT-EU intending to develop a cooperation framework for the organizations. The EVA is envisioned as a participating organization of the JCU in a supporting role. Working relationships with the ESVK, the ECSO, the Hybrid CoE, the HWPCI, the NATO CCDCOE, and ACT exist. The EVA participates in Locked Shields. The Chief Executive of the EVA meets regularly with the SACT (ACT) and Assistant SECGEN's of NATO. The EVA Steering Board is also briefed regularly by the latter[46].

46 European Court of Auditors, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
European Defence Agency, Cooperation between the European Defence Agency and the Eurooean Security and Defence College.
European Defence Agency, Cyber.
European Defence Agency, Cyber Ranges: EDA's First Ever Cyber Defence Pooling & Sharing Project Launched By 11 Member States.
European Defence Agency, EDA participates in "Locked Shields" cyber defence exercise.
European Defence Agency, Exchange of letters: NATO Allied Command Transformation.
European Defence Agency, Four EU cybersecurity organisations enhance cooperation.
European Defence Agency, Governance.
European Defence Agency, Liaison between the European Defence Agency and the Cooperative Cyber Defence Centre of Excellence.
European Defence Agency, Liaison between the European Defence Agency and the European Centre of Excellence for Countering Hybrid Threats.
European Defence Agency, Priority Setting.
European External Action Service, Permanent Structured Cooperation – PESCO.
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.

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 ensures coherent policymaking in the fields of security and cybersecurity policy.

The EAD hosts EUMS INT, INTCEN, and the EU Hybrid Fusion Cell. It is also affiliated with the CMPD and the ESVK. Furthermore, EAD representatives chair the PSK. The HWPCI, the EUISS, and ECSO cooperate with the EAD. The EAD co-chairs the ISG CHT together with the EK and participates in the ISG C3M. Together with the EVA, the EAD forms the secretariat of PESCO. The participation of the EAD in the JCU is envisaged. The EAD receives information and assessments from the STAR (GD HOME). The EAD is represented in the COSI (Council of the EU). The High Representative regularly exchanges views with the NATO Secretary-General and occasionally participates in NAC meetings at the level of defense ministers. In the past, the EAD has met with representatives of the ESCD to discuss cyber defense. The EU delegation to the UN in New York, subordinate to the EAD, has participated in debates on cybersecurity within the UNSC[47].

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 those supervisory authorities supporting his or her duties, are responsible for ensuring the supervision of and adherence to data protection principles 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 techno-

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

logical developments. The EDSB is appointed for a five year-term 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 and 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 the German level, contact and exchange exist with the BfDI[48]*.*

Europäischer Rat (European Council, ER, official translation)
The European Council is responsible for determining the "political objectives and priorities" of the EU. In this respect, it can adopt conclusions on specific topics and occasions and has adopted a Strategic Agenda for the EU for 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 (EAD)[49]*.*

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

48 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.
49 European Council, A New Strategic Agenda 2019 – 2024.
European Council, Der Europäische Rat.

OLAF reports to the EK but is independent in the execution of its mandate. It regularly reports to the Council of the EU's Working Group on Fraud Prevention[50].

Europäisches Polizeiamt (European Police Office, Europol, official translation)
Europol is the law enforcement agency of the European Union. It supports both the European Commission and 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 strengthens law enforcement efforts, particularly through its subordinate European Cybercrime Centre (EC3).

The participation of Europol in the JCU is envisaged. Eurojust, eu-LISA, the ESVK, the HWPCI, and ECSO cooperate with Europol. Europol is a member of the EUCTF, the TGG, and the ICTAC. Europol receives information and assessments from the STAR (GD HOME). Every six months, the INTCEN produces together with Europol a threat analysis transmitted to the COSI (Council of the EU), to which Europol can also be invited as an observer. The EDSB has a supervisory role over Europol regarding the lawful processing of personal data. Europol works together with the BKA. The BKA serves as a Europol National Unit and therefore Europol's German point of contact[51].

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 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 the German level, the AA, BAKS, and the BMVg participate in this network. In turn, the ESVK is a member of the EU CyberNet stakeholder community[52].

50 European Anti-Fraud Office, About Us.
European Anti-Fraud Office, Cooperation with EU institutions.
51 Europol, About Europol.
Europol, European Cybercrime Centre – EC3.
Federal Criminal Police Office, Europol.
52 European Security and Defence College, EAB.Cyber.
European Security and Defence College, Education & Training.
European Security and Defence College, Network Members.
European Security and Defence College, 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)
The ECCC is currently being established in Bucharest. It is meant to promote European autonomy in cybersecurity and the competitiveness of the European cybersecurity industry, and strengthen 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 (NCCs) Network and the Cybersecurity Competence Community.

The ECCC is based on a proposal of the EK (prepared by GD CONNECT), which – together with the EU Member States – is also represented by two representatives in the Governing Board of the ECCC. It is intended to complement the tasks of ENISA and cooperate with ENISA in the performance of its functions. One representative of ENISA has permanent observer status in the ECCC's Governing Board. In addition, the EU Regulation establishing the ECCC provides, inter alia, for cooperative working relations with the EAD, GD JRC, EC3, and the EVA[53].

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 and 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.

53 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.
Matthias Monroy, Neues EU-Kompetenzzentrum für Cybersicherheit bleibt umstritten.
Official Journal of the European Union, Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren.

EC3 is located at Europol. At the European level, EC3's partners are the CERT-EU, CEPOL, Eurojust, ENISA, the European Commission, and ECTEG. A Memorandum of Understanding between EC3, EVA, CERT-EU, and ENISA for cooperation and exchange in the field of cybersecurity has been concluded. Together with ENISA, EC3 hosts annual workshops on cooperation between national Computer Security Incident Response Teams and law enforcement agencies. In cooperation with the CERT-EU, EC3 also provides forensic analysis and other technical information for the CSIRTs network. It is involved in the TGG[54].

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 exchanging best practices between various stakeholders within three Communities of Interest (COI). The COI group focusing on strategy and defense 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 GD 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 EVA agreed to cooperate to contribute to the implementation of priorities outlined in the Capability Development Plan of the EU. Further working relations exist with the ESVK. Germany is among the nine founding nations of the Hybrid CoE. The Hybrid CoE is involved in the EU-HYBNET project, in which also ZITiS is engaged as a project partner[55].

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.

54 European Agency for Cybersecurity, Ninth ENISA-EC3 Workshop on CSIRTs-LE Cooperation: standing shoulder-to-shoulder to counter cybercrime.
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.

55 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.

ECTEG works 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. Further exchange exists with the ESVK. Germany's "Polizeiakademie Hessen" (Police Academy Hesse, own translation) and the "Hochschule Albstadt-Sigmaringen" (Albstadt-Sigmaringen University, official translation) are also involved as members[56].

European Cyber Security Organisation (ECSO)

The ECSO was established in Belgium in 2016 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.

ECSO is a contractual partner of the European Commission. In this function, it is responsible for implementing the contractual Public-Private Partnership for cybersecurity (cPPP). It furthermore maintains 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. It cooperates with the ITU and has supported it, for example, in the creation of the GCI[57].

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 which 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 cooperation with ENISA[58].

56 ECTEG, European Cybercrime Training and Education Group.
ECTEG, Members.
57 ECSO, About ECSO.
58 EGC Group, Contact.
EGC Group, European Government CERTs (EGC) group.
Federal Office for Information Security, Europäische CERTs in Bonn. (Website deleted)

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 EJCN[59].

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.

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 members. Moreover, a cooperation with the EJN exists. The ZIT is a founding member of the EJCN[60].

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[61].

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. The EUCTF is involved in the TGG[62].

59 European Judicial Network, About EJN.
European Judicial Network, Network Atlas.
60 Eurojust, European Judicial Cybercrime Network.
61 Email exchange with CEPOL representatives in August 2019.
EJTN, About us.
62 Europol, EUCTF.

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 and 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 including, 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. Further working relationships exist with GD RTD and ECSO. GD JRC takes part in the EU-HYBNET project, in which also ZITiS and an institute of UniBw are involved as project partners[63].

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 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 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 with inter alia GD CONNECT, GD HOME, GD JRC, and ECSO[64].

Generaldirektion Informatik (Directorate-General for Informatics, GD DIGIT, official translation)
GD DIGIT oversees the IT security of the European Commission's systems. Furthermore, it is 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. Working relations exist with ECSO as well as ICTAC. A representative of GG DIGIT also participates in meetings of the ICTAC[65].

63 EU Science Hub, Information Society.
EU Science Hub, JRC in brief.
EU Science Hub, Organisation.
EU Science Hub, Research Topics.
64 European Commission, Strategic Plan 2016-2020: Directorate-General for Research and Innovation.
65 European Commission, Annual Activity Report: DG CONNECT.
European Commission, Informatics.
European Court of Auditors, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.

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 the 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. Working relationships exist with GD RTD and ECSO. The proposal for the establishment of the ECCC by the European Commission was prepared by GD CONNECT[66].

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 (for example, Europol). Working relationships exist with eu-LISA, Europol, and CEPOL, among others[67].

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 comprises representatives of European

66 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.

67 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.

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), and 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. It collaborates with the ECCG[68].

Horizon 2020

Horizon 2020 is a European Commission program that has made available nearly 80 billion euros 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.

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. Within the framework of Horizon 2020, the EU will invest up to 450 million euros in the cPPP. Two projects in which ZITiS participates (EU-HYBNET and FORMOBILE) are part of Horizon 2020[69].

Horizontale Ratsarbeitsgruppe "Fragen des Cyberraums" (Horizontal Working Party on Cyber Issues, HWPCI, official translation)

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 non-legislative processes.

The HWPCI is a preparatory body of the Council of the EU. It can, for example, prepare meetings of the PSK on a case-by-case basis. The HWPCI works with the EK, the EAD, Europol, Eurojust, the EVA, and the ENISA and also maintains cooperation with other

68 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).

69 European Commission, Security.
European Commission, What Is Horizon 2020?.
Federal Ministry of Education and Research, Netzwerk der Nationalen Kontaktstellen.

working groups. The chair of the HWPCI is designated as a supporting participant of the JCU. ECSO regularly reports to the HWPCI on the current status of its work. Germany participates in the HWPCI through representatives of the BMI and the AA. The last UN GGE also held a regional consultation with EU Member States as part of the HWPCI[70].

ICT Advisory Committee of the EU Agencies (ICTAC)

The ICT Advisory Committee of EU institutions, which meets twice a year, aims to serve as a forum to exchange best practices, experience, and knowledge. Thereby, cross-institutional cooperation in the area of ICT shall be promoted based on common interests. It provides a mechanism to develop common positions and aims to contribute to cooperation among themselves, for example, by sharing resources and best practices in the development, maintenance, or deployment of new ICT systems. In the past, ICTAC has also organized a cybersecurity exercise (ICTAC Ex) to contribute to improved cooperation and information sharing.

ICTAC comprises the responsible heads for ICT within EU institutions, executive agencies, and other bodies. Participants include CEPOL, CERT-EU, ENISA, Europol, and the EVA. It is in permanent exchange with GD DIGIT, from which a representative also participates in ICTAC meetings[71].

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 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 Council of the EU and works together with several institutions, including the European Commission, the European External Action Service, and with the respective governments of EU Member States. It is a member of the stakeholder community of the EU CyberNet[72].

70 Council of the European Union, Establishment of a Horizontal Working Group on Cyber Issues.
European Council, Horizontal Working Party on Cyber Issues (HWP).
Federal Office for Information Security, Cyber-Sicherheit in Europa gestalten. (Website deleted)
Official Journal of the European Union, Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.

71 European Union Agency for Cybersecurity, Cybersecurity exercise boosts preparedness of EU Agencies to respond to cyber incidents.
ICTAC, ICTAC Annual Report 2018.
ICTAC, Terms of Reference of the Network of Heads of ICT of the European Agencies (ICTAC).
ICTAC, ICTAC Work Programme 2019-2020.

72 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.

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 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 is located within the EAD and 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, and the German Military Representative to the European Union[73].

Inter-Service Group "Community Capacity in Crisis-Management" (ISG C3M)
ISG C3M is a network that regularly brings together all European Commission services and EU agencies involved in crisis management 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[74].

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[75].

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

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

75 Ibid.
Kristine Berzina, Nad'a Kovalcikova, David Salvo and Etienne Soula, European Policy Blueprint for Countering Authoritarian Interference In Democracies: Annex A. European Efforts To Counter Disinformation.

Joint Cyber Unit (JCU)

In order to establish the Joint Cyber Unit envisaged in the EU Cyber Security Strategy, the EK has made a proposal at the end of June 2021. The JCU is to reach its operational phase by June 2022 and full operational capability by June 2023. As a physical and virtual platform, it is intended to strengthen cooperation between EU institutions and authorities in EU Member States at the technical and operational levels to prevent, deter, and respond to cyber operations in a coordinated manner. To ensure this coordinated response to and recovery from incidents, the JCU should, among other things, establish EU Cybersecurity Rapid Reaction Teams and create and continuously update an inventory of all operational and technical capabilities available within the EU. In addition, joint situational awareness and joint preparation should also be improved before incidents emerge. To this end, the JCU shall inter alia develop an Integrated EU Cybersecurity Situation Report and, in line with and based on corresponding national plans, an EU Cybersecurity Incident and Crisis Response Plan, as well as a multi-year plan for the coordination of cybersecurity exercises. The cooperation of all participants should be facilitated via memoranda of understandings which also include provisions for mutual assistance. As a final envisioned step in its operationalization, the JCU is also to seek operational cooperation agreements with private sector entities to ensure information sharing.

The JCU is envisaged to be located in Brussels alongside ENISA and CERT-EU. As operational participants of the JCU, the EK proposal envisages ENISA, Europol, CERT-EU, EAD (with INTCEN), the CSIRTs Network, and CyCLONe. In a supporting capacity, the JCU shall also involve the chairs of the NIS Cooperation Group and HWPCI, the EVA, and a representative of relevant PESCO projects. A report on the role and responsibilities of participating actors within the JCU is to be developed by June 2022. It will then be submitted to the Council of the EU for decision[76].

Kontaktgruppe zum Schutz Kritischer Infrastrukturen (CIP Contact Group, SKI-Kontaktgruppe, official translation)

The CIP Contact Group 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 CIP Contact Group also provides Member States with support in the protection of their national critical infrastructure.

The CIP Contact Group 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 the other Member States, the European Commission, and the Council of the EU[77].

76 European Commission, EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents.
European Commission, Factsheet: Joint Cyber Unit.
European Commission, Recommendation on building a Joint Cyber Unit.

77 Commission of the European Communities, Communication from the Commission on a European Programme for Critical Infrastructure Protection.

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 based on 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 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 implementing 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. The chairperson of the NIS Cooperation Group is one of the designated supporting participants of the JCU[78].

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 and maintained by the teams, allowing 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[79].

78 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.

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

Militärausschuss der Europäischen Union (European Union Military Committee, EUMC, official translation)
The European Union Military Committee was established as a part of the EAD. It 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[80].

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 supports implementing measures laid out in the NIS Directive 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[81].

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 usually 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.

It is comprised of Member States' ambassadors in Brussels or representatives of Member States' foreign ministries. For Germany, they are dispatched by the AA. The

80 European External Action Service, European Union Military Committee (EUMC).
Official Journal of the European Communities, Beschluss des Rates vom 22. Januar 2001 zur Einsetzung des Militärausschusses der Europäischen Union.
81 ENISA, NIS Platform.

PSK is chaired by representatives of the EAD. It can voice recommendations on strategic concepts and political options towards the Council of the EU. The Chair of the EUMC participates in meetings of the PSL. Representatives of the EU CyberNet have briefed the PSK on the implementation of the EU Cybersecurity Strategy. The PSK meets regularly with the NAC and also receives periodic briefings from the NATO Secretary-General (or deputy) and the SACEUR (ACO)[82].

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 the 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 the national level, convenes in ten thematic configurations – such as Foreign Affairs, 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 based on 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 the 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 (HWPCI) 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 chairs the Foreign Affairs Council (FAC). The Chairman of the EUMC (CEUMC) is appointed by the Council of the EU and participates in meetings of the Council insofar as defense-related topics are discussed. The COSI includes senior officials from the

82 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.

interior and justice ministries of all EU Member States, representatives of the EK and the EAD. Representatives of Europol, Eurojust, CEPOL, or other relevant bodies can be invited as observers. OLAF reports regularly to the Council's anti-fraud working group. EUISS was established by the Council of the EU. The establishment of EU CyberNet has been provided for, among other things, in documents of the Council of the EU. A report on the role and responsibilities of participating actors within the JCU is to be developed by June 2022, which will then be submitted to the Council of the EU for a decision[83].

Reference Incident Classification Taxonomy Task Force (TF-CSIRT)
The TC-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, inter alia, representatives of ENISA and EC3[84].

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[85].

83 Council of the European Union, Cyberangriffe: EU plant Gegenmaßnahmen, einschließlich Sanktionen.
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, Der Rat der Europäischen Union.
Council of the European Union, The EU Integrated Political Crisis Response – IPCR – Arrangements.
European Commission, Anhang zur Empfehlung der Kommission über die koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen.
European Council/Council of the European Union, Horizontal Working Party on Cyber Issues (HWP).
European Court of Auditors, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
European Union, Rat der Europäischen Union.

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

85 SOGIS, Introduction.

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 created in the framework of PESCO project packages following the initiative of KdoCIR. A representative of relevant PESCO projects is envisaged as a supporting participant of the JCU[86].

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, Computer Security Incident Response Teams (CSIRTs), and prosecutors' offices, and strengthen preventative measures and investigative capabilities. ENISA, EC3/Europol, the EUCTF, CERT-EU and selected CSIRTs take part in the working group via respective subject matter experts[87].

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 has functioned as both the EK's central crisis management agency and as the central EU integrated political crisis response (IPCR) 24/7 contact point. If necessary, activation requests for the EU disaster and crisis management are being forwarded from Germany by the GMLZ to the ERCC[88].

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

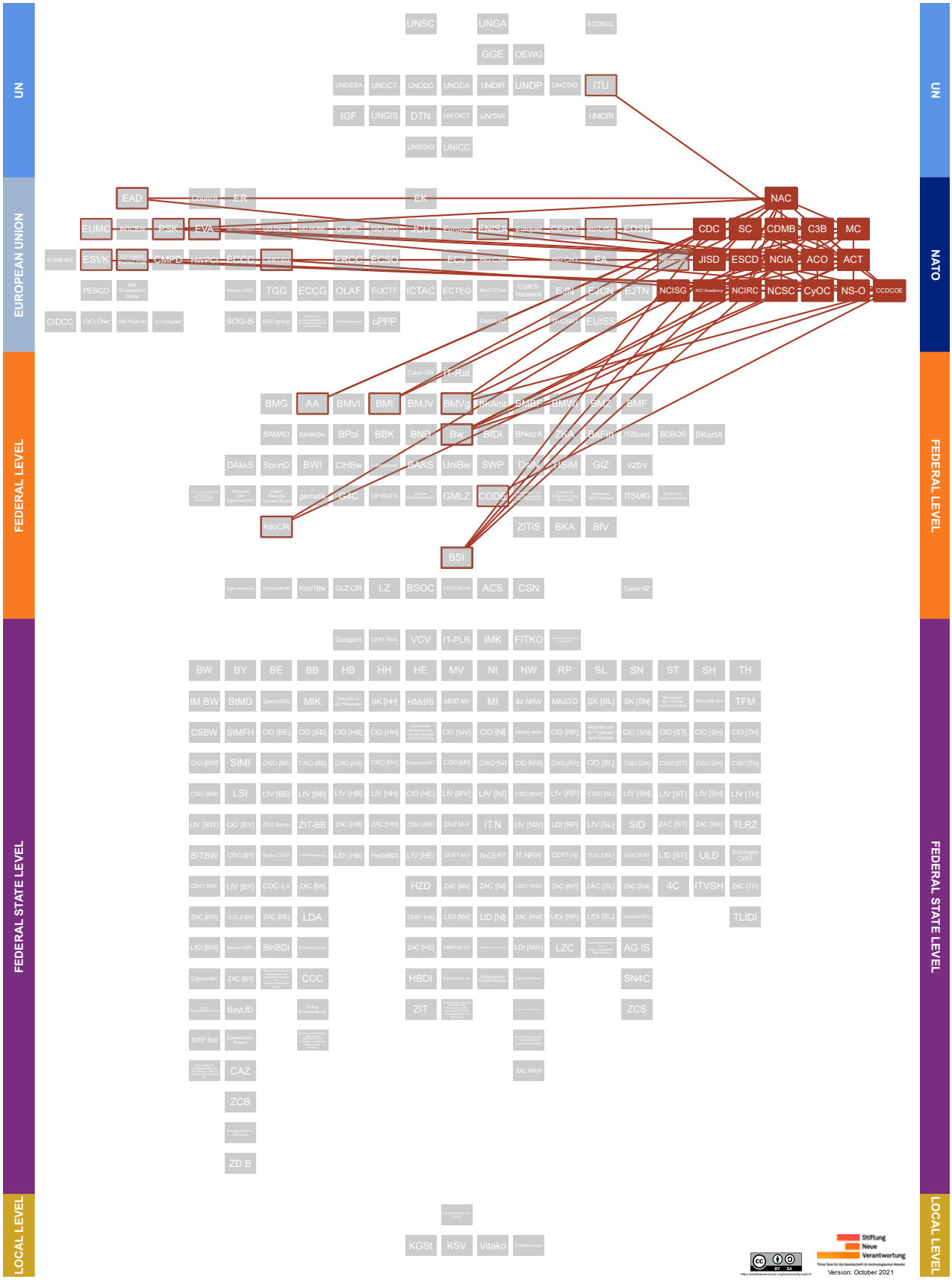
Zentrum für Informationsgewinnung und -analyse (EU Intelligence Analysis Centre, INTCEN, official translation)

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 strategic situational assessments, special reports and derives options for action from them. It forms a component of the 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.

INTCEN is located in the EAD. 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 Single Intelligence Analysis Capacity (SIAC). It collaborates with ENISA and is designated as a participating organization of the JCU. Together with Europol, INTCEN produces a threat analysis every six months, which it submits to COSI[89].

89 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".
European External Action Service, EU INTCEN Factsheet.
German Bundestag (Drucksache 19/489): Antwort der Bundesregierung auf die Kleine Anfrage: Pläne der Europäischen Kommission für eine geheimdienstliche "Europäische Aufklärungseinheit".
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.

6. Explanation – Actors at NATO level



Allied Command Operations (ACO)

Within NATO's military command structure, which consists of the Allied Command Operation (ACO) and the Allied Command Transformation (ACT), the ACO is responsible for planning and executing 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. Representatives of the ACO attend meetings of the C3B, the CDMB, and the SC. The SACEUR receives his or her instructions from the MC. ACO is in exchange with the JISD. The NCISG and the Cyber Defense Division in the ACO at the SACEUR are interdependent in their tasks. Together with the SECGEN, SACEUR has taken part in NATO briefings to the PSK[90].

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. Among others, it prepares cybersecurity exercises such as the NATO Cyber Coalition Exercise or the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX).

ACT representatives attend meetings of the SC, C3B, and CDMB. ACT is in exchange with the JISD. The Bundeswehr takes part in the NATO Cyber Coalition Exercise, which is carried out with the support of the NATO MC. The ENISA is represented in a visiting role. The KdoCIR also participates in CWIX, which the ACT manages on behalf of the NAC, the MC, and the C3B. NATO Centres of Excellence (CoE), such as the CCDCOE, are accredited through the ACT. ACT can commission the CCDCOE to take over specific duties. At the behest of ACT, the CCDCOE is currently taking over the function of Edu-

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

cation and Training Department Head (E&T DH) for areas relating to cyber, and thus coordinates education in this area, for example, at the NATO School Oberammergau (NS-O), which falls within ACT's mandate. Course offerings of the NCI Academy are prepared with the support of the ACT. The SACT and the Chief Executive of the EVA hold regular meetings[91].

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 an expert level, oversees and steers NATO's efforts and activities within the realm of cyber defense.

The 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 coordinated instruction from the AA, BMI, and BMVg. The BSI is involved in an advisory capacity during the instruction process[92].

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) and 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 cyber operations, supports alliance partners in strengthening their resilience, and cultivates political cyber defense collaborations and partnerships. Furthermore, the ESCD commands a Cyber Threat Assessment Cell, which monitors topics and developments relating to cybersecurity.

91 Allied Command Transformation, Who We Are.
German Armed Forces, Multinational Interoperabilität testen – CWIX 2021.
Joint Force Training Centre, CWIX 2021 Execution.
NATO, Cyber defence.

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

The ESCD was established based on the decision of the NAC. The ESCD leads the CDMB. Its Cyber Threat Assessment Cell operates in 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[93].

Joint Intelligence and Security Division (JISD)

The Joint Intelligence and Security Division within 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 analyzing 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 to contribute to a standardized consideration of the threat situation[94].

NATO Communications and Information Agency (NCIA)

The NATO Communications and Information Agency (NCIA) was founded after amalgamating 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.

93 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.

94 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.

Both the NATO Cyber Security Centre (NCSC) and the NCI Academy are subordinate to the NCIA. It also operates the NCIRC 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. It is represented on the CDMB and collaborates with the NCISG. 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 operational level[95].

NATO Communication and Information System Group (NCISG)

The NATO Communication and Information Systems Group is responsible for NATO's three so-called Signal Battalions, located in Wesel (Germany), Grazzanise (Italy), and Bydgoszcz (Poland). Annually, the NCISG organizes "Steadfast Cobalt", the largest communication and information systems exercise within NATO.

NCISG and the Cyber Defense Division in the ACO with the SACEUR are interdependent in their missions. Both are led by the same commander (COM NCISG and DCOS Cyberspace SHAPE). In addition, the NCISG and the NCIA work together. KdoCIR participates in Steadfast Cobalt[96].

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 operations around the clock. In this respect, the NCIRC TC is responsible for preventing, recognizing, and processing 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 incidents 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 is operated by the NCSC, which is subordinate to the NCIA. It supports the CyOC in situational awareness. The NCIRC CC also supports the CDMB with personnel and maintains relationships with other international organizations such as the EU. The NCIRC TC and the CERT-EU cooperate in a technical capacity to better infor-

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

96 German Armed Forces, CWIX 2021 findet als Remote Event statt.
NATO Communications & Information Systems Group, About us.
NATO Communications & Information Systems Group, Exercise STEADFAST COBALT 2021.
NATO Communications & Information Systems Group, Leadership.

mation 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 and Locked Shields[97]*.*

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, 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 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, updating 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 specific 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-O, the NCI Academy, the EVA, the EU Hybrid Fusion Cell, the ESVK, and the CODE at the University of the Bundeswehr. As one of the seven founding nations of CCDCOE, Germany holds the position of Deputy Director and participates in Locked Shield through representatives of the Bw and the BMVg. Together with the ITU and other actors, the CCDCOE was involved in preparing a guide for the development of a national cybersecurity strategy[98]*.*

97 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.

98 Background Conversation, 2021.
Council of the European Union, EU Cyber Defence Policy Framework.
NATO CCDCOE, About Us.
NATO CCDCOE, Training.
NATO CCDCOE, Research.

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), 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 through the NATO Headquarters C3 Staff (NHQC3S), a joint unit of the International Military Staff and the International Staff.

Apart from national and MC representatives, ACT and ACO also participate in the C3B. The C3B may initiate deliberations of the SC. 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[99].

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, 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 and is being supported by the NCIRC CC in terms of personnel[100].

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 CERTs of NATO alliance members. The NATO Industry Cyber Partnership (NCIP) between internal NATO actors, national CERT's, and industry rep-

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

resentatives 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 promote best practices.

The NCSC is housed within the NCIA. The NCIRC is subordinate to the NCSC. Exchange of information and close working relationships exist with the CyOC, promoted through their common location within SHAPE[101].

NATO Cyberspace Operations Centre (CyOC)
The establishment of the NATO Cyberspace Operations Center is slated for completion by 2023, when it should be fully operational. The CyOC aims to support all NATO activities in cyberspace at both strategic and operational levels 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.

To foster situational awareness, the CyOC is reliant on alliance members' intelligence information and is supported in fulfilling its duties inter alia through the Cyber Threat Assessment Cell (CTAC) of the ESCD in NATO HQ, the NCSC as well as the NCIRC. It is in constant communication with the NCIA, from which it receives status updates on NATO networks and to whose operational instructions it responds to in cases of cybersecurity incidents. CyOC is subordinate to the DCOS Cyberspace within the ACO and is located at SHAPE in Belgium[102].

NATO-Militärauschuss (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, cyber operations 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 their Chief of Defences representatives. The latter convene three times per year in the MC format.

101 NCIA, Securing the Cloud.
NCIA, What We Do: NATO's Cybersecurity Centre.
NICP, Objectives and Principles.
102 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.

The MC is responsible for advising the NAC on military policy issues. The Strategic Commanders of the ACT and the ACO receive their directions through the MC. It is among the addressees of JISD products and can initiate meetings of the SC. Germany is represented in the MC through representatives of the Bw. The MC regularly meets with its EU counterpart, the EUMC[103].

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 malicious cyber activity. In this respect, the NS-O among other things established a Cyber Security Certificate Programme together with the Naval Postgraduate School (NPS).

NS-O is subordinate to the ACT. Training and education at the NS-O in the field of cybersecurity and cyber defense is coordinated through the CCDCOE[104].

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 falls 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 fulfill 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[105].

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

103 European Parliament, Understanding EU-NATO cooperation: Theory and practice.
NATO, Military Committee.
U.S. Department of Defense, NATO Military Committee Gets Virtual Check on Alliance Missions.
104 NATO School, NATO School Oberammergau – Naval Postgraduate School Cyber Security Professional Programme Closure in Morocco.
NATO School, Organization.
105 NATO, Security Committee (SC).

Training Facility The Hague, Air Command and Control Systems Training Centre, and SHAPE CIS Training Centre. The standardization of course catalogs 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.

The NCI Academy is subordinate to the NCIA. Current course offerings at the NCI Academy were developed with the support of the ACT. The CCDCOE assumes the E&T DH for the NCI Academy in the field of cyber[106].

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, and 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, the NAC would decide 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 can 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 MC is responsible for advising the NAC on military policy issues, and the SC reports to the NAC at least once annually. The NAC endorsed the establishment of the Hybrid CoE and the establishment of the ESCD followed a decision of the NAC. It receives products from the JISD. 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[107].

106 NCIA, About the NCI Academy.
NCIA, Introducing the NCI Academy.
NCIA, 10,000 Cyber Defenders: Cyber education for the NATO-EU workforce.
107 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 Delegation of the Federal Republic of Germany to the North Atlantic Treaty Organization, Botschafter König.

7. 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 the first commissions are said to have been made by the end of 2020. The task of the Cyberagentur is to identify innovations and 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 instead 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. It is part of the NPCS. 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 a 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, staff councils of the Bw's procurement offices and academia[108].

Agentur für Sprunginnovationen (Federal Agency for Disruptive Innovation, SprinD, official translation)
SprinD, located in Leipzig, serves as a state instrument for innovation development. It supports research ideas deemed suitable as innovations and affiliate companies that promote potential innovations and create new jobs. 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.

108 Andre Meister and Anna Biselli, Bundesrechnungshof bezweifelt Sinn der neuen 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)
Federal Ministry of Defence, Technologiesouveränität erlangen – die neue 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.
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[109].

