October 2023 · Dr. Sven Herpig & Frederic Dutke

Germany's Cybersecurity Architecture

Translation of the 11th edition

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

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Table of Contents

1. Background and Methodology 13

2. Visualization of Cybersecurity Architecture 18

3. Abbreviations and Actor Categorization 19

4. Explanation – Actors at UN Level 48

Policy Overview 49

United Nations Institute for Training and Research (UNITAR) 49
United Nations Office for Disarmament Affairs (UNODA) 49
United Nations Office on Drugs and Crime (UNODC) 50
United Nations Development Programme (UNDP) 51
Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE) 52
United Nations Department of Economic and Social Affairs (UNDESA) 53
International Telecommunication Union (ITU) 53
Internet Governance Forum (IGF) 54
United Nations Conference on Trade and Development (UNCTAD) 55
Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG) 56
United Nations Economic and Social Council (ECOSOC) 56
United Nations General Assembly (UNGA) 57
United Nations Institute for Disarmament Research (UNIDIR) 58
United Nations Interregional Crime and Justice Research Institute (UNICRI) 59
United Nations Security Council (UNSC) 59
United Nations Digital and Technology Network (DTN) 60
United Nations Group on the Information Society (UNGIS) 61
United Nations Information Security Special Interest Group (UNISSIG) 61
United Nations International Computing Centre (UNICC) 62
United Nations Office of Counter-Terrorism (UNOCT) 62
United Nations Office of Information and Communications Technology (UN OICT) 63

5. Explanation – Other International Actors 64

Policy Overview 65

Council of Europe (CoE) 65
European Space Agency (ESA) 66
Forum of Incident Response and Security Teams (FIRST) 67
International Electrotechnical Commission (IEC) 67
International Criminal Police Organization (Interpol) 68
International Organization for Standardization (ISO) 69

Internet Corporation for Assigned Names and Numbers (ICANN) 69
Internet Engineering Task Force (IETF) 70
ISO and IEC Joint Technical Committee (JTC 1) 70
Organization for Security and Co-operation in Europe (OSCE) 71
Trusted Introducer (TI) 71

6. Explanation – Actors at EU Level 72
Policy Overview 73
European Union Agency for Cybersecurity (ENISA) 74
European Union Agency for Law Enforcement Training (CEPOL) 76
European Union Agency for Criminal Justice Cooperation (Eurojust) 76
CEN/CENELEC Cyber Security Coordination Group (CSCG) 77
Computer Emergency Response Team of the European Commission (CERT-EU) 78
Computer Security Incident Response Teams Network (CSIRTs Network) 78
Cyber Crisis Liaison Organisation Network (CyCLONe) 79
Cyber and Information Domain Coordination Centre (CIDCC) 79
Crisis Management and Planning Directorate (CMPD) 80
ENISA Advisory Group (ENISA AG) 80
EU Hybrid Fusion Cell 81
EU Cyber Capacity Building Network (EU CyberNet) 81
Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) 82
European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) 83
European Cybersecurity Certification Group (ECCG) 83
European Commission (EC) 84
European co-operation for Accreditation (EA) 85
European Defence Agency (EDA) 85
European Central Bank (ECB) 86
European External Action Service (EEAS) 87
European Data Protection Supervisor (EDPS) 87
European Council (EUCO) 88
European Anti-Fraud Office (OLAF) 88
European Telecommunications Standards Institute (ETSI) 89
European Committee for Electrotechnical Standardization (CENELEC) 89
European Committee for Standardization (CEN) 90
European Police Office (Europol) 90
European Security and Defence College (ESDC) 91
European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) 91
European Cybercrime Center (EC3) 92
European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) 93

European Cybercrime Training and Education Group (ECTEG) 93
European Cyber Security Organisation (ECSO) 94
European Government CERTs group (EGC group) 94
European Judicial Network (EJN) 95
European Judicial Cybercrime Network (EJCN) 95
European Judicial Training Network (EJTN) 95
European Multidisciplinary Platform Against Criminal Threats (EMPACT) 95
European Union Cybercrime Task Force (EUCTF) 96
Directorate-General Joint Research Centre (DG JRC) 96
Directorate-General for Research and Innovation (DG RTD) 97
Directorate-General for Informatics (DG DIGIT) 97
Directorate-General for Communications Networks, Content and Technologies (DG CONNECT) 97
Directorate-General for Migration and Home Affairs (DG HOME) 98
Stakeholder Cybersecurity Certification Group (SCCG) 98
Horizontal Working Party on Cyber Issues (HWPCI) 98
ICT Advisory Committee of the EU Agencies (ICTAC) 99
European Union Institute for Security Studies (EUISS) 99
Intelligence Directorate of the European Union Military Staff (EUMS INT) 100
Inter-Service Group „Community Capacity in Crisis-Management" (ISG C3M) 100
Inter-Service Group „Countering Hybrid Threats" (ISG CHT) 100
Joint Cyber Unit (JCU) 101
Critical Infrastructure Protection Contact Group (CIP Contact Group) 101
NIS Cooperation Group 102
MeliCERTes 102
European Union Military Committee (EUMC) 103
Political and Security Committee, (PSC) 103
Council of the European Union (Council) 103
Reference Incident Classification Taxonomy Task Force (TF-CSIRT) 105
Senior Officials Group Information Systems Security (SOG-IS) 105
Permanent Structured Cooperation (PESCO) 105
Taxonomy Governance Group (TGG) 106
Emergency Response Coordination Centre (ERCC) 106
EU Intelligence Analysis Centre (INTCEN) 106

7. Explanation – Actors at NATO Level 108

Policy Overview 109
Allied Command Operations (ACO) 109
Allied Command Transformation (ACT) 110
Cyber Defence Committee (CDC) 110
Emerging Security Challenges Division (ESCD) 111
Joint Intelligence and Security Division (JISD) 111

NATO Communications and Information Agency (NCIA) 112
NATO Communication and Information System Group (NCISG) 112
NATO Computer Incident Response Capability (NCIRC) 113
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) 113
NATO Consultation, Control and Command Board (C3B) 114
NATO Cyber Defence Management Board (CDMB) 114
NATO Cyber Security Centre (NCSC) 115
NATO Cyberspace Operations Centre (CyOC) 115
NATO Military Committee (MC) 116
NATO School Oberammergau (NS-O) 116
NATO Security Committee (SC) 116
NCI Academy 117
North Atlantic Council (NAC) 117
Virtual Cyber Incident Support Capability (VCISC) 118

8. Explanation – Actors at Federal Level 119

Policy Overview 120

Agentur für Innovation in der Cybersicherheit (Agency for Innovation in Cybersecurity, Cyberagentur, own translation) 122
Auswärtiges Amt (Federal Foreign Office, AA, official translation) 122
Bundesbeauftragte:r für den Datenschutz und die Informationsfreiheit (Federal Commissioner for Data Protection and Freedom of Information, BfDI, official translation) 124
Bundeskanzleramt (Federal Chancellery, BKAmt, official translation) 124
Bundesnachrichtendienst (Federal Intelligence Service, BND, official translation) 125
Bundesministerium der Justiz (Federal Ministry of Justice, BMJ, official translation) 125
Bundesministerium der Verteidigung (Federal Ministry of Defence, BMVg, official translation) 125
Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (Federal Office of Bundeswehr Equipment, Information Technology, and In-Service Support, BAAINBw, official translation) 127
Bundesweite IT-Systemhaus GmbH (National IT Systems House GmbH, BWI, own translation) 127
Cyber Innovation Hub (Cyber Innovation Hub of the German Armed Forces, CIHBw, official translation) 128
Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr (Federal Office of Infrastructure, Environmental Protection and Services of the Bundeswehr, BAIUDBw, own translation) 128
Bundesakademie für Sicherheitspolitik (Federal Academy for Security Policy, BAKS, official translation) 128

Bundesamt für den Militärischen Abschirmdienst (Federal Office for Military Counter-Intelligence, BAMAD, official translation) 129
Cyber-Reserve (Military Cyber Reserve, own translation) 129
Organisationsbereich Cyber- und Informationsraum (Cyber and Information Domain Service, CIR, official translation) 130
Kommando Cyber- und Informationsraum (Bundeswehr Communication and Information Systems Command, KdoCIR, official translation) 130
Kommando Informationstechnik-Services der Bundeswehr (Bundeswehr Communication and Information Systems Services Centre, KdoIT-SBw, official translation) 131
Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber-und Informationsraum (Bundeswehr Centre for Software Expertise, ZDigBw, official translation) 132
Zentrum für Cyber-Sicherheit der Bundeswehr (Bundeswehr Cyber Security Center, ZCSBw, official translation) 132
Universitäten der Bundeswehr (Universities of the German Federal Armed Forces, UniBw, official translation) 132
Forschungsinstitut Cyber Defence (Cyber Defence Research Institute, CODE, own translation) 133
Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community, BMI, official translation) 133
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Federal Office of Civil Protection and Disaster Assistance, BBK, official translation) 134
Gemeinsames Kompetenzzentrum Bevölkerungsschutz von Bund und Ländern (Joint Competence Center for Civil Protection of the Federal Government and the Federal States, GeKoB, own translation) 135
Gemeinsames Melde- und Lagezentrum von Bund und Ländern (Joint Information and Situation Centre of the Federal Government and the Federal States, GMLZ, official translation) 136
Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, BSI, official translation) 136
Allianz für Cybersicherheit (Alliance for Cybersecurity, ACS, own translation) 139
Bundes Security Operations Center (Federal Security Operations Center, BSOC, own translation) 140
Computer Emergency Response Team der Bundesverwaltung (Computer Emergency Response Team for federal agencies, CERT-Bund, official translation) 140

Cyber-Sicherheitsnetzwerk (Cyber Security Network, CSN, own translation) 141
Nationaler Pakt Cybersicherheit (National Cybersecurity Pact, NPCS, own translation) 141
Nationales IT-Lagezentrum (National IT Situation Centre, LZ, own translation) 142
Nationales IT-Krisenreaktionszentrum (National IT Crisis Response Center, IT-KRZ, own translation) 142
Nationales Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung (National Coordination Centre for cybersecurity in industry, technology, and research, NCC-DE, official translation) 143
Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (Federal Agency for Public Safety Digital Radio, BDBOS, official translation) 143
Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution, BfV, official translation) 144
Bundeskriminalamt (Federal Criminal Police Office, BKA, official translation) 145
Bundespolizei (Federal Police, BPol, official translation) 146
Bündnis für Cybersicherheit (Coalition for Cyber Security, own translation) 147
Initiative Wirtschaftsschutz (Initiative for Economic Protection, own translation) 147
IT-Rat (IT Council, own translation) 148
Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Central Office for Information Technology in the Security Sector, ZITiS, official translation) 148
Bundesministerium für Arbeit und Soziales (German Ministry of Labour and Social Affairs, BMAS, official translation) 149
Bundesministerium für Bildung und Forschung (Federal Ministry of Education and Research, BMBF, official translation) 149
Bundesministerium für Digitales und Verkehr (Federal Ministry for Digital and Transport, BMDV, official translation) 150
Bundesamt für Seeschifffahrt und Hydrographie (Federal Maritime and Hydrographic Agency, BSH, official translation) 150
Bundesministerium für Finanzen (Federal Ministry of Finance, BMF, official translation) 151
Bundesanstalt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority, BaFin, official translation) 151
Informationstechnikzentrum Bund (Federal Information Technology Centre, ITZBund, official translation) 151

Zollkriminalamt (Customs Investigation Bureau, ZKA, official translation) 152
Bundesministerium für Gesundheit (Federal Ministry of Health, BMG, official translation) 153
Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (Federal Ministry for the Environment and Consumer Protection, BMUV, official translation) 153
Bundesministerium für Wirtschaft und Klimaschutz (Federal Ministry for Economic Affairs and Climate Action, BMWK, official translation) 154
Beirat für Standardisierung in der Informations- und Kommunikationstechnologie (Advisory Board for Standardization in Information and Communication Technology, BSIKT, own translation) 154
Bundeskartellamt (Federal Cartel Office, BKartA, official translation) 155
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways, BNetzA, official translation) 155
Initiative IT-Sicherheit in der Wirtschaft (Initiative IT Security in the Economy, own translation) 156
Transferstelle IT-Sicherheit im Mittelstand (Transfer Office "IT Security for Small and Medium-sized Enterprises", TISiM, own translation) 156
Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (Federal Ministry for Economic Cooperation and Development, BMZ, official translation) 156
Bundesverband der Verbraucherzentralen und Verbraucherverbände (Federation of German Consumer Organisations, vzbv, official translation) 157
Cyber Security Cluster Bonn e.V. 157
Deutsche Bundesbank (D BBk) 158
Deutsche Akkreditierungsstelle (German Accreditation Body, DAkkS, official translation) 158
Deutsche Gesellschaft für Internationale Zusammenarbeit (Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH, GIZ, official translation) 159
Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (German Commission for Electrical, Electronic & Information Technologies of DIN and VDE, DKE, official translation) 159
Deutsches Institut für Normung (German Institute for Standardization, DIN, official translation) 159
Deutschland sicher im Netz e.V. (Germany Secure on the Internet e.V., DsiN, own translation) 160
DIN/DKE Gemeinschaftsgremium "Cybersecurity" (DIN/DKE Joint Committee "Cybersecurity", own translation) 160

Deutsches Zentrum für Luft- und Raumfahrt (German Aerospace Center, DLR, official translation) 161
Forschungsrahmenprogramm zur IT-Sicherheit "Digital. Sicher. Souverän." (Research Framework Program on IT Security "Digital. Secure. Sovereign.", own translation) 161
Föderale IT-Kooperation (Federal IT Cooperation, FITKO, own translation) 162
gematik 162
German Competence Centre against Cyber Crime (G4C German Competence Centre against Cyber Crime e.V., G4C, official translation) 163
Innenministerkonferenz (Conference of Interior Ministers, IMK, official translation) 163
IT-Planungsrat (IT Planning Council, IT-PLR, official translation) 163
IT Security made in Germany (ITSMIG) 164
Kompetenz- und Forschungszentren für IT-Sicherheitsforschung (Competence and Research Centers for IT Security Research, own translation) 165
Nationaler CERT-Verbund (National CERT Network, own translation) 165
Nationaler Cyber-Sicherheitsrat (National Cyber Security Council, NCSR, official translation) 165
Nationales Cyber-Abwehrzentrum (National Cyber Defense Centre, Cyber-AZ, official translation) 166
Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen (Public-Private Partnership for Critical Infrastructure Protection, UP KRITIS, own translation) 166
Stiftung Wissenschaft und Politik (German Institute for International and Security Affairs, SWP, official translation) 167
Verwaltungs-CERT-Verbund (Administrative CERT-Group, VCV, own translation) 167

9. Explanation – Actors at Federal State Level 168
Policy Overview 169
9.1 Baden-Württemberg (BW) 172
Overview 173
Cybersicherheitsagentur Baden-Württemberg (Cybersecurity Agency Baden-Württemberg, CSBW, own translation) 175
IT-Rat Baden-Württemberg (IT Council Baden-Württemberg, own translation) 176
Sicherheitszentrum IT der Finanzverwaltung Baden-Württemberg (IT Security Center of the Financial Administration Baden-Württemberg, SITiF BW, own translation) 176
Zentralstelle für die Bekämpfung von Informations- und

Kommunikationskriminalität (Central Office for the Fight against Information and Communication Crime, own translation) 177
9.2 Bavaria (BY) 178
Overview 179
Cyberabwehr Bayern (Cyber Defence Bavaria, own translation) 181
Cyber-Allianz-Zentrum (Cyber-Alliance Centre, CAZ, own translation) 181
Kompetenzzentrum Cybercrime (Cybercrime Competency Center, own translation) 182
Landesamt für Sicherheit in der Informationstechnik Bayern (State Office for Information Security, LSI, own translation) 182
Zentralstelle Cybercrime Bayern (Central Office Cybercrime Bavaria, ZCB, own translation) 182
Zentrum Digitalisierung.Bayern (Center for Digitization Bavaria, ZD.B, own translation) 183
9.3 Berlin (BE) 184
Overview 185
Cyber Defense Center der Landesverwaltung Berlin (Cyber Defense Center of the Berlin State Administration, CDC-Lv, own translation) 186
Digitalagentur Berlin (Digital Agency Berlin, DAB, own translation) 187
Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin (Special Department for the Fight against Cybercrime of Berlin's Public Prosecutor's Office, own translation) 187
9.4 Brandenburg (BB) 188
Overview 189
Ausschuss der Ressort Information Officer (Committee of Departmental Information Officers, RIO-Ausschuss, own translation) 190
Cyber-Competence-Center (CCC) 191
IT-Rat Brandenburg (IT Council Brandenburg, own translation) 191
Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus (Special Public Prosecutor's Office to Combat Computer and Data Network Crime of Cottbus, own translation) 191
9.5 Bremen (HB) 192
Overview 193
9.6 Hamburg (HH) 195
Overview 196
9.7 Hesse (HE) 198
Overview 199
Hessisches Cyberabwehrausbildungszentrum Land/Kommunen (Hessian Cyber Defense Training Center Federal State/Municipalities, HECAAZ L/K, own translation) 200
Hessen Cyber Competence Center (Hessen3C) 201

Kommunales Dienstleistungszentrum Cybersicherheit (Municipal Cyber Security Service Center, KDLZ-CS, own translation) 201
Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (Central Office for Combating Internet and Computer Crime, ZIT, own translation) 202
9.8 Mecklenburg-Western Pomerania (MV) 203
Overview 204
Netzverweis.de 206
Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock (Special Prosecutor for Combatting Information and Communication Crimes of Rostock, own translation) 206
Zentrum für Digitalisierung Mecklenburg-Vorpommern, ZDMV (Center for Digitization Mecklenburg-Western Pomerania, own translation) 206
9.9 Lower Saxony (NI) 207
Overview 208
Cybersicherheitsbündnis (Cybersecurity Alliance, own translation) 210
Digitalagentur Niedersachsen (Digital Agency Lower Saxony, own translation) 210
9.10 North Rhine-Westphalia (NW) 211
Overview 212
Cybercrime-Kompetenzzentrum (Cybercrime Competency Center, own translation) 214
Cyberwehr (Cyber Defence [NW], own translation) 215
Interministerieller Ausschuss Cybersicherheit (Interministerial Cybersecurity Committee, IMA Cybersicherheit, own translation) 215
Kompetenzzentrum für Cybersicherheit in der Wirtschaft (Competence Center for Cybersecurity in the Economy, DIGITAL.SICHER.NRW, own translation) 215
Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen (Coordination Office for Cybersecurity North Rhine-Westphalia, own translation) 216
Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (Central and Contact Office Cybercrime North Rhine-Westphalia, ZAC NRW, own translation) 216
9.11 Rhineland-Palatinate (RP) 217
Overview 218
Landeszentralstelle Cybercrime (Central State Office for Cybercrime, LZC, own translation) 220
9.12 Saarland (SL) 221
Overview 222

Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken (Cybercrime Department of the Public Prosecutor's Office of Saarbrücken, own translation) 223
Netzwerkstelle Digitalisierung, DiNet (Digitization Network, own translation) 224
Initiative für Cybersicherheit, CYBR360 (Initiative für Cybersecurity, own translation) 224
9.13 Saxony (SN) 225
Overview 226
Arbeitsgruppe Informationssicherheit (Information Security Working Group, AG IS, own translation) 227
Cyber Crime Competence Center Sachsen (Cyber Crime Competence Center Saxony, SN4C, own translation) 228
Zentralstelle Cybercrime Sachsen (Central Office Cybercrime Saxony, ZCS, own translation) 228
9.14 Saxony-Anhalt (ST) 229
Overview 230
Cybercrime Competence Center (4C) 231
9.15 Schleswig-Holstein (SH) 232
Overview 233
IT-Verbund Schleswig-Holstein (IT Network Schleswig-Holstein, ITVSH, own translation) 234
9.16 Thuringia (TH) 235
Overview 236
9.17 Actors in multiple federal states 238
CERT Nord (CERT North, own translation) 238
Dataport 238
Sicherheitskooperation Cybercrime (Security Cooperation Cybercrime, own translation) 238

10. Explanation – Actors at Local Level 239
Policy Overview 240
Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister (Federal Working Group of Municipal IT Service Providers, Vitako, own translation) 240
IT-SiBe-Forum (Forum for Municipal IT Security Officers, own translation) 240
Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (Municipal Joint Office for Administrative Management, KGSt, own translation) 241
Kommunale Spitzenverbände (Central Municipal Associations, KSV, own translation) 241
Kommunalgremium des IT-Planungsrates (Municipal Committee of the IT Planning Council, own translation) 243

1. Background and Methodology

The first foundations of Germany's cybersecurity architecture were already laid in the late 1980s when a working group dealing with ICT security was established and the "Bundesamt für Sicherheit in der Informationstechnik" (Federal Office for Information Security, BSI, official translation) was founded subsequently in 1991.

Much has happened 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. In particular, following the publication of the first German Cybersecurity Strategy in 2011[1] – updated in 2016[2] and 2021[3] – German cybersecurity policy caught the public's attention.

Nevertheless, none of the three strategies contains a comprehensive overview of the increasingly complex architecture of German authorities' tasks and competencies in cyberspace, and their relevant international connections. For the first time in 2020, the "Bundesministerium des Innern und Heimat" (Federal Ministry of the Interior and Community, BMI, official translation) has presented a list of cybersecurity actors and initiatives from the state, civil society, academia, and industry as an online compendium[4] within the framework of the "Nationaler Pakt Cybersicherheit" (National Cyber Security Pact, NPCS, own translation) – albeit it has not been updated since.

A structured policy approach is indispensable for effectively and efficiently positioning Germany within the realm of cyberspace, especially when considering limited resources[5]. As part of Stiftung Neue Verantwortung's work on cybersecurity policy[6], we seek to make a respective contribution by continuously updating this publication since 2017.

This publication contains:

- A **visualization** of Germany's cybersecurity architecture, including its international connections (Chapter 2) and level-specific visualizations at the beginning of each chapter, which is also accessible in an interactive format under www.stiftung-nv.de/en/publication/germanys-cybersecurity-architecture,

1 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2011.
2 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.
3 Bundesministerium des Innern, für Bau und Heimat, Cybersicherheitsstrategie für Deutschland 2021.
4 Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland.
5 Julia Schuetze, Warum dem Staat IT-Sicherheitsexpert:innen fehlen.
6 Stiftung Neue Verantwortung, Internationale.

- a **list of abbreviations** of all abbreviations used within the visualization also includes a **list of attributed actor categories** (Chapter 3),
- a **tabular policy overview**[7] for each level at the beginning of each chapter, and
- an **alphabetical registry of actor profiles** sorted by level (Chapters 4–10) with explanations of the actors and their connections.

A country's cybersecurity architecture includes all actors – government agencies, platforms, organizations, etc. – that are part of the (inter)national ecosystem according to the national definition of cybersecurity.

In this publication, we only list the governmental part of the cybersecurity architecture, which means all governmental and directly related actors.[8]

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.

7 Policies in this context include, for example, relevant legislation and strategies at the federal, federal state, local and EU levels, or otherwise relevant documents at the international level, such as conventions or final reports. In particular cases, other forms of policy outputs may be assessed as a useful inclusion. The year indicated refers to the entry into force or the last amendment when multiple options are possible.

8 In doing so, this publication aims to portray respective levels as comprehensively as possible and as deemed useful for the field of cybersecurity policy. For an actor to be included within the international levels (EU, NATO, UN, and others), the identification of a connection with (an) actor(s) within the German levels (federal, federal state, and local) is ideally existent but does not constitute an exclusion criterion.