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. The CSN is linked to the ACS, which it complements with reactive offerings. The ACS is one of the addressees of the "täglicher Lagebericht IT-Sicherheit" (daily situation report IT Security, own translation) of the LZ. ACS participants include inter alia the BBK, BaFin, BKartA, BKA, BMVI, BMWi, Bw, an institute of the UniBw Munich, as well as Vitako. From stakeholders on the federal state and local level, the German County Association (KSV), the MWIDE NRW, the SenInnDS, the SID, and the ZCB are members. The MI of Lower Saxony and the Saarland Ministry of Finance and Europe are involved in the ACS as multipliers. TISiM exchanges information with its project sponsors within the framework of the ACS[110].

Auswärtiges Amt (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. Within its purview and for the federal administration abroad, for example, at German embassies, the AA is responsible for their ICT and ensuring their own communications network.

109 Deutschlandfunk, "Um Erfolg zu haben, müssen wir uns das Scheitern trauen".
Federal Ministry of Defence, Technologiesouveränität erlangen – die neue Cyberagentur.
Federal Ministry for Economic Affairs and Energy, Aufsichtsrat der Agentur für Sprunginnovationen SprinD tritt zur konstituierenden Sitzung zusammen.
Federal Ministry of Education and Research, Agentur für Sprunginnovationen.
Federal Ministry of Education and Research, Bundesregierung setzt Gründungskommission für die Agentur für Sprunginnovationen ein.
Lina Rusch, Potsdam oder Leipzig? Karliczek vertraut auf SprinD-Gründungsdirektor bei Standortfrage.
Tagesschau, Die Suche nach dem nächsten großen Ding.
110 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.

The AA is represented in the Cyber-SR. It alternates with the BMVg in providing the leadership of the BAKS and finances the SWP through third-party funding. It is among the addresses of the BfV's occasion-related classified reports ("Cyber-Spezial"). At the EU level, the AA is inter alia involved in HWPCI processes and discussions, part of the ESVK training network, and a member of the EU CyberNet's Advisory Board. The AA receives reports from the INTCEN and the EUMS INT. At the NATO level, the AA is represented by its Permanent Representative to NATO in the NAC and is involved, among other things, in the instruction process for German representatives in the CDC. Germany is a regular non-permanent member of the UNSC. In the past, representatives from Germany's Permanent Mission to the UN in New York have also participated in UNSC debates on cybersecurity. The AA has been/is responsible for German participation in the GGEs and the OEWGs. Representatives of the AA have also participated in meetings of the CCPCJ (ECOSOC) as well as the IEG Cybercrime (UNODC). Financially, the AA supports UNODA, UNIDIR, and UNODC. Together with the UNIDIR, the AA has hosted a cyber-related event in the past. The German Ambassador to the UN in Geneva is represented on the Board of Trustees of UNITAR, and another AA representative is represented on the Steering Committee of the German IGF (IGF-D)[111].

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 primarily being commissioned and 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 cyber operations.

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. In the future, security by design is to be given greater consideration in new IT procurements of the Bundeswehr as part of trilateral cooperation between the BSI, the Bundeswehr's CISO, and the BAAINBw[112].

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).

111 Federal Foreign Office, Auslands-IT.
Federal Foreign Office, Cyber-Außenpolitik.
Federal Foreign Office, Einrichtung einer Zuständigkeit für Cyber-Außenpolitik.
Federal Office of Justice, Gesetz über den Auswärtigen Dienst (GAD).

112 CIR Bundeswehr [@cirbw], #Informationssicherheit funktioniert am besten, wenn sie von Anfang an mitgedacht wird. Daher wollen @BSI_Bund,@BaainBw und #CISOBw #SecurityByDesign bei #IT-Beschaffungen... [Tweet].
Federal Office of Bundeswehr Equipment, Information Technology, and In-Service Support, Das BAAINBw.

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. The BAKS is part of the network of EU-wide training institutions of the ESVK[113].

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 malicious cyber activity, an exchange of information with the BSI is taking place. BaFin falls under the purview of the BMF and is represented as a partner in the Cyber-AZ[114].

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 cyber operations on the nation's critical infrastructure. In the past, the "Länder- und Ressortübergreifende Krisenmanagementübung" (Interstate and Interdepartmental Crisis Management Exercise, LÜKEX, own translation) organized by the BBK and held every two years has already focused on threats posed by cyber operations. The next LÜKEX in November 2022 will deal with the topic "Cyberangriff auf das Regierungshandeln" (Cyberattack on government action, own translation).

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. It can make usage of the digital radio operated by the BDBOS[115].

113 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.
114 Federal Financial Supervisory Authority, Aufgaben & Geschichte der BaFin.
Federal Financial Supervisory Authority, BaFinPerspektiven. Ausgabe 1 2020: Cybersicherheit.
115 Federal Office of Civil Protection and Disaster Assistance, Gemeinsames Melde- und Lagezentrum von Bund und Ländern.
Federal Office of Civil Protection and Disaster Assistance, Krisenübung für den Bevölkerungsschutz.
Federal Office of Civil Protection and Disaster Assistance, LÜKEX 22: Cyberangriff auf das Regierungshandeln.

Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (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 together with the BSI. The BOS Digital Radio Network is inter alia available to the BPol, BKA, ZKA, BBK, BfV, and LfV[116].

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 "Cyberabschirmung" (cyber shielding, own translation) encompasses all operational, reactive and preventive measures taken by BAMAD to counter intelligence and security-threatening activities, or extremist/terrorist efforts in the cyber and information space.

BAMAD falls under the purview of the BMVg and is represented in the Cyber-AZ. Information is exchanged between the BND, BfV, and BAMAD, and there are mutual obligations to provide information. It can draw on services provided by ZITiS. BAMAD receives reports from the INTCEN[117].

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

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

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-Württemberg and Bavaria). The BSI's second site in Freital oversees 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, the Bürger-CERT and the BSOC. Also, the CSN is located in the BSI. In addition to the federal and state administrations, all federal state CERTs organized in the VCV receive occasion-related cybersecurity alerts from the BSI. The CERT-Bund is also itself involved in the VCV. Together with the ITZ-Bund, the BSI has established a "Lenkungskreis Informationsfreiheit" (Steering Committee for Information Security, own translation) as well as a framework administrative agreement to enable closer cooperation between the two institutions. Moreover, the BSI has agreed on a cooperation agreement with the vzbv, which, among other areas, deals with digital consumer protection. In the event of a cybersecurity incident, BaFin exchanges information with the BSI. To secure the "Netze des Bundes" (Federal Networks, own translation), the BDBOS cooperates with the BSI as a partner authority. In addition, the BSI cooperates with the BfDI and, in the area of digital consumer protection, with the BKartA. The BSI is represented on the Advisory Board of the DsiN as well as the Cyber Security Cluster Bonn and cooperates with the G4C. In addition,

it is represented on the Supervisory Board of DAkkS and in the Steering Committee of the Initiative IT Security in the Economy. It is also involved in the Initiative for Economic Protection. Together with the BNetzA, the BSI has published an IT security catalog for electricity and gas networks, which all operators must implement. In addition to scientific representatives, the scientific working group of the Cyber-SR also includes a representative of the BSI. At the federal state level, the BSI cooperates or exchanges information with the IM BW, the IT.NRW, the LSI, the MASTD, the MEID MV, the MI Lower Saxony, the Ministry of Finance and Europe of Saarland, the SenInnDS, SK [SN], and ZAC NRW, among others. The Coordination Office for Cybersecurity North Rhine-Westphalia is designated as the state's central point of contact vis-à-vis the BSI. The BSI's Berlin liaison office is in exchange with the CDC-Lv. Together with the KSV, the BSI has, among other things, developed a basic IT protection profile for municipalities. It cooperates furthermore with ENISA, is a member of SOG-IS and the Stakeholder Community of the EU CyberNet, and is also 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). From the NATO side, this agreement was concluded with the ESCD[118].

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 cyber operations 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 operations and any respective incidents in Germany. The BfV also publishes publicly accessible so-called "Cyber-Briefs" in irregular intervals which provide 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. Information is

118 Background Conversations, 2019.
Fabienne Tegeler, Angebote des BSI für Kommunen.
Federal Government, Besserer Schutz vor Cyber-Angriffen.
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)
German Bundestag (Drucksache 19/3398), Antwort der Bundesregierung auf die Kleine Anfrage: Nationale und internationale Kooperationen des Bundesamtes für die Sicherheit in der Informationstechnik.
Lina Rusch, BSI bekommt KI-Ableger in Saarbrücken.

exchanged between the BfV, BND, and BAMAD, and there are mutual obligations to provide information. It is represented in the Cyber-AZ as well as the "Initiative Wirtschaftsschutz" and relies on the expertise of ZITiS. It can make usage of the digital radio operated by the BDBOS. In addition, the BfV's cyber defense unit exchanges information with its counterparts in the "Landesbehörden für Verfassungsschutz" (State Authorities for the Protection of the Constitution, LfV, official translation), if existent. In the past, the Berlin SenInnDS has transferred tasks of cyber defense to the BfV under an administrative agreement. It is one of the recipients of INTCEN reports, contributes information itself, and sends staff to the INTCEN[119].

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.

BfDI and BSI are cooperating. He or she is an advisory member of the IT-PLR. The BfDI regularly reviews the data and information processing of the ITZBund and has the right to inspect the files of ZITiS to monitor compliance with data protection regulations. The BfDI is represented in the Advisory Board of DsiN and the Advisory Board of the Cyber Security Cluster Bonn. Further contacts between the BfDI and the EDSB exist[120].

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 with federal ministries through the so-called "Spiegelreferate" (mirror departments, own translation). It encounters cybersecurity topics inter alia through its service and technical supervision of the BND and its financing of the SWP. The office of the "Bundesbeauftragte:r für Digitalisierung" (Federal Government Commissioner for Digitalization, official translation) is institutionally located in the BKAmt.

119 Domestic Intelligence Service of the Federal Republic of Germany, Cyberabwehr.
Domestic Intelligence Service of the Federal Republic of Germany, Akteure und Angriffsmethoden.
German Bundestag (Drucksache 19/2645), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.

120 Federal Commissioner for Data Protection and Freedom of Information, Aufgaben.
Federal Commissioner for Data Protection and Freedom of Information, Europäische Einrichtungen zur Strafverfolgung.
Federal Commissioner for Data Protection and Freedom of Information, Geschäftsverteilungsplan.
Federal Commissioner for Data Protection and Freedom of Information, 28. Tätigkeitsbericht zum Datenschutz 2019.

The BKAmt is represented in the Cyber-SR. The BND is subordinate to the BKAmt. The head of the BKAmt takes note of the activity report of the IT-PLR, acts as the IT Council's chair, the Federal Commissioner for Digitalization acts as one of his or her deputies. Institutional contributions to the SWP are paid from its budget. The BKAmt is among the addressees of classified reports ("Cyber-Spezial") from the BfV and from the INTCEN. It is represented on the Board of Trustees of the BAKS[121].

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[122].

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 cybercrime cases 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 online 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. To combat cybercrime, the BKA has also established various training programs in the area of ICT forensics. An internal basic training course on cybercrime is held annually.

The BKA is part of the BMI and participates in the ACS. It is represented in the Cyber-AZ, as well as in G4C and the "Initiative Wirtschaftsschutz". It is a partner of the GMLZ. The BSI has seconded a CSIRT-LE Liaison Officer to the BKA. It is represented on the

121 Federal Chancellery, Chef des Bundeskanzleramtes.
122 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.

DsiN Advisory Board and relies on the expertise of ZITiS. At the federal level, the CC department of the BKA assumes the tasks of the ZAC. The BKA has access to the digital radio system operated by the BDBOS. In addition to the ZITiS, the BKA is also involved in the KISTRA project funded by the BMBF. At the federal state level, the Cybercrime Department of the Mecklenburg-Western Pomerania State Criminal Police Office, the Central Office for the Fight against Information and Communication Crime [BW], and the ZCB, among others, cooperate with the BKA. The ZIT is the BKA's first point of contact for unresolved internet crimes with local jurisdiction in Germany and mass proceedings against several suspects nationwide. Together with the KSV and the BSI, the BKA has issued recommendations for local authorities on how to respond to ransom demands resulting from the use of encryption Trojans. The BKA is the German contact for Europol and serves as the National Unit. Representatives of the BKA have participated in meetings of the IEG Cybercrime (UNODC) at the UN level[123].

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 that 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 and the BAKS' Board of Trustees. Representatives of the BMJV have participated in meetings of the IEG Cybercrime (UNODC) as well as the CCPCJ (ECOSOC) at the UN level. It funds 97 percent of the vzbv's core work[124].

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 cen-

123 Datensicherheit.de, BKA: Bundeskriminalamt baut Cybercrimebekämpfung aus.
European Union Agency for Cybersecurity, 2020 Report on CSIRT-LE Cooperation: study of roles and synergies among selected countries.
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.
German Bundestag (Drucksache 19/2645), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.

124 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)

ters 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 BAMAD, the BAAINBw and the BAKS also fall under its purview. The Cyberagentur has been set up under joint leadership of the BMVg and BMI. The BMVg is provided with the GLZ CIR's analysis of the situation in the cyber and information space. At the EU level, it also receives reports from the INTCEN and the EUMS INT. Representatives of the BMVg are represented on the CODE Advisory Board and on the SWP Foundation Board. For its work in cyberspace, the BMVg relies on national and international cooperation and partnerships, such as those with the CIHBw or the NATO CCDCOE. It is part of the ESVK's network of EU-wide training institutions. At the NATO level, the BMVg is responsible for German representation in the C3B and is involved in the instruction process for the CDC[125].

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. In addition, a parliamentary state secretary of the BMI is represented in the Quadriga of the NPCS. Representatives of the BMI are also represented on the Advisory Board of the BAKS, the Foundation Board of the SWP, and the Advisory Board of the ITSMIG. The Cyberagentur was established under the joint leadership of BMI and the BMVg. The Federal

125 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.

Minister of the Interior participates in the IMK. The Coalition for Cyber Security is based on an agreement between the BMI and the Federation of German Industries. The BMI plays a coordinating role in the Initiative for Economic Protection. The BMI receives reports from the INTCEN and is involved in the German representation in the HWPCI. At the NATO level, it is represented in the SC and is involved in the instruction process for the German representative in the CDC. Representatives of the BMI have participated in meetings of the IEG Cybercrime (UNODC) and are represented in the Steering Committee of the German IGF (IGF-D)[126].

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 2015-2020" (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 Research Framework Program on IT Security "Digital. Secure. Sovereign." has replaced the research program "Selbstbestimmt und sicher in der digitalen Welt" (Self-determined and secure in the digital world, own translation).

The BMBF is represented in the Cyber-SR and supports the competency centers for IT Security. It has launched the Research Framework Program on IT Security "Digital. Secure. Sovereign." and is supervising it. Together with the BMWi, it has founded the SprinD. It supports the KISTRA project, in which among others the ZITiS and the BKA are involved. It is one of the providers of third-party funding for the SWP. In the context of Horizon 2020, the BMBF has a coordinating office and an initial information center for interested parties[127].

126 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.

127 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. Moreover, also the ITZBund falls within its purview. The BMF and BMZ are shareholders of the GIZ. Representatives of the BMF are represented on the Supervisory Board of the Cyberagentur, the Supervisory Board of SprinD, the Board of Trustees of the BAKS, and the Foundation Board of the SWP[128].

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 to develop an electronic data transmission infrastructure, which is the prerequisite for secure interconnection of the health care system[129].

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 regarding possible cyber operations on digital infrastructure.

The BMVI participates in the ACS. A representative of the BMVI is represented in the Steering Committee of the German IGF (IGF-D)[130].

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 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.

128 Federal Ministry of Finance, Grundelemente zur Cyber-Sicherheit. (Website deleted)
Federal Ministry of Finance, Themen.
129 Federal Ministry of Health, Aufgaben und Organisation.
Federal Ministry of Health, E-Health-Gesetz.
130 Federal Ministry of Transport and Digital Infrastructure, Krisenmanagement.

The BMWi is represented in the Cyber-SR. It has launched the "Initiative IT-Sicherheit in der Wirtschaft" and participates in the ACS. It is represented on the Advisory Board of DsiN, and the BNetzA, as well as the BKartA fall under its purview. SprinD was founded jointly by the BMWi and the BMBF. Representatives of the BMWi are members of the Advisory Board of gematik, the Advisory Board of ITSMIG, the Board of Trustees of the BAKS, and the Foundation Board of the SWP. It represents the Federal Republic of Germany as a shareholder of the DAkkS. The BMWi can participate in meetings of the MAG of the IGF and supports the IGF Trust Fund financially. A representative of the BMWi is also a member of the Steering Committee of the German IGF (IGF-D). A representative of the "Physikalisch-Technische Bundesanstalt" (Physical-Technical Federal Agency, own translation), which is within the BMWi's purview, chairs the UNECE's Working Group 6 (ECOSOC). The ITU lists the BMWi and the BNetzA as German member state institutions[131].

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. It is represented on the BAKS' Board of Trustees and is one of the SWP's third-party funders. The German contribution to the UNDP stems from the BMZ budget[132].

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 malicious cyber activity abroad that could lead to cyber espionage or sabotage in Germany and warns any affected actors within the 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. Information is 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. It can draw on ser-

131 Federal Ministry for Economic Affairs and Energy, IT-Sicherheit.
Federal Ministry for Economic Affairs and Energy, IT-Sicherheit für die Industrie 4.0.
132 Federal Ministry for Economic Cooperation and Development, Digitalisierung in der Entwicklungszusammenarbeit.
Federal Ministry for Economic Cooperation and Development, Grundsatzfrage: Warum brauchen wir Entwicklungspolitik?.

vices provided by ZITiS. Its staff is trained at the UniBw München, among others. The BND receives products from the EUMS INT and contributes reports to the INTCEN[133].

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 translation), the implementation of which is mandatory for all gas and electricity network providers. The ITU lists the BNetzA and the BMWi as participating German member state institutions[134].

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. The Executive Board of vzbv is represented in the Quadriga of the NPCS as a civil society representative[135].

133 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, Sicherheitsreacht des Bundes –Recht der Nachrichtendienste in Deutschland. (Website deleted)
134 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.
135 Federal Ministry of Justice and Consumer Protection, Verbraucherzentralen.
Federal Ministry of Justice and Consumer Protection, BSI und Verbraucherzentrale stärken digitalen Verbraucherschutz.
Verbraucherzentrale Bundesverband, Häufige Fragen (FAQ). (Website deleted)
Verbraucherzentrale Bundesverband, Über Uns.

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.

The BPol falls within the purview of the BMI. It is represented in the Cyber-AZ via liaison officers from the CERT BPol, is a partner of the GMLZ and draws on the expertise of ZITiS. It can make usage of the digital radio operated by the BDBOS. The CERT BPol is a guest of the CERT-Verbund[136].

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 of the "Streitkräftebasis" (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, KdoStratAufkl, as well as the "Zentrum für Cyber-Sicherheit" (Center for Cyber Security of the German Armed Forces, ZCSBw, own translation). Within the scope of "Amtshilfe" (administrative assistance, own translation), the Bundeswehr can support other authorities, for example, in incident management.

The Bw falls under the purview of the BMVg. It trains part of its staff at the UniBw (incl. CODE) and is represented in the Cyber-AZ and various national and international CERT networks. It also participates in the ACS. The Military Cyber Reserve supports the Bundeswehr in the performance of its tasks. Within the Bundeswehr, BAMAD inter alia analyzes and identifies extremist efforts and espionage projects. Germany is represented in the NATO MC by representatives of the Bundeswehr. BAAINBw supplies the Bundeswehr with IT and digitalized weapon systems. The BWI operates as the Bundeswehr's IT system house. At the working level, a cooperation between the Bw's CERT and the NCIRC TC exists. The BWI participates in the Cyber Coalition Exercise organized by the ACT and the Locked Shields exercise organized by the CCDCOE[137].

136 Background Conversations, 2019.
Bundespolizei kompakt, 04/2015.
European Union Agency for Cybersecurity, 2020 Report on CSIRT-LE Cooperation: study of roles and synergies among selected countries.
Federal Police, Startseite.
German Bundestag (Drucksache18/13555), Antwort der Bundesregierung auf die Kleine Anfrage: Aktuelle Situation und Ausrichtung der Bundespolizei.
137 German Armed Forces, Amtshilfe in Bitterfeld – IT-Soldaten im zivilen Einsatz.
German Armed Forces, Auftrag und Aufgaben der Bundeswehr.
German Armed Forces, Das Kommando Cyber- und Informationsraum.

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 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. The BAAINBw is responsible for steering the BWI. The CIHBw is located in the BWI in the form of a separate department. It is a multiplier of the ACS and has supported the Bundeswehr in establishing the GLZ CIR. The CERT of the BWI is represented in the National CERT Network[138].

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 part of the NPCS and based on an agreement between the BMI and the "Bundesverband der deutschen Industrie" (Federation of German Industries, BDI, official translation)[139].

Bundes Security Operations Center (Federal Security Operations Center, BSOC, own translation)
The Federal Security Operations Center uses systems and procedures for detection and analysis, such as antivirus signatures, technical platforms, and detectors to detect targeted and complex operations and thus contribute to the protection of government networks and the federal IT. These tools of operational cybersecurity, which

138 Bundesweite IT-Systemhaus GmbH, Unternehmensbroschüre.
Federal Ministry of Defence, Auf engere Kooperation geeinigt: Bundeswehr und BWI GmbH.
139 Federal Ministry of the Interior, Building and Community, Industrie und BMI etablieren Bündnis für Cybersicherheit.

are constantly being adapted to the threat situation and automated to the greatest possible extent, include, among other things, the collection and analysis of logging and sensor data as well as the detection and defense against malware in e-mails and web traffic. In addition, a "BSOC-Verbund" (BSOC-Alliance, own translation) has also been established to connect the BSI and federal IT service providers.

The BSOC is operated by the BSI[140].

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, 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 located in the BSI and cooperates with the LZ. It also cooperates with federal state-level CERTs within the framework of the VCV and the CERT-Verbund. Further working relationships exist inter alia with Hessen3C. At the European level, CERT-Bund cooperates with the EGC Group as well as ENISA. It is also involved in the CSIRTs network and the TF-CSIRT[141].

Cyber Innovation Hub der Bundeswehr (Cyber Innovation Hub of the German Armed Forces, CIHBw)
The CIHBw of the Bw offers its employees, in cooperation with startups, a platform to research and further develop innovative technologies, the goal is 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 developing disruptive technologies for the Bw.

140 Federal Office for Information Security, Abteilung OC – Operative Cyber-Sicherheit.
Federal Office for Information Security, Die Lage der IT-Sicherheit in Deutschland 2020.
Federal Office for Information Security, Digitalisierung in der Bundesverwaltung absichern.
141 CERT-Bund, Über CERT-Bund.
Federal Office for Information Security, CERT-Bund.
Federal Office for Information Security, Nationale und internationale Zusammenarbeit.

The CIHBw is a 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[142].

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 from 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.

The "Cyber-Reserve" supports the Bundeswehr in the performance of its tasks, in particular KdoCIR[143].

Cyber-Sicherheitsnetzwerk (Cyber Security Network, CSN, own translation)
The recently launched Cyber Security Network operates as a voluntary association of qualified experts. It intends to establish a nationwide decentralized structure to enable a "digital rescue chain" in the reaction and incident response to IT security incidents. The CSN is intended to serve as the first point of contact for SMEs and individual citizens. Its support services can vary and include support to self-help, a contact hotline, digital first responders, incident experts, or IT service providers with a team of incident experts. For this purpose, the CSN has also established a qualification program through which digital first responders and incident experts should be systematically trained on-site according to a standardized training program. In addition, spaces for the collective exchange of experiences should be created. These should also be collected in order to improve the targeting of recommendations with regard to preventive measures as well as reactive activities of the CSN itself. The CSN is supported by a "Geschäfts- und Koordinierungsstelle" (secretariat and coordination office, own translation), which is responsible for the organization of the CSN and its strategic direction.

142 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.
143 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.

The CSN is institutionally located within the BSI and linked to the ACS, which it complements with reactive propositions[144].

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 malicious cyber activity.

The BSI, KdoCIR of the Bw, and the BfDI are members of the Advisory Board of the Cyber Security Clusters Bonn e. V. The association is a multiplier of the ACS. In addition, the cluster is a partner of the North Rhine-Westphalian Competence Center for Cybersecurity in the Economy[145].

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[146].

144 Federal Office for Information Security, Curriculum zur Qualifikation von Vorfall-Experten.
Federal Office for Information Security, Cyber-Sicherheitsnetzwerk.
Federal Office for Information Security, Cyber-Sicherheitsnetzwerk: Informationen zum Cyber-Sicherheitsnetzwerk.

145 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.
Federal Office for Information Security, Liste von Multiplikatoren der Allianz für Cyber-Sicherheit.

146 Deutsche Akkreditierungsstelle, Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Bereich der Informationssicherheit/Cyber-Security für industrielle Automatisierungssysteme gemäß IEC 62443. (Website deleted)
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 (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. A representative of the GIZ is represented in the Advisory Board of the BAKS. Also, one representative of the GIZ is a member of the IGF's MAG[147].

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. It leads the consortium of TISiM[148].

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 deal 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. Every year, CODE holds an annual conference.

As part of the UniBwM, Bw personnel are also becoming scientifically trained at CODE. A representative of the BMVg sits on the CODE Advisory Board. It is in exchange with, among others, the Cyberagentur and the CCDCOE[149].

147 Background Conversations, 2018.
Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH, Bundesregierung.
Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH, Startseite.
148 Deutschland sicher im Netz, Presse.
149 University of the Bundeswehr Munich, Beirat des Forschungsinstituts CODE.
University of the Bundeswehr Munich, Forschungsinstitut CODE.
University of the Bundeswehr Munich, Forschungsinstitut CODE. Unsere Mission.
University of the Bundeswehr Munich, Program to the Annual Meeting CODE 2021.

Forschungsrahmenprogramm zur IT-Sicherheit "Digital. Sicher. Souverän." (Research Framework Program on IT Security "Digital. Secure. Sovereign.", own translation)

In June 2021, the German government approved a research framework program on IT security that will run until 2026 and will be supported with a total of 350 million euros. It replaces the German government's existing IT security research program "Selbstbestimmt und sicher in der digitalen Welt 2015–2020" (Self-determined and secure in the digital world 2015–2020, own translation), which ran from 2015-2020, and brought together interdepartmental measures and activities in this area. The research framework program is intended to further expand technological sovereignty in the field of IT security research and set the framework for future research funding for a secure digital world. To this end, seven strategic goals have been defined: (1) data and know-how, (2) digital change, (3) democracy and society, (4) privacy and data protection, (5) innovation and transfer, (6) leading minds, and (7) Germany and Europe. In its implementation, the research framework program is intended to support scientific competencies and excellence, further develop innovation ecosystems and transfer, bring actors together, enable social dialog, and align research on a European and international level.

The research framework program was introduced by the BMBF and is being supervised by it[150].

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).

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[151].

150 Federal Ministry of Education and Research, Digital.Sicher.Souverän.Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit.
Federal Ministry of Education and Research, Digital, sicher und souverän in die Zukunft.
Federal Ministry of Education and Research, Karliczek: Mit exzellenter IT-Sicherheitsforschung legen wir den Grundstein für eine sichere digitale Welt. Bundesregierung startet 350-Millionen-Rahmenprogramm zur IT-Sicherheitsforschung.

151 Lina Rusch, Digitaler Staat: Agenturen in den Startlöchern.
IT Planning Council, FITKO. (Website deleted)
Matthias Punz, Rechtlicher Rahmen für FITKO-Start steht.

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[152].

Gemeinsames Lagezentrum Cyber- und Informationsraum (GLZ CIR)
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.

KdoCIR was jointly responsible for the establishment of the GLZ CIR, and 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[153].

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. 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. It cooperates with the LZ. If necessary, the GMLZ forwards activation requests for EU disaster and crisis management to the ERCC[154].

152 Federal Ministry of Health, E-Health-Gesetz.
Gematik, Die elektronische Gesundheitskarte. (Website deleted)
Gematik, Telematikinfrastruktur.
Gematik, Über uns.
153 BWI, Von Big Data bis KI – Bundeswehr und BWI starten zweite Ausbaustufe des Gemeinsamen Lagezentrums CIR.
Federal Ministry of Defence, Lagezentrum Cyber- und Informationsraum im Pilotbetrieb.
German Bundestag (Drucksache 19/2645), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.
154 Deutsches Zentrum für Luft- und Raumfahrt, Katastrophen- und Krisenmanagement.
Federal Ministry of the Interior, Building and Community, Das Gemeinsame Melde- und Lagezentrum von Bund und Ländern.

German Competence Centre against Cyber Crime (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 through daily exchange of information between official cooperation partners and members.

The G4C cooperates with the BKA and the BSI[155].

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 by 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 a "Lenkungskreis Informationssicherheit" (Steering Committee for Information Security, own translation) together with the BSI to create closer cooperation between both institutions. The BfDI regularly reviews the data and information processing of the ITZBund[156].

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[157].

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 cybercrime. Within the portal's user area, companies can access official security recommendations and contact them directly, if necessary.

155 German Competence Centre against Cyber Crime e. V. (G4C), Über uns.
156 Federal Information Technology Centre, ITZBund und BSI intensivieren Zusammenarbeit für mehr IT-Sicherheit.
Federal Information Technology Centre, IT-Sicherheit.
Federal Information Technology Centre, Über uns.
157 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.

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[158].

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. The CISO [SN] is represented in federal state working group of the IMK[159].

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 Government 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 chairs of the "IT-Planungsrat". A further part of the "IT-Planungsrat" is

158 Domestic Intelligence Service of the Federal Republic of Germany, Initiative Wirtschaftsschutz.
Domestic Intelligence Service of the Federal Republic of Germany, Initiative Wirtschaftsschutz. Das Informationsportal.

159 CISO der niedersächsischen Landesverwaltung, Cybersicherheit in der Landesverwaltung.
Conference of Interior Ministers, 213. Sitzung der Innenministerkonferenz.
Email exchange with representatives of the BSI in February 2020.
German Bundesrat, Innenministerkonferenz.
Secupedia, Nationales Cyber-Abwehrzentrum.

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. From the federal states, the CIO [BW], CIO [BY], CIO [BE], CIO [HB], CIO [HE], CIO [MV], CIO [NI], CIO [NW], CIO [RP], CIO [SL], CIO [SN], CIO [ST], and CIO [TH] are members. Brandenburg is represented by a state secretary of the MIK, Hamburg by the head of the SK [HH], and Schleswig-Holstein by a state secretary of the MELUND SH. 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[160].

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[161].

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 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[162].

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

160 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. (Website deleted)
IT Planning Council, IT-Planungsrat.
IT Planning Council, Umsetzung Leitlinie InfoSic. (Website deleted)
IT Planning Council, Zusammensetzung des IT-Planungsrates.
161 Der Beauftragte der Bundesregierung für Informationstechnik, IT-Rat.
162 TeleTrust, IT Security made in Germany.

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 deputy, 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) is subordinate to the CISOBw. The latter is home to the CERTBw and provides incident response teams in the event of malicious cyber activity within 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. For Germany's participation in the NATO CWIX conducted by ACT, the KdoCIR acts as exercise coordinating command. It also participates in the Steadfast Cobalt exercise organized annually by the NCISG. 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[163].