In addition to adjustments and updates on all levels, particularly the federal and federal state levels, this edition adds the following new actors at existing levels:

Abbreviation	Name	Level	Kategory
BMAS	Bundesministerium für Arbeit und soziales (Federal Miniytry of Labour and Social Affairs, official translation)	Federal Level	
DLR	Deutsches Zentrum für Luft- und Raumfahrt (German Aerospace Center, official translation)	Federal Level	
ESA	Europäische Weltraum-organisation (European Space Agency, official translation))	Other International Actors	
KdoIT-SBw	Kommando Informations-technik-Services der Bundeswehr (Bundeswehr Communication and Infor-mation Systems Command, official translation)	Federal Level	
VCISC	Virtual Cyber Incident Support Capability	NATO-Level	

As well as the following new Policies on existing levels:

Name	Ebene
Agenda 2025 of the European Space Agency	Other International Actors
Council Conclusions on the EU Policy on Cyber Defence	EU-Level
Hessisches Gesetz zum Schutz der elektronischen Verwaltung, Hessisches IT-Sicherheitsgesetz, HITSIG (Hessian Act on the Protection of Electronic Administration, Hessian IT Security Act, own translation)	Federal State Level
Madrid Summit Declaration	NATO-Level
Nationale Sicherheitsstrategie (National Security Strategy, official translation)	Federal Level
Verordnung über Sicherheit und Gesundheitsschutz bei der Verwendung von Arbeitsmitteln, Betriebssicherheitsverordnung, BetrSichV (Operational Safety Ordinance, official translation)	Federal Level
Vilnius Summit Communiqué	NATO-Level

Other legislative and judicial actors at all levels and 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 details. Do not hesitate to contact Frederic Dutke with suggestions for changes or additions. Corrections to the current version are published on the corresponding website as a "bug tracker."

This document will be periodically updated to account for the latest developments and any additional enhancements to Germany's cybersecurity architecture. The next update will be published in Spring 2024.

This publication is a translation based on the current 11th edition of the German versions. The earlier editions in German can be retrieved accordingly:

Edition	Date	Co-Author	Co-Author	Publication
1st edition	07/2018	Sven Herpig	Tabea Breternitz	Link
2nd edition	04/2019	Sven Herpig	Clara Bredenbrock	Link
3rd edition	11/2019	Sven Herpig	Kira Messing	Link
4th edition	03/2020	Sven Herpig	Rebecca Beigel	Link
5th edition	10/2020	Sven Herpig	Rebecca Beigel	Link
6th edition	04/2021	Sven Herpig	Christina Rupp	German / English
7th edition	10/2021	Sven Herpig	Christina Rupp	German / English Supported by the Data Science Unit: Anna Semenova & Pegah Maham
8th edition	04/2022	Sven Herpig	Christina Rupp	German Supported by the Data Science Unit: Anna Semenova & Pegah Maham
9th edition	09/2022	Sven Herpig	Christina Rupp	German / English Supported by the Data Science Unit: Anna Semenova & Pegah Maham
10th edition	05/2023	Sven Herpig	Christina Rupp Rebecca Beigel Frederic Dutke	German Supported by the Data Science Unit: Anna Semenova & Pegah Maham
11th edition	10/2023	Sven Herpig	Frederic Dutke	Current version

CYBERSECURITY ARCHITECTURE OF GERMANY

UN
EU
FEDERAL LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
INT. ACTORS
NATO

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

CoE OSCE ESA
Interpol IETF ICANN ISO IEC
FIRST TI JTC 1

EC
Council EUCO
NAC
DG JRC DG RTD DG HOME DG DIGIT DG CONNECT ENISA Europol Eurojust PSC EEAS EUMC
CDC SC CDMB C3B MC
CEN CENELEC ETSI ECCC OLAF JCU EDPS CERT-EU ENISA AG EC3 eu-LISA HWPCI INTCEN EDA
JISD ESCD NCIA ACO ACT
CSCG EA ECSO ECB ISG CHT NIS Cooperation Group EGC group EMPACT EUCTF EJN ERCC EU Hybrid Fusion Cell EUMS INT
NCISG NCI Academy NCIRC NCSC CyOC NS-O CCDCOE
ECCG Stakeholder Cybersecurity Certification Group SOG-IS ECRB ISG C3M CSIRTs Network TF-CSIRT ECTEG CEPOL EJCN EU CyberNet ESDC PESCO
Hybrid CoE VCISC
CIP Contact Group ICTAC MeliCERTes TGG EJTN CyCLONe EUISS CMPD CIDCC

NCSR IT Council
BMVg BKAmt BMAS BMI AA BMF BMDV BMWK BMBF BMG BMJ BMZ BMUV
BAAINBw CIR BAMAD BND BfV BKA ZITiS BaFin BNetzA BKartA Forschungsrahmenprogramm zur IT-Sicherheit „Digital. Sicher. Souverän." gematik vzbv GIZ
BAIUDBw KdoCIR BAKS BDBOS BBK BPol ZKA ITZBund BSH D BBk Kompetenz- und Forschungszentren für IT-Sicherheit BfDI SWP
BWI ZDigBw UniBw Cyberagentur GMLZ NPCS ACS CSN Bündnis für Cybersicherheit UP KRITIS DsiN DAkkS DKE DIN
CIHBw ZCSBw CODE G4C GeKoB Initiative IT-Sicherheit in der Wirtschaft Initiative Wirtschaftsschutz ITSMIG TISiM BSIKT DIN/DKE Gemeinschaftsgremium „Cybersecurity"
Cyber Security Cluster Bonn KdoIT-SBw Cyber-Reserve DLR BSI
IT-KRZ LZ CERT-Bund BSOC NCC-DE
Cyber-AZ

Dataport CERT Nord FITKO IMK IT-PLR VCV Nationaler CERT-Verbund 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 MIBD MV MI IM NRW MASTD MWIDE SL SK [SN] MID ST StK SH TFM
CSBW StMFH CIO [BE] CIO [BB] CIO [HB] CIO [HH] Hessisches Ministerium für Digitale Strategie und Entwicklung CIO [MV] CIO [NI] MWIKE NRW CIO [RP] MFW SL CIO [SN] CIO [ST] CIO [SH] CIO [TH]
CIO [BW] StMI CISO [BE] CISO [BB] CISO [HB] CISO [HH] Hessen3C CISO [MV] CISO [NI] MHKBD NRW 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] CIO [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 CISO [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 LfV [NW] 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] IT.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] CERT NRW LfDI [RP] LfDI [SL] SächsDSDG TLfDI
LfDI [BW] Bayern-CERT BlnBDI RIO-Ausschuss ZAC [HE] Netzverweis.de Cybersicherheitsbündnis ZAC [NW] LZC Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken AG IS
IT-Rat Baden-Württemberg ZAC [BY] DAB CCC HBDI Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock Digitalagentur Niedersachsen LDI [NW] DiNet SN4C
SITiF BW BayLfD Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin IT-Rat Brandenburg HECAAZ L/K ZDMV Cybercrime-Kompetenzzentrum CYBR360 ZCS
Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität Cyberabwehr Bayern Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datenerkriminalität Cottbus KDLZ-CS Cyberwehr [NW]
CAZ ZIT IMA Cybersicherheit
ZCB DIGITAL.SICHER.NRW
Kompetenzzentrum Cybercrime Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen
ZD.B ZAC NRW

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

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

Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel

Version: October 2023

3. Abbreviations and Actor Categorization

In the previous edition, the list of abbreviations has been expanded by a column listing the respective actor category. In the framework of the actor categorization, all actors have been classified according to their responsibilities, fields of activity, and functions. If applicable, actors could also be assigned to two or multiple categories. The basis for categorizing an actor constitutes the corresponding actor profile provided in this publication. In addition to describing the actors and explaining their connections, the categorization offers an in-depth and transparent insight into and an overview of the German cybersecurity architecture.

Besides this tabular overview, the category(ies) attributed to the actors are also depicted left to the individual actor profiles with their corresponding icons.

Actors could be assigned one or more of the following six categories:

Education and training
Actors that organize or provide education and training offerings, formats, or platforms for various target groups. This knowledge exchange and transfer can include training, courses, or further education in the areas of cybersecurity or cyber defense, among other things.

Research and research funding
Actors that are actively involved in research on IT and cybersecurity-related topics, for example, as a research institute, or who support respective research externally through appropriate funding, including financing competence centers or the establishment/management of substantially relevant research programs.

Information sharing and collaboration platform
Actors that are dedicated to information sharing and/or networking, and/or improving relationships, and fostering cooperation to strengthen IT and cybersecurity. Corresponding forums and networks can be established with a thematic focus and across topics with varying degrees of institutionalization.

Standardization and certification
Actors that are working on the development and agreement of norms, standards, and certifications for ICT-based applications, systems, and networks that include IT and cybersecurity-related provisions.

Operational IT and cybersecurity
Actors that are operationally implementing measures that are intended to lead to greater IT and cybersecurity, including prevention and detection of and response to incidents, combating cybercrime, or imposing fines for non-compliance.

Policy and strategy
Actors that are responsible for policy-making as well as setting policy goals in the area of IT and cybersecurity and who also often have responsibility for drafting relevant legislation, policies, and/or strategies. The decisions and outputs of these actors often set the course for many other actors within the cybersecurity architecture. In addition, this category includes actors who provide inputs into policy processes, such as consultation.

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
4C	Cybercrime Competence Center	Operational IT and cybersecurity
	A	
AA	Auswärtiges Amt (Federal Foreign Office, official translation)	Policy and strategy
ACO	Allied Command Operations	Operational IT and cybersecurity
ACS	Allianz für Cybersicherheit (Alliance for Cybersecurity, own translation)	Information sharing and collaboration platform
ACT	Allied Command Transformation	Education and training Operational IT and cybersecurity
AG IS	Arbeitsgruppe Informationssicherheit (Information Security Working Group, own translation)	Policy and strategy
	B	
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (Federal Office of Bundeswehr Equipment, Information Technology, and In-Service Support, official translation)	Operational IT and cybersecurity
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority, official translation)	Operational IT and cybersecurity
BAIUDBw	Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr (Federal Office of Infrastructure, Environmental Protection and Services of the Bundeswehr, own translation)	Operational IT and cybersecurity
BAKS	Bundesakademie für Sicherheitspolitik (Federal Academy for Security Policy, official translation)	Education and training

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
BAMAD	Bundesamt für den Militärischen Abschirmdienst (Federal Office for Military Counter-Intelligence, official translation)	Operational IT and cybersecurity
Bayern-CERT	Computer Emergency Response Team Bavaria	Operational IT and cybersecurity
BayLfD	Bayerische:r Landesbe-auftragte:r für den Datenschutz (Bavarian State Commissioner for Data Protection, own translation)	Operational IT and cybersecurity
BB	Land Brandenburg	N/A
BBK	Bundesamt für Bevölkerungs-schutz und Katastrophenhilfe (Federal Office of Civil Protection and Disaster Assistance, official translation)	Operational IT and cybersecurity
BDBOS	Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (Federal Agency for Public Safety Digital Radio, official translation)	Operational IT and cybersecurity
BE	Land Berlin	N/A
Berlin-CERT	Computer Emergency Response Team Berlin	Operational IT and cybersecurity
BfDI	Bundesbeauftragte:r für den Datenschutz und die Informationsfreiheit (Federal Commissioner for Data Protection and Freedom of Information, official translation)	Operational IT and cybersecurity
BfV	Bundesamt für Verfassungs-schutz (Federal Office for the Protection of the Constitution, official translation)	Operational IT and cybersecurity
BITBW	Landesoberbehörde IT Baden-Württemberg (State Authority IT Baden-Württemberg, own translation)	Operational IT and cybersecurity
BKA	Bundeskriminalamt (Federal Criminal Police Office, official translation)	Operational IT and cybersecurity

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
BKAmt	Bundeskanzleramt (Federal Chancellery, official translation)	Policy and strategy
BKartA	Bundeskartellamt (Federal Cartel Office, official translation)	Policy and strategy
BlnBDI	Berliner Beauftragte:r für Datenschutz und Informationsfreiheit (State Commissioner for Data Protection and Freedom of Information Berlin, own translation)	Operational IT and cybersecurity
BMAS	Bundesministerium für Arbeit und Soziales	Policy and strategy
BMBF	Bundesministerium für Bildung und Forschung (Federal Ministry of Education and Research, official translation)	Policy and strategy
BMDV	Bundesministerium für Digitales und Verkehr (Federal Ministry for Digital and Transport, official translation)	Policy and strategy
BMF	Bundesministerium für Finanzen (Federal Ministry of Finance, official translation)	Policy and strategy
BMG	Bundesministerium für Gesundheit (Federal Ministry of Health, official translation)	Policy and strategy
BMI	Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community, official translation)	Policy and strategy
BMJ	Bundesministerium der Justiz (Federal Ministry of Justice, official translation)	Policy and strategy
BMUV	Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (Federal Ministry for the Environment and Consumer Protection, official translation)	Policy and strategy
BMVg	Bundesministerium der Verteidigung (Federal Ministry of Defence, official translation)	Policy and strategy

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
BMWK	Bundesministerium für Wirtschaft und Klimaschutz (Federal Ministry for Economic Affairs and Climate Action, official translation)	Policy and strategy
BMZ	Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (Federal Ministry for Economic Cooperation and Development, official translation)	Policy and strategy
BND	Bundesnachrichtendienst (Federal Intelligence Service, official translation)	Operational IT and cybersecurity
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways, official translation)	Operational IT and cybersecurity
BPol	Bundespolizei (Federal Police, official translation)	Operational IT and cybersecurity
BSH	Bundesamt für Seeschifffahrt und Hydrographie (Federal Maritime and Hydrographic Agency, official translation)	Operational IT and cybersecurity
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, official translation)	Research and research funding Information sharing and collaboration platform Standardization and certification Operational IT and cybersecurity
BSIKT	Beirat für Standardisierung in der Informations- und Kommunikationstechnologie (Advisory Board for Standardization in Information and Communication Technology, own translation)	Standardization and certification
BSOC	Bundes Security Operations Center (Federal Security Operations Center, own translation)	Operational IT and cybersecurity

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
Bündnis für Cybersicherheit	Bündnis für Cybersicherheit (Coalition for Cyber Security, own translation)	Information sharing and collaboration platform
BWI	Bundesweite IT-Systemhaus GmbH (National IT Systems House GmbH, own translation)	Operational IT and cybersecurity
	C	
C3B	NATO Consultation, Control and Command Board	Policy and strategy
CAZ	Cyber-Allianz-Zentrum (Cyber-Alliance Centre, own translation)	Operational IT and cybersecurity
CCC	Cyber-Competence-Center	Operational IT and cybersecurity
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence	Research and research funding Education and training
CDC	Cyber Defence Committee	Policy and strategy
CDC-Lv	Cyber Defense Center der Landesverwaltung Berlin (Cyber Defense Center of the Berlin State Administration, own translation)	Operational IT and cybersecurity
CDMB	NATO Cyber Defence Management Board	Policy and strategy
CEN	European Committee for Standardization	Standardization and certification
CENELEC	European Committee for Electrotechnical Standardization	Standardization and certification
CEPOL	European Union Agency for Law Enforcement Training	Education and training
CERT [HE]	Computer Emergency Response Team Hesse	Operational IT and cybersecurity
CERT BWL	Computer Emergency Response Team Baden-Württemberg	Operational IT and cybersecurity
CERT M-V	Computer Emergency Response Team Mecklenburg-Western Pomerania	Operational IT and cybersecurity

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
CERT Nord	CERT Nord (CERT North, own translation)	Operational IT and cybersecurity
CERT NRW	Computer Emergency Response Team North Rhine-Westphalia	Operational IT and cybersecurity
CERT-Brandenburg	Computer Emergency Response Team Brandenburg	Operational IT and cybersecurity
CERT-Bund	Computer Emergency Response Team der Bundesverwaltung (Computer Emergency Response Team for federal agencies, official translation)	Operational IT and cybersecurity
CERT-EU	Computer Emergency Response Team of the European Commissio	Operational IT and cybersecurity
CERT-rlp	Computer Emergency Response Team Rhineland-Palatinate	Operational IT and cybersecurity
CIDCC	Cyber and Information Domain Coordination Centre	Operational IT and cybersecurity
CIHBw	Cyber Innovation Hub (Cyber Innovation Hub of the German Armed Forces, official translation)	Research and research funding
CIO [Federal State]	State Commissioner for Information Technology [of Federal State]	Policy and strategy
CIR	Organisationsbereich Cyber- und Informationsraum (Cyber and Information Domain Service, official translation)	Operational IT and cybersecurity
CISO [Federal State]	Chief Information Security Officer of the State Administration [of Federal State]	Operational IT and cybersecurity
CMPD	Crisis Management and Planning Directorate	Policy and strategy
CODE	Forschungsinstitut Cyber Defence (Cyber Defence Research Institute, own translation)	Research and research funding
CoE	Council of Europe	Policy and strategy

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
Council	Council of the European Union	Policy and strategy
CSBW	Cybersicherheitsagentur Baden-Württemberg (Cybersecurity Agency Baden-Württemberg, own translation)	Operational IT and cybersecurity
CSCG	CEN/CENELEC Cyber Security Coordination Group	Standardization and certification
EKk	Computer Security Incident Response Teams Network	Operational IT and cybersecurity Information sharing and collaboration platform
CSN	Cyber-Sicherheitsnetzwerk (Cyber Security Network, own translation)	Information sharing and collaboration platform
Cyber Security Cluster Bonn	Cyber Security Cluster Bonn e.V.	Information sharing and collaboration platform
Cyberabwehr Bayern	Cyberabwehr Bayern (Cyber Defence Bavaria, own translation)	Information sharing and collaboration platform Operational IT and cybersecurity
Cyberagentur	Agentur für Innovation in der Cybersicherheit (Agency for Innovation in Cybersecurity, own translation)	Research and research funding
Cyber-AZ	Nationales Cyber-Abwehrzentrum (National Cyber Defense Centre, official translation)	Information sharing and collaboration platform
Cybercrime-Kompetenzzentrum	Cybercrime-Kompetenzzentrum (Cybercrime Competency Center, own translation)	Operational IT and cybersecurity
Cyber-Reserve	Cyber-Reserve (Military Cyber Reserve, own translation)	Operational IT and cybersecurity
Cybersicherheitsbündnis	Cybersicherheitsbündnis (Cybersecurity Alliance, own translation)	Information sharing and collaboration platform
NCSR	Nationaler Cyber-Sicherheitsrat (National Cyber Security Council, official translation)	Policy and strategy

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
Cyberwehr [Federal State]	Cyberwehr (Cyber Defence [Federal State], own translation)	Operational IT and cybersecurity
CyCLONe	Cyber Crisis Liaison Organisation Network	Information sharing and collaboration platform Operational IT and cybersecurity
CyOC	NATO Cyberspace Operations Centre	Operational IT and cybersecurity
CYR360	Initiative für Cybersicherheit (Cybersecurity initiative, own translation)	Information sharing and collaboration platform Operational IT and cybersecurity Education and Training
	D	
D BBk*	Deutsche Bundesbank (German Central Bank, official translation)	Operational IT and cybersecurity
DAB	Digitalagentur Berlin (Digital Agency Berlin, own translation)	Information sharing and collaboration platform
DAkkS	Deutsche Akkreditierungsstelle (German Accreditation Body, official translation)	Standardization and certification
Dataport	Dataport	Operational IT and cybersecurity
Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken	Dezernat Cybercrime der Staatsanwaltschaft Saarbrücken (Cybercrime Department of the Public Prosecutor's Office of Saarbrücken, own translation)	Operational IT and cybersecurity
DG CONNECT	Directorate-General for Communications Networks, Content and Technologies	Policy and strategy
DG DIGIT	Directorate-General for Informatics	Policy and strategy
DG HOME	Directorate-General for Migration and Home Affairs	Policy and strategy
DG JRC	Directorate-General Joint Research Centre	Research and research funding Policy and strategy
DG RTD	DirectorateGeneral for Research and Innovation	Policy and strategy

* Due to the identical abbreviation with the Federal Office for Civil Protection and Disaster Assistance (BBK), the official translation of the Deutsche Bundesbank (BBk) is slightly adjusted to "D BBk" when used in the context of this publication and the corresponding visualization.

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
DIGITAL.SICHER.NRW	Kompetenzzentrum für Cybersicherheit in der Wirtschaft (Competence Center for Cybersecurity in the Economy, own translation)	Information sharing and collaboration platform
Digitalagentur Niedersachsen	Digitalagentur Niedersachsen (Digital Agency Lower Saxony, own translation)	Information sharing and collaboration platform
DIN	Deutsches Institut für Normung (German Institute for Standardization, official translation)	Standardization and certification
DIN/DKE Gemeinschaftsgremium "Cybersecurity"	DIN/DKE Gemeinschaftsgremium "Cybersecurity" (DIN/DKE Joint Committee "Cybersecurity", own translation)	Standardization and certification
DiNet	Netzwerkstelle Digitalisierung (Digitization Network, own translation)	Information sharing and collaboration platform
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (German Commission for Electrical, Electronic & Information Technologies of DIN and VDE, official translation)	Standardization and certification
DLR	Deutsches Zentrum für Luft- und Raumfahrt (German Aerospace Center, official translation)	Information sharing and collaboration platform Research and research funding
DsiN	Deutschland sicher im Netz e.V. (Germany Secure on the Internet e.V., own translation)	Information sharing and collaboration platform
DTN	United Nations Digital and Technology Network	Information sharing and collaboration platform
DVZ M-V	DVZ Datenverarbeitungs-zentrum Mecklenburg-Vorpommern (Service Provider for the State Administration of Mecklenburg-Western Pomerania, official translation)	Operational IT and cybersecurity

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
	E	
EA	European co-operation for Accreditation	Standardization and certification
EC	European Commission	Policy and strategy
EC3	European Cybercrime Center	Operational IT and cybersecurity
ECB	European Central Bank	Operational IT and cybersecurity
ECCC	European Cybersecurity Industrial, Technology and Research Competence Centre	Research and research funding Information sharing and collaboration platform
ECCG	European Cybersecurity Certification Group	Standardization and certification
ECOSOC	United Nations Economic and Social Council	Policy and strategy
ECRB	Euro Cyber Resilience Board for pan-European Financial Infrastructures	Information sharing and collaboration platform
ECSO	European Cyber Security Organisation	Information sharing and collaboration platform
ECTEG	European Cybercrime Training and Education Group	Education and training
EDA	European Defence Agency	Research and research funding Policy and strategy
EDPS	European Data Protection Supervisor	Operational IT and cybersecurity
EEAS	European External Action Service	Policy and strategy
EGC group	European Government CERTs group	Information sharing and collaboration platform
EJCN	European Judicial Cybercrime Network	Information sharing and collaboration platform
EJN	European Judicial Network	Education and training Information sharing and collaboration platform

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
EJTN	European Judicial Training Network	Education and training
EMPACT	European Multidisciplinary Platform Against Criminal Threats	Information sharing and collaboration platform Operational IT and cybersecurity
ENISA	European Union Agency for Cybersecurity	Information sharing and collaboration platform Standardization and certification Policy and strategy
ENISA AG	ENISA Advisory Group	Information sharing and collaboration platform
ERCC	Emergency Response Coordination Centre	Operational IT and cybersecurity
ESA	European Space Agency	Operational IT and cybersecurity Research and research funding
ESCD	Emerging Security Challenges Division	Policy and strategy
ESDC	European Security and Defence College	Education and training
ETSI	European Telecommunications Standards Institute	Standardization and certification
EU CyberNet	EU Cyber Capacity Building Network	Education and training Information sharing and collaboration platform
EU Hybrid Fusion Cell	EU Hybrid Fusion Cell	Information sharing and collaboration platform
EUCO	European Council	Policy and strategy
EUCTF	European Union Cybercrime Task Force	Information sharing and collaboration platform
EUISS	European Union Institute for Security Studies	Research and research funding Policy and strategy
eu-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice	Operational IT and cybersecurity

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
EUMC	European Union Military Committee	Policy and strategy
EUMS INT	Intelligence Directorate of the European Union Military Staff	Operational IT and cybersecurity
Eurojust	European Union Agency for Criminal Justice Cooperation	Operational IT and cybersecurity
Europol	European Union Agency for Law Enforcement Cooperation	Operational IT and cybersecurity
	F	
FIRST	Forum of Incident Response and Security Teams	Information sharing and collaboration platform
FITKO	Föderale IT-Kooperation (Federal IT Cooperation, own translation)	Information sharing and collaboration platform Policy and strategy
Forschungsrahmenprogramm zur IT-Sicherheit "Digital. Sicher. Souverän."	Forschungsrahmenprogramm zur IT-Sicherheit "Digital. Sicher. Souverän." (Research Framework Program on IT Security "Digital. Secure. Sovereign.", own translation)	Research and research funding
	G	
G4C	German Competence Centre against Cyber Crime (G4C German Competence Centre against Cyber Crime e.V., official translation)	Information sharing and collaboration platform
GeKoB	Gemeinsames Kompetenz-zentrum Bevölkerungsschutz von Bund und Ländern (Joint Competence Center for Civil Protection of the Federal Government and the Federal States, own translation)	Information sharing and collaboration platform
gematik	gematik	Operational IT and cybersecurity
GGE	Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security	Policy and strategy

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit (Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH, official translation)	Education and training
GMLZ	Gemeinsames Melde- und Lagezentrum von Bund und Ländern (Joint Information and Situation Centre of the Federal Government and the Federal States, official translation)	Operational IT and cybersecurity
	H	
HB	Free Hanseatic City of Bremen	N/A
HBDI	Hessische:r Beauftragte:r für Datenschutz und Informations-freiheit (Hessian Commissioner for Data Protection and Freedom of Information, own translation)	Operational IT and cybersecurity
HE	State of Hesse	N/A
HECAAZ L/K	Hessisches Cyberabwehraus-bildungszentrum Land/Kom-munen (Hessian Cyber Defense Training Center Federal State/ Municipalities, own translation)	Education and training
Hessen3C	Hessen Cyber Competence Center	Operational IT and cybersecurity
Hessisches Ministerium für Digitale Strategie und Entwicklung	Hessisches Ministerium für Digitale Strategie und Entwicklung (State Ministry for Digital Strategy and Development, own translation)	Policy and strategy
HH	Free and Hanseatic City of Hamburg	N/A
HmbBfDI	Hamburgische:r Beauftragte:r für Datenschutz und Infor-mationsfreiheit der Freien und Hansestadt Hamburg (State Commissioner for Data Protection and Freedom of Information of the Free and Hanseatic City of Hamburg, own translation)	Operational IT and cybersecurity

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
HMdIS	Hessisches Ministerium des Innern und für Sport (State Ministry of the Interior and Sports, own translation)	Policy and strategy
HWPCI	Horizontal Working Party on Cyber Issues	Policy and strategy
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats	Research and research funding Information sharing and collaboration platform
HZD	Hessische Zentrale für Datenverarbeitung (Hessian Central Office for Data Processing, own translation)	Operational IT and cybersecurity
	I	
ICANN	Internet Corporation for Assigned Names and Numbers	Standardization and certification
ICTAC	ICT Advisory Committee of the EU Agencies	Information sharing and collaboration platform
IEC	International Electrotechnical Commission	Standardization and certification
IETF	Internet Engineering Task Force	Standardization and certification
IGF	Internet Governance Forum	Policy and strategy Information sharing and collaboration platform
IM BW	Ministerium für Inneres, Digitalisierung und Kommunen (Ministry of the Interior, Digitalization and Municpalities, own translation)	Policy and strategy
IM NRW	Ministerium des Innern (Ministry of the Interior, official translation)	Policy and strategy
IMA Cybersicherheit	Interministerieller Ausschuss Cybersicherheit (Interministerial Cybersecurity Committee, own translation)	Policy and strategy

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
IMK	Innenministerkonferenz (Conference of Interior Ministers, official translation)	Policy and strategy
Initiative IT-Sicherheit in der Wirtschaft	Initiative IT-Sicherheit in der Wirtschaft (Initiative IT Security in the Economy, own translation)	Information sharing and collaboration platform
Initiative Wirtschaftsschutz	Initiative Wirtschaftsschutz (Initiative for Economic Protection, own translation)	Information sharing and collaboration platform
INTCEN	EU Intelligence Analysis Centre	Operational IT and cybersecurity
Interpol	International Criminal Police Organization	Operational IT and cybersecurity
ISG C3M	Inter-Service Group "Community Capacity in Crisis-Management"	Information sharing and collaboration platform
ISG CHT	Inter-Service Group "Countering Hybrid Threats"	Information sharing and collaboration platform
ISO	International Organization for Standardization	Standardization and certification
IT Council	IT-Rat (IT Council, own translation)	Policy and strategy
IT.N	IT.Niedersachsen (IT Lower Saxony, own translation)	Operational IT and cybersecurity
IT.NRW	Landesbetrieb Information und Technik Nordrhein-Westfalen (State Office Information and Technology North Rhine-Westphalia, own translation)	Operational IT and cybersecurity
IT-DLZ [BY]	IT-Dienstleistungszentrum des Freistaats Bayern (IT Service Center of the Free State of Bavaria, own translation)	Operational IT and cybersecurity
IT-DLZ [SL]	Landesamt für IT-Dienst-leistungen (State Office for IT Services, own translation)	Operational IT and cybersecurity
ITDZ Berlin	IT-Dienstleistungszentrum Berlin (IT Service Center Berlin, own translation)	Operational IT and cybersecurity

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
IT-KRZ	Nationales IT-Krisen-reaktionszentrum (National IT Crisis Response Center, own translation)	Operational IT and cybersecurity
IT-PLR	IT-Planungsrat (IT Planning Council, official translation)	Policy and strategy
IT-Rat Baden-Württemberg	IT-Rat Baden-Württemberg (IT Council Baden-Württemberg, own translation)	Policy and strategy
IT-Rat Brandenburg	IT-Rat Brandenburg (IT Council Brandenburg, own translation)	Policy and strategy
IT-SiBe-Forum	IT-SiBe-Forum (Forum for Municipal IT Security Officers, own translation)	Information sharing and collaboration platform
ITSMIG	IT Security made in Germany	Information sharing and collaboration platform
ITU	International Telecommunication Union	Policy and strategy Standardization and certification
ITVSH	IT-Verbund Schleswig-Holstein (IT Network Schleswig-Holstein, own translation)	Information sharing and collaboration platform
ITZBund	Informationstechnikzentrum Bund (Federal Information Technology Centre, official translation)	Operational IT and cybersecurity
	J	
JCU	Joint Cyber Unit	Information sharing and collaboration platform Operational IT and cybersecurity
JISD	Joint Intelligence and Security Division	Operational IT and cybersecurity
JTC 1	ISO and IEC Joint Technical Committee	Standardization and certification

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
	K	
KDLZ-CS	Kommunales Dienstleistungs-zentrum Cybersicherheit (Municipal Cyber Security Service Center, own translation)	Operational IT and cybersecurity
KdoCIR	Kommando Cyber- und Informationsraum (Cyber and Information Domain Commando, own translation)	Operational IT and cybersecurity
KdoITBw	Kommando Informations-technik (Communication and Information Sytems Command, official translation)	Operational IT and cybersecurity
KdoStratAufkl	Kommando Strategische Aufklärung (Strategic Reconnaissance Command, official translation)	Operational IT and cybersecurity
KGSt	Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (Municipal Joint Office for Administrative Management, own translation)	Information sharing and collaboration platform
Kommunalgremium IT-PLR	Kommunalgremium des IT-Planungsrates (Municipal Committee of the IT Planning Council, own translation)	Policy and strategy
Kompetenz- und Forschungszentren für IT-Sicherheit	Kompetenz- und Forschungszentren für IT-Sicherheitsforschung (Competence and Research Centers for IT Security Research, own translation)	Research and research funding
Kompetenzzentrum Cybercrime	Kompetenzzentrum Cybercrime (Cybercrime Competency Center, own translation)	Operational IT and cybersecurity
Kompetenzzentrum für IT-Sicherheit für Luft- und Raumfahrt	Kompetenzzentrum für IT-Sicherheit für Luft- und Raumfahrt (Competence Center for IT Security for Aviation and Aerospace, own translation)	Operational IT and cybersecurity

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen	Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen (Coordination Office for Cybersecurity North Rhine-Westphalia, own translation)	Information sharing and collaboration platform
KSV	Kommunale Spitzenverbände (Central Municipal Associations, own translation)	Policy and strategy
	L	
LDA	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, own translation)	Operational IT and cybersecurity
LDI [NW]	Landesbeauftragte:r für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (State Commissioner for Data Protection and Freedom of Information North Rhine-Westphalia, own translation)	Operational IT and cybersecurity
LDI [RP]	Landesbetrieb Daten und Information (State Office Data and Information, own translation)	Operational IT and cybersecurity
LfD [Federal State]	Landesbeauftragte:r für den Datenschutz [Bundesland] (State Commissioner for Data Protection [Federal State], own translation)	Operational IT and cybersecurity
LfDI [Federal State]	Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit [Bundesland] (State Commissioner for Data Protection and Freedom of Information [Federal State], own translation)	Operational IT and cybersecurity
LfV [Federal State]]	State Authority for the Protection of the Constitution [Federal State]	Operational IT and cybersecurity
LSI	Landesamt für Sicherheit in der Informationstechnik Bayern (State Office for Information Security, own translation)	Operational IT and cybersecurity

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
LZ	Nationales IT-Lagezentrum (National IT Situation Centre, own translation)	Operational IT and cybersecurity
LZC	Landeszentralstelle Cybercrime (Central State Office for Cybercrime, own translation)	Operational IT and cybersecurity
	M	
MASTD	Ministerium für Arbeit, Soziales, Transformation und Digitalisierung (Ministry of Labor, Social Affairs, Transformation and Digitalization, own translation)	Policy and strategy
MC	NATO Military Committee	Policy and strategy
MeliCERTes	MeliCERTes	Information sharing and collaboration platform
MFW SL	Ministerium der Finanzen und für Wissenschaft (Ministry of Finance and Science, own translation)	Policy and strategy
MI	Niedersächsisches Ministerium für Inneres und Sport (Ministry of the Interior and Sport of Lower Saxony, own translation)	Policy and strategy
MIBD MV	Ministerium für Inneres, Bau und Digitalisierung (Ministry of the Interior, Building and Digitalisation of Mecklenburg-Western Pomerania, official translation)	Policy and strategy
MID ST	Ministerium für Infrastruktur und Digitales Sachsen-Anhalt (Ministry of Infrastructure and Digital Affairs, own translation)	Policy and strategy
MIK	Ministerium des Innern und für Kommunales (Brandenburg Ministry of the Interior and Municipal Affairs, official translation)	Policy and strategy
MV	State Mecklenburg-Western Pomerania	N/A

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
MWIDE SL	Ministerium für Wirtschaft, Arbeit, Energie und Verkehr (Ministry of Economy, Labor, Energy and Transport, own translation)	Policy and strategy
MWIKE NRW	Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie (Ministry of Economic Affairs, Industry, Climate Action and Energy, official translation)	Policy and strategy
	N	
NAC	North Atlantic Council	Policy and strategy
Nationaler CERT-Verbund	Nationaler CERT-Verbund (National CERT Network, own translation)	Information sharing and collaboration platform
N-CERT	Computer Emergency Response Team Lower Saxony	Operational IT and cybersecurity
NCC-DE	Nationales Koordinierungs-zentrum für Cybersicherheit in Industrie, Technologie und Forschung (National Coordination Centre for cybersecurity in industry, technology, and research, official translation)	Research and research funding
NCI Academy	NCI Academy	Education and training
NCIA	NATO Communications and Information Agency	Operational IT and cybersecurity
NCIRC	NATO Computer Incident Response Capability	Operational IT and cybersecurity
NCISG	NATO Communication and Information Systems Group	Operational IT and cybersecurity
NCSC	NATO Cyber Security Centre	Operational IT and cybersecurity
Netzverweis.de	Netzverweis.de	Operational IT and cybersecurity
NI	State Lower Saxony	N/A

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
NIS Cooperation Group	NIS Cooperation Group	Information sharing and collaboration platform
NPCS	Nationaler Pakt Cybersicherheit (National Cybersecurity Pact, NPCS, own translation)	Information sharing and collaboration platform
NS-O	NATO School Oberammergau	Education and training
NW	State North Rhine-Westphalia	N/A
	O	
OEWG	Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security	Policy and strategy
OLAF	European Anti-Fraud Office	Operational IT and cybersecurity
OSCE	Organization for Security and Co-operation in Europe	Policy and strategy
	P	
PESCO	Permanent Structured Cooperation	Information sharing and collaboration platform
PSC	Political and Security Committee	Policy and strategy
	R	
RIO-Ausschuss	Ausschuss der Ressort Information Officer (Committee of Departmental Information Officers, own translation)	Operational IT and cybersecurity
RP	State Rhineland-Palatinate	N/A
	S	
SächsDSDG	Sächsische:r Daten-schutzbeauftragte:r (State Commissioner for Data Protection Saxony, own translation)	Operational IT and cybersecurity
SAX.CERT	Computer Emergency Response Team Saxony	Operational IT and cybersecurity
SC	NATO Security Committee	Policy and strategy

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock	Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock (Special Prosecutor for Combatting Information and Communication Crimes of Rostock, own translation)	Operational IT and cybersecurity
Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus	Schwerpunktstaatsanwaltschaft zur Bekämpfung der Computer- und Datennetzkriminalität Cottbus (Special Public Prosecutor's Office to Combat Computer and Data Network Crime of Cottbus, own translation)	Operational IT and cybersecurity
Senator:in für Finanzen	Der:die Senator:in für Finanzen (Finance Senator of the Free Hanseatic City of Bremen, official translation)	Policy and strategy
SenInnDS	Senatsverwaltung für Inneres, Digitalisierung und Sport (Senate Department for the Interior, Digitization and Sport, own translation)	Policy and strategy
SH	State Schleswig-Holstein	N/A
Sicherheitskooperation Cybercrime	Sicherheitskooperation Cybercrime (Security Cooperation Cybercrime, own translation)	Information sharing and collaboration platform
SID	Staatsbetrieb Sächsische Informatik Dienste (State Enterprise Saxon Information Technology Services, own translation)	Operational IT and cybersecurity
SITiF BW	Sicherheitszentrum IT der Finanzverwaltung Baden-Württemberg (IT Security Center of the Financial Administration Baden-Württemberg, own translation)	Operational IT and cybersecurity
SK [HH]	Senatskanzlei Hamburg (Senate Chancellery Hamburg, own translation)	Policy and strategy

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
SK [SN]	Sächsische Staatskanzlei (State Chancellery of Saxony, own translation)	Policy and strategy
SL	Saarland	N/A
SN	Free State of Saxony	N/A
SN4C	Cyber Crime Competence Center Sachsen (Cyber Crime Competence Center Saxony, own translation)	Operational IT and cybersecurity
SOG-IS	Senior Officials Group Information Systems Security	Standardization and certification
Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin	Spezialabteilung zur Bekämpfung von Internetkriminalität der Staatsanwaltschaft Berlin (Special Department for the Fight against Cybercrime of Berlin's Public Prosecutor's Office, own translation)	Operational IT and cybersecurity
ST	State Saxony-Anhalt	N/A
Stakeholder Cybersecurity Certification Group	Stakeholder Cybersecurity Certification Group	Standardization and certification
StK SH	Staatskanzlei Schleswig-Holstein (State Chancellery Schleswig-Holstein, official translation)	Policy and strategy
StMD	Bayerisches Staatsministerium für Digitalisierung (Bavarian State Ministry for Digitalization, own translation)	Policy and strategy
StMFH	Bayerisches Staatsministerium der Finanzen und für Heimat (Bavarian State Ministry of Finance and Home Affairs, own translation)	Policy and strategy
StMI	Bayerisches Staatsministerium des Innern, für Sport und Integration (Bavarian State Ministry of the Interior, for Sport and Integration, own translation)	Policy and strategy

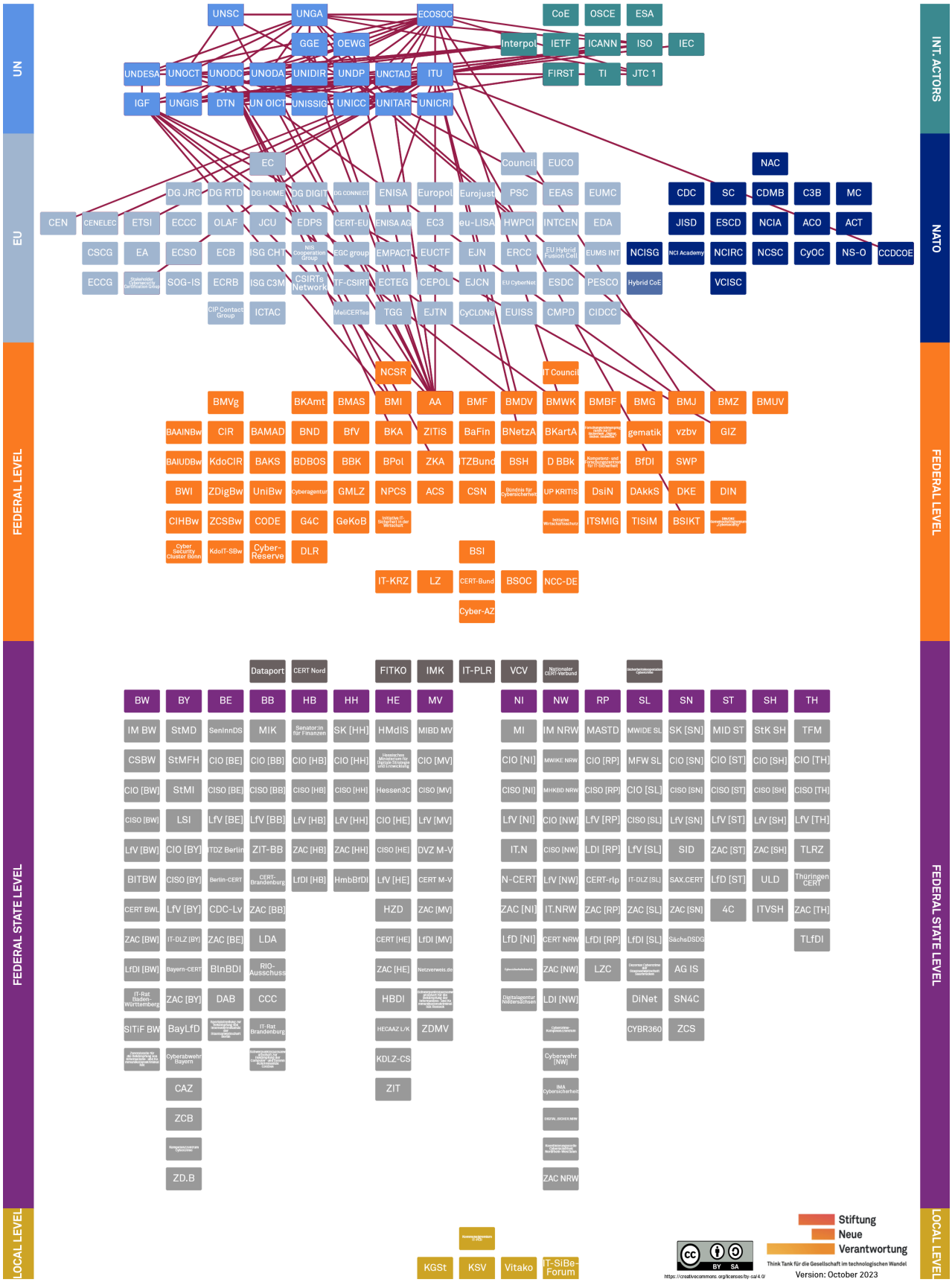
Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
SWP	Stiftung Wissenschaft und Politik (German Institute for International and Security Affairs, official translation)	Research and research funding Policy and strategy
	T	
TF-CSIRT	Reference Incident Classification Taxonomy Task Force	Information sharing and collaboration platform
TFM	Thüringisches Finanzministerium (State Ministry of Finance of Thuringia, own translation)	Policy and strategy
TGG	Taxonomy Governance Group	Information sharing and collaboration platform
TH	Free State of Thuringia	N/A
Thüringen CERT	Computer Emergency Response Team Thuringia	Operational IT and cybersecurity
TI	Trusted Introducer	Information sharing and collaboration platform
TISiM	Transferstelle IT-Sicherheit im Mittelstand (Transfer Office "IT Security for Small and Medium-sized Enterprises", own translation)	Information sharing and collaboration platform
TLfDI	Thüringische:r Landes-beauftragte:r für den Datenschutz und die Informationsfreiheit (State Commissioner for Data Protection and Freedom of Information Thuringia, own translation)	Operational IT and cybersecurity
TLRZ	Thüringer Landesrechen-zentrum (Thuringian Computing Centre, own translation)	Operational IT and cybersecurity
	U	
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Independent State Center for Data Protection Schleswig-Holstein, own translation)	Operational IT and cybersecurity

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
UN OICT	United Nations Office of Information and Communications Technology	Operational IT and cybersecurity
UNCTAD	United Nations Conference on Trade and Development	Policy and strategy
UNDESA	United Nations Department of Economic and Social Affairs	Policy and strategy
UNDP	United Nations Development Programme	Policy and strategy
UNGA	United Nations General Assembly	Policy and strategy
UNGIS	United Nations Group on the Information Society	Information sharing and collaboration platform
UniBw	Universitäten der Bundeswehr (Universities of the German Federal Armed Forces, official translation)	Education and training Research and research funding
UNICC	United Nations International Computing Centre	Operational IT and cybersecurity
UNICRI	United Nations Interregional Crime and Justice Research Institute	Policy and strategy Research and research funding
UNIDIR	United Nations Institute for Disarmament Research	Policy and strategy Research and research funding
UNISSIG	United Nations Information Security Special Interest Group	Information sharing and collaboration platform
UNITAR	United Nations Institute for Training and Research	Education and training Research and research funding
UNOCT	United Nations Office of Counter-Terrorism	Policy and strategy
UNODA	United Nations Office for Disarmament Affairs	Policy and strategy
UNODC	United Nations Office on Drugs and Crime	Policy and strategy

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
UNSC	United Nations Security Council	Policy and strategy
UP KRITIS	Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen (Public-Private Partnership for Critical Infrastructure Protection, own translation)	Information sharing and collaboration platform
	V	
VCV	Verwaltungs-CERT-Verbund (Administrative CERT-Group, own translation)	Information sharing and collaboration platform
Vitako	Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienst-leister (Federal Working Group of Municipal IT Service Providers, own translation)	Information sharing and collaboration platform
vzbv	Bundesverband der Verbraucherzentralen und Verbraucherverbände (Federation of German Consumer Organisations, official translation)	Policy and strategy
	Z	
ZAC [Federal State]	Zentrale Ansprechstelle Cybercrime für die Wirtschaft (Central Contact Points for Cybercrime for the Economy [Federal State], own translation)	Operational IT and cybersecurity
ZAC NRW	Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (Central and Contact Office Cybercrime North Rhine-Westphalia, own translation)	Operational IT and cybersecurity
ZCB	Zentralstelle Cybercrime Bayern (Central Office Cybercrime Bavaria, own translation)	Operational IT and cybersecurity
ZCS	Zentralstelle Cybercrime Sachsen (Central Office Cybercrime Saxony, own translation)	Operational IT and cybersecurity

Abbreviations/Terms Used in Visualization	Name (Official English title/Own translation)	Actor Category
ZCSBw	Zentrum für Cyber-Sicherheit der Bundeswehr (Center for Cyber Security of the Bundeswehr, own translation)	Operational IT and cybersecurity
ZD.B	Zentrum Digitalisierung. Bayern (Center for Digitization Bavaria, own translation)	Research and research funding Information sharing and collaboration platform
Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität	Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität (Central Office for the Fight against Information and Communication Crime, own translation)	Operational IT and cybersecurity
ZIT	Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (Central Office for Combating Internet and Computer Crime, own translation)	Operational IT and cybersecurity
ZIT-BB	Brandenburgischer IT-Dienstleister (Brandenburg IT Service Provider, own translation)	Operational IT and cybersecurity
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Central Office for Information Technology in the Security Sector, official translation)	Operational IT and cybersecurity
ZKA	Zollkriminalamt (Customs Investigation Bureau, official translation)	Operational IT and cybersecurity

4. Explanation – Actors at UN Level



Policy Overview

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

United Nations Institute for Training and Research (UNITAR)

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.[9]

United Nations Office for Disarmament Affairs (UNODA)

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 technolo-

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

gies. 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 the 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. UNODA cooperates with Interpol. The AA supports selected UNODA projects and trust funds financially.[10]

United Nations Office on Drugs and Crime (UNODC)

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.