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). The "Schule für Informationstechnik der Bundeswehr" (Bundeswehr Information Technology School, ITSBw, own translation), which trains Bundeswehr personnel, is under the command of the KdoITBw. Among other things, IT specialists should be recruited at the ITSBw for future assignments in the "Cyber/IT-Dienst" (cyber/IT service, Cyber/ITDst, own translation) within the framework of test screenings at its Cyber/IT Evaluation Center (CITEC).

163 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.
German Armed Forces, Multinational Interoperabilität testen – CWIX 2021.

KdoIITBw is subordinate to the KdoCIR and belongs to the Bw's CIR[164].

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 KdoCIR[165].

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.

The three competency and research centers for IT security are funded by the BMBF[166].

164 Bernd Kammermeier, Zentrum für Cyber-Sicherheit der Bundeswehr – Moderner Dienstleister für IT-Sicherheit.
Bund, Kommando Informationstechnik der Bundeswehr (KdoITBw).
German Armed Forces, CITEC – Experten testen Experten.
German Armed Forces, Kommando Informationstechnik der Bundeswehr.
German Armed Forces, Schule Informationstechnik der Bundeswehr.
German Armed Forces, Zentrum für Cyber-Sicherheit der Bundeswehr.
165 Bund, Kommando Strategische Aufklärung (KdoStratAufkl).
Bund, Zentrum Cyberoperationen (ZCO).
German Armed Forces, Das Zentrum Cyber-Operationen.
German Armed Forces, Kommando Strategische Aufklärung.
166 Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.

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 cyber incidents.

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 BWL, CERT-NRW, and CERT-rlp are involved on the part of federal states[167].

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 supported by a permanent scientific working group, 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. The Cyber-AZ sends its annual report to the Cyber-SR. Besides the federal government, the Cyber-SR is also to provide impetus for the IMK[168].

Nationaler Pakt Cybersicherheit (National Cybersecurity Pact, NPCS, own translation)
The "Nationaler Pakt Cybersicherheit" is an initiative of the BMI 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, users, and pub-

167 Deutscher CERT-Verbund, Überblick.
Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: CERT-Verbund.

168 Der Beauftragte der Bundesregierung für Informationstechnik, Cyber-Sicherheitsrat.
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.
Fraunhofer-Institut für Sichere Informationstechnologie, Beratung aus der Forschung. Wissenschaftliche Arbeitsgemeinschaft Nationale Cyber-Sicherheit.

lic 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", which has recently published a "gesamtgesellschaftliche Erklärung zur Cybersicherheit" (whole-of-society declaration on cybersecurity, own translation).

Part of the pact is 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[169].

Nationales Cyber-Abwehrzentrum (National Cyber Defense Centre, Cyber-AZ, official translation)
The Cyber-AZ is tasked with optimizing operational cooperation between government agencies regarding various hazards in cyberspace and coordinating the appropriate protective and defensive measures. For this purpose, all information about cyber operations on IT infrastructure is collected in the Cyber-AZ, located within the BSI. Daily situation briefings, as well as a weekly meeting dealing with "Koordinierte 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, located in the BSI, is a cooperation platform between the BSI, BPol, BKA, BfV, BBK, BND, KdoCIR, BaFin, and BAMAD. The ZKA is involved on an associated basis. At the federal state level, partners of the Cyber-AZ are the Cyber Defence Bavaria, the Central Office Cybercrime Bavaria as well as the Central and Contact Office Cybercrime North Rhine-Westphalia. It sends its annual report to the Cyber-SR. In addition to the authorities mentioned above, the "Cyber-Lage" is sent to the 16 LfV's as well as the 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. It also receives situation analyses of the GLZ CIR and cooperates with the LZ[170].

169 Federal Ministry of the Interior, Building and Community, Gesamtgesellschaftliche Erklärung zur Cybersicherheit.
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.

170 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, Das Nationale 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.

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 the national IT crisis response center whenever necessary.

The LZ is located in the BSI and works 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[171].

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. A structural reform, "CIR 2.0", has been initiated to be completed by 2025. Among other things, it provides for the bundling of responsibility and competencies in the areas of conception and further development within a "Cyber and Information Domain Warfare Centre" as well as the consolidation of all elements in a "Systemhaus Cyber- und Informationsraum/Zentrum Digitalisierung der Bundeswehr" (System House Cyber and Information Space/Center Digitization of the Bundeswehr, own translation). Moreover, CIR 2.0 envisages the establishment of a CIR training center by 2025. CIR has a Vulnerability Disclosure Policy (VDPBw), in the context of which it seeks active reporting of vulnerabilities in the IT systems of the Bundeswehr by external parties.

CIR is a part of the Bw and is led by the KdoCIR, to which the KdoITBw and the KdoStratAufkl are subordinate. CIR 2.0 is intended to strengthen cooperation with the BSI and further develop collaboration with the Cyber-AZ. In the past, CIR has exchanged information with the BBK on cooperation within the Cyber-AZ[172].

171 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.

172 BBK [@BBK_Bund], BBK-Präsident @armin_schuster sprach heute mit dem Inspekteur #Cyber- und #Informationsraum Vizeadmiral Dr. Thomas Daum über die Zusammenarbeit von @BBK_Bund… [Tweet].
German Armed Forces, Auftrag des Organisationsbereichs CIR.
German Armed Forces, CIR 2.0 – Der Organisationsbereich CIR gliedert sich neu.
German Armed Forces, "Liebe Hacker, hiermit laden wir Sie herzlich ein…".

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, developing common positions, and offering network opportunities that 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. UP KRITIS receives the "täglichen Lagebericht IT-Sicherheit" (daily situation report IT security, own translation) of the LZ[173].

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 of representatives from BKAmt, BMBF, BMZ, BMI, AA, BMF, BMWi, and BMVg, for example. In the past, a representative of the SWP has been invited to a special meeting of the Cyber-SR[174].

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 security with information, instruction manuals, concrete measures, action plans, and best practices. Industry, academic, and administrative experts stand at the ready

173 Federal Office for Information Security. Geschäftsstelle UP KRITIS, UP KRITIS. Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland.
Federal Office for Information Security and Federal Office of Civil Protection and Disaster Assistance, 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.

174 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.

for precisely 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 that is led by DsiN. It also exchanges information with project sponsors within the framework of the ACS[175]*.*

Universitäten der Bundeswehr (Universities of the German Federal Armed Forces, UniBw, official translation)
The UniBw Munich (UniBwM) and UniBw Hamburg (HSU/UniBw Hamburg) scientifically train officers and officer cadets. 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 the UniBwM is home to CODE, an inter-faculty research center in Munich. A representative of the UniBw is a member of the Advisory Board of the BAKS. An institute of UniBwM is participating in the ACS. The UniBw is also involved as a project partner in the EU-HYBNET project, which inter alia also includes ZITiS and GD JRC[176]*.*

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 CERT-Länder 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 a direct reporting channel in the event of IT security incidents.

The BSI, CERT-Bund, CERTs on the federal state level, and the LSI are involved in the VCV. The members of the VCV receive the daily "Lagebericht IT-Sicherheit" (IT security status report, own translation) of the LZ as well as the "Cyber-Lage" (cyber situation report, own translation) of the Cyber-AZ. Working relations exist with the Hessen3C. The CISO [MV] represents Mecklenburg-Western Pomerania in the VCV[177]*.*

175 Deutschland sicher im Netz, Transferstelle.
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.
176 University of the Bundeswehr Munich, Hintergrundinformationen.
University of the Bundeswehr Munich, Studium.
177 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). (Website deleted)

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 crime, and 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), 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. Other project partners of the EU-HYBNET project include the Hybrid CoE, 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 constitutes the establishment of a joint development center for the purpose of IT surveillance together with the BKA. ZITiS maintains exchanges with the Cyberagentur[178].

Zollkriminalamt (Customs Investigation Bureau, ZKA, official translation)
The ZKA is responsible for preventing and solving moderate as well as severe 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.

178 Andre Meister, Hacker-Behörde bekommt 66 Millionen Euro.
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.
EU-HYBNET, Project Partners.
Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: Zentrale Stelle für Informationstechnik im Sicherheitsbereich.
Florian Flade, Mysterium ZITiS. Was macht eigentlich die "Hackerbehörde"?.

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. It has the digital radio of the BDBOS at its disposal. In the past, a representative of the ZKA has been part of the German delegation for a meeting of the IEG Cybercrime at the UN level (UNODC)[179].

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

8. Explanation – Actors at Federal State Level

8.1. Baden-Wuerttemberg

The Baden-Wuerttemberg State Criminal Police Office is participating in the Sicherheitskooperation Cybercrime.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:** "Ministerium für Inneres, Digitalisierung und Migration" (Ministry of the Interior, Digitalization and Migration, IM BW, own translation), "Abteilung 7: Digitalisierung" (Department 7: Digitization, own translation), "Referat 72: Digitalisierungsstrategie und Cybersicherheit" (Division 72: Digitization Strategy and Cybersecurity, own translation).

  The BSI and Baden-Wuerttemberg have agreed to intensify their cooperation[180].

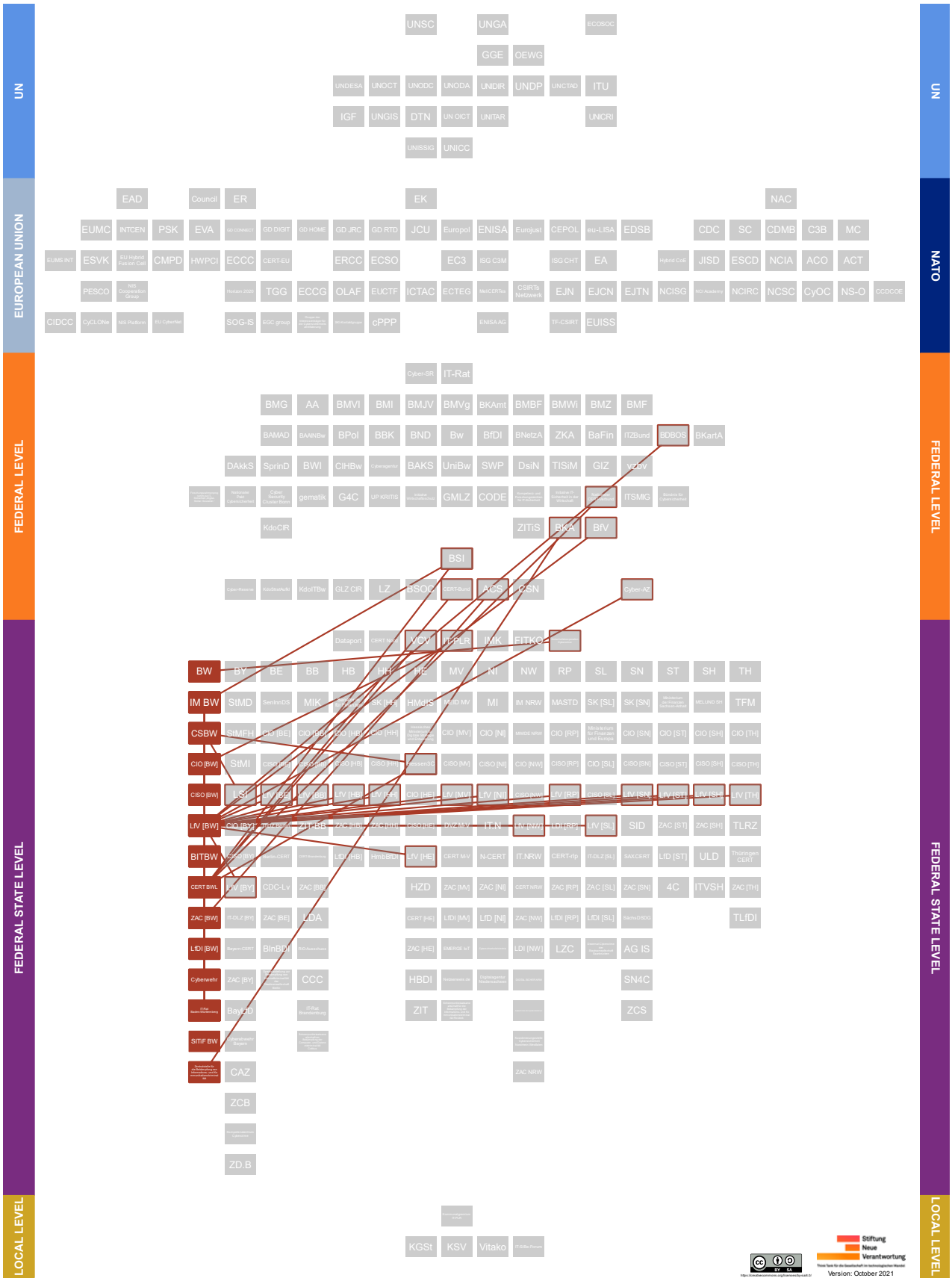
- **State Commissioner for Information Technology (CIO [BW]):** The CIO [BW] is responsible for the IT strategy of the state administration and the E-Government Strategy, among other things. The CIO also acts as Chief Digital Officer (CDO) of the state administration.

  The CIO is assigned to the IM BW. He or she represents Baden-Wuerttemberg in the IT-PLR[181].

- **Chief Information Security Officer of the State Administration (CISO [BW]):** In Baden-Wuerttemberg, the CISO is appointed by the IM BW. The CISO is responsible for defining and updating information security guidelines for the state administration, *advising the CIO [BW], and preparing an annual report on the implementation and effectiveness of IT security measures, which is submitted to the CIO [BW]*[182].

- **IT Service Provider of the Federal State Administration: "**Landesoberbehörde IT Baden-Württemberg" (State Authority IT Baden-Württemberg, BITBW, own translation), *which falls within the purview of the IM BW*[183].

180 Ministerium des Inneren, für Digitalisierung und Migration, Organigramm.
Wim Orth, BSI und BaWü kooperieren eng bei Cyber-Sicherheit. (Website deleted)
181 CIO Baden-Württemberg, Stefan Krebs.
182 Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg, Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit.
183 Landesoberbehörde IT Baden-Württemberg, Über BITBW.


UN
EUROPEAN UNION
FEDERAL LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
NATO
UNSC
UNGA
ECOSOC
GGE
OEWG
UNDESA
UNOCT
UNODC
UNODA
UNIDIR
UNDP
UNCTAD
ITU
IGF
UNGIS
DTN
UN OICT
UNITAR
UNICRI
UNISSIG
UNICC
EAD
Council
ER
EK
NAC
EUMC
INTCEN
PSK
EVA
GD CONNECT
GD DIGIT
GD HOME
GD JRC
GD RTD
JCU
Europol
ENISA
Eurojust
CEPOL
eu-LISA
EDSB
CDC
SC
CDMB
C3B
MC
EUMS INT
ESVK
EU Hybrid Fusion Cell
CMPD
HWPCI
ECCC
CERT-EU
ERCC
ECSO
EC3
ISG C3M
ISG CHT
EA
Hybrid CoE
JISD
ESCD
NCIA
ACO
ACT
PESCO
NIS Cooperation Group
Horizon 2020
TGG
ECCG
OLAF
EUCTF
ICTAC
ECTEG
MeliCERTes
CSIRTs Netzwerk
EJN
EJCN
EJTN
NCISG
NCI Academy
NCIRC
NCSC
CyOC
NS-O
CCDCOE
CIDCC
CyCLONe
NIS Platform
EU CyberNet
SOG-IS
EGC group
cPPP
ENISA AG
TF-CSIRT
EUISS
Cyber-SR
IT-Rat
BMG
AA
BMVI
BMI
BMJV
BMVg
BKAmt
BMBF
BMWi
BMZ
BMF
BAMAD
BAAINBw
BPol
BBK
BND
Bw
BfDI
BNetzA
ZKA
BaFin
ITZBund
BDBOS
BKartA
DAkkS
SprinD
BWI
CIHBw
BAKS
UniBw
SWP
DsiN
TISiM
GIZ
vzbv
gematik
G4C
UP KRITIS
GMLZ
CODE
ITSMIG
KdoCIR
ZITiS
BKA
BfV
BSI
Cyber-Reserve
KdoSKB
KdoITBw
GLZ CIR
LZ
BSOC
CERT-Bund
ACS
LCSN
Cyber-AZ
Dataport
CERT Nord
VIDIS
ITPLR
IMK
FITKO
BW
BY
BE
BB
HB
HH
NI
MV
NI
NW
RP
SL
SN
ST
SH
TH
IM BW
StMD
SenInnDS
MIK
SK [HE]
HMdIS
MIDI MV
MI
IM NRW
MASTD
SK [SL]
SK [SN]
MELUND SH
TFM
CSBW
StMFH
CIO [BE]
CIO [BB]
CIO [HB]
CIO [HH]
CIO [MV]
CIO [NI]
MWIDE NRW
CIO [RP]
CIO [SN]
CIO [ST]
CIO [SH]
CIO [TH]
CIO [BW]
StMI
CISO [BE]
CISO [BB]
CISO [HB]
CISO [HH]
hessen3C
CISO [MV]
CISO [NI]
CIO [NW]
CISO [RP]
CIO [SL]
CISO [SN]
CISO [ST]
CISO [SH]
CISO [TH]
CISO [BW]
LSI
LfV [BE]
LfV [BB]
LfV [HB]
LfV [HH]
LfV [MV]
LfV [NI]
LfV [RP]
LfV [SN]
LfV [ST]
LfV [SH]
LfV [TH]
LfV [BW]
CIO [BY]
ZAC [BB]
ZAC [HB]
ZAC [HH]
DVZ M-V
IT.N
LfV [NW]
LDI [RP]
LfV [SL]
SID
ZAC [ST]
ZAC [SH]
TLRZ
BITBW
CISO [BY]
BaCo-CERT
LDI [HB]
HmbBfDI
LfV [HE]
CERT M-V
N-CERT
IT.NRW
CERT-rlp
IT-DLZ [SL]
SAX.CERT
LfD [ST]
ULD
Thüringen CERT
CERT BWL
LfV [BY]
CDC-LV
ZAC [BB]
HZD
ZAC [MV]
ZAC [NI]
CERT NRW
ZAC [RP]
ZAC [SL]
ZAC [SN]
4C
ITVSH
ZAC [TH]
ZAC [BW]
IT-DLZ [BY]
ZAC [BE]
LDA
CERT [HE]
LfDI [MV]
LfD [NI]
ZAC [NW]
LfDI [RP]
LfDI [SL]
SaxInfoSID
TLfDI
LfDI [BW]
Bayern-CERT
BlnBDI
RIO-Assistenz
ZAC [HE]
EMERGE IoT
LDI [NW]
LZC
AG IS
Cyberwehr
ZAC [BY]
CCC
HBDI
SN4C
BayLfD
IT-Rat Brandenburg
ZIT
ZCS
SITiF BW
CAZ
ZAC NRW
ZCB
ZD.B
KGSt
KSV
Vitako
Stiftung Neue Verantwortung
Version: October 2021

- **Computer Emergency Response Team (CERT):** The CERT BWL is located at BIT-BW. *It cooperates with ZAC [BW] and is represented in the CERT-Verbund*[184].

- **State Authority for the Protection of the Constitution185 (LfV [BW]):** Within the Baden-Wuerttemberg State Authority for the Protection of the Constitution, Department 4 is primarily concerned with cybersecurity-related fields of work. It is responsible for counterintelligence and cyber defense as well as secret and sabotage protection. In the future, the area of cyber defense shall be strengthened.

  LfV and LKA cooperate, among other things, within the framework of the "Gemeinsame Informations- und Analysestelle" (Joint Information and Analysis Center, GIAS, own translation)[186].

- **Institutional location of the "Zentrale Ansprechstelle Cybercrime für die Wirtschaft" (Central Contact Points for Cybercrime of the Police Forces of the Federal States for the Economy, ZAC [BW], own translation**[187]): "Landeskriminalamt Baden-Württemberg" (State Criminal Police Office Baden Wuerttemberg, LKA BW, own translation). If required, the ZAC also has an internal task force "Digitale Spuren" (Digital Traces, own translation), which is constituted of experts from all areas of specialization.

  When contacted by companies from Karlsruhe, Rastatt, or Baden-Baden, reference is made to the possible involvement of the Cyberwehr. The LKA BW is participating in the ACS as a multiplier[188].

- **State Data Protection Authority**: "Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit Baden-Württemberg" (State Commissioner for Data Protection and Freedom of Information Baden-Wuerttemberg, LfDI [BW], own translation)[189].

184 Landtag von Baden-Württemberg, Stellungnahme des Ministeriums für Inneres, Digitalisierung und Migration: Verhinderung und Aufklärung von Cybercrime-Straftaten.
Staatsministerium Baden-Württemberg, Systeme des Landesamtes für Geoinformation wieder in Betrieb.

185 For the sake of uniformity, all LfV are referred to as state authorities ("Landesbehörden"). In BW, BY, HB, HH, HE, and SN, the LfV's are organized as a state office ("Landesamt").

186 Landesamt für Verfassungsschutz Baden-Württemberg, Aufbau und Organisation.
Landesamt für Verfassungsschutz Baden-Württemberg, Cyberspionage.
Landtag von Baden-Württemberg, Stellungnahme des Ministeriums für Inneres, Digitalisierung und Migration: Verhinderung und Aufklärung von Cybercrime-Straftaten.
Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg, Berichterstattung zur Cybersicherheitsagentur.

187 The ZAC make themselves 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.

188 Landespolizeipräsidium Baden-Württemberg, Zentrale Ansprechstelle Cybercrime für Unternehmen und Behörden.
Landtag von Baden-Württemberg, Stellungnahme des Ministeriums für Inneres, Digitalisierung und Migration: Verhinderung und Aufklärung von Cybercrime-Straftaten.

189 Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Aufgaben und Zuständigkeiten.

Other actors in Baden-Wuerttemberg:

Cybersicherheitsagentur Baden-Württemberg (Cybersecurity Agency Baden-Wuerttemberg, CSBW, own translation)
In February 2021, Baden-Wuerttemberg began setting up its cybersecurity agency based in Stuttgart. Its tasks include defending against cybersecurity threats and protecting societal processes from cyber operations. Furthermore, the CSBW shall provide information, offer advice, connect existing players and act as a competence center, for example, for training courses, on cyber security. In addition, the CSBW operates as a central coordination and reporting point for Baden-Wuerttemberg's public administration in all cybersecurity-related contexts. As such, the CSBW is inter alia dedicated to coordinating statewide measures as well as collecting and evaluating all information required for the defense against cybersecurity threats – particularly on security vulnerabilities, malware, operations that have occurred or been attempted against cybersecurity as well as the approach observed in these activities. Among other things, these findings are supposed to be incorporated into a statewide current situation picture that will be shared with other agencies. The CSBW can also issue warnings, advice, and recommendations. If necessary and with the agreement of the respective state agency, it can also investigate the information technology security of their respective infrastructure.

The IM BW is responsible for the official and technical supervision of the CSBW, to which it is subordinate. The CSBW reports to the IM BW and the IT Council Baden-Wuerttemberg at least once a year in the form of a report. The CSBW can – under the condition of necessity and upon explicit request – support the LfV [BW] and law enforcement agencies by providing technical expertise, for example, in the context of searches. The LKA and LfV [BW] were involved in drafting the "Cybersicherheitsgesetz" (Cybersecurity law, own translation), which established the CSBW. The CSBW shall serve as the central Baden-Wuerttemberg's point of contact for cybersecurity issues for other actors at the federal state (including Hessen3C and LSI), federal, EU, and international levels[190].

Cyberwehr (Cyber Defence, own translation)
The "Cyberwehr" is a contact and information center for small and medium-sized businesses as well as a cyber incident 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 the nationwide development of regional first-response infrastructures for IT security incidents. The established hotline serves as a

190 Landesrecht BW Bürgerservice, Gesetz für die Cybersicherheit in Baden-Württemberg (Cybersicherheitsgesetz – CSG).
Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg, Cybersicherheitsagentur Baden-Württemberg.

first point of contact and consistent emergency number in the event of a cyber incident; it usually 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 operation. Through legal regulations, it has exclusive powers in the context of law enforcement in solving a case or in the prevention of further malicious cyber activity.

The Cyberwehr works closely with the ZAC [BW], and the LfV [BW] in the field of cyber-espionage as well as the CERT BW[191].

IT-Rat Baden-Württemberg (IT Council Baden-Wuerttemberg, own translation)
The IT Council decides on Baden-Wuerttemberg's IT standards, prepares both its e-government as well as IT strategy, and advises the state's CIO on coordinating the interdepartmental use of e-government and information technology. Its deliberations are prepared by an "Arbeitskreis Informationstechnik" (Information technology working group, AK-IT, own translation), which also monitors the implementation of previous decisions.

The IT Council is chaired by the state CIO [BW] and is managed by the IM BW. The IT Council is made up of the "Amtschefs:innen" (heads, own translation) of the ministries in Baden-Wuerttemberg. Members in an advisory capacity include the BITBW, the CSBW, and the LfDI. Representatives of the latter three are also represented in the AK-IT as advisory members[192].

Sicherheitszentrum IT der Finanzverwaltung Baden-Württemberg (IT Security Center of the Financial Administration Baden-Württemberg, SITiF BW, own translation)
The SITiF BW, which is based in Karlsruhe, pools the IT security of various offices of Baden-Wuerttemberg's financial administration. It conducts permanent monitoring as well as regular penetration tests and audits to protect the IT infrastructure. By these means, it intends to identify incident scenarios and IT security-related anomalies as early as possible. In addition, employees should be supported through training courses, among other things. SITiF BW is located at the Landeszentrum für Datenverarbeitung (State Center for Data Processing, LZfD, own translation) at the "Oberfinanzdirektion Karlsruhe" (Karlsruhe Regional Finance Office, own translation)[193].

191 Cyberwehr, Die Cyberwehr.
Staatsministerium Baden-Württemberg, Landesregierung initiiert "Cyberwehr Baden-Württemberg".
192 CIO Baden-Württemberg, Aufgaben des CIO/CDO.
Landesrecht BW Bürgerservice, Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg (E-Government-Gesetz Baden-Württemberg – EGovG BW).
193 Staatsministerium Baden-Württemberg, Sicherheitszentrum IT in der Finanzverwaltung vorgestellt.

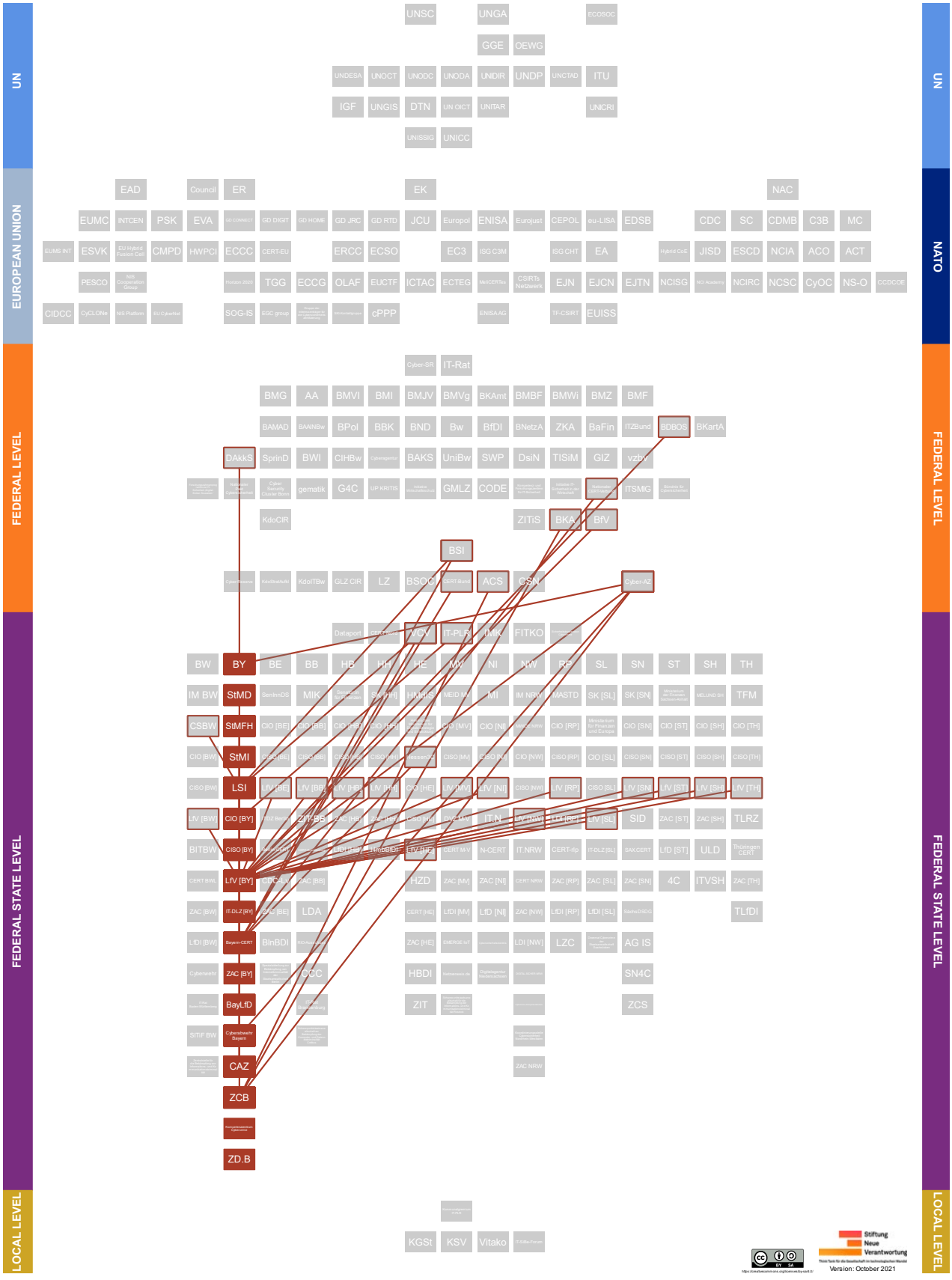
Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität (Central Office for the Fight against Information and Communication Crime, own translation)

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-Wuerttemberg[194].

194 Ministerium der Justiz und für Europa Baden-Württemberg, Zentralstelle für die Bekämpfung von informations- und Kommunikationskriminalität eingerichtet. (Website deleted)

8.2. Bavaria


UN
EUROPEAN UNION
NATO
FEDERAL LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
UNSC
UNGA
ECOSOC
GGE
OEWG
UNDESA
UNOCT
UNODC
UNODA
UNIDIR
UNDP
UNCTAD
ITU
IGF
UNGIS
DTN
UN OICT
UNITAR
UNICRI
UNISSIG
UNICC
EAD
Council
ER
EK
NAC
EUMC
INTCEN
PSK
EVA
GD CONNECT
GD DIGIT
GD HOME
GD JRC
GD RTD
JCU
Europol
ENISA
Eurojust
CEPOL
eu-LISA
EDSB
CDC
SC
CDMB
C3B
MC
EUMS INT
ESVK
EU Hybrid Fusion Cell
CMPD
HWPCI
ECCC
CERT-EU
ERCC
ECSO
EC3
ISG C3M
ISG CHT
EA
Hybrid CoE
JISD
ESCD
NCIA
ACO
ACT
PESCO
NIS Cooperation Group
Horizon 2020
TGG
ECCG
OLAF
EUCTF
ICTAC
ECTEG
MeliCERTes
CSIRTs Netzwerk
EJN
EJCN
EJTN
NCISG
NCI Academy
NCIRC
NCSC
CyOC
NS-O
CCDCOE
CIDCC
CyCLONe
NIS Platform
EU CyberNet
SOG-IS
EGC group
cPPP
ENISA AG
TF-CSIRT
EUISS
Cyber-SR
IT-Rat
BMG
AA
BMVI
BMI
BMJV
BMVg
BKAmt
BMBF
BMWi
BMZ
BMF
BAMAD
BAAINBw
BPol
BBK
BND
Bw
BfDI
BNetzA
ZKA
BaFin
ITZBund
BDBOS
BKartA
BAkkS
SprinD
BWI
CIHBw
BAKS
UniBw
SWP
DsiN
TISiM
GIZ
vzbv
Cyber Security Cluster Bonn
gematik
G4C
UP KRITIS
GMLZ
CODE
ITSMIG
KdoCIR
ZITiS
BKA
BfV
BSI
Cyber Reserve
KdoSKUA
KdoITBw
GLZ CIR
LZ
BSOC
CERT-Bund
ACS
CSN
Cyber-AZ
Dataport
VIVOV
IT-PLR
IMK
FITKO
BW
BY
BE
BB
HB
HH
HE
MV
NI
NW
RP
SL
SN
ST
SH
TH
IM BW
StMD
SenInnDS
MIK
HMdIS
MEID
MI
IM NRW
MASTD
SK [SL]
SK [SN]
MELUND SH
TFM
CSBW
StMFH
CIO [BE]
CIO [BB]
CIO [HB]
CIO [HE]
CIO [MV]
CIO [NI]
CIO [RP]
CIO [SN]
CIO [ST]
CIO [SH]
CIO [TH]
CIO [BW]
StMI
CISO [BE]
CISO [BB]
CISO [HB]
CISO [HE]
CISO [M]
CISO [NI]
CIO [NW]
CISO [RP]
CIO [SL]
CISO [SN]
CISO [ST]
CISO [SH]
CISO [TH]
CISO [BW]
LSI
LfV [BE]
LfV [BB]
LfV [HB]
LfV [HE]
LfV [MV]
LfV [NI]
CISO [NW]
LfV [RP]
CISO [SL]
LfV [SN]
LfV [ST]
LfV [SH]
LfV [TH]
LfV [BW]
CIO [BY]
ZITiS Base
ZITiS BE
ZAC HB
ZAC HE
ZAC MV
IT.N
LfV [NW]
LfD [RP]
LfV [SL]
SID
ZAC [ST]
ZAC [SH]
TLRZ
BITBW
CISO [BY]
LfV [HE]
CERT-Rip
CERT-MV
N-CERT
IT.NRW
CERT-rlp
IT-DLZ [SL]
SAX.CERT
LfD [ST]
ULD
Thüringen CERT
CERT BWL
LfV [BY]
CCDCoE
ZAC [BB]
HZD
ZAC [MV]
ZAC [NI]
CERT NRW
ZAC [RP]
ZAC [SL]
ZAC [SN]
4C
ITVSH
ZAC [TH]
ZAC [BW]
IT-DLZ [BY]
ZAC [BE]
LDA
CERT [HE]
LfDI [MV]
LfD [NI]
ZAC [NW]
LfDI [RP]
LfDI [SL]
SächsDSDG
TLfDI
LfDI [BW]
Bayern-CERT
BInBDI
ZAC [HE]
EMERGE IoT
LDI [NW]
LZC
AG IS
Cyberwehr
ZAC [BY]
CCC
HBDI
SN4C
BayLfD
ZIT
ZCS
SITiF BW
Cybersabwehr Bayern
CAZ
ZCB
ZD.B
KGSt
KSV
Vitako
Stiftung Neue Verantwortung
Version: October 2021

Bavaria is represented in the Cyber-AZ by its Cyberabwehr Bayern and the "Bamberger Schwerpunktsstaatsanwaltschaft Cyber" (Bamberg Focus Prosecutor's Office Cyber, own translation). It is also one of the shareholders of DAkkS.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:**
  - "Bayerisches Staatsministerium für Digitalisierung" (Bavarian State Ministry for Digitalization, StMD, own translation), "Abteilung B: Digitale Verwaltung, IT-Strategie und IT-Recht" (Department B: Digital Management, IT Strategy and IT Law, own translation), "Referat B1: Grundsatzfragen, IT-Strategie und IT-Recht, Unternehmensportal + Referat B2: IT-Planungsrat, Föderale IT-Kooperation (FITKO), Single Digital Gateway" (Division B1: Policy Issues, IT Strategy and IT Law, Company portal + Division B2: IT Planning Council, Federal IT Cooperation, Single Digital Gateway, own translation)[195].
  - "Bayerisches Staatsministerium der Finanzen und für Heimat" (Bavarian State Ministry of Finance and Home Affairs, StMFH, own translation), "Abteilung VII: Digitalisierung, Breitband und Vermessung" (Department VII: Digitization, Broadband and Measurement, own translation), "Referat 77: IT-Strategie, IT-Sicherheit, IT-Infrastruktur" (Division 77: IT Strategy, IT Security, IT Infrastructure, own translation)[196].
  - "Bayerisches Staatsministerium des Innern, für Sport und Integration" (Bavarian State Ministry of the Interior, for Sport and Integration, StMI, own translation), "Abteilung E: Verfassungsschutz, Cybersicherheit" (Department E: Protection of the Constitution, Cybersecurity, own translation)[197].

- **State Commissioner for Information Technology (CIO [BY]):** The CIO in Bavaria is responsible, for example, for the IT and E-Government Strategies and administrative digitization.

  The position is currently being filled by the "Bayerische Staatsministerin für Digitales" (Bavarian Minister of State for Digital Affairs, own translation) of the StMD. He or she represents Bavaria on the IT-PLR[198].

- **Chief Information Security Officer of the State Administration (CISO [BY]):** Bavaria's CISO is responsible for the implementation of IT security measures within the Bavarian public administration and reports to the head of StMFH's Department VII.

195 Bayerisches Staatsministerium für Digitales, Organisationsplan.
196 Bayerisches Staatsministeriums der Finanzen und für Heimat, Organisationsplan.
197 Bayerisches Staatsministerium des Innern, für Sport und Integration, Organigramm.
Bayerisches Staatsministerium des Innern, für Sport und Integration, Schutz vor Cybergefahren.
198 Bayerisches Staatsministerium für Digitales, IT-Beauftragte der Bayerischen Staatsregierung.

He or she is based in the StMFH and is responsible for the technical supervision of the Bavarian CERT[199].

- **IT Service Provider of the Federal State Administration:** "IT-Dienstleistungszentrum des Freistaats Bayern" (IT Service Center of the Free State of Bavaria, IT-DLZ [BY], own translation) is attached to the "Bayerische Landesamt für Digitalisierung, Breitband und Vermessung" (Bavarian State Office for Digitization, Broadband, and Measurement, LDBV, own translation), *which is part of the StMFH*[200].

- **CERT**: The Bayern-CERT is located at the LSI.

  It participates in the National CERT Network[201].

- **State Authority for the Protection of the Constitution (LfV [BY]):** In Bavaria, Department 5 of the Bavarian State Authority for the Protection of the Constitution is inter alia responsible for economic protection and counterintelligence.

  The CAZ and its subordinate Cyberabwehr Bayern are located at the LfV [BY][202].

- **Institutional location of the ZAC [BY]**: "Bayerisches Landeskriminalamt" (State Criminal Police Office, own translation). The Bavarian ZAC also offers preventive advice and is available not only to companies but also to citizens[203].

- **State Data Protection Authority**: "Bayerische:r Landesbeauftragte:r für den Datenschutz" (Bavarian State Commissioner for Data Protection, BayLfD, own translation).

  He or she participates in the Cyberabwehr Bayern[204].

199 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.
200 Bayerisches Staatsministerium der Finanzen und für Heimat, Behörden und Staatsbetriebe im Ressort.
Landesamt für Digitalisierung, Breitband und Vermessung, IT-Dienstleistungszentrum des Freistaats Bayern.
201 Landesamt für Sicherheit in der Informationstechnik, Staatsverwaltung.
202 Landesamt für Verfassungsschutz Bayern, Organisation.
Landesamt für Verfassungsschutz Bayern, Spionageabwehr / Wirtschaftsschutz.
203 Bayerische Polizei, Zentrale Ansprechstelle Cybercrime – Kontakt für Unternehmen.
Cyberabwehr Bayern, Cybersicherheit für bayerische Unternehmen und Behörden.
Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: Initiativen der Landespolizeien.
204 Der Bayerische Landesbeauftragte für den Datenschutz, Cybersicherheit.

Other actors in Bavaria:

Cyberabwehr Bayern (Cyber Defence Bavaria, own translation)
"Cyberabwehr Bayern" is an information and coordination platform established that guarantees the 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 assisting in acute situations by means of recording, evaluating, and passing on information on operations 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. 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 located within the CAZ of the LfV [BY]. Part of the Cyberabwehr Bayern is the "Bayerisches Landeskriminalamt" (State Criminal Police Office, LKA [BY], own translation), the LSI, the ZCB, the "Bayerische Landesamt für Datenschutzaufsicht" (State Office for Data Protection Supervision of Bavaria, own translation), the BayLfD, as well as the CAZ. It is represented as a partner in the Cyber-AZ[205].

Cyber-Allianz-Zentrum (Cyber-Alliance Centre, CAZ, own translation)
The CAZ supports companies based in Bavaria, as well as local universities and operators of critical infrastructure, in the fields of prevention and defense against electronic operations. 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 operations.

The CAZ was the first institutional pillar of the "Initiative Cybersicherheit Bayern" (Cybersecurity Initiative of Bavaria, own translation) of the StMI and falls under the purview of the LfV [BY][206].

Kompetenzzentrum Cybercrime (Cybercrime Competency Center, own translation)
The "Kompetenzzentrum Cybercrime – Bayern" (Department 54) was established at the "Landeskriminalamt Bayern" (State Criminal Police Office, own translation). One of its main tasks is to simulate crisis management with companies and author-

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

ities responsible for public order – especially during emergency situations, such as a cyber incident. It also takes on cases of cybercrime that are of supra-regional significance and cannot be processed by local police services[207].

Landesamt für Sicherheit in der Informationstechnik Bayern (State Office for Information Security, LSI, own translation)
Since its founding, the LSI has been responsible for protecting Bavarian IT infrastructure. Its mission is to prevent threats to the security of information technology, assist public agencies connected to the government network in defending against such threats, develop minimum standards and verify compliance with them, and issue warnings. Upon request, the LSI can also provide advice and assistance to state and local government entities, public companies, critical infrastructure operators, and other entities of critical importance to the body politic.

The LSI is a member of the VCV. It hosts the Bayern-CERT and cooperates with the BSI. It participates in the Cyberabwehr Bayern. When necessary and explicitly requested, the LSI can support the LfV [BY], Bavarian law enforcement agencies, and the state police by providing technical expertise. The LSI is subordinate to the StMFH[208].

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 ZCB is a member of the ACS[209].

Zentrum Digitalisierung.Bayern (Center for Digitization Bavaria, ZD.B, own translation)
The ZD.B is intended to serve as a cross-regional research and cooperation platform in Bavaria and promote cooperation between industry and science, help shape so-

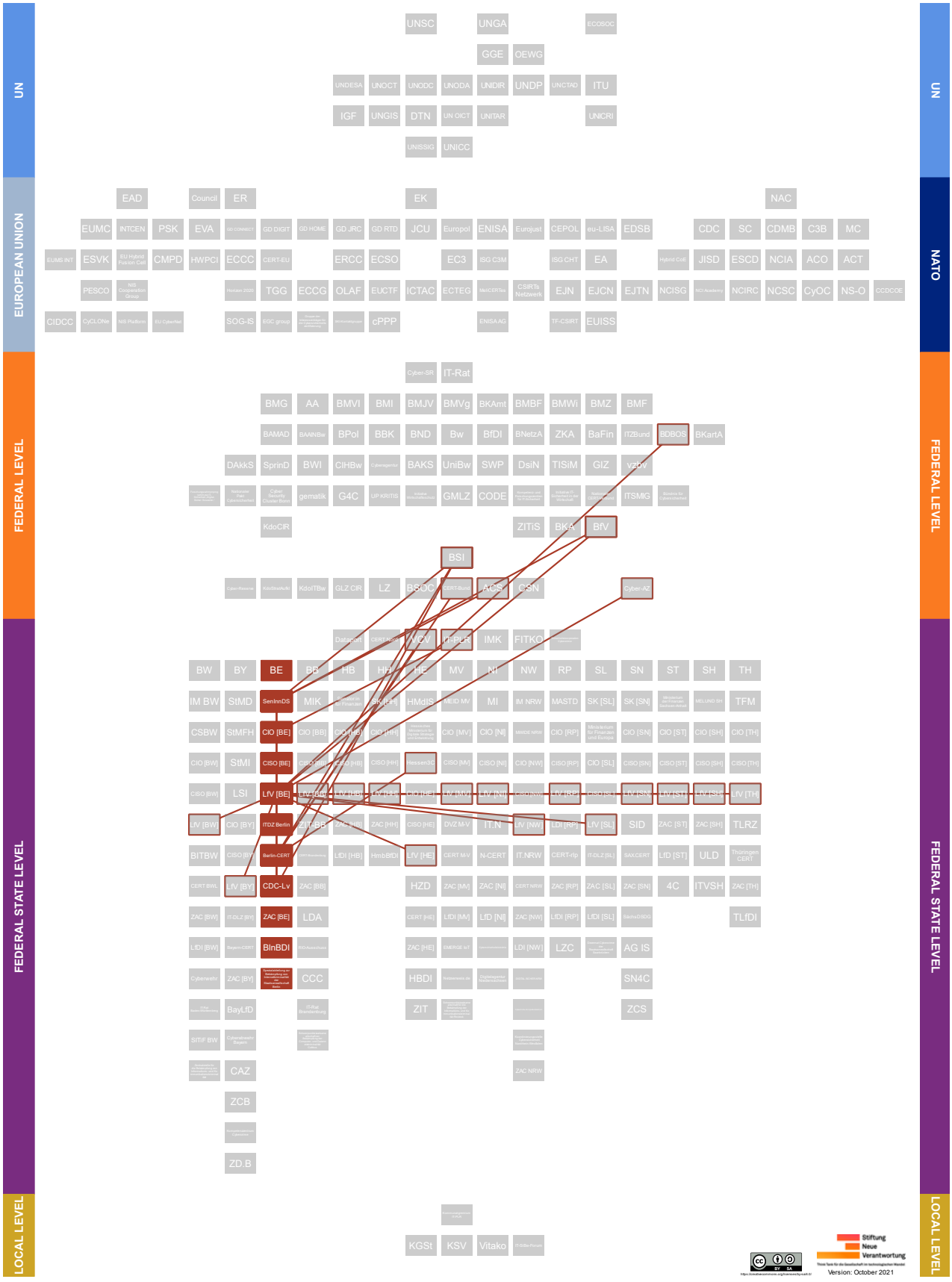
207 Bayerische Staatsregierung, Cyber-Kompetenzzentrum im Landeskriminalamt.
208 Bayerische Staatskanzlei, Gesetz über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz – BayEGovG).
Landesamt für Sicherheit in der Informationstechnik Bayern, Startseite.
209 Federal Office for Information Security, Teilnehmerliste der Allianz für Cyber-Sicherheit.
Generalstaatsanwaltschaft Bamberg, Zentralstelle Cybercrime Bayern (ZCB).

cietal dialog, and support the promotion of young people and researchers. As one of a total of 11 platforms, the ZD.B also has a thematic platform for cybersecurity. Offers of the thematic platforms are open to the Bavarian economy, science, and municipalities. The platform for cybersecurity aims to improve the competitiveness of Bavarian companies and their resilience to cyber operations, raise awareness for cybersecurity issues in the economy and society, and contribute to public discourse in this context.

The ZD.B was established by the "Bayerische Staatsministerium für Wirtschaft, Landesentwicklung und Energie" (Bavarian Ministry of Economy, Regional Development and Energy, StMWi, own translation) as a lead project of the "BAYERN DIGITAL" (Bavaria Digital, own translation) set of measures[210].

210 Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie, Zentrum Digitalisierung.Bayern. Bayerisches Staatsministerium für Wissenschaft und Kunst, Zentrum Digitalisierung.Bayern. Zentrum Digitalisierung.Bayern, ZD.B-Themenplattform Cybersecurity. Schutz gegen digitale Bedrohungen.

8.3. Berlin


UN
EUROPEAN UNION
NATO
FEDERAL LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
UNSC
UNGA
ECOSOC
GGE
OEWG
UNDESA
UNOCT
UNODC
UNODA
UNIDIR
UNDP
UNCTAD
ITU
IGF
UNGIS
DTN
UN OICT
UNITAR
UNICRI
UNISSIG
UNICC
EAD
Council
ER
EK
NAC
EUMC
INTCEN
PSK
EVA
GD CONNECT
GD DIGIT
GD HOME
GD JRC
GD RTD
JCU
Europol
ENISA
Eurojust
CEPOL
eu-LISA
EDSB
CDC
SC
CDMB
C3B
MC
EUMS INT
ESVK
EU Hybrid Fusion Cell
CMPD
HWPCI
ECCC
CERT-EU
ERCC
ECSO
EC3
ISG C3M
ISG CHT
EA
Hybrid CoE
JISD
ESCD
NCIA
ACO
ACT
PESCO
NIS Cooperation Group
Horizon 2020
TGG
ECCG
OLAF
EUCTF
ICTAC
ECTEG
MeliCERTes
CSIRTs Netzwerk
EJN
EJCN
EJTN
NCISG
NCI Academy
NCIRC
NCSC
CyOC
NS-O
CCDCOE
CIDCC
CyCLONe
NIS Platform
EU CyberNet
SOG-IS
EGC group
cPPP
ENISA AG
TF-CSIRT
EUISS
Cyber-SR
IT-Rat
BMG
AA
BMVI
BMI
BMJV
BMVg
BKAmt
BMBF
BMWi
BMZ
BMF
BAMAD
BAAINBw
BPol
BBK
BND
Bw
BfDI
BNetzA
ZKA
BaFin
ITZBund
BDBOS
BKartA
DAkkS
SprinD
BWI
CIHBw
Cyberagentur
BAKS
UniBw
SWP
DsiN
TISiM
GIZ
vzbv
Cyber Security Cluster Bonn
gematik
G4C
UP KRITIS
GMLZ
CODE
ITSMIG
KdoCIR
ZITiS
BKA
BfV
BSI
Cyber-Reserve
KdoStratAufkl
KdoITBw
GLZ CIR
LZ
BSOC
CERT-Bund
ACS
CSN
Cyber-AZ
DataLab
CERT-Bund
NCAZ
IT-PLR
IMK
FITKO
BW
BY
BE
BB
HB
HH
HE
MV
NI
NW
RP
SL
SN
ST
SH
TH
IM BW
StMD
SenInnDS
MIK
HMdIS
MEID MV
MI
IM NRW
MASTD
SK [SL]
SK [SN]
MELUND SH
TFM
CSBW
StMFH
CIO [BE]
CIO [BB]
CIO [HB]
CIO [HH]
CIO [MV]
CIO [NI]
MWIDE NRW
CIO [RP]
CIO [SN]
CIO [ST]
CIO [SH]
CIO [TH]
CIO [BW]
StMI
CISO [BE]
CISO [BB]
CISO [HB]
CISO [HH]
hessen3C
CISO [MV]
CISO [NI]
CISO [NW]
CISO [RP]
CISO [SL]
CISO [SN]
CISO [ST]
CISO [SH]
CISO [TH]
CISO [BW]
LSI
LfV [BE]
LfV [BB]
LfV [HB]
LfV [HH]
BLfV [HE]
LfV [MV]
LfV [NI]
LfV [NW]
LfV [RP]
LfV [SN]
LfV [ST]
LfV [SH]
LfV [TH]
LfV [BW]
CIO [BY]
ITDZ Berlin
ZIT SH
ZAC [HB]
ZAC [HH]
CISO [HE]
DVZ M-V
IT.N
LfV [NW]
LDI [RP]
LfV [SL]
SID
ZAC [ST]
ZAC [SH]
TLRZ
BITBW
CISO [BY]
Berlin-CERT
LfD [HB]
HmbBfDI
LfV [HE]
CERT M-V
N-CERT
IT.NRW
CERT-rlp
IT-DLZ [SL]
SAX.CERT
LfD [ST]
ULD
Thüringen CERT
CERT BWL
LfV [BY]
CDC-Lv
ZAC [BB]
HZD
ZAC [MV]
ZAC [NI]
CERT NRW
ZAC [RP]
ZAC [SL]
ZAC [SN]
4C
ITVSH
ZAC [TH]
ZAC [BW]
IT-DLZ [BY]
ZAC [BE]
LDA
CERT [HE]
LfD [MV]
LfD [NI]
ZAC [NW]
LfD [RP]
LfD [SL]
SAxInfoDSG
TLfDI
LfD [BW]
Bayern-CERT
BInBDI
ZAC [HE]
EMERGE IoT
LDI [NW]
LZC
AG IS
Cyberwehr
ZAC [BY]
CCC
HBDI
Notdienst.de
SN4C
BayLfD
ZIT
ZCS
SITiF BW
Cyberabwehr Bayern
CAZ
ZAC NRW
ZCB
ZD.B
KGSt
KSV
Vitako
Stiftung Neue Verantwortung
Version: October 2021

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics: "**Senatsverwaltung für Inneres und Sport" (Senate Department for the Interior and Sport, SenInnDS, own translation), **"**Abteilung III: Öffentliche Sicherheit und Ordnung" (Department III: Public Safety and Order, own translation), **"**Referat III E: Ressourcen, IT-Angelegenheiten für Polizei und Feuerwehr, Cybersicherheit" (Division III E: Resources, IT matters for police and fire departments, cybersecurity, own translation). Division III C hosts a "Arbeitsgruppe Cybersicherheit" (Working Group Cybersecurity, AG Cybersicherheit, own translation) and works primarily on critical infrastructure protection and cybercrime as identified areas of expertise.

  SenInnDS and the BSI have signed a declaration of intent to strengthen their cooperation. Division III of the SenInnDS is a member of the ACS[211].

- **State Commissioner for Information Technology (CIO [BE]):** In Berlin, the "Staatssekretär:in für Informations- und Kommunikationstechnik" (State Secretary for Information and Communications Technologies, own translation) in the SenInnDS assumes the position of the state's CIO and reports to the "Innensenator" (Interior Senator, own translation).

  He or she represents the state of Berlin on the IT-PLR[212].

- **Chief Information Security Officer of the State Administration (CISO [BE]):** Berlin's CISO is directly attached to the State Secretary for Information and Communications Technologies in the SenInnDS. In addition to performing tasks for the implementation and control of processes and standards in the area of information security, the CISO [BE] disposes a direct right of presentation towards the CIO [BE]. *For the realm of IT security, the CISO [BE] oversees technical control of the ITDZ Berlin*[213].

- **IT Service Provider of the Federal State Administration:** "IT-Dienstleistungszentrum Berlin" (IT Service Center Berlin, ITDZ Berlin, own translation).

  Legal supervision falls under the responsibility of the SenInnDS[214].

211 Bundesamt für Sicherheit in der Informationstechnik und Senatsverwaltung für Inneres und Sport, Absichtserklärung zur vertieften Kooperation zwischen dem Bundesamt für Sicherheit in der Informationstechnik und der Senatsverwaltung für Inneres und Sport des Landes Berlin.
Senatsverwaltung für Inneres und Sport, Arbeitsgruppe Cybersicherheit: Über uns.
Senatsverwaltung für Inneres und Sport, Organigramm.
Senatsverwaltung für Inneres und Sport, Stärkung der Bund-Länder-Zusammenarbeit im Bereich Cyber-Sicherheit.

212 CIO, Sabine Smentek wird CIO vom Land Berlin.

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

214 Berliner Vorschriften- und Rechtsprechungsdatenbank, Gesetz über die Anstalt des öffentlichen Rechts IT-Dienstleistungszentrum Berlin.
ITDZ Berlin, Profil.

- **CERT**: The Berlin-CERT is operated by the ITDZ Berlin[215].

- **State Authority for the Protection of the Constitution (LfV [BE]):** Berlin's SenInnDS 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[216].

- **Institutional location of the ZAC [BE]**: "Landeskriminalamt Berlin" (State Criminal Police Office Berlin, own translation)[217].

- **State Data Protection Authority: "**Berliner Beauftragte:r für Datenschutz und Informationsfreiheit" (State Commissioner for Data Protection and Freedom of Information Berlin, BlnBDI, own translation)[218].

Other actors in Berlin:

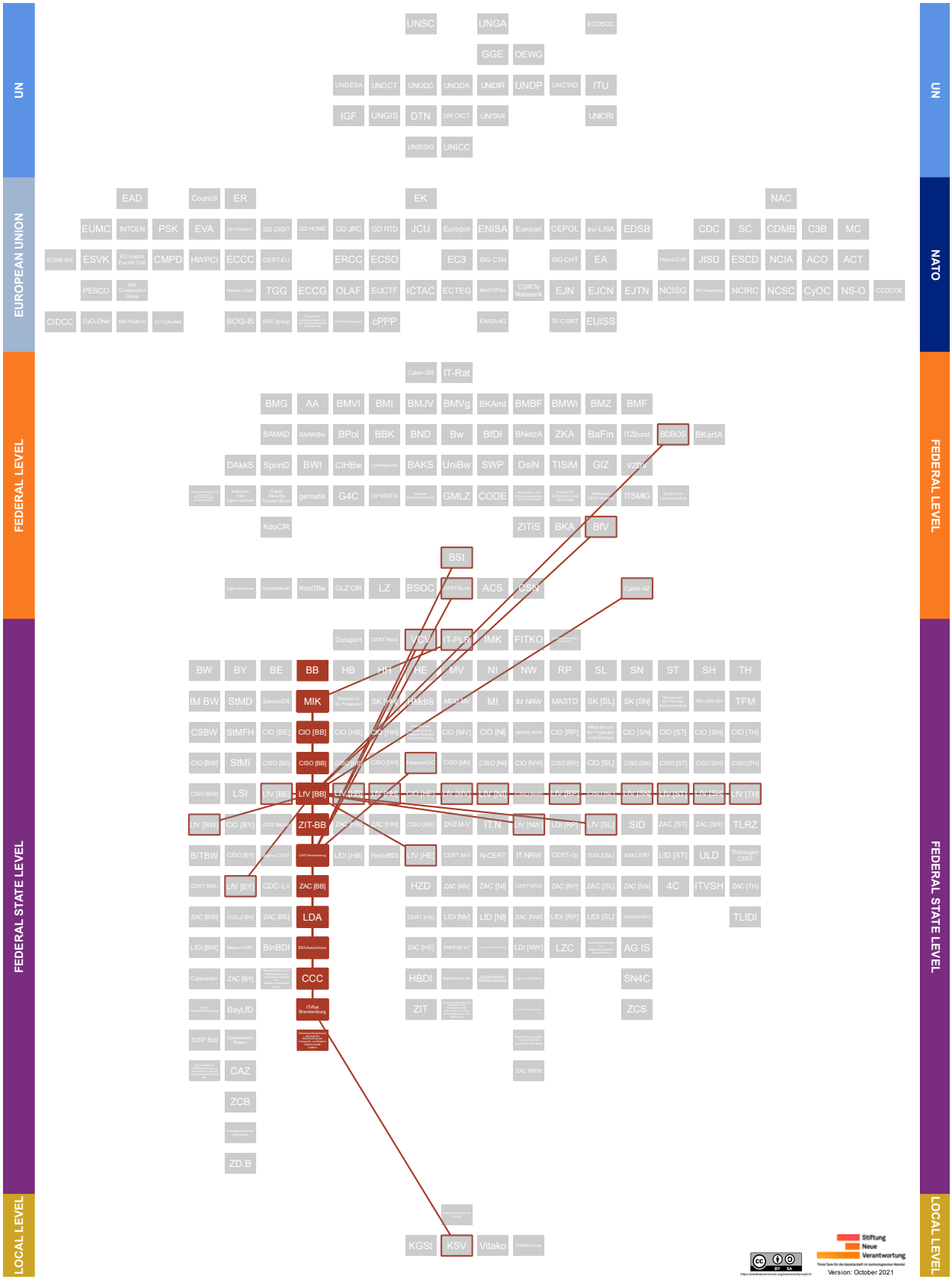
Cyber Defense Center der Landesverwaltung Berlin (Cyber Defense Center of the Berlin State Administration, CDC-Lv, own translation)
The Cyber Defense Center of the Berlin State Administration is located in the "IT-Dienstleistungszentrum" (IT Service Center Berlin, ITDZ Berlin, own translation). It consists 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 operations on the Berlin state network.

The CDC-Lv reports via the Berlin-CERT to Berlin's State Commissioner for Information Security (CIO [BE]). At the working level, there is an exchange with the Berlin liaison office of the BSI[219].

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 focus of the department is the fraud of goods and trade credit in connection with online trading[220].

215 ITDZ Berlin, Sicherheit.
216 Senatsverwaltung für Inneres und Sport Berlin, Organigramm.
Senatsverwaltung für Inneres und Sport Berlin, Verfassungsschutzbericht 2019.
217 Polizei Berlin, Zentrale Ansprechstelle Cybercrime für die Wirtschaft im LKA Berlin.
218 Berliner Beauftragte für Datenschutz und Informationsfreiheit, Über uns.
219 ITDZ Berlin, Innovationsmanagement im ITDZ Berlin.
Background Conversation, 2021.
220 Diana Nadeborn, Berliner Staatsanwaltschaft rüstet auf gegen Cyberkriminalität.

8.4. Brandenburg



Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:** "Ministerium des Innern und für Kommunales" (Brandenburg Ministry of the Interior and Municipal Affairs, MIK, official translation), "Abteilung 6: Digitalisierung, E-Government und IT-Leitstelle" (Department 6: Digitization, eGovernment and IT Control Center, own translation), "Referat 64: IT-Leitstelle, IT-Sicherheit und CERT sowie IT-Infrastruktur des Landes Brandenburg, Koordinierungsstelle für IT- und Cyber-Sicherheit im MIK, Verfahrensverantwortung für die IT-Basiskomponenten gemäß BbgEGovG für Land und Kommune" (Division 64: IT control center, IT security and CERT as well as IT infrastructure of the state of Brandenburg, coordination office for IT and cyber security in the MIK, procedural responsibility for the basic IT components in accordance with BbgEGovG for the state and local authorities, own translation)[221].

- **State Commissioner for Information Technology (CIO [BB]):** The state of Brandenburg has appointed a Chief Process Innovation Officer who looks after the state's IT affairs.

  He or she is based in the MIK[222].

- **Chief Information Security Officer of the State Administration (CISO [BB]):** In Brandenburg, a statewide CISO is appointed by Department 6 within the MIK. 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[223].

- **IT Service Provider of the Federal State Administration:** "Brandenburgischer IT-Dienstleister" (Brandenburg IT Service Provider, ZIT-BB, own translation), *which falls in the purview of the MIK[224].*

- **CERT**: The CERT-Brandenburg is being operated by the ZIT-BB[225].

- **State Authority for the Protection of the Constitution (LfV [BB]):** In Brandenburg, the State Authority for the Protection of the Constitution is located in the MIK (Department 5). Its fields of activity include counterintelligence and economic protection. In the latest "Verfassungsschutzbericht" (Report on the protection of

221 Ministerium des Innern und für Kommunales Brandenburg, Organigramm.
222 CIO, Die IT-Chefs der Bundesländer.
223 Brandenburgisches Vorschriftensystem, Leitlinie zur Gewährleistung der IT-Sicherheit in der Landesverwaltung Brandenburg.
224 Brandenburgischer IT-Dienstleister, Start.
225 Brandenburgischer IT-Dienstleister, CERT-Brandenburg.

the constitution, own translation) of Brandenburg references to inter alia current developments in so-called "cyber-extremism" have been made[226].