10 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.

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. UNODC cooperates with Interpol. Representatives of the AA, the BKA, the BMI, the BMJ, and the ZKA have attended meetings of the IEG as part of the German delegations in various combinations. The BMJ 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.[11]

United Nations Development Programme (UNDP)

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. UNDP is involved in FIRST and is listed by the ISO as a cooperating organization. Germany is a

11 Commission on Crime Prevention and Criminal Justice (Resolution 26/4), Strengthening international cooperation to combat cybercrime.
Federal Ministry of Finance, Bundeshaushaltsplan 2021 Einzelplan 05: Auswärtiges Amt.
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.

member of the UNDP Executive Board and the largest contributor to the UNDP budget, which originates from the budget of the BMZ.[12]

Group of Governmental Experts on Advancing responsible State behaviour 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.[13]

12 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 Contributors.
United Nations Development Programme, UNDP and FIRST to host third annual Cybersecurity for Developing Nations Conference.

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

United Nations Department of Economic and Social Affairs (UNDESA)

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 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.[14]

International Telecommunication Union (ITU)

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.

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

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

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 participates 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. A representative of the ITU is represented on ICANN's Governmental Advisory Committee. The ITU is one of FIRST's partners. The ITU cooperates with the IEC and ISO, with whom it also works jointly as World Standards Cooperation (WSC). The ITU is a partner organization of the JTC 1 and is among the liaisons of the JTC 1/SC 27. Together with the EC, 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. ETSI's TC Cyber cooperates with the ITU and CEN/CENELEC's CEN/CLC/JTC 13 considers, among others, the adoption of ITU standards. The ITU is a member of the SCCG. The ITU lists the BMDV and the BNetzA as participating member state institutions from Germany. ITU-related developments are also dealt with in the BSIKT.[15]

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 are 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).

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

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 BMWK, the EC, 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 BMWK. The EC is an institutional partner of the European Dialogue on Internet Governance (EuroDIG), which takes place at the European level. Representatives of the AA, BMI, BMDV, and BMWK are represented on the Steering Committee of the German IGF (IGF-D).[16]

United Nations Conference on Trade and Development (UNCTAD)

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. UNCTAD is one of the partner organizations of the JTC 1 and is listed by the ISO as a cooperating organization.[17]

16 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 Deutschland, Über uns.

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

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 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.[18]

United Nations Economic and Social Council (ECOSOC)

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

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

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.

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 the 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. In addition, UNECE is a partner organization of the JTC 1 and is listed by the ISO as a cooperating organization. UNECE has also collaborated with the JTC 1/SC 27 in the past, for example, on gender-specific standards development in the cybersecurity domain. Germany is a member of the ECOSOC (until 2023) and the CCPCJ (also until 2023). In the past, representatives of the AA and the BMJ 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 BMWK, chairs Working Group 6 of the UNECE.[19]

United Nations General Assembly (UNGA)

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

19 Physikalisch-Technische Bundesanstalt, 9.3: Personal. (Website deleted)
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.

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 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 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.[20]

United Nations Institute for Disarmament Research (UNIDIR)

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.

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

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. In the past, JTC 1/SC 27 has worked with UNIDIR, among others, on gender-specific standards development in the cybersecurity domain. The AA has co-hosted a cyber-related event with UNIDIR as well as financially supported corresponding thematic UNIDIR conferences.[21]

United Nations Interregional Crime and Justice Research Institute (UNICRI)

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.[22]

United Nations Security Council (UNSC)

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

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

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

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.

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 EEAS' 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.[23]

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).

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

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.[24]

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 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.[25]

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.[26]

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

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

26 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.

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.

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. UNICC is involved in FIRST.[27]

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. UNOCT cooperates with Interpol. The EU

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

and Germany are among the top 10 contributors to UNOCT. Germany is a member of the Advisory Board of the UNCCT.[28]

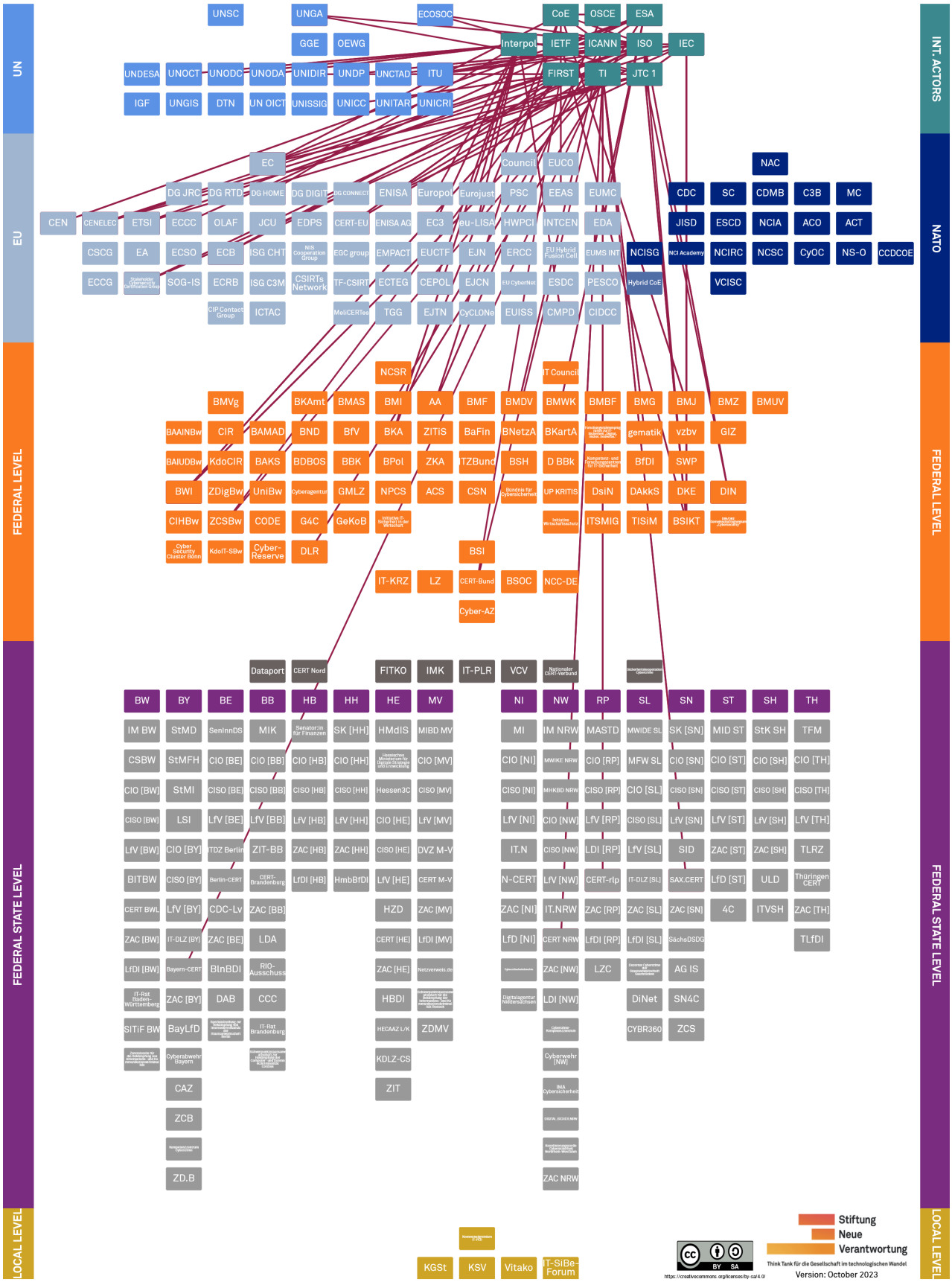
United Nations Office of Information and Communications Technology (UN OICT)
In the area of cybersecurity, the UN OICT has set itself the task of identifying cyber threats to the UN, preventing them, and contributing to their remediation when they occur as a focal point for partners within the UN. To 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.[29]

28 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.

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

5. Explanation – Other International Actors



Policy Overview

Year	Actor	Name
2022*	CoE	Second Adional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence
2021	ESA	Agenda 2025
2016	OSCE	OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies
2013	OSCE	Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming From the Use of Information and Communication Technologies
2006	CoE	Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems
2004	CoE	Convention on Cybercrime ("Budapest Convention")

* open for signatures since May 2022, not yet entered into force.

Council of Europe (CoE)

Within the framework of the Council of Europe, an intergovernmental organization, a convention on cybercrime, the so-called Budapest Convention has been concluded, among other things. The implementation of the convention, as well as the examination of possible amendments and the cooperation between its contracting parties, is supported by a Cybercrime Convention Committee (T-CY). The Information Society and Action against Crime Directorate is responsible for cybercrime, among other priority areas, within the organizational structure of the CoE. To implement the Budapest Convention, the CoE also publishes various reports and guidelines, for example, on the cooperation between law enforcement agencies and Internet service providers. The CoE has established a Cybercrime Programme Office (C-PROC) in Bucharest, which organizes capacity-building projects in the area of cybercrime investigation, prosecution, and sentencing based on the requirements of the Budapest Convention. The CoE also provides an information portal, the so-called Octopus Community, where thematic resources such as country profiles are made available. Every one to two years, the CoE organizes the Octopus Conference, a conference dealing with combatting cybercrime. Together with the EU, the CoE has initiated the GLACY+ project, which aims to strengthen, among other things, capabilities to apply the provisions of the Budapest Convention and international cooperation in certain focus countries.

Germany is a member of the CoE and has ratified the Budapest Convention. The German Foreign Minister or the Head of the Permanent Representation of Germany to the Council of Europe (AA) represents Germany in the CoE Ministerial Committee. In the

framework of the Budapest Convention, the AA also assumes the function of the point of contact for requests for mutual legal assistance or extraditions by other contracting parties. In this context, the BKA assumes the role of Germany's 24/7 contact point. From Germany, representatives of the BMJ participate in meetings of the T-CY. The EEAS dispatches a delegation to the CoE and representatives of the EC can – upon invitation – participate in CoE meetings from the Committee of Ministers to working groups. The Council of Europe also maintains liaison offices with the EU, the OSCE, and the UN. A CoE representative is represented in the ICANN Governmental Advisory Committee. The ISO lists the CoE as a cooperating organization.[30]

European Space Agency (ESA)

ESA is an intergovernmental organization in Europe that focuses on the exploration and exploitation of space. ESA activities are divided into four pillars, one of which, "Safety and Security", specializes in space security, security applications and cyber security. Within this framework, ESA maintains the European Space Security and Education Centre (ESEC). This hosts the Cyber Security Center of Excellence and supporting Technologies (CSCE), which provides various cyber security services. These include education and training, test and evaluation, R&D and security-by-design services, and secure operations centers. These services are implemented through three technology platforms: Collaborative coordination of Incident Response Platform (CIRP), Cyber-security Integration, Test and Evaluation Framework (CITEF), and the Security Aware Concurrent Design Platform (SACDP). In addition, building on ESA's Agenda 2025 to increase the cyber resilience of all European space assets, the C-SOC and SCCoE cybersecurity centers are currently being established. These are suspended in the ESA Security Office. The C-SOC is intended to serve as an operational platform from which ESA-wide information technology assets and satellites can be monitored. It is to detect security incidents and support the ESA emergency response team. These capabilities shall also be available to Member States at national level. The SCCoE is designed as a laboratory for testing space systems. Risk

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

analysis, forensics and pen testing of information and operational technologies, as well as education and training of cybersecurity experts are located here. Through the ESA CSC, ESA promotes and coordinates various other cybersecurity projects together with the EU.

ESA cooperates with most European space agencies such as DLR. Funding for German space contributions is managed by the BMWK. ESA cooperates with EDA, the EC, ECCC, and ENISA. ESA contributes standardization interests to CEN.[31]

Forum of Incident Response and Security Teams (FIRST)

As a forum and exchange platform, FIRST aims to strengthen the sharing of information on a trustworthy basis, inter alia on vulnerabilities and security flaws, as well as the cooperation between member CERTs in order to make the Internet more secure and minimize any damages after incidents.

From Germany, CERT-Bund, the CERT of the BWI, and the CERT of the Bundeswehr (ZCSBw) are participating in FIRST. Internationally, CERT-EU, the CERT of the ECB, UNICC, and UNDP are also involved. FIRST partners include the ITU and ICANN. The FIRST liaisons also include representatives of the ITU and ENISA.[32]

International Electrotechnical Commission (IEC)

As a standards organization, the IEC works on international standardization in the areas of electrical and electronic technologies. In the field of cyber security, the IEC is oriented toward a holistic approach to building cyber resilience, which consists of the components of people, processes, and technologies. The corresponding regulations can either be developed in a technology-independent and flexible manner, so-called horizontal standards, or specifically for certain technical application areas, so-called vertical standards. An example of horizontal standards in the area of cybersecurity is the IEC 62443 standard series which deals with the cybersecurity of industrial automation and control systems.

IEC, ISO, and the ITU work together as the World Standards Cooperation (WSC). Together with ISO, the IEC has established JTC 1. At the European level, it also co-

31 The European Space Agency, Cybersecurity at ESA.The European Space Agency, Agenda 2025.Connectivity and Secure Communications. Cyber Security Centre of Excellence and supporting technologies.
The European Space Agency, ESA and EDA renew cooperation.
The European Space Agency, Cooperation with the European Comission.

32 Forum of Incident Response and Security Teams, About FIRST.
Forum of Incident Response and Security Teams, FIRST Liaison Members.
Forum of Incident Response and Security Teams, FIRST Teams.
Forum of Incident Response and Security Teams, FIRST Vision and Mission Statement.
Forum of Incident Response and Security Teams, Partners.

operates with CENELEC. The German member of the IEC is the DKE, while the IEC is a member of the SCCG. IEC-related developments are also dealt with in the BSIKT.[33]

International Criminal Police Organization (Interpol)

Interpol supports its member states in carrying out and coordinating cross-border investigations and operations to combat cybercrime. Partially, it also takes over the management of latter operations in the form of so-called "cyber surges". For these purposes, Interpol houses a Cyber Fusion Centre (CFC) as well as two relevant communication and collaboration platforms, the Cybercrime Knowledge Exchange Workspace (CKE) and the Cybercrime Collaborative Platform – Operation (CCP-Operation). Within the CFC, information from law enforcement agencies as well as the private sector is gathered and analyzed. Based on this information, reports are shared with any threatened states. In contrast to the CCP-Operation, only not police-related technical information, for example, on trends or prevention, is exchanged in the framework of the CKE between authorized members. The CKE is conceived as a network that comprises representatives from law enforcement agencies, governments, and international organizations, as well as other subject-matter experts. The CCP-Operation, in addition, also enables active coordination of global law enforcement efforts to combat cybercrime through information sharing and resource pooling among operational points of contact. Interpol also partakes in respective capacity-building in its member countries and provides a training format for cyber investigators through its Digital Security Challenge. Moreover, it has published a guide for the creation or revision of a national cybercrime strategy.

For Germany, the BKA assumes the function as National Central Bureau (NCB). At the EU level, Interpol cooperates with Europol, Eurojust, CEPOL, eu-LISA, the CMPD, and DG HOME, among others. Annually, Europol (through the EC3) and Interpol host a joint conference on cybercrime. In addition, it collaborates UN level with UNODC, UNODA, and UNOCT, for example. Representatives of Interpol are represented in ICANN's

33 German Commission for Electrical, Electronic & Information Technologies of DIN and VDE, IEC 62443: Die internationale Normenreihe für Cybersecurity in der Industrieautomatisierung.
German Commission for Electrical, Electronic & Information Technologies of DIN and VDE, Frankfurt Agreement stärkt Zusammenarbeit zwischen IEC und CENELEC.
International Electrotechnical Commission, Cyber security [1].
International Electrotechnical Commission, Cyber security [2].
International Electrotechnical Commission, National Committees.
International Electrotechnical Commission, Frequently asked questions.

Governmental Advisory Committee, and Interpol is listed by the ISO as a cooperating organization.[34]

International Organization for Standardization (ISO)
With a cross-thematic mandate, the ISO is a standards organization that develops international standards for a wide variety of fields (except for electrics, electronics, and telecommunications). ISO standards dealing with IT and cybersecurity include, for example, the "27000 family" developed in coordination with the IEC or the ISO/SAE 21434 standard, which addresses technical requirements for the cybersecurity of electrical or electronic systems within automotive vehicles.

The German member of ISO is the DIN. ISO cooperates with the IEC and the ITU, which also work together as the World Standards Cooperation (WSC). Together with the IEC, ISO has established the JTC 1. ETSI's TC CYBER cooperates with ISO and CENELEC's CEN/CLC/JTC 13 examines, among other things, the adoption of ISO standards. ISO is a member of the SCCG. In addition, ISO's list of cooperating organizations includes the EC, the ECB, the ENISA, the CoE, the ETSI, the IETF, the ICANN, Interpol, UNCTAD, UNDP, and UNECE (ECOSOC).[35]

Internet Corporation for Assigned Names and Numbers (ICANN)
ICANN is committed to ensuring the security, stability, and interoperability of the global Internet, as well as its expansion and development. To this end, it works on unique identifiers and coordinates the Internet's underlying Domain Name System (DNS). ICANN advocates the full adoption of Domain Name System Security Extensions (DNSSEC) for all domain names by all members of the domain name ecosystem to increase the level of security and protect communications between end users and the domain. Within ICANN's organizational structure, the Security and Stability Advisory Committee (SSAC) addresses the security and integrity of the DNS and uses

34 Federal Criminal Police Office, Interpol (IKPO).
International Criminal Police Organization, Cooperation with United Nations entities.
International Criminal Police Organization, Cyber capabilities development.
International Criminal Police Organization, Cybercrime.
International Criminal Police Organization, Cybercrime Collaboration Services.
International Criminal Police Organization, Cybercrime threat response.
International Criminal Police Organization, Cybercrime operations.
International Criminal Police Organization, Germany.
International Criminal Police Organization, Innovation to beat cybercrime acceleration the theme of 2021 Europol-INTERPOL Cybercrime Conference.
International Criminal Police Organization, INTERPOL and the European Union.
International Criminal Police Organization, National Cybercrime Strategy Guidebook.

35 Institut der Wirtschaftsprüfer in Deutschland, CYBERRISK.
International Organization for Standardization, Cybersecurity in cars.
International Organization for Standardization, Members.
International Organization for Standardization, Organizations in cooperation with ISO.
International Organization for Standardization, Structure and Governance.
International Organization for Standardization, What we do.
World Standards Cooperation, Who we are.

its analysis and assessments to advise the ICANN Board of Directors and the ICANN community. ICANN also provides various publications that address relevant issues within ICANN's portfolio of responsibilities from a technical or policy perspective.

Representatives of the BMDV and BMI are members of the ICANN Governmental Advisory Committee (GAC) for Germany. The CoE, Interpol, and the ITU are also represented by representatives in the GAC. A representative of the IETF is involved in the ICANN Board of Directors as a liaison. ICANN is a partner of FIRST and is listed by the ISO as a cooperating organization.[36]

Internet Engineering Task Force (IETF)

The IETF is dedicated to developing voluntary technical standards for the Internet to improve its functioning and security. Different working groups within the IETF's Security Area are working, for example, on ensuring high-security levels of IETF protocols, authentication, and authorization. The IETF also offers training on the functioning of the Internet for policymakers in the context of the IETF Policy Program.

A representative of the IETF is involved as a liaison on the ICANN Board of Directors. The ISO lists the IETF as a cooperating organization. IETF-related developments are also dealt with in the BSIKT.[37]

ISO and IEC Joint Technical Committee (JTC 1)

JTC 1 discusses and develops standards in the field of information technologies. Within JTC 1, subcommittee 27 (JTC 1/SC 27) deals with information and cyber security as well as privacy protection. It is responsible, for example, for the (further) development of the horizontal ISO/IEC 27000 standard series.

JTC 1 is a joint technical committee of ISO and IEC. For Germany, the DIN participates in JTC 1. The DIN also provides the secretariat of ISO/IEC JTC 1/SC 27. JTC 1-related developments are also dealt with in the BSIKT. The EC, ENISA, ETSI and the ITU, UNCTAD, and the UNECE (ECOSOC) are partner organizations of JTC 1. JTC 1/SC 27 maintains liaisons with the ETSI and the ITU, among others. CENELEC's CEN/CLC/JTC 13 examines, inter alia, the adoption of standards developed in JTC 1. In the past, JTC 1/

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

37 Internet Engineering Task Force, Security & privacy.
Internet Engineering Task Force, Security Area (sec).
Internet Engineering Task Force, Mission and principles.
Internet Engineering Task Force, Groups.
Internet Engineering Task Force, Internet standards.
Internet Society, IETF Policymakers Program.

SC 27 has also collaborated with the UN organizations UNECE and UNIDIR on gender-specific standards development for the cybersecurity domain.[38]

Organization for Security and Co-operation in Europe (OSCE)

In the area of cyber and IT security, the OSCE's primary focus lies in promoting confidence-building among its member states to prevent and mitigate potential conflicts. In the past, OSCE member states have adopted two corresponding packages of confidence-building measures (CBMs) in the past. These include, among other things, an inter-state consultative mechanism on possible incidents and the creation of other substantive exchange platforms. The OSCE also provides an e-learning course on these agreed CBMs. In addition to a CBM focus, the OSCE also aims to work more generally on appropriate and timely responses by state authorities to threats from cyberspace, such as cybercrime or the use of the Internet by non-state actors, for example, for terrorist purposes. Within the OSCE's organizational structure, the Transnational Threats Department is responsible for IT and cybersecurity. It also organizes other thematic activities, such as exercises on cyber operations targeting critical infrastructure or workshops. Every year, the OSCE hosts a Cyber/ICT Security Conference.

Germany is a member of the OSCE and is represented in Vienna by its permanent mission to the OSCE (AA). The CoE maintains a liaison office to the OSCE.[39]

Trusted Introducer (TI)

As an information exchange platform, Trusted Introducer aims to contribute to improved cooperation, exchange on threat situations, and, if necessary, accelerated response capabilities between CERTs worldwide. It provides a respective infrastructure for this purpose. CERTs can participate in TI as listed, accredited, or certified teams.