- **Institutional location of the ZAC [BB]**: Cyber-Competence-Center (CCC), actor description see below[227].

- **State Data Protection Authority:** "Landesbeauftragte:r für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg" (State Commissioner for Data Protection and for the Right to Inspect Files Brandenburg, LDA, own translation)[228].

Other actors in Brandenburg:

Ausschuss der Ressort Information Officer (Committee of Departmental Information Officers, RIO-Ausschuss, own translation)
In Brandenburg, the "Ressort Information Officers" (departmental information officers, RIO, own translation) of all departments, as well as the State Chancellery, form the RIO-Auschuss together with the first managing director of ZIT-BB and a chairperson. At the operational level, the RIO-Auschuss, which meets at least once every quarter and may establish working groups, inter alia decides on the IT standards of the state administration and the requirements for further statewide development of IT infrastructure.

The chair of the RIO-Auschuss is a representative of the MIK, who also acts as the contact person for the RIO-Auschuss vis-à-vis the state's CIO [BB]. Among others, the LDA may attend meetings in an advisory capacity[229].

Cyber-Competence-Center (CCC)
The CCC Brandenburg was established as a new specialist unit in the "Landeskriminalamt Brandenburg" (State Criminal Police Office 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 [BB] for commercial enterprises and authorities was also established here[230].

226 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.
227 Polizei Brandenburg, Internetkriminalität.
228 Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht, Über uns.
229 Landesregierung Brandenburg, Richtlinie für die Organisation des E-Government und des Einsatzes der Informationstechnik in der Landesverwaltung Brandenburg (E-Government- und IT-Organisationsrichtlinie).
230 Polizei Brandenburg, Cyber-Competence-Center im Landeskriminalamt.

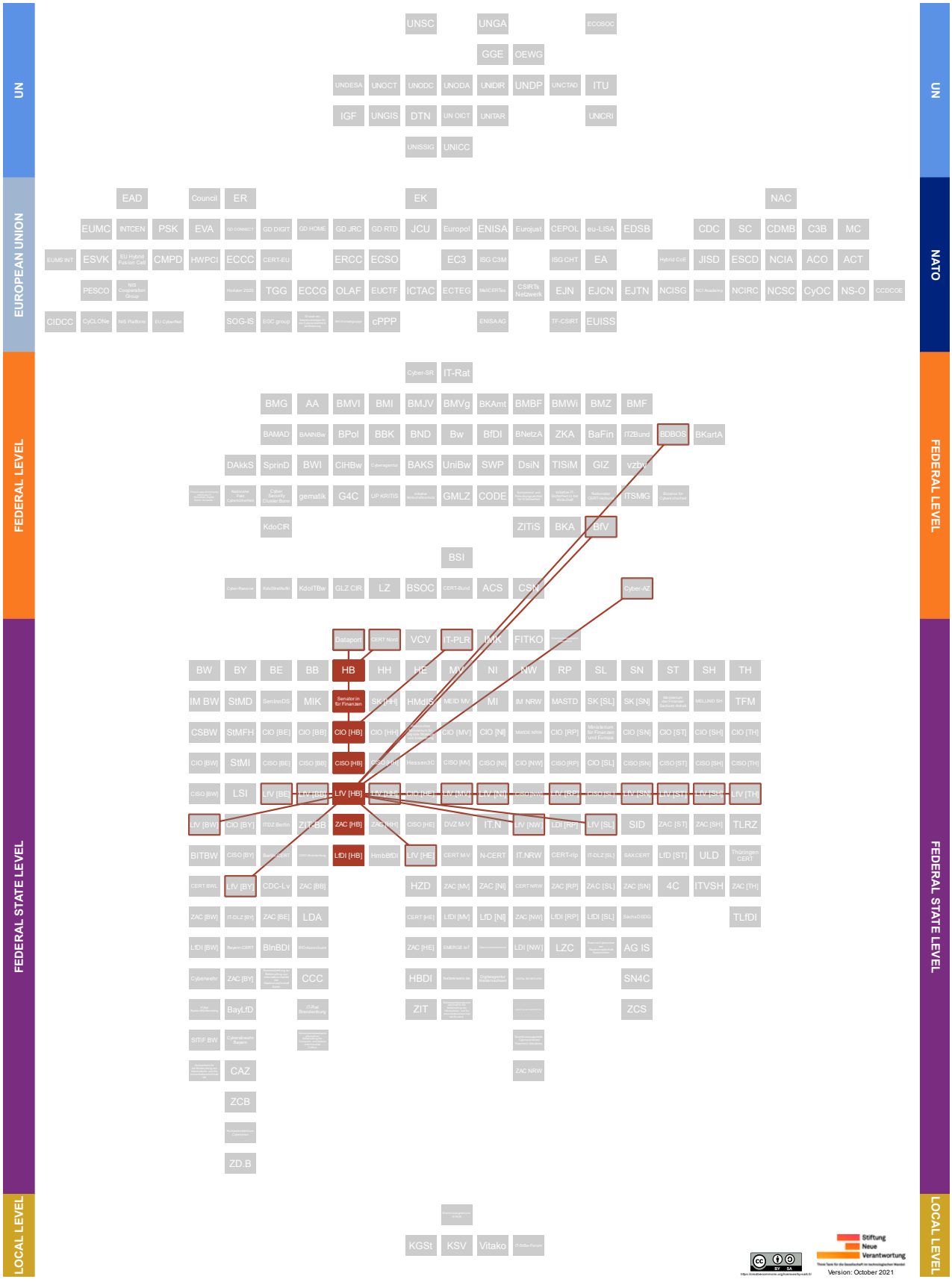
IT-Rat Brandenburg (IT Council Brandenburg, own translation)
The IT Council Brandenburg has been set up to permit the strategic coordination and joint management of information technology matters relating to cross-level cooperation between the federal state and its municipalities. Among other things, it discusses emerging topics of the IT-PLR, future development options for Brandenburg's IT and e-government strategy, as well as IT interoperability and IT security standards for cross-level communication.

The IT Council comprises the head of the State Chancellery, the state's CIO [BB], the state secretaries of the ministries responsible for finance and economics, and two representatives each from the Brandenburg Association of Towns and Municipalities and the Brandenburg County Association (KSV). The state CIO [BB] chairs the council. A representative of the ZIT-BB may attend the meetings in an advisory capacity[231].

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"[232].

231 Landesregierung Brandenburg, Gesetz über die elektronische Verwaltung im Land Brandenburg (Brandenburgisches E-Government-Gesetz – BbgEGovG).
Ministerium des Innern und für Kommunales des Landes Brandenburg, Bericht des IT-Beauftragten der Landesregierung.
232 Staatsanwaltschaft Cottbus, Schwerpunktstaatsanwaltschaft. (Website deleted)

8.5. Bremen


UN
EUROPEAN UNION
FEDERAL LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
NATO
UNSC
UNGA
ECOSOC
GGE
OEWG
UNDESA
UNOCT
UNODC
UNODA
UNIDIR
UNDP
UNCTAD
ITU
IGF
UNGIS
DTN
UN OICT
UNITAR
UNICRI
UNISSIG
UNICC
EAD
Council
ER
EK
NAC
EUMC
INTCEN
PSK
EVA
GD CONNECT
GD DIGIT
GD HOME
GD JRC
GD RTD
JCU
Europol
ENISA
Eurojust
CEPOL
eu-LISA
EDSB
CDC
SC
CDMB
C3B
MC
EUMS INT
ESVK
EU Hybrid Fusion Cell
CMPD
HWPCI
ECCC
CERT-EU
ERCC
ECSO
EC3
ISG C3M
ISG CHT
EA
Hybrid CoE
JISD
ESCD
NCIA
ACO
ACT
PESCO
NIS Cooperation Group
Horizon 2020
TGG
ECCG
OLAF
EUCTF
ICTAC
ECTEG
MeliCERTes
CSIRTs Netzwerk
EJN
EJCN
EJTN
NCISG
NCI Academy
NCIRC
NCSC
CyOC
NS-O
CCDCOE
CIDCC
CyCLONe
NIS Platform
EU CyberNet
SOG-IS
EGC group
cPPP
ENISA AG
TF-CSIRT
EUISS
Cyber-SR
IT-Rat
BMG
AA
BMVI
BMI
BMJV
BMVg
BKAmt
BMBF
BMWi
BMZ
BMF
BAMAD
BAAINBw
BPol
BBK
BND
Bw
BfDI
BNetzA
ZKA
BaFin
ITZBund
BDBOS
BKartA
DAkkS
SprinD
BWI
CIHBw
Cyberagentur
BAKS
UniBw
SWP
DsiN
TISiM
GIZ
vzbv
Nationales Cyberabwehrzentrum
Nationaler Cyber-Sicherheitsrat
Cyber Security Cluster Bonn
gematik
G4C
UP KRITIS
Initiative Wirtschaftsschutz
GMLZ
CODE
Kompetenzzentrum Digitale Souveränität
Initiative IT-Sicherheit in der Wirtschaft
Nationales CERT-Verbund
ITSMIG
Bündnis für Cybersicherheit
KdoCIR
ZITiS
BKA
BfV
BSI
Cyber-Reserve
KdoStratAufkl
KdoITBw
GLZ CIR
LZ
BSOC
CERT-Bund
ACS
CSK
Cyber-AZ
Dataport
CERT Nord
VCV
IT-PLR
FITKO
BW
BY
BE
BB
HB
HH
HE
MV
NI
NW
RP
SL
SN
ST
SH
TH
IM BW
StMD
SenInnDS
MIK
Senator für Finanzen
SK [HH]
HMdIS
MEID MV
MI
IM NRW
MASTD
SK [SL]
SK [SN]
Ministerium der Finanzen Sachsen-Anhalt
MELUND SH
TFM
CSBW
StMFH
CIO [BE]
CIO [BB]
CIO [HB]
CIO [HH]
Ministerium für Finanzen und Europa
CIO [MV]
CIO [NI]
MWIDE NRW
CIO [RP]
CIO [SN]
CIO [ST]
CIO [SH]
CIO [TH]
CIO [BW]
StMI
CISO [BE]
CISO [BB]
CISO [HB]
Hessen3C
CISO [MV]
CISO [NI]
CIO [NW]
CISO [RP]
CIO [SL]
CISO [SN]
CISO [ST]
CISO [SH]
CISO [TH]
CISO [BW]
LSI
LfV [BE]
LfV [BB]
LfV [HB]
LfV [HH]
BLfV [HE]
LfV [MV]
LfV [NI]
BfDI-CERT
LfV [RP]
BfDI-CERT
LfV [SN]
LfV [ST]
LfV [SH]
LfV [TH]
LfV [BW]
CIO [BY]
ITDZ Berlin
ZIT BB
ZAC [HB]
ZAC [HH]
CISO [HE]
DVZ M-V
IT.N
LfV [NW]
LDI [RP]
LfV [SL]
SID
ZAC [ST]
ZAC [SH]
TLRZ
BITBW
CISO [BY]
BerlinCERT
CERT Brandenburg
LfDI [HB]
HmbBfDI
LfV [HE]
CERT M-V
N-CERT
IT.NRW
CERT-rlp
IT-DLZ [SL]
SAX.CERT
LfD [ST]
ULD
Thüringen CERT
CERT BWL
LfV [BY]
CDC-Lv
ZAC [BB]
HZD
ZAC [MV]
ZAC [NI]
CERT NRW
ZAC [RP]
ZAC [SL]
ZAC [SN]
4C
ITVSH
ZAC [TH]
ZAC [BW]
IT-DLZ [BY]
ZAC [BE]
LDA
CERT [HE]
LfDI [MV]
LfD [NI]
ZAC [NW]
LfDI [RP]
LfDI [SL]
SächsDSDG
TLfDI
LfDI [BW]
Bayern-CERT
BInBDI
BIG Access Point
ZAC [HE]
EMERGE IoT
LDI [NW]
LZC
AG IS
Cyberwehr
ZAC [BY]
CCC
HBDI
SN4C
BayLfD
IT-Rat Brandenburg
ZIT
ZCS
SITiF BW
Cyberabwehr Bayern
ZAC NRW
CAZ
ZCB
ZD.B
KGSt
KSV
Vitako
IT-SiBe-Forum
Stiftung Neue Verantwortung
Version: October 2021

The state of Bremen is one of the signatories to the interstate treaty which established Dataport.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics: "**Der:die Senator:in für Finanzen" (Finance Senator of the Free Hanseatic City of Bremen, official translation), "Abteilung 4: Zentrales IT-Management, Digitalisierung öffentlicher Dienste" (Department 4: Central IT Management, Digitization of Public Services, own translation).

  A representative of the Finance Senator is a member of Dataport's Board of Directors[233].

- **State Commissioner for Information Technology (CIO [HB]):** In Bremen, the CIO position is filled by the "Staatsrat" (State Councillor, own translation) of the Finance Senator.

  He or she represents Bremen on the IT-PLR[234].

- **Chief Information Security Officer of the State Administration (CISO [HB]):** Bremen's CISO is organizationally located at the Finance Senator. He or she is producing a non-public annual report on information security in the Bremen state administration which addresses problems, solutions, and alternatives[235].

- **IT Service Provider of the Federal State Administration:** Dataport, actor description see below (Chapter 8.17.).

- **CERT:** CERT Nord, actor description see below (Chapter 8.17.).

- **State Authority for the Protection of the Constitution (LfV [HB]):** The self-description of the Bremen State Authority for the Protection of the Constitution or its 2019 report on the protection of the constitution includes no reference to any responsibilities within the fields of economic protection or cyber defense[236].

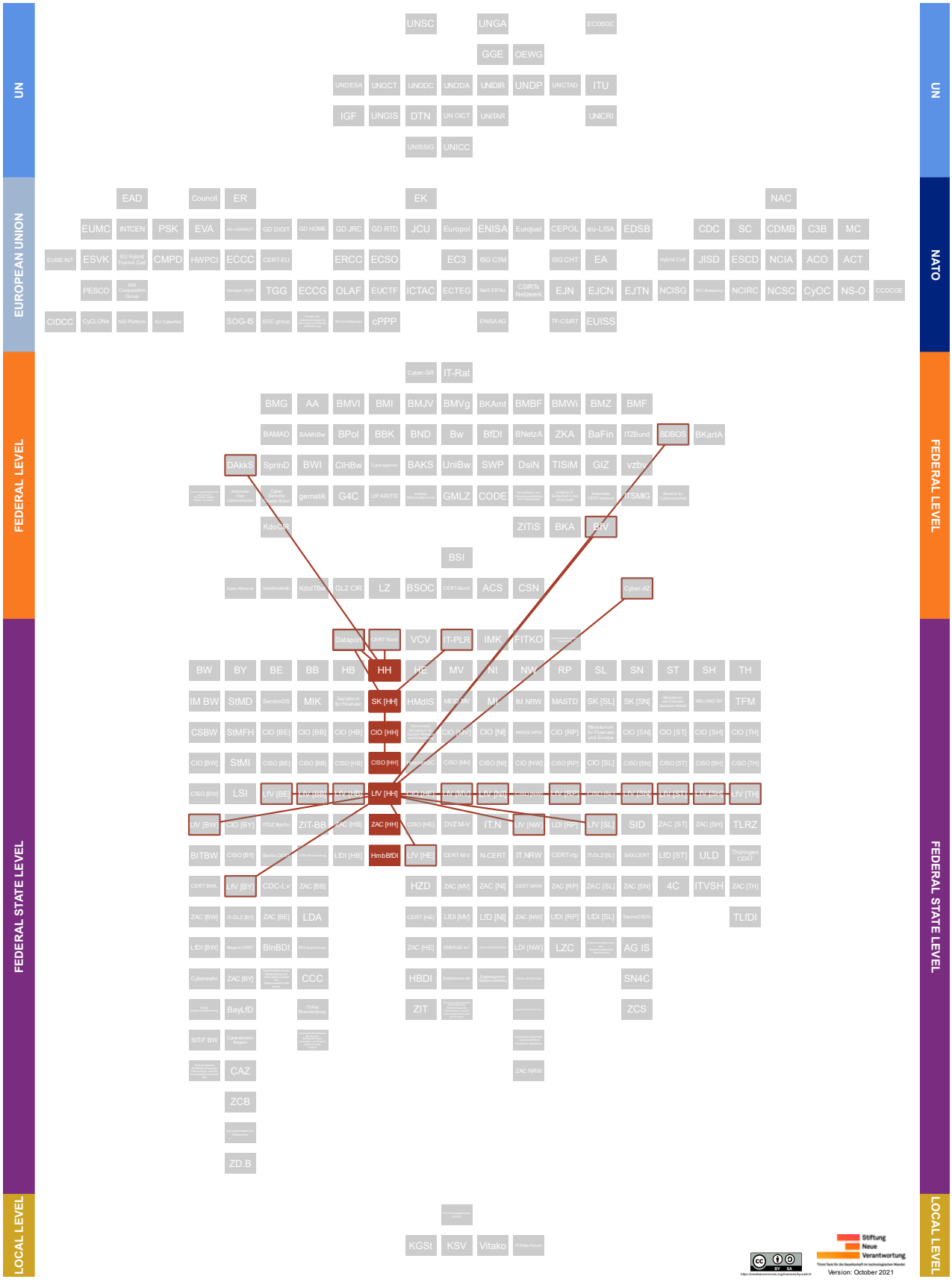
233 Bremische Bürgerschaft, Mitteilung des Senats vom 15. Januar 2019: Cybersicherheit in Bremen.
Der Senator für Finanzen Bremen, Abteilung 4: Zentrales IT-Management, Digitalisierung öffentlicher Dienste.
234 Freie Hansestadt Bremen, Staatsrat Dr. Martin Hagen.
235 CISO Bremen, Vorlage für die Sitzung des Senats am 14.7.2020. Jahresbericht zur Informationssicherheit in der bremischen Verwaltung.
236 Landesamt für Verfassungsschutz Bremen, Über Uns.
Freie Hansestadt Bremen, Verfassungsschutzbericht 2019.

- **Institutional location of the ZAC [HB]**: "Polizei Bremen" (Bremen Police, own translation). There, police department K13 deals with cybercrime and digital traces[237].

- **State Data Protection Authority:** Landesbeauftragte:r für Datenschutz und Informationsfreiheit (State Commissioner for Data Protection and Freedom of Information Bremen, LfDI [BE], own translation)[238].

237 Polizei Bremen, Organigramm Direktion Kriminalpolizei / untere Ebene.
238 Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen, Wir über uns.

8.6. Hamburg


UN
EUROPEAN UNION
NATO
FEDERAL LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
UNSC
UNGA
ECOSOC
GGE
OEWG
UNDESA
UNOCT
UNODC
UNODA
UNIDIR
UNDP
UNCTAD
ITU
IGF
UNGIS
DTN
UN OICT
UNITAR
UNICRI
UNISSIG
UNICC
EAD
Council
ER
EK
NAC
EUMC
INTCEN
PSK
EVA
JCU
Europol
ENISA
Eurojust
CEPOL
eu-LISA
EDSB
CDC
SC
CDMB
C3B
MC
ESVK
CMPD
HWPCI
ECCC
ERCC
ECSO
EC3
ISG C3M
ISG CHT
EA
JISD
ESCD
NCIA
ACO
ACT
PESCO
TGG
ECCG
OLAF
EUCTF
ICTAC
ECTEG
CSIRTs Netzwerk
EJN
EJCN
EJTN
NCISG
NCIRC
NCSC
CyOC
NS-O
CIDCC
CyCLONe
SOG-IS
cPPP
ENISA AG
TF-CSIRT
EUISS
Cyber-SR
IT-Rat
BMG
AA
BMVI
BMI
BMJV
BMVg
BKAmt
BMBF
BMWi
BMZ
BMF
BAMAD
BPol
BBK
BND
Bw
BfDI
BNetzA
ZKA
BaFin
ITZBund
BDBOS
BKartA
DAkkS
SprinD
BWI
CIHBw
BAKS
UniBw
SWP
DsiN
TISiM
GIZ
gematik
G4C
GMLZ
CODE
ITSMIG
ZITiS
BKA
BfV
BSI
BSOC
CERT-Bund
ACS
CSN
Cyber-AZ
Datapol
CERT Nord
VCV
IT-PLR
IMK
FITKO
BW
BY
BE
BB
HB
HH
HE
MV
NI
NW
RP
SL
SN
ST
SH
TH
IM BW
StMD
MIK
SK [HH]
HMdIS
IM NRW
MASTD
SK [SL]
SK [SN]
TFM
CSBW
StMFH
CIO [BE]
CIO [BB]
CIO [HB]
CIO [HH]
CIO [NI]
CIO [RP]
CIO [SN]
CIO [ST]
CIO [SH]
CIO [TH]
StMI
CISO [BE]
CISO [BB]
CISO [HB]
CISO [HH]
CISO [MV]
CISO [NI]
CISO [NW]
CISO [RP]
CISO [SL]
CISO [SN]
CISO [ST]
CISO [SH]
CISO [TH]
LSI
LfV [BE]
LfV [BB]
LfV [HB]
LfV [HH]
LfV [MV]
LfV [NI]
LfV [RP]
LfV [SN]
LfV [ST]
LfV [SH]
LfV [TH]
LfV [BW]
CIO [BY]
ZIT-BB
ZAC [HH]
CISO [HE]
DVZ M-V
IT.N
LfV [NW]
LDI [RP]
LfV [SL]
SID
ZAC [ST]
ZAC [SH]
TLRZ
BITBW
CISO [BY]
LfD [HB]
HmbBfDI
LfV [HE]
CERT M-V
N-CERT
IT.NRW
CERT-rlp
LfD [ST]
ULD
Thüringen CERT
LfV [BY]
CDC-Lv
ZAC [BB]
HZD
ZAC [MV]
ZAC [NI]
ZAC [NW]
ZAC [RP]
ZAC [SL]
ZAC [SN]
4C
ITVSH
ZAC [TH]
LDA
CERT [HE]
LfD [MV]
LfD [NI]
LfD [RP]
LfD [SL]
TLfDI
BInBDI
ZAC [HE]
LDI [NW]
LZC
AG IS
CCC
HBDI
SN4C
BayLfD
ZIT
ZCS
CAZ
ZAC NRW
ZCB
ZD.B
KGSt
KSV
Vitako
Stiftung Neue Verantwortung
Version: October 2021

The state of Hamburg is one of the shareholders of DAkkS. It is also one of the signatories to the interstate treaty which established Dataport.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:** "Senatskanzlei Hamburg" (Senate Chancellery Hamburg, SK [HH], own translation), "Amt für IT und Digitalisierung" (Office for IT and Digitalization, ITD, own translation).

  A representative of the SK is a member of Dataport's Board of Directors[239].

- **State Commissioner for Information Technology (CIO [HH]):** Hamburg has appointed a Chief Digital Officer (CDO) who heads the ITD (SK [HH]). In addition, the ITD is also home to the state's s CIO, who is the deputy head of the ITD[240].

- **Chief Information Security Officer of the State Administration (CISO [HH]):** Hamburg's CISO has been established within the ITD of the SK [HH], *which is headed by the state's CIO [HH]*[241].

- **IT Service Provider of the Federal State Administration:** Dataport, actor description see below (Chapter 8.17.).

- **CERT**: CERT Nord, actor description see below (Chapter 8.17.).

- **State Authority for the Protection of the Constitution (LfV [HH]):** Department V3 of the Hamburg State Authority for the Protection of the Constitution works inter alia on counterintelligence. Its subordinate Division V32 has competencies and tasks in the field of economic protection. In its reports on the protection of the constitution by Hamburg also refers to threats from cyber espionage, cyber sabotage, and cyber operations[242].

- **Institutional location of the ZAC [HH]:** Polizei Hamburg, LKA 54 Fachkommissariat Cybercrime "Hamburg Police, LKA 54 Special Commissioner's Office for Cybercrime, own translation). With LKA 54, the Hamburg police has created a department that pools the competencies of criminal investigators and computer scientists to combine technological and police knowledge. IT security and cyber-

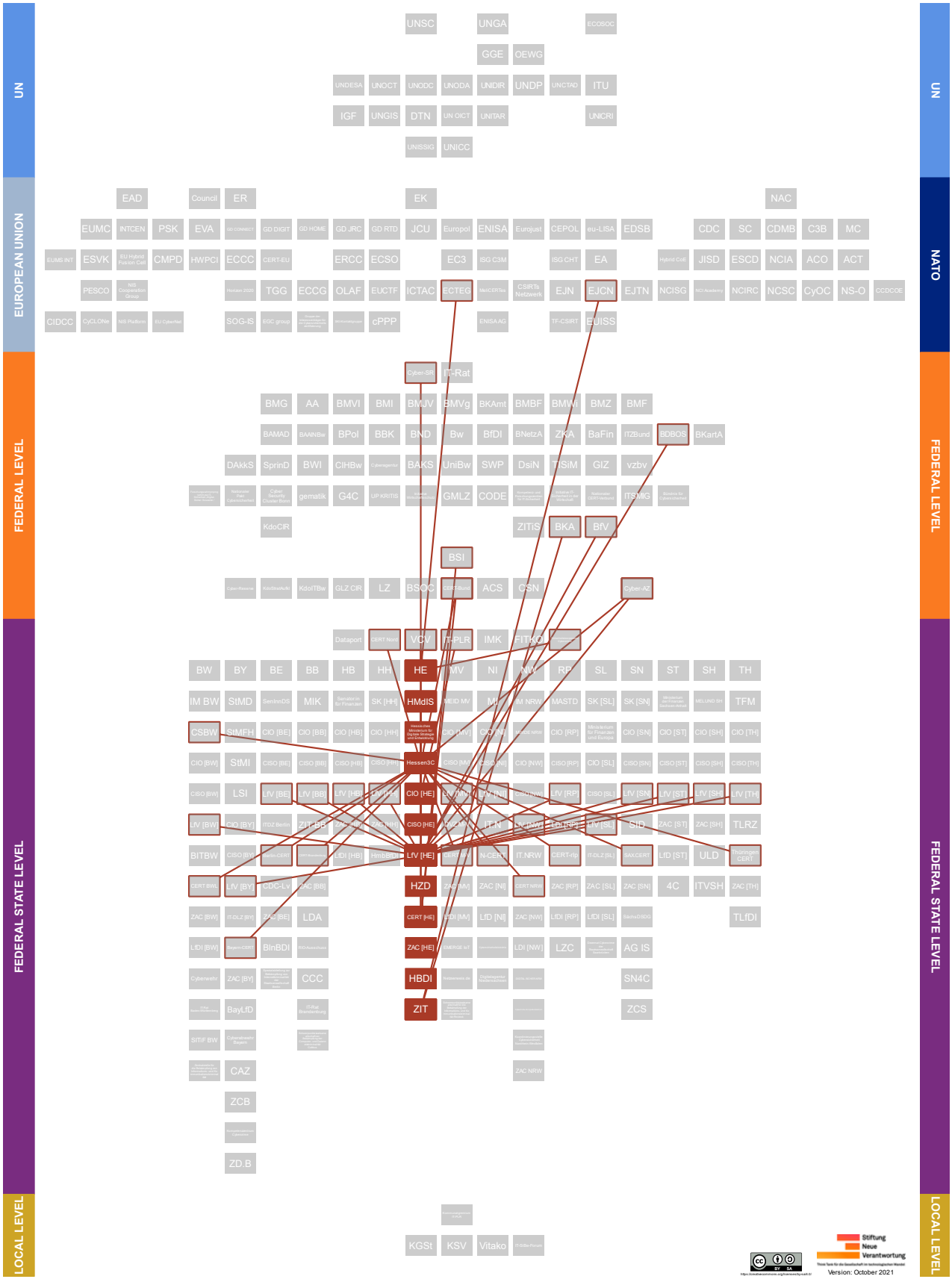
239 Senat der Freien und Hansestadt Hamburg Senatskanzlei, Arbeitsstrukturen des Amtes für IT und Digitalisierung (ITD).
240 Senatskanzlei Hamburg, Senatskanzlei Amt für IT und Digitalisierung.
241 Freie Hansestadt Hamburg, Rahmen-Sicherheitskonzept.
242 Landesamt für Verfassungsschutz Hamburg, Organigramm des Landesamtes für Verfassungsschutz. Behörde für Inneres und Sport Freie Hansestadt Hamburg, Verfassungsschutzbericht 2019.

crime are also an area of activity of the "Netzwerk Standortsicherheit Hamburg" (Hamburg Site Safety Network, own translation) coordinated by the Hamburg police[243].

- **State Data Protection Authority:** "Hamburgische:r Beauftragte:r für Datenschutz und Informationsfreiheit der Freien und Hansestadt Hamburg" (State Commissioner for Data Protection and Freedom of Information of the Free and Hanseatic City of Hamburg, HmbBfDI, own translation)[244].

243 Koordinierungsbüro "Netzwerk Standortsicherheit Hamburg", IT-Sicherheit und Cybercrime. Polizei Hamburg, Zentrale Ansprechstelle Cybercrime (ZAC).
244 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit der Freien und Hansestadt Hamburg, Tätigkeitsberichte des HmbBfDI.

8.7. Hesse


UN
EUROPEAN UNION
NATO
FEDERAL LEVEL
FEDERAL LEVEL
FEDERAL STATE LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
LOCAL LEVEL
UNSC
UNGA
ECOSOC
GGE
OEWG
UNDESA
UNOCT
UNODC
UNODA
UNIDIR
UNDP
UNCTAD
ITU
IGF
UNGIS
DTN
UN OICT
UNITAR
UNICRI
UNISSIG
UNICC
EAD
Council
ER
EK
NAC
EUMC
INTCEN
PSK
EVA
JCU
Europol
ENISA
Eurojust
CEPOL
eu-LISA
EDSB
CDC
SC
CDMB
C3B
MC
ESVK
CMPD
HWPCI
ECCC
CERT-EU
ERCC
ECSO
EC3
ISG C3M
ISG CHT
EA
JISD
ESCD
NCIA
ACO
ACT
PESCO
TGG
ECCG
OLAF
EUCTF
ICTAC
ECTEG
CSIRTs Netzwerk
EJN
EJCN
EJTN
NCISG
NCIRC
NCSC
CyOC
NS-O
CIDCC
CyCLONe
SOG-IS
cPPP
ENISA AG
TF-CSIRT
EUISS
Cyber-SR
IT-Rat
BMG
AA
BMVI
BMI
BMJV
BMVg
BKAmt
BMBF
BMWi
BMZ
BMF
BAMAD
BPol
BBK
BND
Bw
BfDI
BNetzA
ZKA
BaFin
ITZBund
BDBOS
BKartA
DAkkS
SprinD
BWI
CIHBw
BAKS
UniBw
SWP
DsiN
TISiM
GIZ
vzbv
gematik
G4C
GMLZ
CODE
ITSMIG
KdoCIR
ZITiS
BKA
BfV
BSI
GLZ CIR
LZ
BSOC
ACS
CSN
Cyber-AZ
Dataport
VCV
IT-PLR
IMK
BW
BY
BE
BB
HB
HH
HE
MV
NI
NW
RP
SL
SN
ST
SH
TH
IM BW
StMD
MIK
SK [HH]
HMdIS
MASTD
SK [SL]
SK [SN]
TFM
CSBW
StMFH
CIO [BE]
CIO [BB]
CIO [HB]
CIO [HH]
CIO [MV]
CIO [NI]
CIO [RP]
CIO [SN]
CIO [ST]
CIO [SH]
CIO [TH]
CIO [BW]
StMI
CISO [BE]
CISO [BB]
CISO [HB]
CISO [HH]
Hessen3C
CISO [MV]
CISO [NI]
CISO [NW]
CISO [RP]
CISO [SL]
CISO [SN]
CISO [ST]
CISO [SH]
CISO [TH]
CISO [BW]
LSI
LfV [BE]
LfV [BB]
LfV [HB]
LfV [HH]
CIO [HE]
LfV [MV]
LfV [NI]
LfV [RP]
LfV [SN]
LfV [ST]
LfV [SH]
LfV [TH]
LfV [BW]
CIO [BY]
ZIT BB
CISO [HE]
LfV [NW]
LfV [SL]
SID
ZAC [ST]
ZAC [SH]
TLRZ
BITBW
CISO [BY]
LfV [HE]
N-CERT
IT.NRW
CERT-rlp
IT-DLZ [SL]
FAX.CERT
LfD [ST]
ULD
Thüringen CERT
CERT BW
LfV [BY]
CDC-LfV
ZAC [BB]
HZD
ZAC [MV]
ZAC [NI]
CERT NRW
ZAC [RP]
ZAC [SL]
ZAC [SN]
4C
ITVSH
ZAC [TH]
ZAC [BW]
IT-DLZ [BY]
ZAC [BE]
LDA
CERT [HE]
LfD [MV]
LfD [NI]
ZAC [NW]
LfD [RP]
LfD [SL]
SächsDSDG
TLfDI
LfD [BW]
Bayern-CERT
BInBDI
ZAC [HE]
EMERGE IoT
LDI [NW]
LZC
AG IS
Cyberwehr
ZAC [BY]
CCC
HBDI
SN4C
BayLfD
ZIT
ZCS
SITiF BW
CAZ
ZCB
ZD.B
KGSt
KSV
Vitako
Stiftung Neue Verantwortung
Version: October 2021

The state of Hesse is represented in the Cyber-SR and participates in the ECTEG with its police academy. The "Landeskriminalamt Hessen" (Hessian State Criminal Police Office, own translation) participates in the Sicherheitskooperation Cybercrime.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:**
  - "Hessisches Ministerium des Innern und für Sport" (State Ministry of the Interior and Sports, HMdIS, own translation), "Abteilung VII: Cyber-und IT-Sicherheit, Verwaltungsdigitalisierung" (Department VII: Cyber and IT Security, Administrative Digitization, own translation)[245].
  - "Hessisches Ministerium für Digitale Strategie und Entwicklung" (State Ministry for Digital Strategy and Development, own translation)[246].

- **State Commissioner for Information Technology (CIO [HE]):** The CIO of the state of Hesse is responsible for the state's information technology and e-government.

  The CIO is based in the State Ministry for Digital Strategy and Development. He or she is supported by a Co-CIO and represents Hesse on the IT-PLR[247].

- **Chief Information Security Officer of the State Administration (CISO [HE]):** In Hesse, the head of the Department VII of the HMdIS also assumes the function of the state's CISO.

  A representative of the Hessen3C acts as his or her deputy[248].

- **IT Service Provider of the Federal State Administration: "**Hessische Zentrale für Datenverarbeitung" (Hessian Central Office for Data Processing, HZD, own translation), which is subject to the official and technical supervision of the "Hessische Ministerium der Finanzen (Hessian Ministry of Finance, HMdF, own translation)[249].

- **CERT**: Upon the founding of Hessen3C, the Hessian CERT was integrated into its cybersecurity jurisdiction and now performs all tasks of the CERT[250].

245 Hessisches Ministerium des Innern und für Sport, Organisationsplan des Hessischen Ministerium des Innern und für Sport.
246 Hessische Staatskanzlei: Organisationsplan.
247 Hessische Ministerin für Digitale Strategie und Entwicklung, CIO.
Hessische Ministerin für Digitale Strategie und Entwicklung, Drei Fragen an Roland Jabkowski.
248 Ministerium des Innern und für Sport Hessen, Der zentrale Informationssicherheitsbeauftragte der Landesverwaltung.
Hessischer Landtag (Drucksache 20/1520), Antwort auf Kleine Anfrage: Umsetzung Informationssicherheitsrichtlinie.
249 Hessische Zentrale für Datenverarbeitung, Organisation.
250 Hessisches Ministerium des Innern und für Sport, Der Bereich Cybersecurity im Hessen3C.

- **State Authority for the Protection of the Constitution (LfV [HE])**: Within the Hessian State Authority for the Protection of the Constitution Department 30 oversees counterintelligence and economic protection. In an effort to protect the economy, cyber espionage is listed as an explicit area of responsibility[251].

- **Institutional location of the ZAC [HE]**: "Landeskriminalamt Hessen" (State Criminal Police Office Hesse, own translation)[252].

- **State Data Protection Authority:** "Hessische:r Beauftragte:r für Datenschutz und Informationsfreiheit" (State Commissioner for Data Protection and Freedom of Information Hesse, HBDI, own translation)[253].

Other actors in Hesse:

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 is located within the HMdIS. It exchanges information on cyber issues with the Hessian police and the LfV [HE]. Together, they create a situational overview. Employees of the Hessen3C come from the CERT Hesse, the police, and the LfV [HE] in order to make cross-organizational expertise and services in the field of cybersecurity available. Hessen3C operates the CERT Hesse and heads the IT crisis management of the state's public administration. Working relationships exist with 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[254].

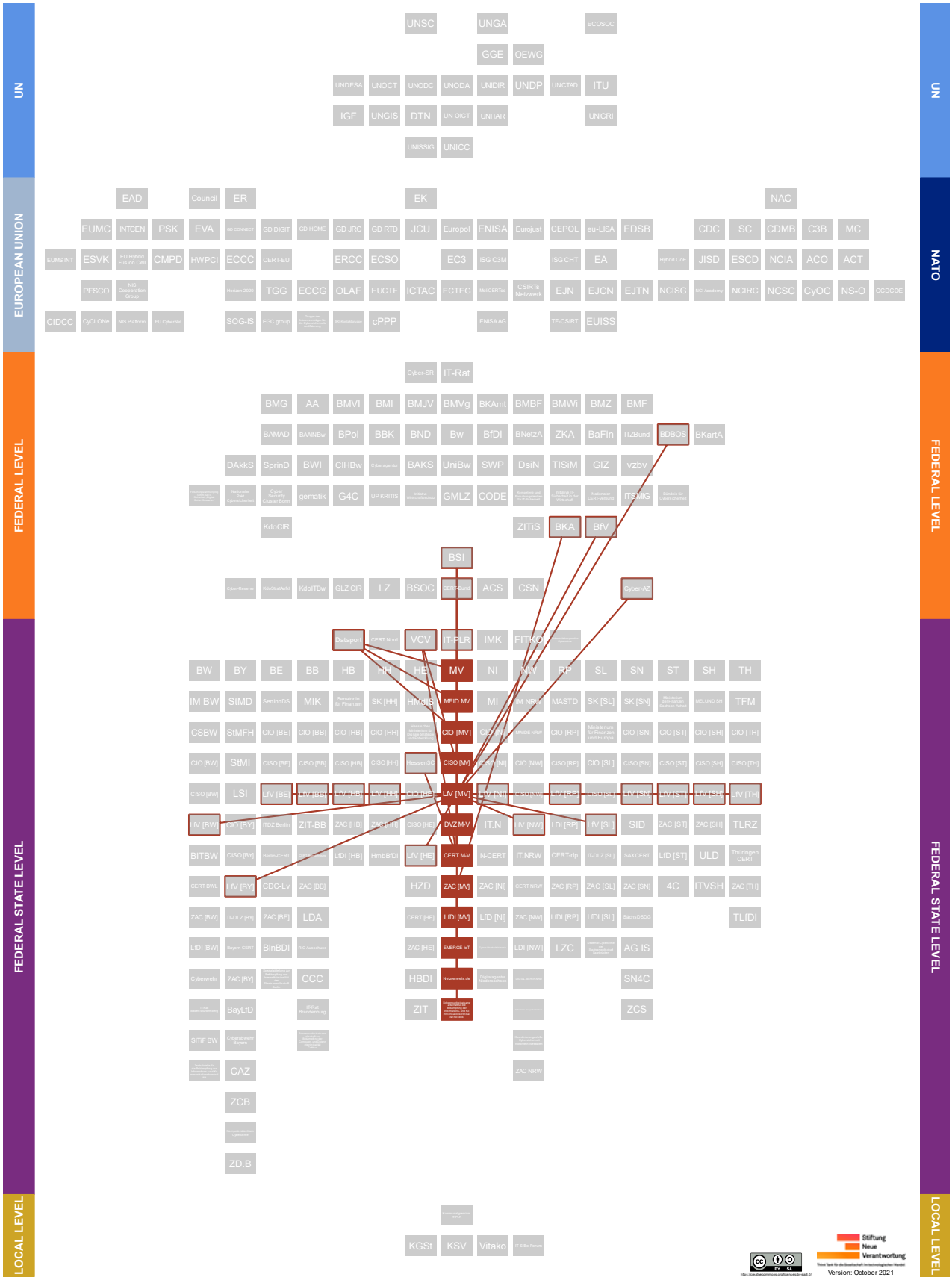
251 Landesamt für Verfassungsschutz Hessen, Organigramm.
Landesamt für Verfassungsschutz Hessen, Wirtschaftsschutz. Was ist Cyberspionage?.
252 Bundeskriminalamt, Polizei – Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen.
253 Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Über uns.
254 Bundesverwaltungsamt, Referentin/Referent (m/w/d) im Hessen CyberCompetenceCenter. (This link has expired. A copy can be requested from the authors)
Email exchange with representatives of the Hessen Cyber Competence Center in November 2019.
Hessisches Ministerium des Innern und für Sport, Der Bereich Cybersecurity im Hessen3C.
Hessisches Ministerium des Innern und für Sport, Hessen3C.

Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (Central Office for Combating Internet and Computer Crime, 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 mass proceedings against several suspects nationwide. It is also a founding member of the EJCN[255].

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

8.8. Mecklenburg-Western Pomerania



The state of Mecklenburg-Western Pomerania is also one of the signatories to the interstate treaty which established Dataport.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics: "**Ministerium für Energie, Infrastruktur und Digitalisierung" (State Ministry of Energy, Infrastructure and Digitalization of Mecklenburg-Western Pomerania, MEID MV, own translation), "Abteilung 5 Digitalisierung in Wirtschaft und Verwaltung, Breitbandausbau" (Department 5: Digitization in Economy and Administration, Broadband Expansion, own translation).

  MEID MV (as well as the Ministry of the Interior of Mecklenburg-Western Pomerania) cooperate with the BSI in the field of cybersecurity[256]*.*

- **State Commissioner for Information Technology (CIO [MV]):** In Mecklenburg-Western Pomerania, the position of CIO is staffed by the MEID MV.

  He or she represents Mecklenburg-Western Pomerania in the IT-PLR and is a member of Dataport's Board of Directors[257]*.*

- **Chief Information Security Officer of the State Administration (CISO [MV]):** In Mecklenburg-Western Pomerania, the state's CISO is based in the state's "Ministerium für Inneres und Europa" (Ministry of the Interior and Europe, MIE MV, official translation).

  He or she reports to the CIO [MV] and coordinates interdepartmental information security management. The CISO [MV] is responsible for the CERT M-V and represents Mecklenburg-Western Pomerania in the VCV[258]*.*

- **IT Service Provider of the Federal State Administration:** DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern (Service Provider for the State Administration of Mecklenburg-Western Pomerania, DVZ M-V, official translation).

  The State Secretary of the MEID MV assumes the function as Chairman of DVZ M-V's Supervisory Board[259]*.*

256 Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern, Verstärkte Kooperation zwischen Bund und Land bei IT-Sicherheit.
Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern, Organigramm.
257 Regierung Mecklenburg-Vorpommern, Staatssekretärin Ina-Maria Ulbrich.
258 DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH, DVZ.info 02/14.
Ministerium für Inneres und Sport Mecklenburg-Vorpommern, Stellenausschreibung Beauftragte/Beauftragter der Landesverwaltung für Informationssicherheit.
259 DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern, Über uns.

- **CERT:** The CERT M-V is being operated by the DVZ M-V.

- **State Authority for the Protection of the Constitution (LfV [MV]):** In Mecklenburg-Western Pomerania, the State Authority for the Protection of the Constitution is located in the "Ministerium für Inneres und Europa" (Ministry of the Interior and Europe, MIE MV, official translation), Department 5. Counterintelligence and economic protection as its fields of work include threats from cyber operations and industrial espionage[260].

- **Institutional location of the ZAC [MV]:** "Dezernat 45 Cybercrime des Landeskriminalamtes Mecklenburg-Vorpommern" (Department 45 Cybercrime of the Mecklenburg-Western Pomerania State Criminal Police Office, own translation).

  It receives and follows up on tips received on the Netzverweis platform. It also co-operates 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[261].

- **State Data Protection Authority:** "Landesbeauftragte:r für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern" (State Commissioner for Data Protection and Freedom of Information Mecklenburg-Western Pomerania, LfDI, own translation)[262].

Other actors in Mecklenburg-Western Pomerania:

EMERGE IoT
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 offenses 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 operation scenarios on the Internet of Things.

The LKA [MV] and the "Universität Rostock" (University of Rostock, official translation) are involved[263].

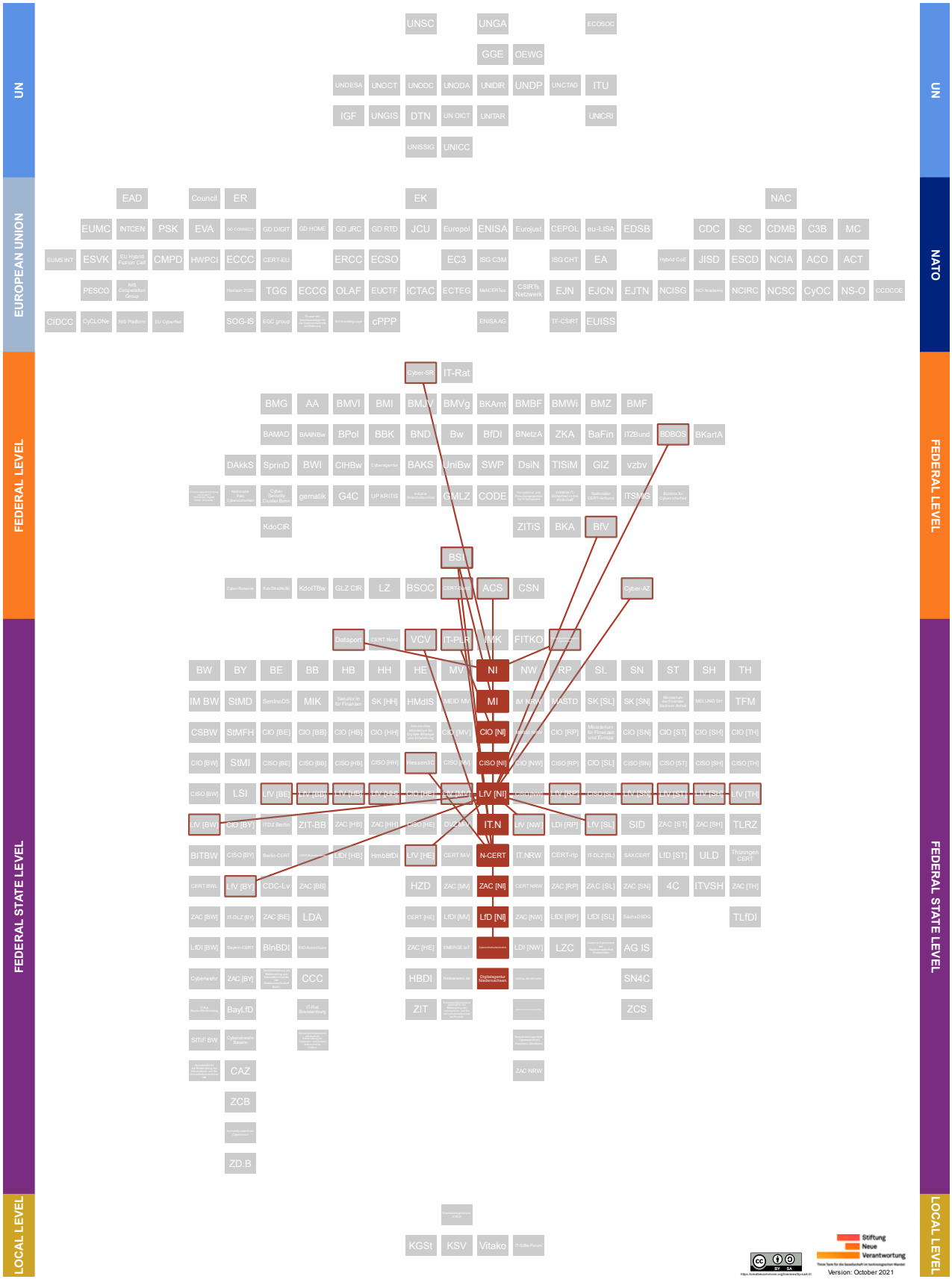
260 Ministerium für Inneres und Europa Mecklenburg-Vorpommern, Spionageabwehr und Wirtschaftsschutz.
261 Landeskriminalamt Mecklenburg-Vorpommern, Cybercrime in M-V. Aktuelle Aspekte. (Website deleted)
Landespolizei Mecklenburg-Vorpommern, LKA-MV: Internationaler Ermittlungserfolg gegen Kinderpornografieplattform im Darknet.
262 Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Behörde.
263 Universität Rostock, Universität Rostock unterstützt das Landeskriminalamt Mecklenburg-Vorpommern in Sachen Cyber-Kriminalitätsbekämpfung.

Netzverweis.de
The website netzverweis.de is a joint initiative of the "Landeskriminalamtes Mecklenburg-Vormpommern" (State Criminal Police Office of Mecklenburg-Western Pomerania, own translation) and the DVZ M-V under the patronage of the MIE MV. 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[264].

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 "Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock," thus also covering the area of cybercrime[265].

264 Netzverweis, Online-Meldestelle.
Regierung Mecklenburg-Vorpommern, Landesregierung.
265 Justiz Online in Mecklenburg-Vorpommern, Zuständigkeit.

8.9. Lower Saxony



The state of Lower Saxony is represented on the Cyber-SR. It is also one of the signatories to the interstate treaty which established Dataport. The "Landeskriminalamt Niedersachsen" (State Criminal Police Office of Lower Saxony, own translation) participates in the Sicherheitskooperation Cybercrime.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics: "**Niedersächsisches Ministerium für Inneres und Sport" (State Ministry of the Interior and Sport of Lower Saxony, MI, own translation), "Stabsstelle CIO und IT-Bevollmächtigter der Landesregierung" (Staff Office CIO and IT Representative of the State Government, own translation), "Referat IT2: Informationssicherheit, Cybersicherheit" (Division IT2: Information Security, Cybersecurity, own translation).

  The BSI and MI work together on cybersecurity issues. The MI is also a multiplier of the ACS[266]*.*

- **State Commissioner for Information Technology (CIO [NI]):** The CIO of Lower Saxony heads the "Stabsstelle Informationstechnik der Landesverwaltung" (Office for Information Technology of the State Administration own translation) within the MI. In addition to IT strategy and e-government, the CIO's tasks also include the modernization of administration.

  He or she represents Lower Saxony in the IT-PLR[267]*.*

- **Chief Information Security Officer of the State Administration (CISO [NI]):** 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 MI*[268].

- **IT Service Provider of the Federal State Administration: "**IT.Niedersachsen" (IT Lower Saxony, IT.N, own translation). Among other things, IT.N also operates a Cyber Defense Operations Center (CDOC)[269].

- **CERT**: Das N-CERT is located at the MI. Recently, N-CERT was expanded into a cyber defense center to provide, among other things, a comprehensive real-time

266 Niedersächsisches Ministerium für Inneres und Sport, Land und Bund vertiefen Zusammenarbeit gegen Cyberkriminalität.
Niedersächsisches Ministerium für Inneres und Sport, Organisationsplan.
Niedersächsisches Ministerium für Inneres und Sport, Sicherheit in der digitalen Welt.
267 Niedersächsisches Ministerium für Inneres und Sport, Neuer CIO in Niedersachsen: Dr. Horst Baier ist IT-Bevollmächtigter der Landesregierung.
268 Ministerium für Inneres und Sport Niedersachsen, Informationssicherheit.
Ministerium für Inneres und Sport, Informationssicherheit in Niedersachsen.
269 Landesbetrieb IT.Niedersachsen, Das Organigramm von IT.Niedersachsen.

cybersecurity situation picture. More than 100 municipalities in Lower Saxony rely on support services offered by N-CERT[270].

- **State Authority for the Protection of the Constitution (LfV [NI]):** The Lower Saxony State Authority for the Protection of the Constitution (Department 5) is located in the MI 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[271].

- **Institutional location of the ZAC [NI]:** "Landeskriminalamt Niedersachsen" (Lower Saxony State Criminal Police Office, own translation). The Lower Saxony State Criminal Police Office also provides a guide on internet crime. The Lower Saxony ZAC is supported by 12 cybercrime/digital traces task forces (TF CC/DS) in local police departments[272].

- **State Data Protection Authority:** Landesbeauftragte:r für den Datenschutz Niedersachsen (State Commissioner for Data Protection Lower Saxony, LfD, own translation)[273].

Other actors in Lower Saxony:

Cybersicherheitsbündnis (Cybersecurity Alliance, own translation)
The state of Lower Saxony and municipalities have formed a cybersecurity alliance to improve information security and strengthen cooperation. Within the framework of this alliance, relationships should be institutionalized and joint measures to increase the level of IT security are to be agreed upon and implemented.

Moreover, municipalities can make use of services provided by the N-CERT[274].

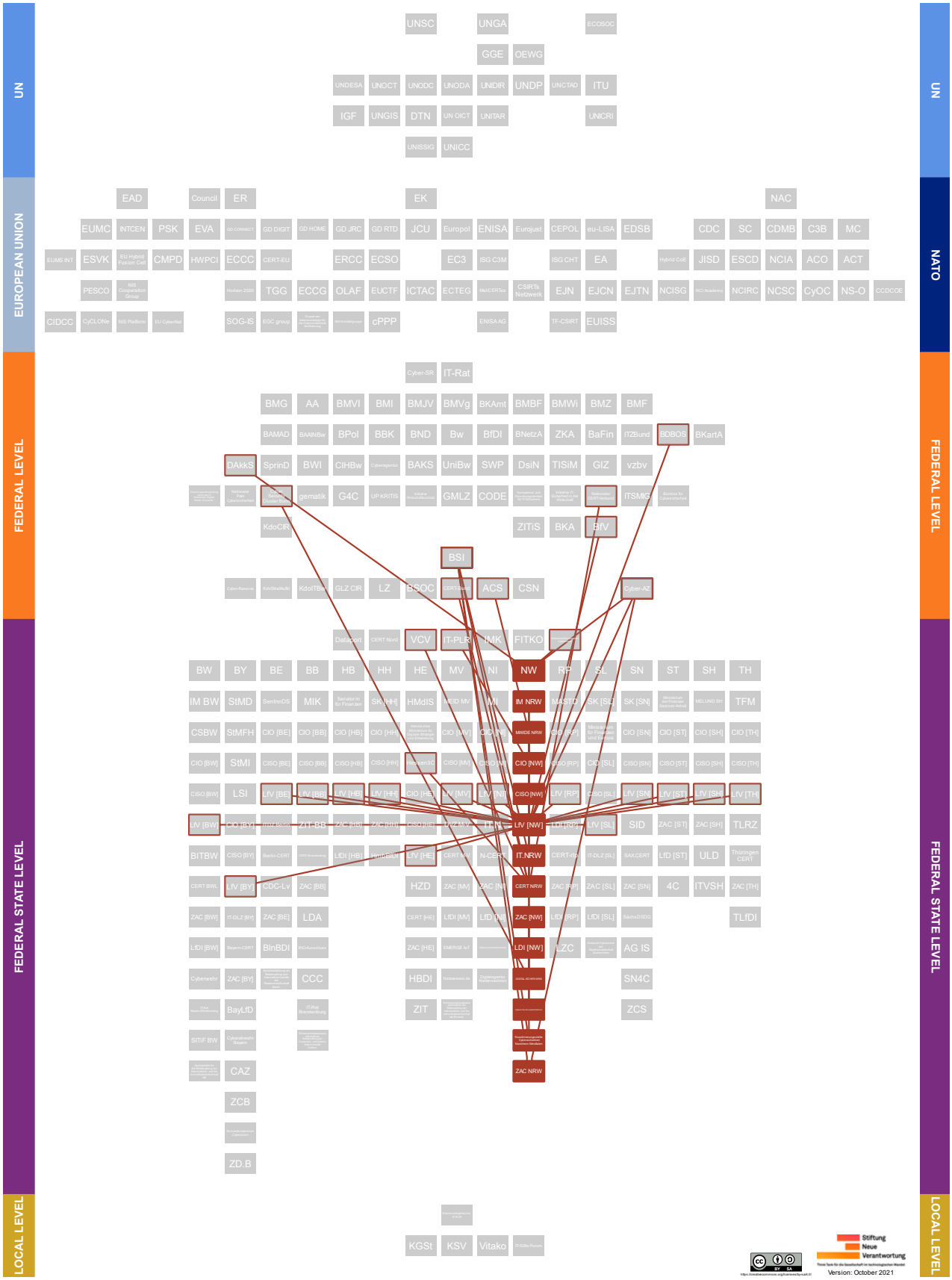
270 Niedersächsisches Computer Emergency Response Team N-CERT, 2016, Kooperation der CERTS im Verwaltungs-CERT-Verbund (VCV). (Website deleted)
Niedersächsisches Ministerium für Inneres und Sport, Praxisbeispiel Digitalisierung: Ausbau des N-CERT zum Cyber-Defense-Center (CDC).
Niedersächsisches Ministerium für Inneres und Sport, 100. Kommune nutzt N-CERT-Angebot des Innenministeriums zur Abwehr von Cyberangriffen.
Niedersächsische Ministerium für Inneres und Sport, Niedersachsen-CERT.
271 Ministerium für Inneres und Spor Niedersachsen, Die Cyberabwehr beim Verfassungsschutz Niedersachsen.
Ministerium für Inneres und Sport Niedersachsen, Organisationsplan des Niedersächsischen Ministeriums für Inneres und Sport.
272 Landeskriminalamt Niedersachsen, Ratgeber Internetkriminalität.
Landeskriminalamt Niedersachsen, Zentrale Ansprechstelle Cybercrime (ZAC).
Niedersächsischer Landtag, Kleine Anfrage zur schriftlichen Beantwortung mit Antwort der Landesregierung: Wie sicher ist die IT der Ministerien und von Landeseinrichtungen?.
273 Die Landesbeauftragte für den Datenschutz Niedersachsen, Die Behörde.
274 Niedersächsisches Ministerium des Innern und für Sport, Sicherheit in der digitalen Welt.

Digitalagentur Niedersachsen (Digital Agency Lower Saxony, own translation)
As a "one-stop-shop", the Digital Agency of Lower Saxony aims at supporting the economy of Lower Saxony in developing innovations and thus creating and securing jobs. Its "Arbeitskreis IT-Sicherheit" (IT security working group, own translation) provides, among other things, a central information point that prepares information on contact points, consulting and support services, or the general threat environment.

The Digital Agency of Lower Saxony is supported by the "Niedersächsische Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung" (Lower Saxony Ministry of Economy, Labor, Transport and Digitalization, MW, own translation)[275].

275 Digitalagentur Niedersachsen, IT-Sicherheit für Niedersachsen.
Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: Digitalagentur Niedersachsen.
Niedersächsisches Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung, Digitalagentur und weitere Angebote zur Unterstützung.

8.10. North-Rhine Westphalia



The state of North Rhine-Westphalia is represented as a partner in the Cyber-AZ by its "Kölner Schwerpunktstaatsanwaltschaft Cyber" (Cologne Focus Prosecutor's Office Cyber, own translation). It is also one of the shareholders of DAkkS. The "Landeskriminalamt Nordrhein-Westfalen" (State Criminal Police Office North-Rhine Westphalia, own translation) participates in the Sicherheitskooperation Cybercrime.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:**
  - "Ministerium des Innern des Landes Nordrhein-Westfalen" (Ministry of the Interior of North Rhine-Westphalia, IM NRW, official translation), "Abteilung 7: Digitalisierung im IM und Geschäftsbereich" (Division 7: Digitization within the IM and portfolio, own translation), "Referat 73: Koordinierungsstelle für Cybersicherheit NRW, Informationssicherheit im IM und Geschäftsbereich" (Division 73: Coordination Office for Cyber Security NRW, Information Security within in the IM and portfolio, own translation)[276].
  - "Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen" (Ministry of Economy, Innovation, Digitization and Energy of North Rhine-Westphalia, MWIDE NRW, own translation), "Abteilung I: Zentralabteilung" (Department I: Central Department, own translation), "Referat I.1: Informationssicherheit" (Division I.1: Information Security, own translation) and "Abteilung IV: Innovation und Märkte" (Department IV: Innovation and Markets, own translation), "Referat IV A 3: IKT, Mobilfunk und Cybersicherheit in der Wirtschaft" (Division IV A 3: ICT, mobile communications and cyber security in the economy, own translation).

    The MWIDE NRW is participating in the ACS[277].

- **State Commissioner for Information Technology (CIO [NW]):** The CIO of North Rhine-Westphalia is based in the MWIDE NRW. The CIO is responsible for IT management as well as standardization tasks.

  He or she is representing the North-Rhine Westphalia in the IT-PLR[278].

- **Chief Information Security Officer of the State Administration (CISO [NW]):** 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 MWIDE NRW[279].

276 Ministerium des Innern des Landes Nordrhein-Westfalen, Geschäftsverteilungsplan.
277 Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen, Geschäftsverteilungsplan.
278 Die Landesregierung Nordrhein-Westfalen, Prof. Andreas Meyer-Falcke neuer CIO.
279 Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie Nordrhein-Westfalen, Geschäftsverteilungsplan.

- **IT Service Provider of the Federal State Administration:** "Landesbetrieb Information und Technik Nordrhein-Westfalen" (State Office Information and Technology North Rhine-Westphalia, IT.NRW, own translation) in the portfolio of the MWIDE NRW.

  The BSI and IT.NRW are cooperating[280].

- **CERT**: The CERT NRW is operated by IT.NRW.

  It takes part in the National CERT Network[281].

- **State Authority for the Protection of the Constitution (LfV [NW]):** The IM NRW 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 (Division 611) and works on counterintelligence, economic protection, and cyber defense (Division 613)[282].

- **Institutional location of the ZAC [NW]**: Cybercrime Competency Center, actor description see below.

- **State Data Protection Authority:** Landesbeauftragte:r für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia, LDI, own translation)[283].