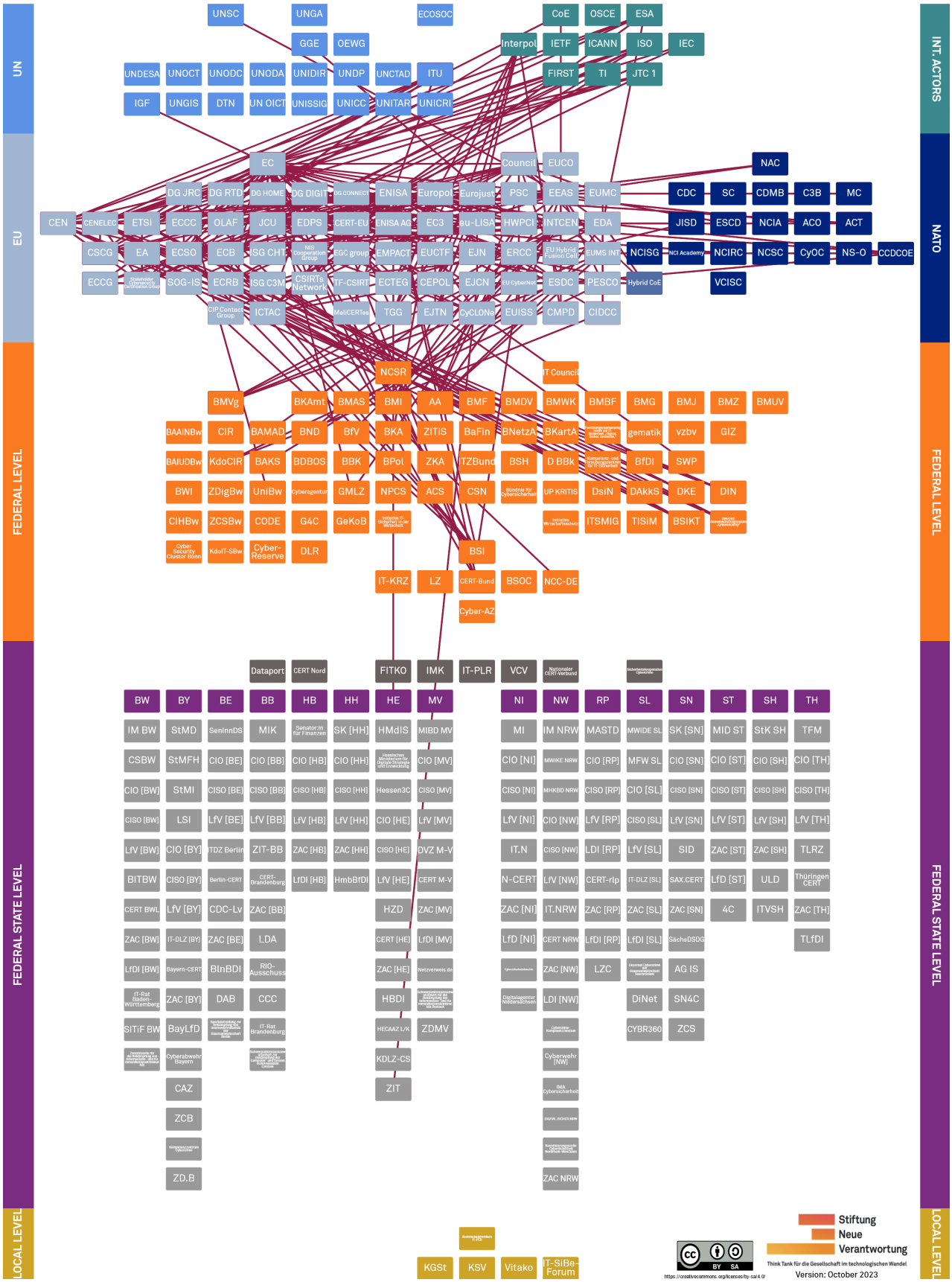
From Germany, the CERT of the Bundeswehr (ZCSBw), the CERT of gematik, the Bayern-CERT, the CERT NRW, the CERT-rlp as well as the SAX.CERT are listed as participating teams. The CERT-Bund is accredited at Trusted Introducer, and the CERT of the BWI is certified. The CERT-EU is a certification candidate.[40]

38 International Electrotechnical Commission, ISO/IEC JTC 1/SC 27.
International Organization for Standardization, ISO/IEC JTC 1 Participation.
International Organization for Standardization, Keeping Cybersafe.
JTC 1, JTC 1/SC 27 celebrates 30 years.
JTC 1, Partners.

39 Organization for Security and Co-operation in Europe, Cyber/ICT Security.
Organization for Security and Co-operation in Europe, Multilateral engagement key to open and secure cyberspace.
Organization for Security and Co-operation in Europe, New e-learning course on OSCE cyber/ICT security Confidence-Building Measures now available.
Organization for Security and Co-operation in Europe, Transnational Threats Department: Cyber/ICT Security.
Permanent Mission of the Federal Republic of Germany to the OSCE, Ständige Vertretung.

40 Trusted Introducer, Processes.
Trusted Introducer, Services for Security and Incident Response Teams.
Trusted Introducer, Team Database.

6. Explanation – Actors at EU Level



Policy Overview

Year	Name
2023	Council Conclusions on the EU Policy on Cyber Defence
2022	Directive on the resilience of critical entities and repealing Council Directive 2008/114/EC (Directive 2022/2557)
2022	Directive on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 ("NIS 2 Directive", Directive 2022/2555)
2022	Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 ("Dora", Regulation 2022/2554)
2022	Joint Communication: EU Policy on Cyber Defence (JOIN 2022/49)
2022	Council conclusions on the development of the European Union's cyber posture
2021	International Strategy of the EU Agency for Cybersecurity
2021	Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (Regulation 2021/887)
2020	Communication from the Commission: Shaping Europe's Digital Future ("Digital Strategy")
2020	EU Cybersecurity Strategy for the Digital Decade Previous documents: • 2017: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU • 2013: EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace
2019	EU Cybersecurity Act (Regulation 2019/881) Previous documents: • 2013: Regulation 526/2013
2019	EU Law Enforcement Emergency Response Protocol for Major Cross-Border Cyber-Attacks (LE ERP) (Europol-Pressemitteilung)
2019	Regulation on ENISA (The European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification And Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Regulation 2019/881)
2018	EU Cyber Defence Policy Framework Previous documents: • 2014: EU Cyber Defence Policy Framework
2018	Joint Communication: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats (JOIN(2018) 16)

Year	Name
2017	Commission Recommendation on coordinated response to large-scale cybersecurity incidents and crises ("Blueprint", 2017/1584)
2017	Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities
2016	Directive concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive", Directive 2016/1148)
2016	Joint Communication: Joint Framework on Countering Hybrid Threats. A European Union Response ("Playbook", JOIN(2016) 18)
2013	Directive on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Directive 2013/40/EU)

European Union Agency for Cybersecurity (ENISA)

ENISA[41] 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.

DG CONNECT is the DG responsible for ENISA and represents the EC in ENISA's Management and Executive Board together with DG DIGIT. ENISA supports the EC

41 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.

in the development of a cybersecurity certification scheme to succeed the existing Mutual Recognition Agreement (MRA) of SOG-IS. 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 EDA, 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 DG JRC, ECSO, ESA, ESDC, 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 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. ENISA participates in EMPACT and meetings of the ECRB. The ENISA AG advises ENISA on, among other things, the implementation of its tasks. Upon request, also the SCCG may advise ENISA. It is responsible for the implementation and deployment of key aspects of the MeliCERTes facility and is part of the CSCG. The ECCG, in addition to the EC, 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.

The TC CYBER of ETSI cooperates with the ENISA. There is a cooperation agreement between CEN, CENELEC and ENISA. ENISA is also among the institutional stakeholders of CEN. On the part of ISO, ENISA is listed as a cooperating organization. ENISA is a partner organization of the JTC 1. Among the FIRST liaisons there is also a representative of the ENISA. 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.[42]

European Union Agency for Law Enforcement Training (CEPOL)

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 EC, EC3, EJTN, Eurojust, the EUCTF, and ECTEG. Further exchange and working relations exist with the ESDC and DG HOME. CEPOL is also a member of the stakeholder community of EU CyberNet and is involved in the ICTAC as well as EMPACT. It may be invited as an observer to meetings of COSI (Council of the EU). CEPOL cooperates with Interpol.[43]

European Union Agency for Criminal Justice Cooperation (Eurojust)

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,

42 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.

43 CEPOL, About us.
CEPOL, CEPOL Cybercrime Academy Inaugurated.
Mail exchange with CEPOL representatives in August 2019.

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.

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 EC. Partnership relations exist with the following EU institutions: Europol, EC3, CEPOL, eu-LISA, OLAF, and EJTN. It also cooperates with the HWPCI. Eurojust is involved in EMPACT. 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 EDPS has a supervisory role over Eurojust regarding the lawful processing of personal data. Eurojust cooperates with Interpol.[44]

CEN/CENELEC Cyber Security Coordination Group (CSCG)

As a cross-organizational coordination body, the CSCG's objectives include analyzing cyber-relevant developments, assessing the potential of standards to support relevant regulations or political measures in the field of cyber security, and issuing recommendations on the European positioning in international standardization bodies and committees.

The CSCG is a joint coordinating body of CEN and CENELEC. Among other things, it can issue recommendations to the EC and advise it on cybersecurity standardization. In addition to member state institutions, CSCG participants include representatives from ENISA, EDA, DG CONNECT, DG HOME and DG JRC. The CSCG secretariat is located at DIN, which also participates in the CSCG on behalf of Germany.[45]

44 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)

45 CEN/CENELEC/ETSI, CEN/CENELEC/ETSI Cyber Security Coordination Group (CSCG) White Paper.
German Institute for Standardization, Cyber Security Coordination Group (CSCG).

Computer Emergency Response Team of the European Commission (CERT-EU)
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 EC and General Secretariat of the Council of the EU). DG DIGIT is the responsible DG but DG CONNECT is also 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, the CERT of the ECB, 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 and exchange in the field of cybersecurity was concluded between EDA, 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 ESDC. 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. It is a certification candidate at TI and involved in FIRST.[46]

Computer Security Incident Response Teams Network (CSIRTs Network)
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 EC 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

46 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.

provide forensic analysis and other technical information to the network. The participation of the CSIRTs Network in the JCU is envisaged.[47]

Cyber Crisis Liaison Organisation Network (CyCLONe)

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 EC, 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.[48]

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 par-

47 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.

48 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 Commission Representation in Germany, EU-Staaten testen ihre Zusammenarbeit im Falle von Cyber-Angriffen.
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 and Community, BMI und BSI beteiligen sich an Cyberkrisenübung Blue OLEx 2020.

ticipating 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 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 EDA, the EUMS, and ENISA. It is currently chaired by the commander of the KdoITBw. The KdoCIR coordinated with the EUMS and the EDA in its conceptualization of the CIDCC.[49]

Crisis Management and Planning Directorate (CMPD)

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. The CMPD provides earmarked funding and support for the protection of CSDP's IT systems and cybersecurity capacity building.

The CMPD is located in the EEAS. The CMPD cooperates with Interpol.[50]

ENISA Advisory Group (ENISA AG)

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 EC 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, without the right to vote. 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 com-

49 Bundeswehr, Europäisches Verteidigungsprojekt für Cybersicherheit – Das Cyber and Information Domain Coordination Centre.
Dorothee Frank, Meilenstein für die europäische Cyberlage.
Federal Ministry of Defence, Cyber and Information Domain Coordination Centre (CIDCCC).
PESCO, Cyber and Information Domain Coordination Center (CIDCC).

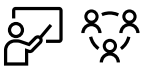
50 European Union External Action Service, The Crisis Management and Planning Directorate (CMPD). (Website deleted)

munication with relevant stakeholders can be improved regarding the annual work program. Furthermore, it deals with the question of how to ensure communication with the relevant stakeholders regarding the annual work program. In addition to the 33 appointed members and their representatives, Europol, EC3, CEN, CENELEC, ETSI, eu-LISA and CERT-EU, among others, are invited to nominate representatives for the 2023–2025 term of ENISA AG.[51]

EU Hybrid Fusion Cell

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 EEAS. 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.[52]



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

51 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).

52 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.

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.

The establishment of EU CyberNet was foreseen in documents of the Council of the EU and the EC. EU CyberNet is funded by the EC 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 PSC on the implementation of the EU Cyber Security Strategy. CEPOL, ESDC, EUISS, and BSI are already members of the stakeholder community.[53]

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

The ECRB was created as a forum for exchange and discussion on strategic issues between private and public stakeholders in the financial sector. The ECRB's goals include sharing best practices, raising awareness of cyber resilience, and undertaking joint initiatives. An output of the ECRB is the Cyber Information and Intelligence Sharing Initiative (CIISI-EU), which aims to contribute to the protection of the financial system and its infrastructure against threats from cyberspace, for example, through prevention, identification, and mutual information sharing.

ECRB meetings are attended by representatives of the EC, Europol, ENISA, and the D BBk, among others. Among other actors, the ECB, ENISA, and Europol are also involved in the CIISI-EU. Upon request, the ECRB can also act in an advisory capacity vis-à-vis the EC, ECB, or other EU organizations. The secretariat of the ECRB is provided by the ECB.[54]

53 Council of the EU, 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.

54 European Central Bank, Euro Cyber Resilience Board for pan-European Financial Infrastructures.
European Central Bank, Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB). Cyber Information & Intelligence Sharing Initiative: Terms of Reference.
European Central Bank, Third meeting of Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB).
European Central Bank, Mandate of the Euro Cyber Resilience Board for pan-European Financial Infrastructures.

European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA)

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 is also responsible for the technical implementation and development of the interoperability of EU information systems.

The Agency cooperates closely with the Member States, and at EU level with the EDBS, the Council of the EU, the EC, CEPOL, Eurojust, and Europol and DG 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 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. eu-LISA is involved in EMPACT. Contacts on working-level have also been established with NATO CCDCOE. eu-LISA cooperates with Interpol. The BMI is represented by a representative on the Management Board of eu-LISA.[55]

European Cybersecurity Certification Group (ECCG)

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 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 SCCG. To respond to rapid developments in the technology field, the group can, parallel to the EC, request that ENISA develops new possible certification schemes not yet included in the work program.[56]

55 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.

56 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).

European Commission (EC)

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. In the Digital Europe program, the EC also provides strategic funding in various fields, including cybersecurity, to promote the digital transformation of society and economy. Digital Europe is complemented by other programs such as Horizon Europe.

Several Directorates-General work in the field of cybersecurity, including CONNECT, DIGIT, HOME, JRC and RTD. The CERT-EU, and the ERCC (ERCC through DG ECHO) are also affiliated with the European Commission. The Council of the EU may entrust the EC with the negotiation of international agreements, the conclusion of which is decided by the Council based on a proposal from the EC. OLAF is subordinate to the EC. The ECCC is based on a proposal of the EC, which is also, together with the EU Member States, represented by two representatives on the ECCC Governing Board. The EC chairs the CIP Contact Group and the SCCG (the latter jointly with ENISA). It is also represented on the Advisory Board of the EA. The eu-LISA, the EC3, the HWPCI, the ECB, ESA and the EUISS cooperate with the EC. The EC is involved in the development and implementation of CEPOL trainings and EMPACT. The ECCG is assisting the EC in establishing a European work program for cybersecurity certification schemes. Upon request, the EDPS may act in an advisory capacity for the EC. Representatives of the EC participate in meetings of the ECRB. Upon request, the ECRB may also act in an advisory capacity to the EC, among others. The EC participates in the CSIRTs Network as an observer and is a member of the EUCTF. ENISA is assisting the EC in developing a cybersecurity certification scheme to serve as a successor to the existing SOG-IS Mutual Recognition Agreement (MRA). The establishment of the EU CyberNet has been foreseen, among others, in documents of the EC. ECSO is a contractual partner of the EC. The ITU cooperates with the EC in the context of harmonization of ICT policies within ACP countries. The EC may participate in meetings of the MAG of the IGF. Representatives of the EC can participate upon invitation in meetings of the CoE from the Committee of Ministers to working group. The CSCG can make recommendations to the EC and advise it on cybersecurity standardization. ETSI and CENELEC are in exchange with the EC. The ISO lists the EC as a cooperating organization. The EC is one of the partner organizations of the JTC 1. In the past, the EC, together with the EUCO, 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 EC funds the OVERCLOCK project, in which the BKA and ZITiS participate. Every

two years, the BSI must submit certain information to the EC. The EC is one of the partners of the GMLZ and is also among the third-party funders of the SWP.[57]

European co-operation for Accreditation (EA)

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 49 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. Furthermore, the EA is a member of the SCCG.[58]

European Defence Agency (EDA)

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 EDA'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 EDA 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 EDA 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 EDA's head. The Steering Board of the EDA meets at the level of the Member States' defense ministers; for Germany, the Federal Minister of Defense (BMVg) is a member. Together with the EEAS, EDA jointly manages all secretarial functions for the PESCO. The EDA is represented in the Steering Board of the CIDCC and participates in the ICTAC. The EDA signed a Memorandum of Understanding with ENISA, the EC3, and CERT-EU intending to develop a cooperation framework for the organizations. The EDA is envisioned as a participating organization of the JCU in a supporting role. Working relationships with the ESDC, ESA, the

57 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.

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

ECSO, the Hybrid CoE, the HWPCI, the NATO CCDCOE, and ACT exist. The EDA participates in Locked Shields. The Chief Executive of the EDA meets regularly with the SACT (ACT) and Assistant SECGEN's of NATO. The EDA Steering Board is also briefed regularly by the latter. The EDA is among the institutional stakeholders of the CEN and one of the participants of the CSCG.[59]

European Central Bank (ECB)

As the supervisory authority for the euro area, the ECB is also responsible for monitoring and ensuring the operational capability of financial market infrastructure and system-relevant payment systems by building the greatest possible cyber resilience. To this end, the ECB promotes, among other things, the international exchange of security-related information, identifies best practices and has established a common European framework for "threat intelligence-based ethical red-teaming" (TIBER-EU) to inter alia diagnose strengths and weaknesses. In addition, national central banks in the euro area are required to report significant cybersecurity incidents to the ECB. The ECB also oversees how they manage relevant risks in relation to their IT systems.

The ECB supervises the national central banks of the euro area, including the D BBk. It cooperates with other EU institutions such as the EC and the CERT-EU, as well as national cybersecurity authorities such as the BSI. The Deutsche Bundesbank also participates in TIBER-EU and has established a corresponding national TIBER-DE based on a joint decision with the BMF. The President of the Deutsche Bundesbank is a member of the ECB's Governing Council. The CERT of the ECB is involved in FIRST.[60]

59 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.
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.
European Union, Europäische Verteidigungsagentur (EVA).

60 Deutsche Bundesbank, TIBER-DE: Threat Intelligence-based Ethical Red Teaming in Germany.
European Central Bank, Cyber resilience and financial market infrastructures.
European Central Bank, TIBER-EU FRAMEWORK: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming.
European Central Bank, What is cyber resilience?.
European Central Bank, What is TIBER-EU?.

European External Action Service (EEAS)

The European External Action Service is a leader in the field of conflict prevention, cyber diplomacy, and strategic communication. The EEAS 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 EEAS 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 Defense Policy, while simultaneously acting as Vice President of the European Commission. This ensures coherent policymaking in the fields of security and cybersecurity policy.

The EEAS hosts EUMS INT, INTCEN, and the EU Hybrid Fusion Cell. It is also affiliated with the CMPD and the ESDC. Furthermore, EEAS representatives chair the PSC. The HWPCI, the EUISS, and ECSO cooperate with the EEAS. The EEAS co-chairs the ISG CHT together with the EC and participates in the ISG C3M. Together with the EDA, the EEAS forms the secretariat of PESCO. The participation of the EEAS in the JCU is envisaged. The EEAS receives information and assessments from the STAR (DG HOME). The EEAS 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 EEAS has met with representatives of the ESCD to discuss cyber defense. In addition, the EEAS has published reports in the past together with ENISA, for example on "Foreign Information Manipulation Interference (FIMI) and Cybersecurity – Threat Landscape." The EU delegation to the UN in New York, subordinate to the EEAS, has participated in debates on cybersecurity within the UNSC. The ERCC coordinates with the EEAS, among others, and the EEAS dispatches a delegation to the CoE.[61]

European Data Protection Supervisor (EDPS)

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 EDPS observes and

61 Annegret Bendiek, Gemeinsame Außen- und Sicherheitspolitik: von der Transformation zur Resilienz.
Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats "EU Playbook".
European Council/Council of the European Union, Politisches und Sicherheitspolitisches Komitee (PSK).
European Union External Action, The Crisis Management and Planning Directorate (CMPD). (Website deleted)
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.

evaluates possible implications for data protection that arise through new technological developments. The EDPS is appointed for a five year-term and works together with national data protection authorities within EU Member States. In the past, the EDPS 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 EDPS 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 EDPS. The EDPS assumes a supervisory role over Europol and Eurojust. At the German level, contact and exchange exist with the BfDI.[62]

European Council (EUCO)

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 EC 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 (EEAS).[63]

European Anti-Fraud Office (OLAF)

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.

OLAF reports to the EC but is independent in the execution of its mandate. It regularly reports to the Council of the EU's Working Group on Fraud Prevention.[64]

62 BfDI, Stellungnahme zu überarbeiteten Standarddatenschutzklauseln.
EDPS, Über den EDSB.
EDPS, EDPS formal comments in response to the "Cybersecurity Package" adopted by the Commission.
EDPS, Häufig gestellte Fragen.

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

64 European Anti-Fraud Office, About Us.
European Anti-Fraud Office, Cooperation with EU institutions.

European Telecommunications Standards Institute (ETSI)

As a European standardization organization, ETSI works on the development and adoption of supra-regional standards for ICT-based applications and systems. Its main activities in the area of cybersecurity take place within the framework of its Cybersecurity Technical Committee (TC CYBER). Focal points constitute for example the cybersecurity of national critical infrastructures, companies, or individuals.

ETSI is in exchange with CEN, CENELEC and the EC. The DKE is ETSI's German member. The ISO lists ETSI as a cooperating organization. TC CYBER cooperates with ITU, ISO and the ENISA and nominates representatives for ENISA AG. ETSI is also a member of the SCCG. The German participation in the TC Cyber is coordinated, among others, within the DIN/DKE Joint Committee "Cybersecurity". ETSI is one of the partner organizations of JTC 1. ETSI-related developments are also dealt with in the BSIKT.[65]

European Committee for Electrotechnical Standardization (CENELEC)

CENELEC has set itself the goal of developing voluntary standards in the field of electrical engineering. Cybersecurity constitutes one of its standardization priorities. A joint technical committee with CEN deals with standards which are relevant for cybersecurity and data protection (CEN/CLC/JTC 13). CEN/CLC/JTC 13 aims to incorporate already developed international standards on the European level and to develop its own European standards in case identifiable gaps exist.

CENELEC cooperates with the IEC and exchanges information with the EC and ETSI. A cooperation agreement exists between CEN, CENELEC and the ENISA. CEN and CENELEC nominate shared representatives for ENISA AG. The CSCG is a joint coordination body of CEN and CENELEC. The DKE is the German member of CENELEC. The DIN provides the secretariat of CEN/CLC/JTC 13. CEN/CLC/JTC 13 cooperates with the ENISA. For example, it examines the adoption of standards which have been developed within the framework of ISO/IEC JTC 1, ISO, IEC or the ITU. The DIN/DKE Joint Committee "Cybersecurity", for example, steers the German participation in CEN/CLC/JTC 13. CENELEC-related developments are also dealt with in the BSIKT. It is also a member of the SCCG.[66]

65 European Telecommunications Standards Institute, About Us.
European Telecommunications Standards Institute, Cybersecurity.
European Telecommunications Standards Institute, ETSI in Europe.
European Telecommunications Standards Institute, TC CYBER Roadmap.
European Telecommunications Standards Institute, TC CYBER Activity Report 2020.

66 CEN/CENELEC, Business Plan CEN/CENELEC JTC 13: Cybersecurity and data protectionv.
European Committee for Electrotechnical Standardization, About CENELEC.
European Committee for Electrotechnical Standardization, CEN and CENELEC.
European Committee for Electrotechnical Standardization, CEN/CLC/JTC 13 – Cybersecurity and Data Protection.
European Committee for Electrotechnical Standardization, CEN/CLC/JTC 13/WG 4 – Cybersecurity services.
European Committee for Electrotechnical Standardization, Cybersecurity and data protection.
European Committee for Electrotechnical Standardization, ISO and IEC.
European Committee for Electrotechnical Standardization, List of CENELEC Members.

European Committee for Standardization (CEN)

The CEN describes itself as a platform for the development of standards and other technical documents at the European level. A joint technical committee with CENELEC, CEN/CLC/JTC 13, deals with standards which are relevant for cybersecurity and data protection (for a more detailed description, see entry on CENELEC).

DIN is the German member of CEN. A cooperation agreement exists between CEN, CENELEC, and the ENISA. The CSCG is a joint coordination body of CEN and CENELEC. ENISA, EDA, and DG JRC are among the institutional stakeholders of CEN and ETSI and ESA are in exchange with CEN. The DIN/DKE Joint Committee "Cybersecurity", for example, steers the German participation in CEN/CLC/JTC 13. CEN-related developments are also dealt with in the BSIKT. It is also a member of the SCCG[67].

European Police Office (Europol)

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. Europol thus supports member states in previously initiated investigations and analyzes crime trends in the EU. Europol also cooperates with non-EU member states and international organizations.

In the area of cybercrime, Europol is strengthening law enforcement in particular through the EC3, which is subordinate to it. The participation of Europol in the JCU is envisaged. Eurojust, eu-LISA, the ESDC, the HWPCI, and ECSO cooperate with Europol. Europol is a member of the EUCTF, the TGG, and the ICTAC. Europol participates in EMPACT and meetings of the ECRB. Together with the EC3, Europol nominates representatives for the ENISA AG. Europol representatives are also part of the Advisory Board of the ECTEG. Europol receives information and assessments from the STAR (DG 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 EDPS has a supervisory role over Europol regarding the lawful processing of personal data. Europol works together with Interpol and the BKA. The BKA serves as a Europol National Unit and therefore Europol's German point of contact. Annually, Europol (through its EC3) and Interpol host a joint conference on cybercrime.[68]

67 European Committee for Standardization, About CEN.
European Committee for Standardization, CEN Communities.
European Committee for Standardization, List of CEN Members.
European Union Agency for Cybersecurity, Cyber-security collaboration agreement between ENISA & European standardisation bodies, CEN and CENLEC.

68 Europol, About Europol.
Europol, European Cybercrime Centre – EC3.
Federal Criminal Police Office, Europol.

European Security and Defence College (ESDC)

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 ESDC. A Cyber Education, Training, Evaluation and Exercise Platform (ETEE) was established at the ESDC to this end.

The ESDC is institutionally housed within the EEAS. 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 ESDC 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 ESDC is a member of the EU CyberNet stakeholder community.[69]

European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC)

The ECCC was founded to promote European autonomy in cybersecurity, the competitiveness of the European cybersecurity industry and strengthen the Digital Single Market. The ECCC, whose existence is initially planned until 2029, wil to bundle existing funds for cybersecurity within the European Union and investments in a targeted manner (Horizon Europe and Digital Europe funding programs) and coordinate research projects in the EU in the field of cybersecurity. Outside of these functions, the ECCC is financing the National Coordination Centers (NCCs), with wich it cooperates.

The ECCC is based on a proposal of the EC (prepared by DG 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. The ECSO coordinates with the ECCC in the establishment of the ECCO In addition, the EU Regulation establishing the ECCC provides, inter alia, for cooperative working relations with the EEAS, DG JRC, EC3, and the EDA. From Germany, representatives of the BSI are represented on the ECCC's Management Board. As a national counterpart, the

69 ESDC, EAB.Cyber.
ESDC, Education & Training.
ESDC, Network Members.
ESDC, Who We Are.

NCC-DE complements the tasks of the ECCC at EU level. The ECCC cooperates with ESA.[70]

European Cybercrime Center (EC3)

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, expertise and stakeholder management, 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.

EC3 is located at Europol. At the European level, EC3's partners are the CERT-EU, CEPOL, Eurojust, ENISA, the EC, and ECTEG. A Memorandum of Understanding between EC3, EDA, 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. The EC3 also nominates representatives for ENISA AG together with Europol. It is involved in the TGG. Annually, Europol (through its EC3) and Interpol host a joint conference on cybercrime.[71]

70 Bundesamt für Sicherheit in der Informationstechnik, Nationales Koordinierungszentrum für Cybersicherheit (NKCS).
Council of the European Union, New Cybersecurity Competence Centre and network: informal agreement with the European Parliament.
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.
European Council, EU to pool and network its cybersecurity expertise – Council agrees its position on cybersecurity centres.
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.
Matthias Monroy, Neues EU-Kompetenzzentrum für Cybersicherheit bleibt umstritten.

71 European Agency for Cybersecurity, Ninth ENISA-EC3 Workshop on CSIRTs-LE Cooperation: standing shoulder-to-shoulder to counter cybercrime.
Europol, Cybercrime.
Europol, European Cybercrime Center – EC3.
Europol, EC3 Partners.
Europäischer Rechnungshof, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
Official Journal of the European Union, Recommendations Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.

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 Hybrid CoE focuses on the cyber domain and new options for hybrid activities in the gray area of the intersection of peace and war. It also addresses exploitation of the cyber realm and the emergence of new and disruptive technologies. The COI Strategy and Defense also comprises a workstrand on Cyber Power in Hybrid Warfare (CPH). Its main objective is to is to identify, raise awareness of, and address relevant strategic questions and issues regarding cyber power and the cyber domain in the context of hybrid conflicts and warfare. The work of the CPH workstrand also includes identifying potential stakeholders and contributors to create a network of experts, primarily from military, academia, and industry, on these issues and the organization of an annual "CPH Symposium".

The idea of establishing the Hybrid CoE was supported by the Council of the EU and the NAC. Together with the DG 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 EDA 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 ESDC. Germany is among the nine founding nations of the Hybrid CoE. It maintains connections with the BMVg, the KdoCIR, the BMI, and the AA at the German federal level. The Hybrid CoE is involved in the EU-HYBNET project, in which also ZITiS is engaged as a project partner.[72]

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

ECTEG 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. Representatives of Europol and CEPOL are part of the ECTEG Advisory Board. Further exchange exists with the ESDC. Germany's "Polizeiakademie Hessen" (Police Academy Hesse, own translation) and the "Hochschule

72 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.

Albstadt-Sigmaringen" (Albstadt-Sigmaringen University, official translation) are also involved as members.[73]

European Cyber Security Organisation (ECSO)

The European Cyber Security Organization was founded in Belgium as a non-profit organization to implement the expired Contractual Public Private Partnership on Cybersecurity (cPPP). 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. 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.

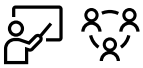
ECSO is a partner of the EC and maintains working relations with representatives from DG CONNECT, DG RTD, DG JRC, DG DIGIT, and the EEAS. At the invitation of the respective Council Presidency, ECSO is regularly invited to report on the status of its work to the HWPCI. ECSO is a member of the ECCG. There is also continuous cooperation with ENISA, Europol, CEN, CENELEC and EDA, among others. The BSI is also a member of the ECSO Board It cooperates with the ITU and has supported it, for example, in the creation of the GCI. ECSO also leads the strategic support activities for the development of the European Cyber Security Community (ECCO) under the ECCC Regulation.[74]

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.[75]

73 ECTEG, European Cybercrime Training and Education Group.
ECTEG, Members.
74 ECSO, About ECSO.
75 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.[76]

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.[77]

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, as well as with the EC. Based on a MoU, EJTN also cooperates with Eurojust, for example in the framework of an exchange program in which practicing judges and prosecutors are seconded to Eurojust.[78]

European Multidisciplinary Platform Against Criminal Threats (EMPACT)

EMPACT is a European initiative to identify and combat threats originating from organized and serious crime. Among other things, it aims to contribute to this aim by exchanging information or criminal intelligence, enhancing cooperation, and coordinating activities within the framework of EMPACT. EMPACT involves all EU member states, EU organizations, and when necessary, also third countries, international or-

76 European Judicial Network, About EJN.
European Judicial Network, Network Atlas.
77 Eurojust, European Judicial Cybercrime Network.
78 EJTN, About us.
Mail exchange with CEPOL representatives in August 2019.

ganizations, or other actors. Threats from cyberspace are one of the priorities of the EMPACT 2022–2025 cycle. For example, in the past, the takedown of Emotet or VPN providers were carried out within the framework of EMPACT.

EMPACT involves the EC, Europol, Eurojust, CEPOL, ENISA and eu-LISA on EU level, among others.[79]

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 the National Cybercrime Units of the Member States, representatives of CEPOL, the EC, Eurojust and Europol. Together with CEPOL, Eurojust, Europol and DG HOME, the meetings identify, discuss and prioritise challenges and actions in the fight against cybercrime. The EUCTF participates in the TGG together with ENISA, CERT-EU and EC3.[80]

Directorate-General Joint Research Centre (DG JRC)

The Joint Research Centre is subordinate to the European Commission. 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 DG RTD and ECSO. DG JRC is among the institutional stakeholders of the CEN. It is a participant of the CSCG. DG JRC takes part in the EU-HYBNET project, in which also ZITiS and an institute of UniBw are involved as project partners.[81]

79 Council of Europe, EMPACT Terms of Reference.
Council of Europe, General Factsheet — Operational Action Plans (OAPS): 2020 Results.
European Commission, EMPACT fighting crime together.
Europol, Coordinated action cuts off access to VPN service used by ransomware groups.
Europol, EU Policy Cycle – EMPACT.
Europol, World's most dangerous malware EMOTET disrupted through global action.

80 ENISA, Common Taxonomy for Law Enforcement and The National Network of CSIRTs.
Europol, EUCTF.

81 EU Science Hub, Information Society. (Website deleted)
EU Science Hub, JRC in brief.
EU Science Hub, Organisation.
EU Science Hub, Research Topics.

Directorate-General for Research and Innovation (DG RTD)

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.

In fulfilling its duties, DG RTD works together with inter alia DG CONNECT, DG HOME, DG JRC, and ECSO.[82]

Directorate-General for Informatics (DG DIGIT)

DG 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 DG CONNECT, the Director of DG DIGIT represents the European Commission in the Management and Executive Board of ENISA. A representative of DG DIGIT participates in meetings of the ECSO as well as ICTAC. CERT-EU is institutionally located at DG DIGIT. Together, they are working on an IT security program to protect the EC from cyber threats.[83]

Directorate-General for Communications Networks, Content and Technologies (DG CONNECT)

The Directorate-General for Communications Networks, Content and Technology is responsible for the development and implementation of EC policies in the areas of the digital economy ("digital single market") and society, as well as research and development. To this end, it promotes, among other things, selected "critical digital technologies" and strives for a European leadership position in the areas of data economy and cybersecurity.

DG CONNECT is the Directorate-General responsible for ENISA and represents it at Directorate-General level on the CERT-EU Board. Depending on the incident, DG CONNECT may be the lead service of the ERCC. Labour relations are in place with DG RTD and ECSO. The European Commission's proposal to establish the ECCC was prepared by DG CONNECT, which continues to support its work. GD CONNECT is one of the participants of the CSCG.[84]

82 European Commission, Strategic Plan 2016–2020: Directorate-General for Research and Innovation.
83 European Commission, Annual Activity Report: DG CONNECT.
European Commission, Informatics.
European Commission, Themenpapier: Herausforderungen für eine wirksame Cybersicherheitspolitik der EU.
84 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.

Directorate-General for Migration and Home Affairs (DG HOME)

DG 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, DG 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 DG 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 EEAS, and other relevant agencies (for example, Europol). Working relationships exist with eu-LISA, Europol, Interpol, and CEPOL, among others. DG HOME participates in the CSCG.[85]

Stakeholder Cybersecurity Certification Group (SCCG)

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 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. Members of the SCCG include CEN, CENELEC, ETSI, ISO, ITU, IEC, ECSO and the EA.[86]

Horizontal Working Party on Cyber Issues (HWPCI)

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.

85 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.

86 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).

The HWPCI is a preparatory body of the Council of the EU. It can, for example, prepare meetings of the PSC on a case-by-case basis. The HWPCI works with the EC, the EEAS, Europol, Eurojust, the EDA, and the ENISA. It also maintains cooperation with other working groups. The chair of the HWPCI is designated as a supporting participant of the JCU. ECSO regularly reports to the HWPCI on the 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.[87]

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 EDA. It is in permanent exchange with DG DIGIT, from which a representative also participates in ICTAC meetings.[88]

European Union Institute for Security Studies (EUISS)

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 EC, the EEAS, and with the respective governments of EU Member States. It is a member of the stakeholder community of the EU CyberNet. EUISS is supervised by the PSC.[89]

87 Council of the European Union, Establishment of a Horizontal Working Group on Cyber Issues.
European Council Rat, 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.

88 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.

89 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 of the European Union Military Staff (EUMS INT)

The Intelligence Directorate of the EU Military Staff consists mainly of national experts from EU Member States and is organizationally attached to the EEAS. Based on classified information from EU Member States or EU deployment areas, it provides military situation analyses and assessments for early warning, decision-making and planning of civilian and military operations within the framework of the Common Foreign and Security Policy. The EUMS INT thus contributes to the core tasks of the EUMS, early warning, situational awareness and strategic planning. The EUMS provides military expertise within the European External Action Service (EEAS).

EUMS INT is located within the EEAS 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.[90]

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 EEAS takes part in ISG C3M.[91]

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 EEAS and by the European Commission at Directorate-General or Deputy Secretary-General level. It receives quarterly reports from the EU Hybrid Fusion Cell.[92]

90 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.
European Parliament, Parlamentarische Anfragen: Antwort von Frau Catherine Ashton — Hohe Vertreterin/Vizepräsidentin im Namen der Kommission.
Raphael Bossong, Die nachrichtendienstlichen Schnittstellen der EU-Sicherheitspolitik.

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

92 Ibid.
Kristine Berzina et al., 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 EC has made a proposal to this end. The JCU is to reach its operational phase by June 2023 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 EC proposal envisages ENISA, Europol, CERT-EU, EEAS (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 EDA, and a representative of relevant PESCO projects.[93]

Critical Infrastructure Protection Contact Group (CIP Contact Group)

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 EC. 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.[94]

93 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.

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

NIS Cooperation Group

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. The BSI reports to the NIS Cooperation Group annually, for example, the number and type of security incidents reported.[95]

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 hosts the original MeliCERTes platform. This is currently being further developed by a consortium consisting of five national CERTs from EU member states in cooperation with ENISA.[96]

95 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.

96 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.

European Union Military Committee (EUMC)

The European Union Military Committee was established as a part of the EEAS. 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 PSC, 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 PSC 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.[97]

Political and Security Committee, (PSC)

The PSC 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 PSC 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 PSC is chaired by representatives of the EEAS. 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 PSC on the implementation of the EU Cybersecurity Strategy. The PSC is supervising the EUISS. The PSC meets regularly with the NAC and receives periodic briefings from the NATO Secretary-General (or deputy) and the SACEUR (ACO).[98]

Council of the European Union (Council)

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,

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

98 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.

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 several 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 EC 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 interior and justice ministries of all EU Member States, representatives of the EC and the EEAS. 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.[99]

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

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 TGG, inter alia, representatives of ENISA and EC3.[100]

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.[101]

Permanent Structured Cooperation (PESCO)
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. In the framework of PESCO, so-called Cyber Rapid Response Teams (CRRTs) were also created, coordinated by Lithuania and composed of cybersecurity experts from the six participating EU member states. CRRTs are designed to support EU member states, EU institutions, EU CSDP missions and operations, and certain partner countries in preventing and responding to IT security incidents.

The EEAS (incl. EUMS) and the EDA 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.[102]

100 ENISA, Building a common language to face future incidents – ENISA and European CSIRTs establish a dedicated task force.
ENISA, Reference Incident Classification Taxonomy.
101 SOGIS, Introduction.
102 Council of the European Union, EU-Politikrahmen für die Cyberabwehr (Aktualisierung 2018).
EEAS, Ständige Strukturierte Zusammenarbeit – SSZ.
PESCO, About PESCO.
PESCO, PESCO Secretariat.

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.[103]

Emergency Response Coordination Centre (ERCC)

The ERCC of the European Commission, housed within the Directorate-General for European Civil Protection and Humanitarian Aid Operations (DG ECHO), supports, and coordinates various activities in the areas of prevention, preparedness and response.

ERCC has functioned as both the EC's central crisis management agency and as the central EU integrated political crisis response (IPCR) 24/7 contact point. The ERCC can be deployed to "manage security incidents during a cybersecurity crisis" at the technical level in cooperation with other actors. The ERCC's lead service in this case would be DG CONNECT. In addition to EU Member States, the ERCC coordinates with the EEAS and the EUCO. If necessary, activation requests for the EU disaster and crisis management are being forwarded from Germany by the GMLZ to the ERCC.[104]

EU Intelligence Analysis Centre (INTCEN)

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 EEAS' crisis management structures alongside the Military Intelligence Directorate of EU Military Staff (EUMS INT) and the Crisis Management and Planning Directo-

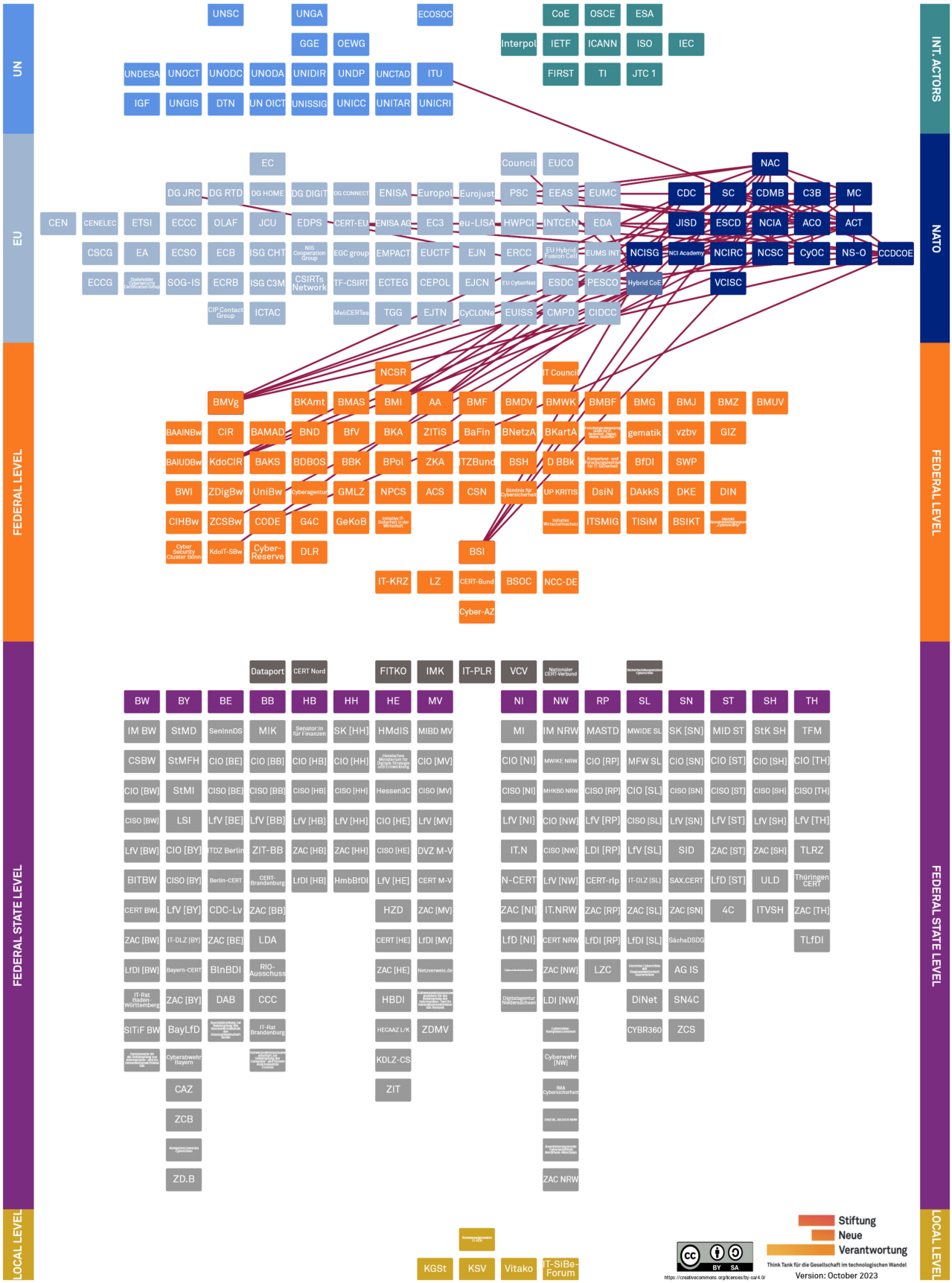
103 Europol, Common Taxonomy for Law Enforcement and The National Network of CSIRTs.
Rossella Mattioli und Yonas Leguesse, Reference Incident Classification Taxonomy Task Force Update.
104 Council of the European Union, Joint Staff Working Document EU: operational protocol for countering hybrid threats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

rate (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 EEAS. 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.[105]

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

7. Explanation – Actors at NATO Level



Policy Overview

Year	Name
2023	Vilnius Summit Communiqué
2022	Madrid Summit Declaration
2021	Brussels Summit Communiqué
2018	Brussels Summit Declaration
2016	Cyber Defence Pledge
2016	Warsaw Summit Communiqué
2014	Wales Summit Declaration
2012	Chicago Summit Declaration

Allied Command Operations (ACO)

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 on 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 cyber operations 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 PSC. [106]

106 NATO, Allied Command Operation.
NATO Public Diplomacy Division, Allied Command Operations.
SHAPE, Allied Command Operations overview: An introduction to the organisation and responsibilities. (Website deleted)

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 Education 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 EDA hold regular meetings.[107]

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.[108]

107 Allied Command Transformation, Who We Are.
Bundeswehr, Multinationale Interoperabilität testen – CWIX 2021.
Joint Force Training Centre, CWIX 2021 Execution.
NATO, Cyber defence.

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

Emerging Security Challenges Division (ESCD)

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. Within the ESCD, the Cyber and Hybrid Policy Section is responsible for issues related to cybersecurity. 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.

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 EEAS 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.[109]

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.[110]

109 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.

110 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.

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.

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.[111]

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. Subordinate to the KdoIT-SBw is the German part of the 1st NATO Signal Battalion, which is also part of the NCISG.[112]

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

112 Bundeswehr, CWIX 2021 findet als Remote Event statt.
NATO Communications & Information Systems Group, About us.
NATO Communications & Information Systems Group, Exercise STEADFAST COBALT 2021.
NATO Communications & Information Systems Group, Leadership.

NATO Computer Incident Response Capability (NCIRC)

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 relaying 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 information exchange and share best practices. Further cooperation exists at the working level between the NCIRC TC and the CERT-Bw. Requests to deploy RRT's must be granted by the CDMB for alliance states and by the NAC for non-NATO states. Experts of the RRT's participate in the cybersecurity exercises Cyber Coalition Exercise and Locked Shields.[113]

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.

113 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.

On the part of NATO, ACT handles the accreditation of the CCDCOE, which can also instruct the CCDCOE to perform specific tasks. 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 EDA, the EU Hybrid Fusion Cell, the ESDC, and the CODE at the University of the Bundeswehr. The CCDCOE maintains working-level contacts with eu-LISA. 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.[114]

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. Regarding 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.[115]

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.

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

115 NATO, Consultation, Command and Control Board (C3B).
NATO, Cyber defence.

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.[116]

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 representatives also exists under the umbrella of the NCSC. The NICP aims to improve cyber defense within the NATO supply chain, strengthen quick information pathways and exchange during cyber threats, and 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.[117]

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 in cases of cybersecurity incidents. CyOC is subordinate to the DCOS Cyberspace within the ACO and is located at SHAPE in Belgium.[118]

116 Jeffrey L. Caton, NATO Cyberspace Capability: A Strategic and Operational Evolution.
NATO, Cyber defence.
117 NCIA, Securing the Cloud.
NCIA, What We Do: NATO's Cybersecurity Centre.
NICP, Objectives and Principles.
118 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.