Other actors in North-Rhine Westphalia:

Cybercrime-Kompetenzzentrum (Cybercrime Competency Center, own translation)
The Cybercrime Competence Center established at the North Rhine-Westphalia State Criminal Police Office houses investigative commissions for outstanding proceedings as well as, experts for computer forensics, telecommunications surveillance, evaluation, analysis, and prevention. The center is also home to a "Zentrales Informations- und Servicezentrum Cybercrime" (Central Cybercrime Information and Service Center, ZISC, own translation), a "Cyber-Recherche- und Fahndungszentrum" (Cyber Research and Investigation Center, CRuFz, own translation), the

280 Landesbetrieb Information und Technik Nordrhein-Westfalen, Aufbau und Geschäftsverteilung.
Landtag Nordrhein-Westfalen, Stellungnahme des Vizepräsidenten des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Herr Dr. Gerhard Schabhüser zu den Anträgen der Fraktion der AfD (17/4803) "Lehren aus Hackerangriff ziehen – IT-Sicherheit in NRW verbessern" und der Fraktion Bündnis 90/DIE GRÜNEN (17/5056) "IT-Sicherheit in NRW stärken – Freiheit sichern" im Rahmen der Anhörung "Lehren aus dem Hackerangriff ziehen – IT-Sicherheit in NRW verbessern" des Ausschusses für Digitalisierung und Innovation des Landtags Nordrhein-Westfalen am 16. Mai 2019.
281 Information und Technik Nordrhein-Westfalen, Informationssicherheit für die Landesverwaltung NRW.
282 Ministerium des Innern Nordrhein-Westfalen, Organisationsplan.
283 Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Über uns.

"TKÜ-Dienststelle" (Telecommunication Surveillance Bureau, own translation) and the "Zentrale Auswertungs- und Sammelstelle Kinderpornografie" Central Child Pornography Analysis and Collection Center, ZASt, own translation). A cybercrime situation report is published annually.

The ZISC is also home to the ZAC [NW] for the economy[284].

Kompetenzzentrum für Cybersicherheit in der Wirtschaft (Competence Center for Cybersecurity in the Economy, DIGITAL.SICHER.NRW, own translation)
With offices in Bonn and Bochum, the Competence Center for Cyber Security in the Economy was established at the beginning of 2021. It is intended to support SMEs in North-Rhine-Westphalia in IT and cybersecurity issues, for example, by providing information, acting as a point of contact, or by helping to identify needs for basic IT protection. In addition, the center seeks to organize events and establish a network of those responsible for cyber security within the economy. The center's services are free of charge for SMEs.

DIGITAL.SICHER.NRW was established by the MWIDE NRW. The Cyber Security Cluster Bonn is a partner of the competence center[285].

Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen (Coordination Office for Cybersecurity North Rhine-Westphalia, own translation)
The Coordination Office for Cybersecurity in North Rhine-Westphalia has set itself the task of contributing to transparency for citizens, companies, and critical infrastructures, pooling information on the state's cyber security for the state administration, coordinating processes between the federal and federal state governments as well as in cross-state bodies, and creating effective synergies in the state through networking and cooperation with, among others, the LfV [NW] or the Cybercrime Competence Center. The Coordination Office submits an annual report on cyber security in NRW to the state cabinet.

The Coordination Office for Cybersecurity is located within the purview of the IM NRW and is designated as the state's central point of contact vis-à-vis the BSI[286].

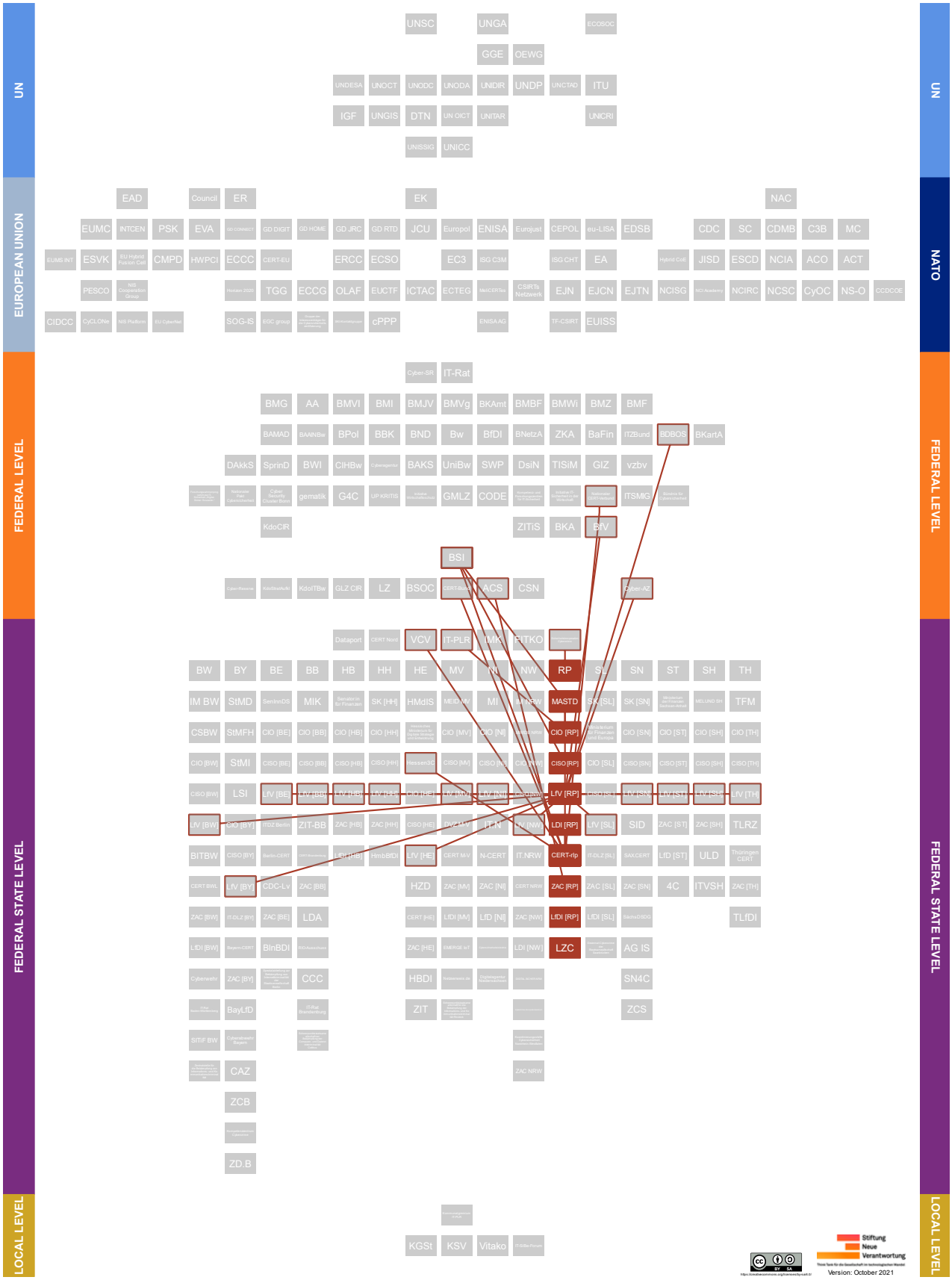
284 Polizei Nordrhein-Westfalen, Das Cybercrime-Kompetenzzentrum beim LKA NRW.
Polizei Nordrhein-Westfalen, Lagebild Cybercrime.
285 DIGITAL.SICHER.NRW, Die Partner des Kompetenzzentrums.
Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen, DIGITAL.SICHER.NRW: Land startet Kompetenzzentrum für Cybersicherheit in der Wirtschaft.
286 Behörden Spiegel, Neue Koordinierungsstelle für Cyber-Sicherheit in NRW. (Website deleted)
Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen, Über Uns.
Ministerium des Inneren des Landes Nordrhein-Westfalen, Kabinett beschließt Einrichtung von Koordinierungsstelle für Cybersicherheit.

Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (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 [NW] in the visualization and located in the Cybercrime Competency Center of the state's LKA – has been the "Staatsanwaltschaft Köln's" (Public Prosecutor's Office Cologne, own translation) responsible nationwide cybercrime unit of the judiciary. It is the largest judiciary cybercrime unit in Germany, 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, companies, and the BSI[287].

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

8.11. Rhineland-Palatinate



The "Landeskriminalamt Rheinland-Pfalz" (State Criminal Police Office Rhineland-Palatinate, own translation) is participating in the Sicherheitskooperation Cybercrime.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:** In May 2021, the lead responsibility was passed from the "Ministerium des Innern und für Sport" (Ministry of the Interior and Sports, own translation) to the "Ministerium für Arbeit, Soziales, Transformation und Digitalisierung" (Ministry of Labor, Social Affairs, Transformation and Digitalization, MASTD, own translation), "Abteilung 63: Digitalisierung" (Department 63: Digitalization), "Referat 633: Ressortübergreifende Informationssicherheit" (Division 633: Interdepartmental Information Security).

  In the past, the Ministry of the Interior and the BSI had signed a cooperation agreement on cybersecurity issues[288].

- **State Commissioner for Information Technology (CIO [RP]):** 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. He or she also assumes the function of the Chief Digital Officer (CDO).

  Simultaneously, he or she is State Secretary in the MASTD and represents Rhineland-Palatinate in the IT-PLR[289].

- **Chief Information Security Officer of the State Administration (CISO [RP]):** In Rhineland-Palatinate, the information security officer for the state administration (CISO-rlp) is based in Division 632 of Department 6 within the MASTD.

  He or she entertains exchange with the BSI, CERT-rlp, and the security authorities of the state[290].

- **IT Service Provider of the Federal State Administration:** "Landesbetrieb Daten und Information" (State Office Data and Information, LDI, own translation). The LDI is supervised by the state's Interior Ministry[291].

288 Ministerium des Innern und für Sport, Kooperationsvereinbarung zur Cybersicherheit abgeschlossen.
Ministerium für Arbeit, Soziales, Transformation und Digitalisierung Rheinland-Pfalz, Organigramm.
289 Ministerium des Innern und für Sport Rheinland-Pfalz, Digitale Verwaltung Rheinland-Pfalz.
Ministerium für Arbeit, Soziales, Transformation und Digitalisierung, Fedor Ruhose ist neuer Beauftragter der Landesregierung für Informationstechnik und Digitalisierung.
290 Ministerium der Justiz Rheinland-Pfalz, Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Rheinland-Pfalz.
291 Landesbetrieb Daten und Information, Der LDI: Der IT-Dienstleister der Landesverwaltung Rheinland-Pfalz.
Landesbetrieb Daten und Information, Impressum.

- **CERT**: The CERT-rlp is located within the LDI.

  It takes part in the National CERT Network[292].

- **State Authority for the Protection of the Constitution (LfV [RP]):** In Rhineland-Palatinate, the State Authority for the Protection of the Constitution is institutionally located in the state's Ministry of the Interior and Sports. Its areas of responsibility include espionage, cyber defense, and economic protection[293].

- **Institutional location of the ZAC [RP]:** "Dezernat 47 Cybercrime des Landeskriminalamtes Rheinland-Pfalz" (Department 47 of the Rhineland-Palatinate State Criminal Police Office, own translation). It functions as a central department and supports local authorities. It also deals with outstanding cybercrime investigations, particularly procedures piloting new investigative techniques that build upon precedent or those of special public interest, procedures with new technical and/or investigative tactics, and cases in the field of international, gang-related, or organized crime.

  The LKA of Rhineland-Palatinate has been a member of the ACS[294].

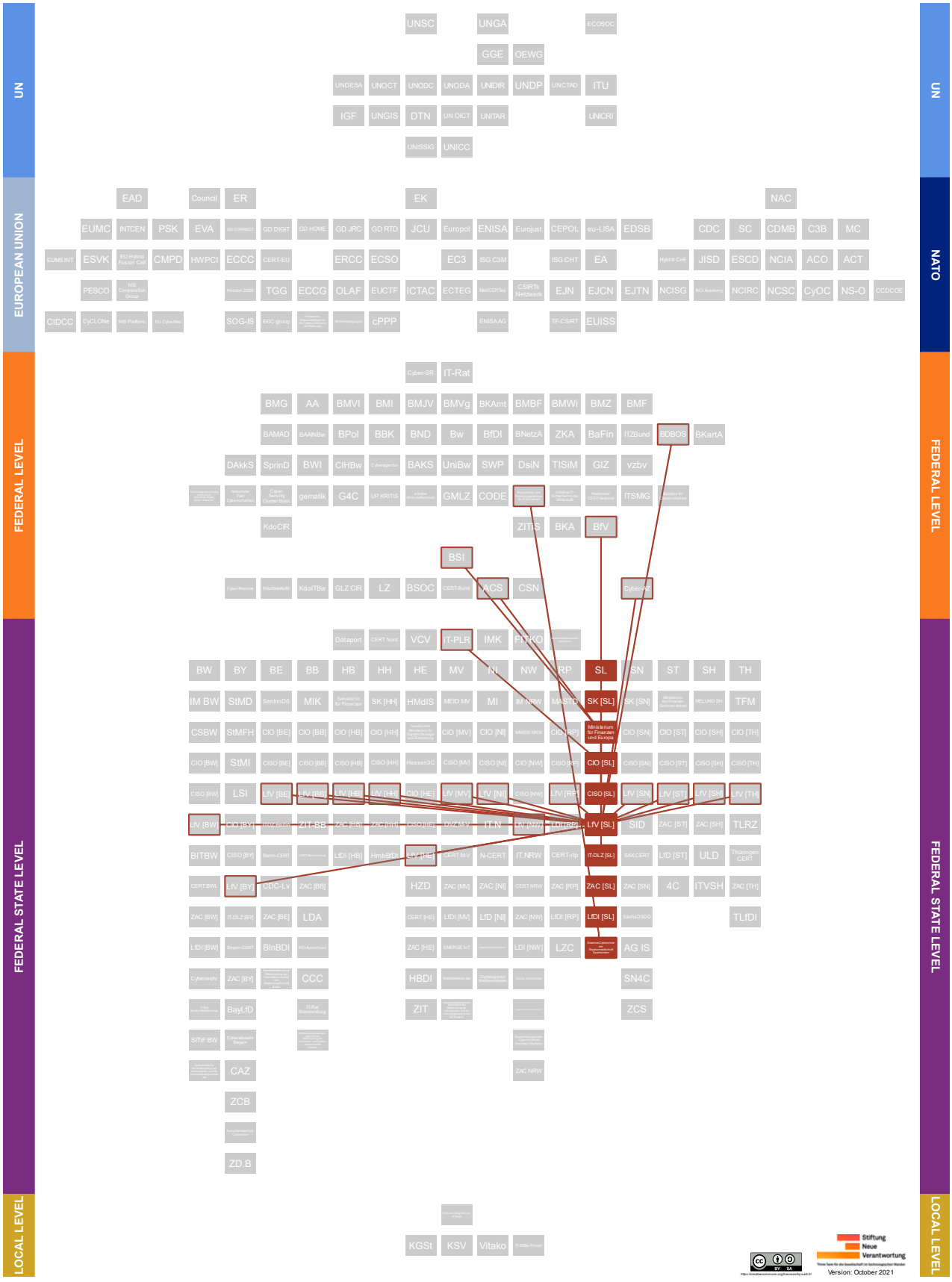
- **State Data Protection Authority:** Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (State Commissioner for Data Protection and Freedom of Information Rhineland-Palatinate, LfDI, own translation)[295].

Other actors in Rhineland-Palatinate:

Landeszentralstelle Cybercrime (Central State Office for Cybercrime, LZC, own translation)
The Central State Office for Cybercrime is located at the "Generalstaatsanwaltschaft Koblenz" (Koblenz General Public Prosecutor's Office, own translation) and performs coordination, support, and investigative tasks for the entire state. These include participation in federal and federal state committees, the leadership of the statewide cybercrime working group with the participation of all federal state prosecutors' offices, and the investigation of cases of particular importance, difficulty, and/or scope. The latter include, for example, high-profile investigations or those closely related to organized crime[296].

292 Ministerium des Innern und für Sport Rheinland-Pfalz, CERT-rlp.
293 Ministerium des Innern und für Sport Rheinland-Pfalz, Spionageabwehr, Wirtschaftsschutz und Cybersicherheit.
294 Polizei Rheinland-Pfalz, Aufgaben des Dezernates Cybercrime.
295 Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Über uns.
296 Generalstaatsanwaltschaft Koblenz, Landeszentralstelle Cybercrime (LZC).

8.12. Saarland



Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:**
  - "Staatskanzlei des Saarlandes" (State Chancellery of the Saarland, SK [SL], own translation), "Abteilung B: Grundsatzangelegenheiten und Digitalisierung" (Department B: Policy Issues and Digitization, own translation). The portfolio of the State Chancellery also includes an IT Innovation Center[297].
  - "Ministerium für Finanzen und Europa Saarland" (Ministry of Finance and Europe of Saarland, own translation), "Abteilung A: Organisation, Personal, Haushalt, Recht und IT" (Department A: Organization, Personnel, Budget, Law and IT, own translation). A "Stabsstelle Informationssicherheit und IT-Recht" (Administrative Department for information security and IT law, own translation) is also located there.

  The Ministry of Finance and Europe is participating in the ACS as a multiplier and has agreed on a cooperation with the BSI[298].

- **State Commissioner for Information Technology (CIO [SL]):** Saarland's CIO is at the same time "Bevollmächtigte:r des Saarlandes für Innovation und Strategie" (State Government Commissioner for Innovation and Strategy of Saarland, own translation). He or she is based in the "saarländische Staatskanzlei" (Saarland State Chancellery, own translation) and is supported by the "IT-Innovationszentrum" (IT Innovation Center, own translation).

  He or she represents Saarland in the IT-PLR[299].

- **Chief Information Security Officer of the State Administration (CISO [SL]):** 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 [SL], reports on risks and the status of implementation of IT security measures, and can recommend measures to mitigate these hazards, if necessary[300].

297 Staatskanzlei des Saarlandes, Abteilung B: Grundsatzangelegenheiten und Digitalisierung.
Staatskanzlei des Saarlandes, IT-Innovationszentrum.
298 Federal Office for Information Security, Liste von Multiplikatoren der Allianz für Cyber-Sicherheit.
Medien Saarland, Das Saarland unterzeichnet Kooperationsvereinbarung mit dem BSI und tritt als Multiplikator der Allianz für Cyber-Sicherheit (ACS) bei.
Ministerium für Finanzen und Saarland, Organigramm.
299 Staatskanzlei Saarland, Bevollmächtigter für Innovation und Strategie Chief Information Officer (CIO).
300 Ministerium für Finanzen und Europa Saarland, Stabstelle Informationssicherheit und IT-Recht.

- **IT Service Provider of the Federal State Administration:** "Landesamt für IT-Dienstleistungen" (State Office for IT Services, IT-DLZ [SL], own translation), which is subordinated to the state's Ministry of Finance and Europe[301].

- **CERT:** CERT Saarland is being provided by CERT-rlp in line with an agreement between the federal states of Saarland and Rhineland-Palatinate[302].

- **State Authority for the Protection of the Constitution (LfV [SL]):** The "Ministerium für Inneres, Bauen und Sport des Saarlandes" (Saarland Ministry for Internal Affairs, Construction and Sport, official translation) is home to the State Authority 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 operations[303].

- **Institutional location of the ZAC [SL]:** "Dezernat Cybercrime der saarländischen Kriminalpolizei" (Cybercrime Department of the Saarland Criminal Investigation Department, own translation). It deals with particularly severe cases – especially when the public sector is affected – with a very high potential for damage or high technical requirements[304].

- **State Data Protection Authority:** Unabhängiges Datenschutzzentrum Saarland mit Landesbeauftragter:m für Datenschutz und Informationsfreiheit (Saarland Independent Data Protection Center with State Commissioner for Data Protection and Freedom of Information, LfDI, own translation)[305].

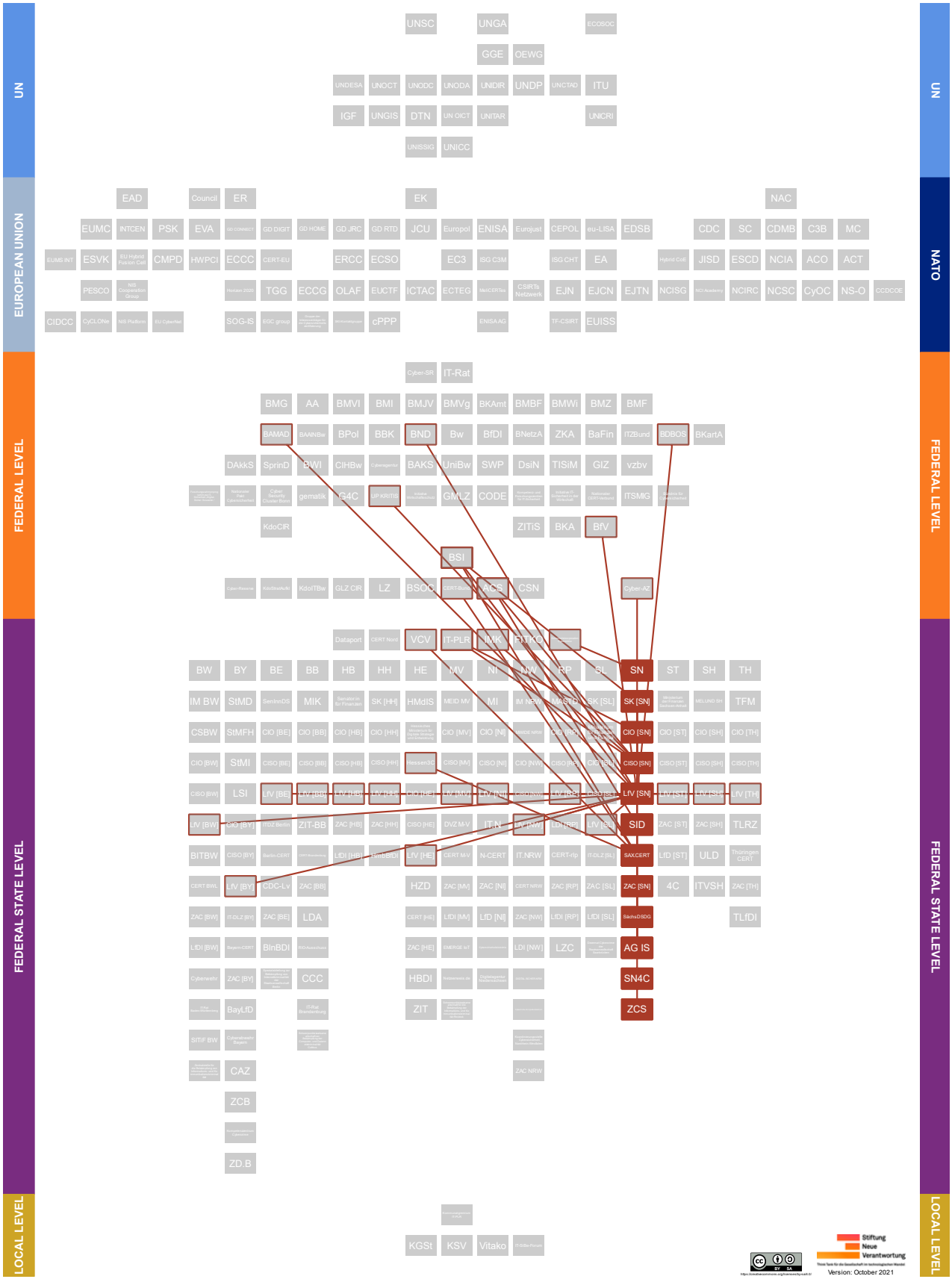
Other actors in Saarland:

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[306].

301 Ministerium für Finanzen und Europa Saarland, Themen & Aufgaben.
302 Kommune 21, CERT für saarländische Kommunen.
303 Ministerium des Innern, Bauen und Sport Saarland, Lagebild Verfassungsschutz 2019.
304 sol.de, Saar-Kripo eröffnet neue "Cybercrime"-Dienststelle. (Website deleted)
305 Unabhängiges Datenschutzzentrum Saarland, Über Uns.
306 Juristisches Internetprojekt Saarbrücken, Neues Dezernat "Cybercrime" bei der Staatsanwaltschaft Saarbrücken.

8.13. Saxony


UN
EUROPEAN UNION
NATO
FEDERAL LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
UNSC
UNGA
ECOSOC
GGE
OEWG
UNDESA
UNOCT
UNODC
UNODA
UNIDIR
UNDP
UNCTAD
ITU
IGF
UNGIS
DTN
UN OICT
UNITAR
UNICRI
UNISSIG
UNICC
EAD
Council
ER
EK
NAC
EUMC
INTCEN
PSK
EVA
GD CONNECT
GD DIGIT
GD HOME
GD JRC
GD RTD
JCU
Europol
ENISA
Eurojust
CEPOL
eu-LISA
EDSB
CDC
SC
CDMB
C3B
MC
EUMS INT
ESVK
EU Hybrid Fusion Cell
CMPD
HWPCI
ECCC
CERT-EU
ERCC
ECSO
EC3
ISG C3M
ISG CHT
EA
Hybrid CoE
JISD
ESCD
NCIA
ACO
ACT
PESCO
NIS Cooperation Group
Horizon 2020
TGG
ECCG
OLAF
EUCTF
ICTAC
ECTEG
MeliCERTes
CSIRTs Netzwerk
EJN
EJCN
EJTN
NCISG
NCI Academy
NCIRC
NCSC
CyOC
NS-O
CCDCOE
CIDCC
CyCLONe
NIS Platform
EU CyberNet
SOG-IS
EGC group
cPPP
ENISA AG
TF-CSIRT
EUISS
Cyber-SR
IT-Rat
BMG
AA
BMVI
BMI
BMJV
BMVg
BKAmt
BMBF
BMWi
BMZ
BMF
BAMAD
BAAINBw
BPol
BBK
BND
Bw
BfDI
BNetzA
ZKA
BaFin
ITZBund
BDBOS
BKartA
DAkkS
SprinD
BWI
CIHBw
Cyberagentur
BAKS
UniBw
SWP
DsiN
TISiM
GIZ
vzbv
gematik
G4C
LIP KRITIS
GMLZ
CODE
ITSMIG
KdoCIR
ZITiS
BKA
BfV
BSI
Cyber-Reserve
KdoStratAufkl
KdoITBw
GLZ CIR
LZ
BSOC
CERT-Bund
ACS
CSN
Cyber-AZ
Dataport
CERT Nord
VCV
IT-PLR
VMK
FIUKO
BW
BY
BE
BB
HB
HH
HE
MV
NI
NW
RP
SL
SN
ST
SH
TH
IM BW
StMD
SenInnDS
MIK
Senatorin für Finanzen
SK [HH]
HMdIS
MEID MV
MI
IM NRW
MDI RP
SK [SL]
SK [SN]
Ministerium der Finanzen Sachsen-Anhalt
MELUND SH
TFM
CSBW
StMFH
CIO [BE]
CIO [BB]
CIO [HB]
CIO [HH]
CIO [MV]
CIO [NI]
CIO NRW
CIO [RP]
Ministerium für Digitale Strategie und Entbürokratie
CIO [SN]
CIO [ST]
CIO [SH]
CIO [TH]
CIO [BW]
StMI
CISO [BE]
CISO [BB]
CISO [HB]
CISO [HH]
Hessen3C
CISO [MV]
CISO [NI]
CISO [NW]
CISO [RP]
CISO [SL]
CISO [SN]
CISO [ST]
CISO [SH]
CISO [TH]
CISO [BW]
LSI
LfV [BE]
LfV [BB]
LfV [HB]
LfV [HH]
LfV [HE]
LfV [MV]
LfV [NI]
LfV [NW]
LfV [RP]
LfV [SL]
LfV [SN]
LfV [ST]
LfV [SH]
LfV [TH]
LfV [BW]
CISO [BY]
ITDZ Berlin
ZIT-BB
ZAC [HB]
ZAC [HH]
CISO [HE]
DVZ M-V
IT.N
LKA NW
LDI [RP]
LfV [SL]
SID
ZAC [ST]
ZAC [SH]
TLRZ
BITBW
CISO [BY]
Berlin-CERT
LfD [HB]
HmbBfDI
LfV [HE]
CERT M-V
N-CERT
IT.NRW
CERT-rlp
IT-DLZ [SL]
SAX.CERT
LfD [ST]
ULD
Thüringen CERT
CERT BWL
LfV [BY]
CDC-Lv
ZAC [BB]
HZD
ZAC [MV]
ZAC [NI]
CERT NRW
ZAC [RP]
ZAC [SL]
ZAC [SN]
4C
ITVSH
ZAC [TH]
ZAC [BW]
IT-DLZ [BY]
ZAC [BE]
LDA
CERT [HE]
LfDI [MV]
LfD [NI]
ZAC [NW]
LfDI [RP]
LfDI [SL]
SächsDSDG
TLfDI
LfDI [BW]
Bayern-CERT
BlnBDI
BIG Ausschuss
ZAC [HE]
EMERGE IoT
LDI [NW]
LZC
AG IS
Cyberwehr
ZAC [BY]
CCC
HBDI
SN4C
BayLfD
IT-Rat Brandenburg
ZIT
ZCS
SITiF BW
Cyberabwehr Bayern
ZAC NRW
CAZ
ZCB
ZD.B
KGSt
KSV
Vitako
IT-SiBe-Forum
Stiftung Neue Verantwortung
Version: October 2021

The "Landeskriminalamt Sachsen" (State Criminal Police Office, own translation) participates in the Sicherheitskooperation Cybercrime.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:** "Sächsische Staatskanzlei" (State Chancellery of Saxony, SK [SN], own translation), "Abteilung 4: Digitale Verwaltung" (Department 4: Digital Administration, own translation), "Referat 45: Informations- und Cybersicherheit, Kritische Infrastrukturen" (Division 45: Information and Cybersecurity, Critical Infrastructures, own translation).

  The SK [SN] and the BSI have agreed on closer cooperation in the field of cybersecurity[307].

- **State Commissioner for Information Technology (CIO [SN]):** Saxony's CIO leads the SK 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).

  He or she represents Saxony in the IT-PLR[308].

- **Chief Information Security Officer of the State Administration (CISO [SN]):** Saxony's CISO is also the head of Division 45 of the SK [SN].

  He or she is appointed by the state CIO [SN] and can exercise a direct right of consultation. The CISO [SN] is a member of the "Arbeitsgruppe Informationssicherheit des IT-PLR" (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[309].

- **IT Service Provider of the Federal State Administration: "**Staatsbetrieb Sächsische Informatik Dienste" (State Enterprise Saxon Information Technology Services, SID, own translation), which is subordinate to the SK [SN].

- The SID participates in the ACS[310].

307 Sächsische Staatskanzlei, Organisation.
Sächsische Staatskanzlei, Sachsen und Bund kooperieren bei Cyber-Sicherheit.
308 Sächsische Staatskanzlei, Staatssekretäre.
309 Sächsische Staatskanzlei, Beauftragter für Informationssicherheit des Landes (BfIS).
310 Sächsische Staatskanzlei, Nachgeordnete Behörden.
Staatsbetrieb Sächsische Informatik Dienste, Aufgaben, Leistungen.

- **CERT:** The SAX.CERT is attached to the SID. SAX.CERT also offers free security services, such as a vulnerability warning service or Identity Leak Checker, for the federal state administration and municipalities[311].

- **State Authority for the Protection of the Constitution (LfV [SN]):** The Saxon State Authority for the Protection of the Constitution is institutionally attached to the "Staatsministerium des Innern" (State Ministry of the Interior, SMI, own translation).

  Relationships on working level exist with the BfV, its counterparts in all federal states (LfV's), the BND, the BAMAD, the BSI, and the Cyber-AZ[312].

- **Institutional location of the ZAC [SN]:** SN4C, actor description see below.

- **State Data Protection Authority:** Sächsische:r Datenschutzbeauftragte:r (State Commissioner for Data Protection Saxony, SächsDSDG, own translation)[313].