NATO Military Committee (MC)

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 strength and capability assessment of countries threatening NATO interests. The MC meets at least once a week at the level of nationally deployed military representatives as representatives of their respective Chief of Defence. The latter convene three times per year in the MC format.

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.[119]

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 are coordinated through the CCDCOE.[120]

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.

119 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.

120 NATO School, NATO School Oberammergau – Naval Postgraduate School Cyber Security Professional Programme Closure in Morocco.
NATO School, Organization.

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.[121]

NCI Academy

The establishment of the NCI Academy combined four previously separate NATO training institutions under the umbrella of the NCIA: NATO CIS School, Applications Training Facility The Hague, Air Command and Control Systems Training Centre, and SHAPE CIS Training Centre. The standardization of course 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.[122]

North Atlantic Council (NAC)

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 the 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

121 NATO, Security Committee (SC).
122 NCIA, About the NCI Academy.
NCIA, Introducing the NCI Academy.
NCIA, 10,000 Cyber Defenders: Cyber education for the NATO-EU workforce.

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 PSC 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 EEAS) has regularly participated in meetings of the NAC at the level of the defense ministers.[123]

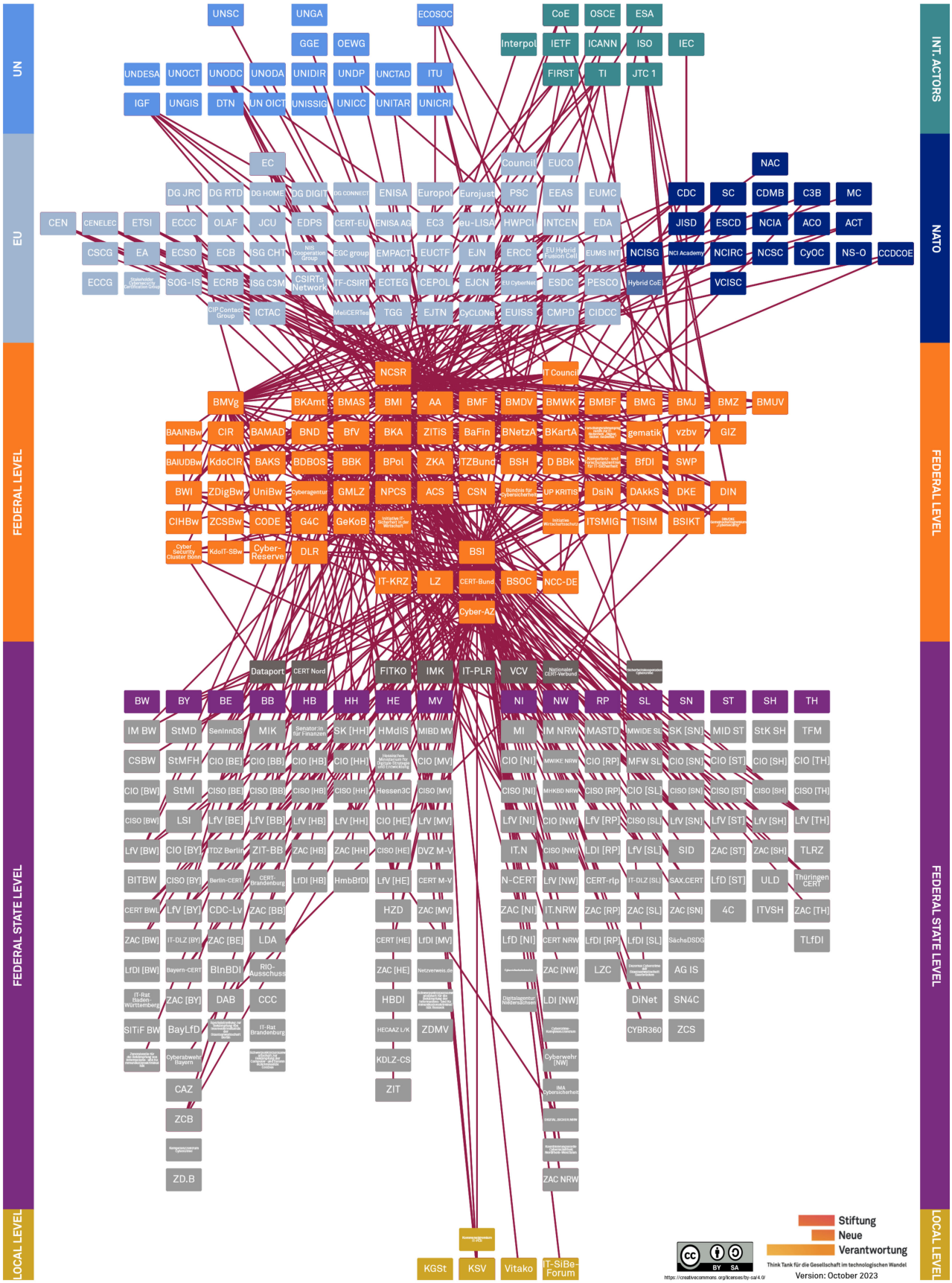
Virtual Cyber Incident Support Capability (VCISC)

The NATO has established the Virtual Cyber Incident Support Capability (VCISC) as part of the NATO Summit 2023 to provide member states with remote, location-independent support options for national damage limitation of severe, harmful cyber activities. In addition to specific expertise, technical support and training, the rapid exchange of information to strengthen effective responses to cyber incidents is paramount. In July 2023, the newly established VCISC was successfully tested for the first time. Participation in this capability is voluntary for alliance partners[124].

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

124 North Atlantic Treaty Organization, Cyber defence.
Spanisches Verteidigungsministerium, the joint cyberspace command takes part in the first NATO virtual cyber incident support capability organized by Lithuania.

8. Explanation – Actors at Federal Level



Policy Overview

Year	Name
2023	Nationale Sicherheitsstrategie (National Security Strategy, own translation)
2023	Agenda Cybersicherheitsforschung des Bundesministeriums für Bildung und Forschung. Maßnahmen im Zuge der Zeitenwende („Agenda for Cybersecurity-Research of the Federal Ministry of education and Research. Measures in the Wake of "Zeitenwende", own translation)
2022	Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Ziele und Maßnahmen für die 20. Legislaturperiode (in German, "Cybersecurity agenda of the Federal Ministry of the Interior and Community. Goals and measures for the 20th legislative period", own translation)
2022	Digitales Deutschland – Souverän. Sicher. Bürgerzentriert. Digitalpolitische Ziele und Maßnahmen bis 2025 des Bundesministeriums des Innern und für Heimat (in German, "Digital Germany – Sovereign. Secure. Citizen-centric. Digital policy goals and measures of the Federal Ministry of the Interior and Community up to 2025", own translation)
2022	Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (in German, "Regulation to ensure the IT security of the IT components used in the portal network and for connection to the portal network", own translation)
2022	Zweite Verordnung zur Änderung der BSI-Kritisverordnung (in German, "Second regulation amending the BSI-CRITIS-regulation", own translation) Previous documents: • 2016: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (in German, "Regulation on the designation of Critical Infrastructures according to the BSI Act", own translation)
2021	Cybersicherheitsstrategie für Deutschland (in German, "Cybersecurity Strategy for Germany", own translation) Previous documents: • 2016: Cyber-Sicherheitsstrategie für Deutschland (in German, "Cybersecurity Strategy for Germany", own translation) • 2011: Cyber-Sicherheitsstrategie für Deutschland (in German, "Cybersecurity Strategy for Germany", own translation)
2021	Digitalisierung gestalten. Umsetzungsstrategie der Bundesregierung (in German, "Shaping Digitization. Implementation Strategy of the German Federal Government, own translation)
2021	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (in German, Act on the Federal Office for Information Security, BSI Act, official translation)
2021	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (in German, "Law on the Federal Criminal Police Office and cooperation between the federal and federal state level in criminal police matters", own translation)
2021	Gesetz über den Bundesnachrichtendienst (in German, "Law on the Federal Intelligence Service", own translation)

Year	Name
2021	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (in German, "Law on the cooperation between the federal and federal state level in matters relating to the protection of the constitution and on the Federal Office for the Protection of the Constitution", own translation)
2021	Gesetz zur Anpassung des Verfassungsschutzrechts (in German, "Law on the adaptation of the constitutional protection law", own translation)
2021	Position Paper on the Application of International Law in Cyberspace
2021	Telekommunikationsgesetz (in English here, "Telecommunications Act", official translation)
2021	Telemediengesetz (in German, "Telemedia Act", official translation)
2021	Weißbuch Multilateralismus (in English here, "Federal Government White Paper. A Multilateralism for the People", official translation)
2021	Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (in German, "Second Law on increasing the security of information technology systems", own translation) Previous documents: • 2015: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (in German, "Law on increasing the security of information technology systems", own translation)
2020	Gesetz für ein Zukunftsprogramm Krankenhäuser (in German, "Law for a future program for hospitals", own translation)
2020	Non-Paper on EU Cyber Diplomacy by Estonia, France, Germany, Poland, Portugal and Slovenia
2018	Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung (in German, "Guideline for information security in public administration", own translation)
2017	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (in German, "Law to improve online access to administrative services", own translation)
2017	Umsetzungsplan Bund 2017: Leitlinie für Informationssicherheit in der Bundesverwaltung (in German, "Federal Implementation Plan 2017: Guideline for information security in public administration", own translation)
2016	Digitale Strategie 2025 (in English here, "Digital Strategy 2025", official translation)
2016	Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr (in English here, "White Paper on German Security Policy and the Future of the Bundeswehr", official translation)
2014	Digitale Agenda 2014–2017 (in English here, Digital Agenda 2014–2017, official translation) • 2017: Legislaturbericht Digitale Agenda 2014–2017 (in German, "Legislation Report Digital Agenda 2014-2017", own translation)

Year	Name
2009	Nationale Strategie zum Schutz Kritischer Infrastrukturen (in English here, National Strategy for Critical Infrastructure Protection, official translation)
2005	Nationaler Plan zum Schutz der Informationsinfrastrukturen (in English here, National Plan for Information Infrastructure Protection, official translation) • 2007: Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen (in German, "Implementation Plan CRITIS of the National Plan for Information Infrastructure Protection", own translation)
1999	Eckpunkte der deutschen Kryptopolitik (in German, "Key elements of German encryption policy", own translation)

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. 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 an emerged as initiatives within the German government's "High-Tech Strategy 2025". 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.[125]

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

125 Andre Meister and Anna Biselli, Bundesrechnungshof bezweifelt Sinn der neuen Cyberagentur.
Bundesministerium des Innern, für Bau und Heimat, Cyberagentur des Bundes nach Halle/Saale und Leipzig.
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 the Interior and Community, Startschuss für die Cyberagentur.
Federal Ministry of Defence, Technologiesouveränität erlangen – die neue Cyberagentur.
Lina Rusch, Cyberagentur kommt – mit strengen Auflagen.

"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 among other things 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 its own communications network. The AA coordinates the federal government's national attribution process, which governs the attribution of responsibility for significant cyber operations of international origin.

The AA is represented in the NCSR. 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"). The AA is also involved in the BSOC Network and represented in the IT Council as well as the Administrative Board of the ITZBund. German offers of assistance within the GMLZ are coordinated in consultation with the AA and BMI. At the EU level, the AA is inter alia involved in HWPCI processes and discussions, part of the ESDC 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. Another AA representative is represented on the German IGF's (IGF-D) Steering Committee. The German Foreign Minister or the Head of the Permanent Representation of Germany to the Council of Europe represents Germany in the CoE Committee of Ministers. The AA is also the point of contact for requests for mutual legal assistance or extraditions by other contracting parties in the framework of the Budapest Convention. The AA also maintains the Permanent Mission of Germany to the OSCE.[126]

126 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).
German Bundestag (Drucksache 20/1657), Unterrichtung durch die Bundesregierung Bericht der Bundesregierung zum Stand der Bemühungen um Rüstungskontrolle, Abrüstung und Nichtverbreitung sowie über die Entwicklung der Streitkräftepotenziale (Jahresabrüstungsbericht 2021).

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. Department 25 of the BfDI deals with technical data protection and is also responsible, among other things, for advising, raising awareness, and educating, especially federal public agencies, on the use of information technology in a technically adequate and legally compliant manner. In the past, the BfDI has also issued statements on planned legislative proposals such as the IT Security Act 2.0 or a hearing of the Bundestag's Interior Committee on the right to encryption. 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 EDPS exist.[127]

Bundeskanzleramt (Federal Chancellery, BKAmt, official translation)

The BKAmt supports the Federal Chancellor in his or her substantial work. 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 SWP.

The BKAmt is represented in the NCSR. The BND is subordinate to the BKAmt. The IT Council is chaired by the head of the Federal Chancellery and the CIO Bund. The BKAmt is also represented on the Administrative Board of the ITZBund. The head of the BKAmt takes note of the activity report of the IT-PLR. 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 the INTCEN. It is represented on the Board of Trustees of the BAKS.[128]

127 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, Stellungnahme an den Deutschen Bundestag zum IT-Sicherheitsgesetz 2.0.
Federal Commissioner for Data Protection and Freedom of Information, Stellungnahme zur öffentlichen Anhörung des Innenausschusses zum Thema „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken".
Federal Commissioner for Data Protection and Freedom of Information, 28. Tätigkeitsbericht zum Datenschutz 2019.

128 Federal Chancellery, Chef des Bundeskanzleramtes. (Website deleted)

- **Bundesnachrichtendienst (Federal Intelligence Service, 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 communications and electronic intelligence work is 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 services provided by ZITiS. If necessary to prevent or investigate activities that compromise the security or use of information technology, the BND can be supported by the BSI. Its staff is trained at the UniBw München, among others. The BND receives products from the EUMS INT and contributes reports to the INTCEN.[129]

Bundesministerium der Justiz (Federal Ministry of Justice, BMJ, official translation)
The BMJ is, first and foremost, a legislative ministry that supports other federal ministries in their legislative ambitions.

The BMJ is represented in the NCSR and the BAKS' Board of Trustees. It is also represented in the IT Council, the Administrative Board of the ITZBund, as well as the Advisory Board of CODE. Representatives of the BMJ have participated in meetings of the IEG Cybercrime (UNODC) as well as the CCPCJ (ECOSOC) at the UN level. Representatives of the BMJ participate in discussions of the CoE's Cybercrime Convention Committee (T-CY). It funds 97 percent of the vzbv's core work.[130]

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

129 Federal Intelligence Service, Cybersicherheit.
Federal Intelligence Service, Die Arbeit.
Heinz Fromm, Stellungnahme zur Vorbereitung der öffentlichen Anhörung am 17. Mai 2018 zum Thema „Föderale Sicherheitsarchitektur".
Kurt Graulich, Sicherheitsrecht des Bundes –Recht der Nachrichtendienste in Deutschland. (Website deleted)

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

data centers of the Bundeswehr. Within the ministry, the Chief Information Security Officer Bundeswehr (CISOBw) in the Cyber/IT (CIT) department is responsible for this. The Bundeswehr is subordinate to the BMVg, which 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.

The BMVg is represented in the NCSR. The Bundeswehr (Bw) along with the BAMAD, BAAINBw, BAIUDBw, KdoCIR, KdoIT-SBw, ZDigBw, ZCSBw, UniBw and CODE are subordinate to the BMVg and the BAKS falls within its purview. The Bw trains parts of its personnel at the UniBw (incl. CODE). The Bundeswehr participates in the ACS and will also participate in the GeKoB. The BMVg is represented on the IT Council and the Administrative Board of the ITZBund. The Military Cyber Reserve supports the Bundeswehr's performance of tasks. Within the Bundeswehr, the BAMAD analyzes and identifies extremist as well as espionage efforts, among other things. Germany is represented in the NATO MC by representatives of the Bundeswehr. The BAAINBw supplies the Bundeswehr with IT and digitalized weapon systems. The BWI operates as the Bundeswehr's IT system house. The Cyberagentur has been set up under the joint leadership of the BMVg and BMI. The BMVg is involved in the NCC-DE. The BMVg receives the situation analysis of the cyber and information domain via KdoCIR's operation center. 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 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 ESDC'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. The Bundeswehr participates in the Cyber Coalition Exercise organized by the ACT as well as Locked Shields organized by the CCDCOE.[131]

131 Bundeswehr, Amtshilfe in Bitterfeld – IT-Soldaten im zivilen Einsatz.
Bundeswehr, Auftrag und Aufgaben der Bundeswehr.
Bundeswehr, Das Kommando Cyber- und Informationsraum.
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.

- **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's leadership and project directors are supported by a "CISO Rüstung" (CISO Armament, own translation).

  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 managing 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 CISOBw, and the BAAINBw.[132]

  – **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 the BWI for the Bw. 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 work for the BWI.

    BWI GmbH is a state-owned company and IT system house for Bw (BMVg) 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 has concluded a memorandum of understanding with the BSI for increased cooperation. In this context, the BWI has also joined the BSOC Network. It is a multiplier of the ACS. The CERT of the BWI is represented in the National CERT Network, certified at TI, and involved in FIRST.[133]

132 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 Ministry of Defence, Zentrale Dienstvorschrift Informationssicherheit (A-960/1).
Federal Office of Bundeswehr Equipment, Information Technology, and In-Service Support,, Das BAAINBw.

133 Bundesweite IT-Systemhaus GmbH, Cyber-Sicherheit: BSI und BWI wollen künftig enger zusammenarbeiten.
Bundesweite IT-Systemhaus GmbH, Unternehmensbroschüre.
Federal Ministry of Defence, Auf engere Kooperation geeinigt: Bundeswehr und BWI GmbH.

→ **Cyber Innovation Hub (Cyber Innovation Hub of the German Armed Forces, CIHBw, official translation)**
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 with civilians, especially on developing disruptive technologies for the Bw.

The CIHBw is a department within the BWI and therefore exists within an administration with a clear line of command. To avoid redundancies, the CIHBw exchanges information with the Cyberagentur[134].

- **Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr (Federal Office of Infrastructure, Environmental Protection and Services of the Bundeswehr, BAIUDBw, own translation)**
Within the framework of its "Infrastructure Department," the BAIUDBw is responsible for the corresponding requirements of the Bundeswehr in Germany, abroad, and in situations of deployment, among other things, by planning and operating properties. Considering the increasing digitization of building and property technology and Bundeswehr systems operationally dependent on it, BAIUDBw is also concerned with cyber security. Within BAIUDBw, a "CISO Infrastructure" advises the BAIUDBw's leadership and all divisions tasked with infrastructure on information security issues.

The BAIUDBw falls within the purview of the BMVg.[135]

- **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, which also address security policy challenges in the cyber realm.

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

134 Federal Government, Regierungspressekonferenz vom 2. Dezember 2019.
Federal Ministry of Defence, Cyber Innovation Hub.
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.
135 Bundeswehr, Das Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr.
Federal Ministry of Defence, Zentrale Dienstvorschrift Informationssicherheit (A-960/1).

is chaired by the Federal Chancellor. It includes representatives of all ministries represented on the Federal Security Council (AA, BMVg, BMF, BMJ, BMWK, BMZ, and the BKAmt). Representatives of the Bundeswehr 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 ESDC.[136]

- **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 counterintelligence 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. If necessary to prevent or investigate activities that compromise the security or use of information technology, the BAMAD can be supported by the BSI. It can draw on services provided by ZITiS. BAMAD receives reports from the INTCEN.[137]

- **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). To ensure rapid response capability, a "Speerspitze Cyber-Reserve" (spearhead cyber reserve, own translation) is being established, which can be activated, if necessary, at an early stage to provide support in the event of IT incidents in relation to the Bundeswehr or administrative assistance. Unlike other reserve units, the cyber reserve is meant to explicitly recruit civilian personnel and executives with IT expertise in addition to former Bundeswehr

136 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.
137 Federal Office for Military Counter-Intelligence, Über uns.
Federal Office for Military Counter-Intelligence, Aufgaben und Befugnisse.
Federal Ministry of the Interior and Community, Online Kompendium Cybersicherheit in Deutschland: Militärischer Abschirmdienst (MAD).

soldiers. Pooling these diverse backgrounds shall enable joint exercises between cyber specialists from authorities, society, and the 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 and the ZCSBw.[138]

- **Organisationsbereich Cyber- und Informationsraum (Cyber and Information Domain Service, CIR, official translation)**
  The Bundeswehr's Military Organization Area Cyber and Information Space (MilOrgBer) is responsible for the military domain of cyber and information space. It is the sixth military organization area of the Bundeswehr and comprises approximately 16,000 employees. CIR is responsible for protecting the Bundeswehr's IT infrastructure. In addition, it is responsible for the capabilities for reconnaissance and impact in cyberspace, the provision of geoinformation data to other units of the Bundeswehr, as well as the exchange with other institutions for security precautions. Since the "CIR 2.0" reform, it has bundled all the responsibilities and competencies of the Bundeswehr in the cyber and information space and is divided into 9 sub-areas.

  CIR is part of the Bw (BMVg) and is managed by the KdoCIR, which in turn is subordinate to the ZCSBw, KdoIT-SBw and the ZDigBw. In the past, CIR has exchanged information with the BBK on cooperation in Cyber-AZ. The CIR cooperates with DLR on various research projects [139].

  - **Kommando Cyber- und Informationsraum (Bundeswehr Communication and Information Systems Command, KdoCIR, official translation)**
    The KdoCIR leads the CIR. As the commando of the CIR, KdoCIR manages the cyber, IT, strategic reconnaissance, geographic information systems of the Bw, and its operative communications. The KdoCIR's operations center prepares a situation analysis of the cyber and information domain. 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 represent-

138 Benjamin Vorhölter, Cyber-Reserve: Dienstleister für die Bundeswehr.
Bundeswehr, Reservist im Cyber- und Informationsraum.
Federal Ministry of Defence, Cyber-Reserve: Bundeswehr öffnet sich für IT-Community.
Federal Ministry of the Interior and Community, Online Kompendium Cybersicherheit in Deutschland: RAG Cyber des VdRBw.
Reservistenverband, Die Cyber-Reserve geht neue Wege.

139 BBK [@BBK_Bund], BBK President @armin_schuster spoke today with Inspector #Cyber and #Informationsraum Vice Admiral Dr. Thomas Daum about the cooperation between @BBK_Bund... [Tweet].
Bundeswehr, mission of the CIR division.
Bundeswehr, CIR 2.0 – The CIR organisational area is being restructured.
Bundeswehr, "Dear hackers, we hereby cordially invite you...".

ative, who has overall responsibility for the information security of the Bw as Chief Information Security Officer (CISOBw). The CIR has a vulnerability disclosure policy (VDPBw), for which the CISOBw is responsible. In the context of the VDPBw, it seeks the active reporting of vulnerabilities in IT systems of the Bundeswehr by external parties.

Among other organizations, the ZdigBw, KdoIT-SBw and the ZCSBw fall within its purview. 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 KdoCIR's situation analysis is shared with the BMVg and the Cyber-AZ, among other actors. KdoCIR initiated the establishment of the CIDCC as a PESCO project. For Germany's participation in the NATO CWIX conducted by ACT, the KdoCIR acts as an 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 to its Cyber-Reserve are managed by KdoCIR.[140]

– **Kommando Informationstechnik-Services der Bundeswehr (Bundeswehr Communication and Information Systems Services Centre, KdoIT-SBw, official translation)**
The Bundeswehr Information Technology Services Command is responsible for the deployment and operation of the Bundeswehr's IT systems. It provides the IT infrastructure and services for the Bundeswehr in training, exercise and deployment, monitors the entire IT infrastructure and ensures the command capability of the units. It works with the ZCSBw, which provides expertise and personnel as well as emergency response in the event of incidents to ensure cybersecurity in the operation of the systems.