Other actors in Saxony:

Arbeitsgruppe Informationssicherheit (Information Security Working Group, AG IS, own translation)
The Information Security Working Group is intended to contribute to interdepartmental cooperation in Saxony by advising the CISO [SN] in the area of information security as well as developing and adapting minimum standards. The latter are adopted as recommendations and then passed on to the "sächsischer Lenkungsauschuss für IT und E-Government" (Saxon Steering Committee for IT and E-Government, LA ITEG, own translation) for final decision-making.

The AG IS is chaired by the CISO [SN]. Members of the AG IS comprise the information security officers of the SächsDSDG and the SID (without voting rights), as well as the head of the SAX.CERT[314].

Cyber Crime Competence Center Sachsen (Cyber Crime Competence Center Saxony, SN4C, own translation)
The SN4C was established within the "Landeskriminalamt Sachsen" (State Criminal Police Office of Saxony, own translation). It focuses on various types of criminality

311 Sächsische Staatskanzlei, Jahresbericht Informationssicherheit 2020 des Beauftragten für Informationssicherheit des Landes.
Staatsbetrieb Sächsische Informatik Dienste, CERT & Informationssicherheit.
312 Staatsministerium des Innern Sachsen, Sächsischer Verfassungsschutzbericht 2019.
313 Sächsischer Datenschutzbeauftragter, Über uns.
314 Sächsische Staatskanzlei, Arbeitsgruppe Informationssicherheit.
Sächsische Staatskanzlei, Sächsisches Informationssicherheitsgesetz.

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 the ZAC [SN] and cooperates with the ZCS[315].

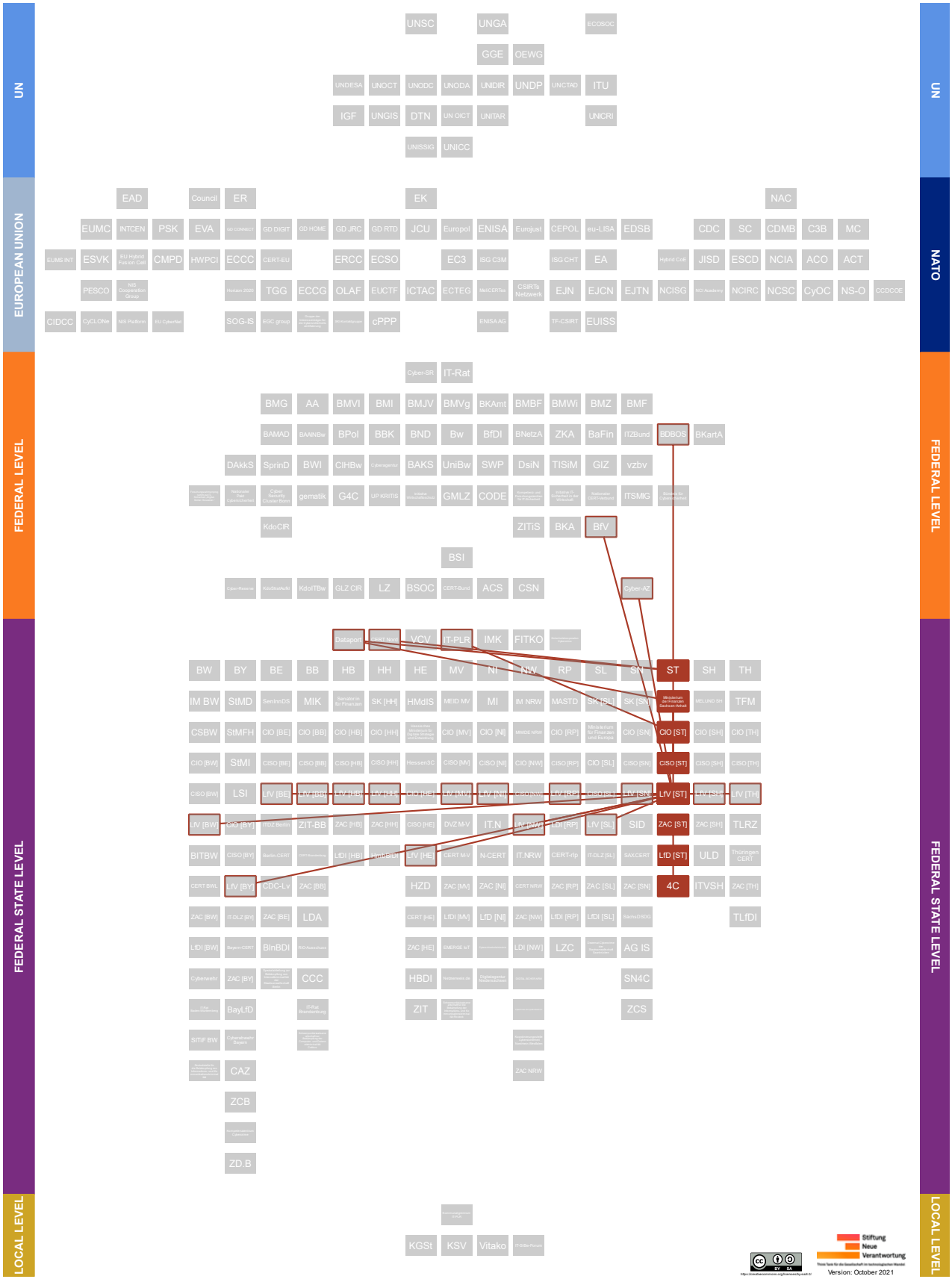
Zentralstelle Cybercrime Sachsen (Central Office Cybercrime Saxony, ZCS, own translation)
The ZCS, housed within the "Generalstaatsanwaltschaft Dresden" (Public Prosecutor General's Office of Dresden, own translation), is the judicial counterpart to the SN4C of the LKA Sachsen. It focuses on the prosecution of internet-related crimes. The ZCS only conducts investigations itself in cases involving, for example, internal and external security in Germany. It acts primarily as a coordinating and advisory body for investigators and provides thematic training and continuing education.

ZCS and SN4C cooperate closely[316].

315 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.

316 Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: Spezialisierte Einrichtungen der Justiz.
Staatsministerium der Justiz, Sächsisches Justizministerialblatt Nr. 5/2018.

8.14. Saxony-Anhalt



The state of Saxony-Anhalt is one of the signatories to the interstate treaty which established Dataport.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:** "Ministerium der Finanzen Sachsen-Anhalt" (Ministry of Finance Saxony-Anhalt, own translation), "Abteilung 5: Informations- und Kommunikationstechnologie (IKT) des Landes Sachsen-Anhalt" (Department 5: Information and Communication Technology (ICT) of the State of Saxony-Anhalt, own translation).

  A representative of the ministry is a member of Dataport's Board of Directors[317].

- **State Commissioner for Information Technology CIO [ST]:** Currently, Saxony-Anhalt's Ministry of Finance provides the state CIO, also known as the "Beauftragte der Landesregierung für Informations- und Kommunikationstechnik" (State Government Commissioner for Information and Communication Technology of Saxony-Anhalt, own translation).

  He or she represents Saxony-Anhalt on the IT-PLR[318].

- **Chief Information Security Officer of the State Administration (CISO [ST]):** In addition to the state's CIO, the Ministry of Finance in Saxony-Anhalt is also home to the state's CISO.

  He or she informs the CIO [ST] and is responsible for processes to implement and comply with information security standards[319].

- **IT Service Provider of the Federal State Administration:** Dataport, actor description see below (Chapter 8.17).

- **CERT:** CERT Nord, actor description see below (Chapter 8.17).

- **State Authority for the Protection of the Constitution (LfV [ST]):** In Saxony-Anhalt, the State Authority for the Protection of the Constitution is located in Department 4 of its "Ministerium für Inneres und Sport" (Ministry of the Interior and Sports, own translation). Division 44 is responsible for counterintelligence and economic protection. According to the Saxony-Anhalt report on the protection of the constitution, counterintelligence also includes cyber operations[320].

317 Ministerium der Finanzen Sachsen-Anhalt, Organigramm.
318 Sachsen-Anhalt, Der Beauftragte der Landesregierung für Informationstechnik (CIO).
319 Ministerium der Finanzen Sachsen-Anhalt, Organisationsplan.
Ministerium für Justiz und Gleichstellung Sachsen-Anhalt, Leitlinie zur Informationssicherheit in der unmittelbaren Landesverwaltung Sachsen-Anhalt.
320 Ministerium für Inneres und Sport Sachsen-Anhalt, Organisationsplan.
Ministerium für Inneres und Sport des Landes Sachsen-Anhalt, Verfassungsschutzbericht 2019.

- **Institutional location of the ZAC [ST]:** Cybercrime Competence Center, actor description see below.

- **State Data Protection Authority:** Landesbeauftragte:r für den Datenschutz Sachsen-Anhalt (State Commissioner for Data Protection Saxony-Anhalt, LfD, own translation)[321].

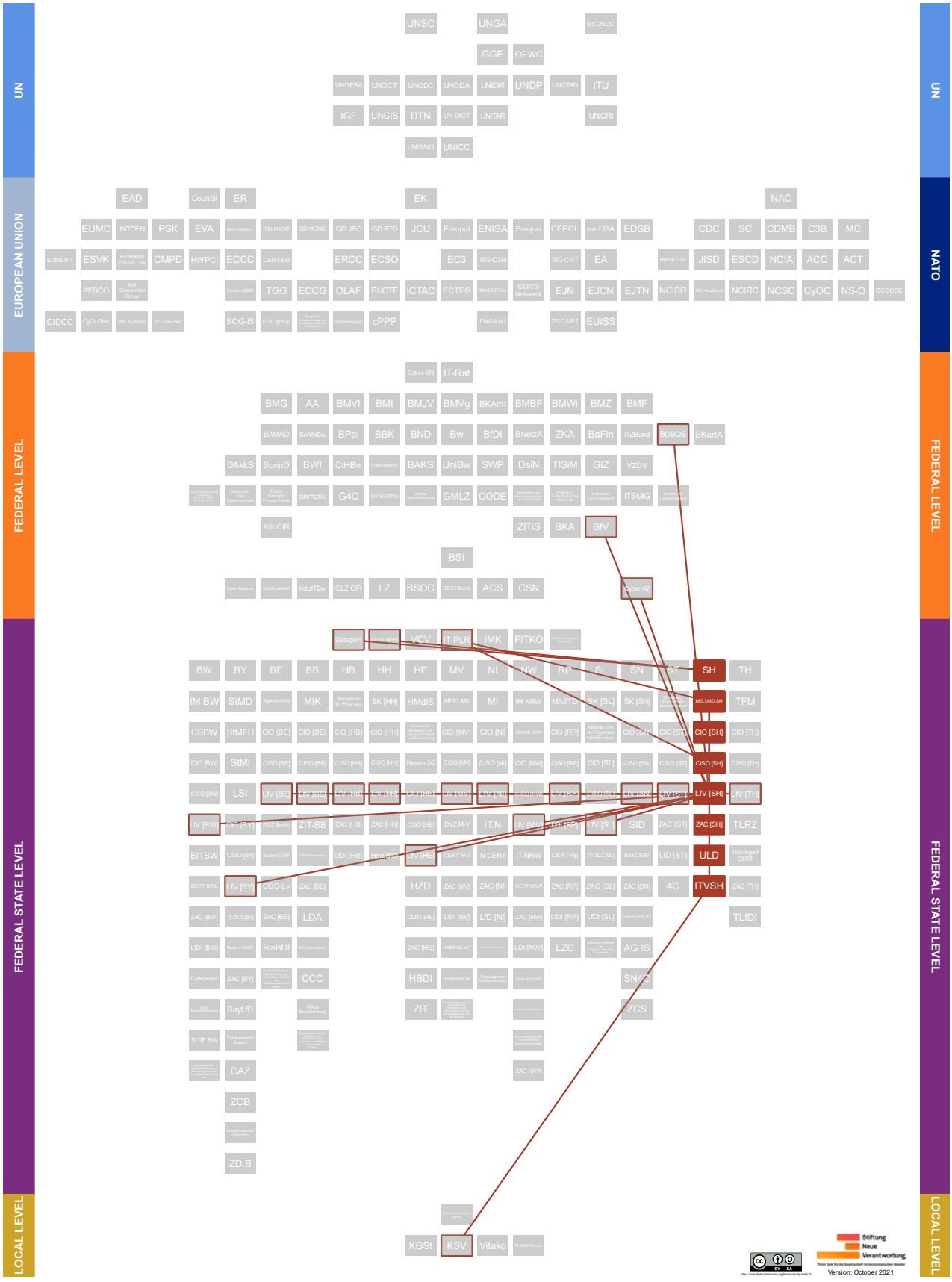
Other actors in Saxony-Anhalt:

Cybercrime Competence Center (4C)
The 4C was established within the "Landeskriminalamt Sachsen-Anhalt" (State Criminal Police Office 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 supports the police in simple fraud cases.

The center also assumes the function of the ZAC [ST][322].

321 Landesbeauftragter für den Datenschutz Sachsen-Anhalt, Gesetzliche Aufgaben und Zuständigkeiten.
322 Hallelife.de, Sachsen-Anhalt startet Kompetenzzentrum gegen Internetkriminalität.

8.15. Schleswig-Holstein



The state of Schleswig-Holstein is one of the signatories to the interstate treaty which established Dataport.

Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:** "Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung" (Ministry of Energy, Agriculture, the Environment, Nature and Digitalization, MELUND SH, official translation), "Abteilung V 3: Digitalisierung und Zentrales IT-Management der Landesregierung" (Department V 3: Digitization and Central IT Management of the State Government, own translation)[323].

- **State Commissioner for Information Technology (CIO [SH])**: The CIO of Schleswig-Holstein is responsible for the state's central IT management and is based in the MELUND SH[324].

- **Chief Information Security Officer of the State Administration (CISO [SH])**: In Schleswig-Holstein, the state's CISO is located within Department 3 of the MELUND SH. He or she is responsible for interdepartmental information security management.

  He or she has the right of presentation towards the state's CIO [SH] and is also represented in the "Arbeitsgruppe Informationssicherheit des IT-PLR" (Working Party on Information Security of the IT Planning Council, AG InfoSic, own translation) for Schleswig-Holstein[325].

- **IT Service Provider of the Federal State Administration:** Dataport, actor description see below (Chapter 8.17).

- **CERT:** CERT Nord, actor description see below (Chapter 8.17).

- **State Authority for the Protection of the Constitution (LfV [SH]):** The State Authority 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, MILIG SH, official translation), Department IV 7. Its fields of work include counterintelligence and economic pro-

323 Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung des Landes Schleswig-Holstein, Organisationsplan.
324 Schleswig-Holstein, E-Government – Steuerung und Zusammenarbeit.
325 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.

tection. A different department (IV 76) also deals with digital work, IT, G10, and secret protection[326].

- **Institutional location of the ZAC [SH]:** "Landeskriminalamt Schleswig-Holstein" (State Criminal Police Office Schleswig-Holstein, own translation). It also coordinates cross-state cybercrime investigations in the event of malicious cyber activity against companies and public authorities[327].

- **State Data Protection Authority:** Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Independent State Center for Data Protection Schleswig-Holstein, ULD, own translation) with a "Landesbeauftragter:m für Datenschutz" (State Commissioner for Data Protection, own translation)[328].

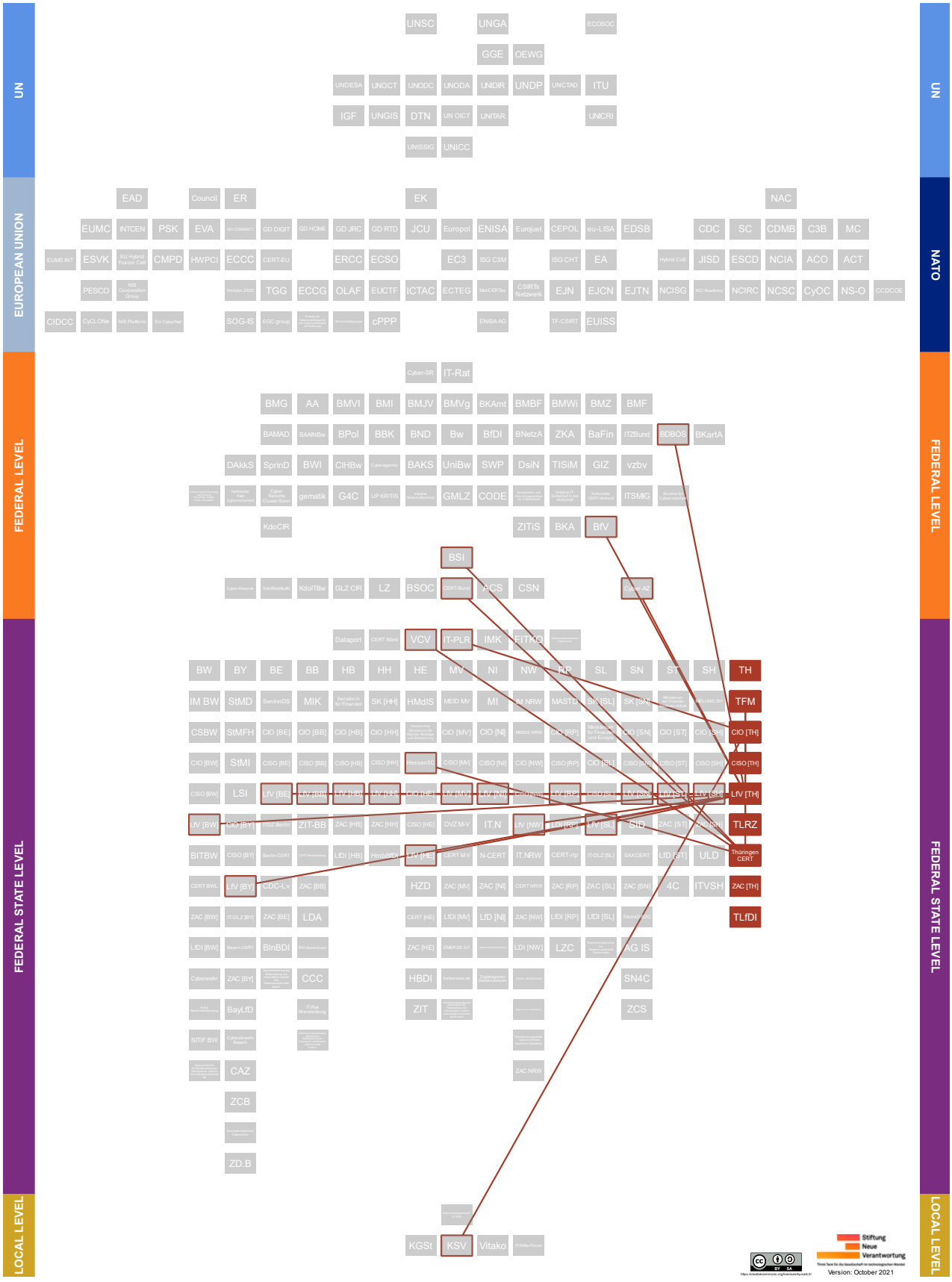
Other actors in Schleswig-Holstein:

IT-Verbund Schleswig-Holstein (IT Network Schleswig-Holstein, ITVSH, own translation)
Jointly funded by the state of Schleswig-Holstein and its municipalities, the ITSVH is available to municipalities as a point of contact for digitization issues. It also implements specific projects. The ITVSH project "Sicherheit für Kommunen in Schleswig-Holstein" (Seurity for Municipalities in Schleswig-Holstein, SiKoSH, own translation) supports Schleswig-Holstein municipalities in establishing an information security management and implementing the "BSI-IT-Grundschutzprofile" (BSI IT baseline protection profiles, own translation).

The MELUND SH is responsible for the legal supervision of the ITVSH. The Administrative Board of the ITVSH includes representatives of the KSV at the federal state level[329].

326 Der Ministerpräsident des Landes Schleswig-Holstein, Spionageabwehr und Wirtschaftsschutz.
Ministerium für Inneres, ländliche Räume, Integration und Gleichstellung, Organisationsplan.
327 Landespolizei Cybercrime, Zentrale Ansprechstelle Cybercrime (ZAC).
328 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Wir über uns.
329 Federal Ministry of the Interior, Building and Community, Online Kompendium Cybersicherheit in Deutschland: IT-Verbund Schleswig-Holstein (ITVSH).
IT-Verbund Schleswig-Holstein, SiKoSH.
Landesregierung Schleswig-Holstein, Gesetz zur Errichtung einer Anstalt öffentlichen Rechts „IT-Verbund Schleswig-Holstein" (Errichtungsgesetz ITVSH).

8.16. Thuringia



Overview

- **Ministerial responsibility(ies) for cyber and IT security topics:** "Thüringisches Finanzministerium" (State Ministry of Finance of Thuringia, TFM, own translation), "Abteilung 5: E-Government und IT" (Department 5: E-Government and IT, own translation), "Referat 53: Informationssicherheit, Rechtsfragen von E-Government und IT, Vergabe" (Division 53: Information Security, Legal Issues of E-Government and IT, Procurement, own translation)[330].

- **State Commissioner for Information Technology (CIO [TH]):** The CIO of Thuringia is based in the TFM and is responsible for the standardization of IT and e-government structures. A "Koordinierungsstelle für E-Government and IT" is subordinate to the CIO [TH].

  He or she is a member of the IT-PLR and is responsible for the technical supervision of the "Thüringer Landesrechenzentrum" (Thuringian State Computer Center, TLRZ, own translation). In addition, he or she is the contact person for the KSV in strategic matters[331].

- **Chief Information Security Officer of the State Administration (CISO [TH]):** The Thuringian CISO is appointed by the TFM and is based in its Department 5. He or she heads the information security team, which is inter alia made up of information security officers from all departments.

  He or she is directly subordinate to the CIO [TH][332].

- **IT Service Provider of the Federal State Administration:** TLRZ, which falls under the purview of the TFM[333].

- **CERT**: The ThüringenCERT is being operated by the TLRZ[334].

- **State Authority for the Protection of the Constitution (LfV [TH]):** In Thuringia, the State Authority for the Protection of the Constitution is organizationally located

330 Thüringer Finanzministerium, Geschäftsverteilungsplan.
Thüringer Finanzministerium, Informationssicherheit.
Thüringer Landtag, Unterrichtung durch die Landesregierung: Aktionsplan 2016 zur Umsetzung der Strategie für E-Government und IT des Freistaats Thüringen.

331 Freistaat Thüringen, CIO des Freistaats Thüringen.
Thüringer Finanzministerium, Verwaltungsvorschrift für die Organisation des E-Government und des IT-Einsatzes in der Landesverwaltung des Freistaats Thüringen vom 12. März 2019.

332 Finanzministerium Thüringen, Informationssicherheitsleitlinie der Thüringer Landesverwaltung.

333 Thüringer Landesrechenzentrum, Über uns.

334 Federal Office for Information Security, BSI und Thüringen: Engere Zusammenarbeit bei der Cyber-Sicherheit. (Website deleted)
Thüringer Landesrechenzentrum, ThüringenCERT.

within the "Ministerium für Inneres und Kommunales" (Thuringian Ministry of the Interior and Municipal Affairs, TMIK, own translation). Department 54 oversees counterintelligence as an area of work, also including cyber defense and economic protection[335].

- **Institutional location of the ZAC [TH]**: "Dezernat Cybercrime des Landeskriminalamtes Thüringen" (Cybercrime Department of the State Criminal Police Office Thuringia, TLKA, own translation). This department inter alia deals with fraud on the internet and investigations of child and adolescent sexual exploitation on the internet[336].

- **State Data Protection Authority:** Thüringische:r Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit (State Commissioner for Data Protection and Freedom of Information Thuringia, TLfDI, own translation)[337].

335 Ministerium für Inneres und Kommunales Thüringen, Organigramm.
Ministerium für Inneres und Kommunales Thüringen, Wirtschaftsspionage / Wirtschaftsschutz.
336 Heise Online, Cybercrime: Neue Herausforderungen für Thüringer LKA.
Ministerium für Inneres und Kommunales Thüringen, Internetkriminellen gemeinsam mit den Unternehmen das Handwerk legen. (Website deleted)
337 Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Aufgaben.

8.17. Actors in multiple federal states

CERT Nord (CERT North, own translation)
The federal states of Bremen, Schleswig-Holstein, Hamburg, and Saxony-Anhalt have a joint CERT called "CERT Nord". Information on IT security incidents is shared via internal platforms. If necessary, CERT Nord coordinates reactive measures in the event of incidents with effects among various departments or possibly beyond one federal state. CERT Nord also makes recommendations for preventive IT security measures and standards.

CERT Nord is located at Dataport and is a member of VCV[338].

Dataport
As an institution under public law, Dataport is based on a "Staatsvertrag" (state treaty, own translation) between the states of Bremen, Hamburg, Lower Saxony, Mecklenburg-Western Pomerania, Saxony-Anhalt, and Schleswig-Holstein. Dataport acts as a central IT service provider for these six federal states and their public administrations. To identify and defend against malicious cyber activity, Dataport also maintains a Security Operations Center (SOC), which, among other things, is also continuously and proactively searching for vulnerabilities.

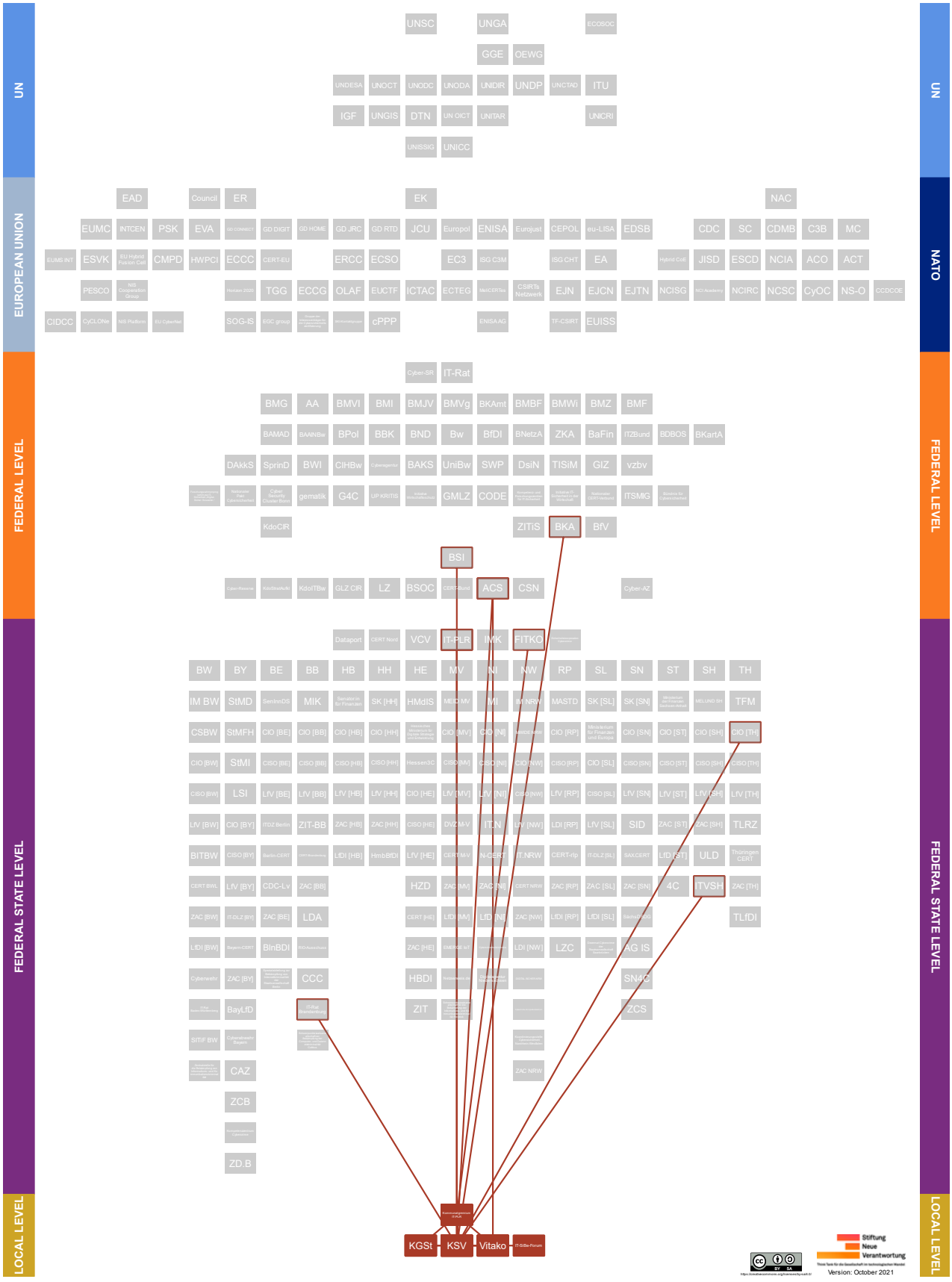
Dataport's Board of Directors includes representatives of the Finance Senator [HB], the SK [HH], the Ministry of Finance [NI], the MEID MV (the CIO [MV]), the Ministry of Finance [ST], and the StK SH[339].

Sicherheitskooperation Cybercrime (Security Cooperation Cybercrime, own translation)
"Sicherheitskooperation Cybercrime" is an initiative that 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.

It is an initiative of the criminal investigation offices of six federal states (Baden-Wuerttemberg, Hesse, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate, and Saxony) and the Bitkom[340].

338 CERT Nord, CERT Nord.
339 Dataport, Die Organe von Dataport.
Dataport, Dataport.Digitalisierung. Mit Sicherheit.
Dataport, Security Operations Center.
340 Sicherheitskooperation Cybercrime, Aktivitäten.
Sicherheitskooperation Cybercrime, Die Kooperation.

9. Explanation – Actors at Local Level



Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister (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 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 to exchange information and develop 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 Vitako supports 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. It is a multiplicator of the ACS[341]*.*

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[342]. 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

341 Vitako, Gremien.
Vitako. Satzung.
Vitako, Verband.
Vitako, Verein.
342 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)[343].

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[344].

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 the federalstate 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 the federal state level, to cultivate and facilitate the exchange of experiences and information between its members.

343 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.
344 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. Together with the BSI and the BKA, the KSV have issued recommendations for local authorities on how to respond to ransom demands resulting from the use of encryption Trojans. 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-PLR 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[345].

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

A municipal committee of the IT Planning Council was established 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 (KSV), three representatives from Vitako, and two representatives from the KGSt[346].

345 Deutscher Landkreistag, Bundesvereinigung der kommunalen Spitzenverbände.
Deutscher Landkreistag, Der Verband.
Deutscher Städtetag, Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen.
DStGB, Wir über uns.
Federal Office for Information Security, Empfehlungen bei IT-Angriffen auf kommunale Verwaltungen.
Federal Office for Information Security, IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung.
IT Planning Council, Zusammensetzung des IT-Planungsrats.
Schubert & Klein, Kommunale Spitzenverbände.

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

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

Christina Rupp is a Project Assistant for International Cybersecurity Policy at Stiftung Neue Verantwortung. Her research interests lie in the field of cyber diplomacy and cyber foreign policy, particularly how international law applies in cyberspace as well as international norms for responsible behavior.

Dr. Sven Herpig is Director for International Cybersecurity Policy at Stiftung Neue Verantwortung. Sven primarily deals with Germany's cybersecurity policy, government hacking (including the "Bundestrojaner") and IT vulnerability management, as well as government responses to cyber operations, attacks on machine-learning applications, and active cyber defense.

Contact the authors:

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

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

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