The KdoIT-SBw is integrated into the CIR and is subordinate to the KdoCIR. It is supported by the ZCSBw and, if the CSOCBw assesses it accordingly, can make adjustments to the entire IT system in response to cyberattacks. Subordinate to the KdoIT-SBw is the German part of the 1st NATO Signal Battalion, which is part of the NCISG.[141]

140 Bundeswehr, Auftrag des Organisationsbereichs CIR.
Bundeswehr, Kommando Cyber- und Informationsraum.
Bundeswehr, Multinational Interoperabilität testen – CWIX 2021.
BWI, Von Big Data bis KI – Bundeswehr und BWI starten zweite Ausbaustufe des Gemeinsamen Lagezentrums CIR.
Federal Ministry of Defence, FAQ: Cyber-Abwehr.
Federal Ministry of Defence, Lagezentrum Cyber- und Informationsraum im Pilotbetrieb.
Federal Office for Information Security, BSI Magazin 2020/01: Mit Sicherheit.
German Bundestag (Drucksache 19/2645), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.
141 Bundeswehr, Bundeswehr Information Technology Services Command.
Federal Ministry of Defence, Threats in Cyberspace.

– **Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber-und Informationsraum (Bundeswehr Centre for Software Expertise, ZDigBw, official translation)**
The ZDigBw bundles digitization tasks in the BMVg's area of responsibility. It is divided into nine competence centers, each of which covers different areas of content. Existing or upcoming IT projects (especially software projects) are to be centralized in ZDigBW for the entire BMVg division. The responsibility includes development, certification, verification, validation, integration and testing, as well as ensuring interoperability in NATO. The recycling of existing or completed projects as well as the procurement and in-house development will be part of the ZDigBw's portfolio in order to create a growing "construction kit" for various areas of application.

The ZDigBw is part of the CIR.[142]

– **Zentrum für Cyber-Sicherheit der Bundeswehr (Bundeswehr Cyber Security Center, ZCSBw, official translation)**
The ZCSBw is responsible for the information technology protection of Bundeswehr systems in Germany and abroad as well as in operational contexts. It pools expertise and personnel in this area and makes them available to the services and units involved in the IT infrastructure. The Bundeswehr Cyber Security Operations Centre (CSOCBw) is located in the ZCSBw, which assesses the situation in the event of cyber incidents and initiates any responses. It includes the CERTBw, from which it can dispatch incident response teams in response.

The physical operation of the IT systems is assigned to the KdoIT-SBw, which supports the ZCSBw in implementing any security measures in the IT system. The IT security measures in regular operation of the KdoIT-SBw build on the expertise of the ZCSBw. ZCSBw is part of the CIR and reports to the KdoCIR. The CSOCBw and the BSOC work together. Working-level liaisons exist between the CERTBw and the NCIRC TC. The cyber reserve supports the ZCSBw, among others. Personnel of the ZCSBw participate in ENISA advanced training programs[143].

• **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 include computer science, cybersecurity, information technology, mathematical engineering, and business informatics.

142 Bundeswehr, ZDigBw.
143 Bundeswehr, Zentrum für Cyber-Sicherheit der Bundeswehr.
Bundeswehr, Cyber-Security, wie die Bundeswehr ihre IT-Systeme schützt.
Bundeswehr, Zentrum für Cyber-Sicherheit der Bundeswehr.

UniBw provides scientific training for Bw personnel. 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. UniBwM conducts research together with DLR. 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 DG JRC[144].

– **Forschungsinstitut Cyber Defence (Cyber Defence Research Institute, CODE, own translation)**
CODE at the UniBw München was founded by the BMVg to develop technical innovations for the Bw and the Federal Government to protect data, software, and systems. For this purpose, CODE has established three research clusters dealing with cyber defense: smart data, AI, and machine learning, as well as quantum technology. Furthermore, this interdisciplinary, independent research institute is linked to the scientific training and education at the UniBwM. Every year, CODE holds an annual conference.

As part of the UniBwM, Bw personnel are also trained scientifically at CODE. CODE is involved in the NCC-DE. A representative of the BMVg sits on the CODE Advisory Board. It is in exchange with, among others, the Cyberagentur and the CCDCOE. The CODE is represented on the Advisory Board of DsiN.[145]

Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior 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, CIO Bund, official translation), who is also responsible for steering the "Bundes-IT" (Federal IT, own translation). Other divisions of the BMI's CI Department also deal with cybersecurity research, cybersecurity for the economy and society, and the cyber capabilities of German security agencies, especially the BfV and BKA.

144 University of the Bundeswehr München, Hintergrundinformationen.
University of the Bundeswehr Hamburg, Studium.
145 University of the Bundeswehr München, Beirat des Forschungsinstituts CODE.
University of the Bundeswehr München, Forschungsinstitut CODE.
University of the Bundeswehr München, Forschungsinstitut CODE. Unsere Mission.
University of the Bundeswehr München, Program to the Annual Meeting CODE 2021.

The BMI is represented in the NCSR, which the CIO Bund chairs. BPol, BKA, BSI, BfV, BDBOS, and BBK all fall within its purview. ZITiS was founded following a BMI decree. The BMI's CI Department assumes the subject-specific supervision of the BSI, the BDBOS, the ZITiS, as well as specific units of the BfV and BKA. It is also responsible supervising the DAkkS in matters relating to cybersecurity. The BMI is represented in the initiatives UP KRITIS, DsiN (Advisory Board), and the ACS. The BMI is involved in the NCC-DE. The NPCS can be traced back to an initiative of the BMI, which is continued by the BSI operatively. The BMI is responsible for the IT Council, which is chaired jointly by the head of the BKAmt and the CIO Bund. The CIO Bund also chairs the IT-PLR. The BMI is among the contracting authorities for the implementation of IT consolidation measures on the part of the ITZBund and is also represented on its Administrative Board. Representatives of the BMI are also represented on 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 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. German offers of assistance within the framework of the GMLZ are coordinated in consultation with the BMI and the AA. The establishment of the GeKoB is based on an agreement between the BMI and the authorities in the federal states responsible for the interior portfolio. The BMI receives reports from the INTCEN and is involved in the German representation in the HWPCI. The BMI is represented on the Management Board of eu-LISA. At the NATO level, it is represented in the SC and is engaged 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). A BMI representative is represented on the ICANN Governmental Advisory Committee.[146]

- **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 2023 will deal with the topic "Cyberangriff auf das Regierungshandeln" (Cyberattack on government action, own translation).

146 Federal Ministry of the Interior and Community, Cyber-Sicherheitsstrategie für Deutschland.
Federal Ministry of the Interior and Community, IT & Cybersicherheit.
Federal Ministry of the Interior 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.

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 use of the digital radio operated by the BDBOS. The GeKoB was established at the BBK, which also provides the GeKoB office. The BBK cooperates with the BSI to analyze the effects of risks relating to the availability of critical infrastructures.[147]

– **Gemeinsames Kompetenzzentrum Bevölkerungsschutz von Bund und Ländern (Joint Competence Center for Civil Protection of the Federal Government and the Federal States, GeKoB, own translation)**
The GeKoB shall improve coordination between actors in civil protection inter alia through intensified information exchange, the development of capabilities in the area of forecasting, and the support of federal and federal state political-strategic crisis teams. Thereby, the GeKoB seeks to contribute to the prevention of possible crises, intensified crisis management, and – depending on the prevailing situation or emerging dangers – a timely joint response, if required. The GeKoB is responsible for the "Gemeinsame Lagebild Bevölkerungsschutz" (Joint Situation Picture Civil Protection, own translation), prepared every two weeks. When necessary, the GeKoB can increase the number of personnel or ensure 24/7-operation depending on the situation.

The GeKoB was established at the BBK, which also provides the GeKoB's office. Its establishment is based on an agreement concluded between the BMI (for the federal government) and the authorities in the federal states responsible for the interior portfolio (including IM BW, StMI [BY], SenInnDS [BE], MIK [BB], MIBD MV, MI [NI], and IM NRW), who form the core of the competence center. Also, the Bundeswehr (BMVg) and the BPol will participate in GeKoB from the federal level. If necessary, other specialist authorities can also be involved. The leadership of GeKoB will alternate between the federal and federal state governments every two years. The strategic management of GeKoB falls under the responsibility of a steering committee in which the German federal government and the sixteen federal states are represented equally. The GeKoB cooperates and exercises together with the Cyber-AZ and the BNetzA. The GeKoB works closely with the GMLZ, with which it also ensures (together with

147 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.

the "KRITIS-Zelle" (Critical Infrastructure Cell, own translation)) the editorial supervision of the Joint Situation Picture Civil Protection.[148]

– **Gemeinsames Melde- und Lagezentrum von Bund und Ländern (Joint Information and Situation Centre of the Federal Government and the Federal States, GMLZ, official translation)**
The 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. In addition to its role in situation management and as a national point of contact, the GMLZ can also provide support in resource management and broker bottleneck resources, for example, in situations of large-scale events of relevance to the protection of the population, events across federal states or of national significance as well as significant disruptions to critical infrastructure, which could among other conceivable scenarios be caused by targeted cyber operations.

The BBK is represented in the GMLZ. Partners of the GMLZ include BPol, BKA, and the EC. It cooperates with the LZ. If necessary, the GMLZ forwards activation requests for EU disaster and crisis management to the ERCC. The GMLZ coordinates offer of assistance by Germany in consultation with the BMI and AA. The GeKoB works closely with the GMLZ, with which it also ensures (together with the "KRITIS-Zelle" (Critical Infrastructure Cell, own translation)) the editorial support of the Joint Situation Picture Civil Protection.[149]

• **Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, BSI, official translation)**
The BSI, as the central national body for information security, is responsible for strengthening the security of the Federal Government's information technology and ensuring the protection of government networks. To this end, it is authorized, among other things, to defend against corresponding threats and risks and to collect and analyze them. It also provides IT security products for federal institutions. Furthermore, it is the central reporting office for both federal author-

148 Federal Office of Civil Protection and Disaster Assistance, Das Gemeinsame Kompetenzzentrum Bevölkerungsschutz.
Federal Government, Das Gemeinsame Kompetenzzentrum Bevölkerungsschutz von Bund und Ländern.
Federal Ministry of the Interior and Community, Bund und Länder geben Startschuss für das Gemeinsame Kompetenzzentrum Bevölkerungsschutz.
Ministerium des Innern des Landes Nordrhein-Westfalen, Verwaltungsvereinbarung über die Errichtung des Gemeinsamen Kompetenzzentrum Bevölkerungsschutz.

149 Deutsches Zentrum für Luft- und Raumfahrt, Katastrophen- und Krisenmanagement.
Federal Ministry of the Interior and Community, Das Gemeinsame Melde- und Lagezentrum von Bund und Ländern.
Federal Office of Civil Protection and Disaster Assistance, Ressourcenmanagement.

ities as well as third parties and assumes the function as the central national office regarding the security of information technology of critical infrastructure, "Unternehmen im besonderen öffentlichen Interesse" (companies in the special public interest, own translation), or digital services. The BSI can issue respective target-group-specific warnings, for example, about security vulnerabilities, or recommend security measures and the use of specific security products. In addition, the BSI is responsible for cybersecurity certification. The BSI also defines security-related minimum standards for the federal government's information technology in consultation with the federal ministries, which must be implemented by federal government agencies, among others. Vis-à-vis ministries of the federal government, the BSI only acts on the "Grundlage wissenschaftlich-technischer Erkenntnisse" (basis of scientific-technical knowledge, own translation, cf. § 1 BSI Act). In order 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 and companies in charge of critical infrastructure. 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, has been established. Annually, the BSI publishes a "Lagebericht zur IT-Sicherheit in Deutschland" (Situation report on German IT security, own translation). The coalition agreement of the federal government envisages making the BSI more independent during the current legislative period.

The BSI falls under the purview of the BMI (subject-specific supervision by Department CI) and is involved in UP KRITIS. Among others, it hosts the Cyber-AZ, ACS, LZ, CERT-Bund, the Bürger-CERT and the BSOC and the CSN. The BSI acts as the single point of contact of the NCC-DE. It is a member of the NCSR. It is an advisory member of the AG InfoSic of the IT-PLR. The NPCS, originally an initiative of the BMI, is being continued by the BSI operatively. If necessary to prevent

or investigate activities that compromise the security or use of information technology, the BSI can support other agencies such as the police, law enforcement agencies, but also constitutional protection agencies (BfV and LfV's), the MAD or the BND. The BSI cooperates with the BBK to analyze the effects of risks on the availability of critical infrastructures. 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 involved in the VCV. Together with the ITZBund, 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. The technical rules for operational security of the BMAS are based on cybersecurity regulations and standards of the BSI. 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 BSH has signed an administrative agreement with the BSI to strengthen cybersecurity in maritime shipping. Likewise, a memorandum of understanding was concluded between the BSI and the BWI to enhance cooperation. The implementation framework of TIBER-DE of the D BBk was developed with the involvement of the BSI. 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 on the Steering Committee of the Initiative IT Security in the Economy. Within the framework of an administrative agreement, the BSI and the DAkkS have also agreed on increased cooperation, including a focus on accreditation procedures for cybersecurity tests. 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 NCSR also includes a representative of the BSI. The DLR created the "IT-Grundschutzprofil" for space infrastructures of the "IT-Grundschutz" compendium At the federal state level, the BSI cooperates or exchanges information with the IM BW, the IT.NRW, the LSI, the MASTD, the MIBD 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 has signed a cooperation agreement with the states of Lower Saxony (NI) and Saarland (SL) and is working with DiNet and CYBR360 in Saarland within this framework. Moreover, the BSI has concluded an agreement on the exchange of information and cooperation in information security matters with Dataport. The BSI's Berlin liaison office is in exchange

with the CDC-Lv. The BSI supports the IT-SiBe-Forum and has developed a basic IT protection profile for municipalities together with the KSV, among other things. Every two years, the BSI must submit certain information to the EC. It also reports annually to the NIS Cooperation Group, for example, on the number and type of security incidents reported. It cooperates furthermore with ENISA and the ECB, is represented on the ECCC Administrative Board on behalf of Germany, 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.[150]

– **Allianz für Cybersicherheit (Alliance for Cybersecurity, ACS, own translation)**
The ACS offers confidential exchange, networking, and event formats between its over 6,000 members and the BSI on cyber threats, protective measures, and incident management. Members also receive information such as current situation reports or warnings in the framework of an online information pool and can expand their cybersecurity competencies through free partner offerings. Any institution headquartered in Germany can become a member; the participation is complimentary. Members can also become involved in the ACS as partners or multipliers. The work of the ACS is accompanied by an advisory board, which also provides impetus to its future positioning.

The ACS is located in the BSI and was established as a public-private partnership between the BSI and Bitkom. 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, BMDV, BMWK,

150 Background Conversation, 2019.
Federal Government, Besserer Schutz vor Cyber-Angriffen.
Federal Office for Information Security, Auftrag.
Federal Office for Information Security, BSI und das Saarland rücken enger zur Stärkung der Cyber-Sicherheit zusammen.
Federal Office for Information Security, Bundesgesetzblatt Teil I Nr. 54, Jahrgang 2009, Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes.
Federal Office for Information Security, Themen.
Federal Office for Information Security, Vorfallsunterstützung.
Federal Office for Information Security, Zweitstandort der Bundesbehörde BSI entsteht in Freital. (Website deleted)
Federal Office of Justice, Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG).
German Bundestag (Drucksache 19/3398), Antwort der Bundesregierung auf die Kleine Anfrage: Nationale und internationale Kooperationen des Bundesamtes für die Sicherheit in der Informationstechnik.
Fabienne Tegeler, Angebote des BSI für Kommunen.
Lina Rusch, BSI bekommt KI-Ableger in Saarbrücken.
Sozialdemokratische Partei Deutschlands, BÜNDNIS 90/DIE GRÜNEN, Freie Demokratische Partei, Mehr Fortschritt Wagen: Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit.

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 MWIKE NRW, the SenInnDS, the SID, and the ZCB are members. The MI of Lower Saxony is involved in the ACS as multipliers. TISiM exchanges information with its project sponsors within the framework of the ACS. The ACS cooperates with DsiN.[151]

– **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 federal IT. These tools of operational cybersecurity, which 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 Network, own translation) has also been established to connect the BSI and federal IT service providers.

The BSOC is operated by the BSI and cooperates with the CSOCBw (ZCSBw). In addition to the BWI, the AA, BDBOS, and the ITZBund are part of the BSOC Network.[152]

– **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.

151 Federal Office for Information Security, 10 Jahre Allianz für Cyber-Sicherheit.
Federal Office for Information Security, Allianz für Cyber-Sicherheit.
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.
152 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.
Bundesweite IT-Systemhaus GmbH, Cyber-Sicherheit: BSI und BWI wollen künftig enger zusammenarbeiten.

The CERT-Bund is located in the BSI and cooperates with the LZ. If necessary, the IT-KRZ is established by the CERT-Bund and 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, the TF-CSIRT, FIRST, and accredited at TI.[153]

– **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.

The CSN is institutionally located within the BSI and linked to the ACS, which it complements with reactive propositions. The Saarland (SL) is a pilot region of the CSN.[154]

– **Nationaler Pakt Cybersicherheit (National Cybersecurity Pact, NPCS, own translation)**
The NPCS is intended to support the Paris Call for Trust and Security in Cyberspace as a German contribution, for which a national contribution is to be published annually. Its aim is to involve all groups relevant to society, manufacturers, suppliers, users, and public administration, in a national pact es-

153 Federal Office for Information Security, CERT-Bund.
Federal Office for Information Security, Nationale und internationale Zusammenarbeit.
CERT-Bund, Über CERT-Bund.

154 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.
Federal Office for Information Security, Saarland wird zweite Pilotregion des Cyber-Sicherheitsnetzwerks.

tablishing joint responsibility for digital security. As part of the pact, key players in German cybersecurity were collected in an online compendium, and a "gesamtgesellschaftliche Erklärung zur Cybersicherheit" (whole-of-society declaration on cybersecurity, own translation) was published.

The NPCS can be traced back to an initiative of the BMI and is continued operatively by the BSI. Part of the pact is the "Bündnis für Cybersicherheit" and the Cyberagentur.[155]

- **Nationales IT-Lagezentrum (National IT Situation Centre, LZ, own translation)**
  The LZ 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 and prepare recommendations for action. 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 findings of the LZ also make a long-term contribution to the work of the BSI, as they can be used to identify the need to adapt or update relevant measures or guidelines. Operators of critical infrastructures have a special contact person at the LZ.

  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. If necessary, the capacities and structures of the LZ also allow it to establish the IT-KRZ together with the CERT-Bund.[156]

- **Nationales IT-Krisenreaktionszentrum (National IT Crisis Response Center, IT-KRZ, own translation)**
  The IT-KRZ convenes as needed to respond to and manage serious cyber security incidents and IT-related crises. In such situations, the IT-KRZ undertakes case-specific analyses and assessments. Further measures can be taken on this basis. In addition, it also assumes a coordinating function between relevant or affected organizations. In terms of organization, the IT-KRZ is flexible

155 Federal Ministry of the Interior and Community, Gesamtgesellschaftliche Erklärung zur Cybersicherheit.
Federal Ministry of the Interior and Community, Nationaler Pakt Cybersicherheit.
Federal Ministry of the Interior and Community, Online Kompendium Cybersicherheit in Deutschland: Nationaler Pakt Cybersicherheit.

156 Federal Office for Information Security, Die Lage der IT-Sicherheit in Deutschland 2021.
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.

and can be composed in terms of quantity and expertise depending on the degree of escalation or the assessment of the situation.

If necessary, the IT-KRZ is established by LZ and CERT-Bund.[157]

– **Nationales Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung (National Coordination Centre for cybersecurity in industry, technology, and research, NCC-DE, official translation)**
The NCC-DE complements the tasks of the ECCC at EU level. It is embedded in a network of national coordination centers (NCCs) to be established in all EU member states, which is intended to simplify and increasingly coordinate investments in cybersecurity research and development within the EU across national borders and between different sectors. At the national level, the NCC-DE seeks to establish an information platform for interested parties, support networking among each other, and provide consulting opportunities. Primarily SMEs and start-ups will be addressed and involved as target group.

As a national counterpart, the NCC-DE complements the tasks of the ECCC at the EU level. The BMI, BMWK, BMBF, BMVg, DLR and CODE are involved in the NCC-DE. While the BMI is responsible for the overall coordination of the NCC-DE, the BSI assumes the function as the NCC-DE's single point of contact.[158]

- **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).

157 Federal Office for Information Security, Das Nationale IT-Krisenreaktionszentrum im BSI.
158 Federal Office for Information Security, Das Nationale Koordinierungszentrum für Cybersicherheit nimmt Arbeit auf.
Federal Office for Information Security, Nationales Koordinierungszentrum für Cybersicherheit (NKCS).
Federal Ministry of the Interior and Community, Nationales Koordinierungszentrum für Cybersicherheit (NKCS).

BDBOS falls under the purview of the BMI, and the CIO Bund 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. It is also involved in the BSOC Network.[159]

- **Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution, BfV, official translation)**
  The BfV investigates and observes how new technological possibilities are used, for example, by extremists, terrorists, or foreign intelligence services, to conduct espionage, disinformation, or to sabotage computer systems in Germany. This also includes the use of infrastructure hosted in Germany by foreign actors, which are used to conduct cyber operations against other foreign actors. Cyber operations with a criminal background are explicitly not among the BfV's portfolio of tasks. It seeks to defend public and private institutions against cyber operations in Germany and illuminate their origins. In addition to detection and prevention, the BfV's "Cyberabwehr" (cyber defense, own translation) also performs tasks to attribute cyber operations, for example, to a state or an APT group. 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 exchanged between the BfV, BND, and BAMAD, and there are mutual obligations to provide information. If necessary to prevent or investigate activities that compromise the security or use of information technology, the BfV can be supported by the BSI. It is represented in the Cyber-AZ as well as the "Initiative Wirtschaftsschutz" and relies on the expertise of ZITiS. It can make use 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

159 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.

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.[160]

- **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. In other cases, the respective police in the federal states are – in principle – responsible in the first instance. The BKA has established a new "Cybercrime" Department (CC), in which competencies are concentrated on tracking "Cybercrime im engeren Sinne" (cyber-dependent crimes, official translation). To this end, it conducts, among other measures, corresponding investigations and investigates cyber operations on federal entities and critical infrastructures. It also disrupts criminal networks and structures on the basis of which, for example, such cyber operations are carried out. The BKA also maintains a Quick Reaction Force (QRF), which can rapidly initiate initial criminal procedural measures. The BKA's CC Department is also home to the "Nationale Kooperationsstelle Cybercrime" (National Cybercrime Cooperation Center, NKC, own translation), which is responsible for cooperation between authorities and the private sector. To combat cybercrime, 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) Department. 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 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. The BKA

160 Federal Office for the Protection of the Constitution, Cyberabwehr.
Federal Office for the Protection of the Constitution, Cyberabwehr: Begriff und Auftrag.
Federal Office for the Protection of the Constitution, Akteure und Angriffsmethoden.
German Bundestag (Drucksache 19/2645), Antwort der Bundesregierung auf die Kleine Anfrage: Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien.

participates with ZITiS in the EC-funded project "OVERCLOCK". 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. The BKA's CC Department is also responsible for the management of the "Bund-Länder-Verbund der ZAC's" (Network of Central Contact Points for Cybercrime for the Economy of the Police Forces on the Federal Level and within the Federal States, own translation). 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. It also serves as Germany's National Central Bureau within Interpol. Representatives of the BKA have participated in meetings of the IEG Cybercrime (UNODC) at the UN level. The BKA assumes the role of Germany's 24/7 contact point envisaged within the CoE's Budapest Convention.[161]

- **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. For this purpose, the Federal Police can, for example, deploy the GSG 9 as a special unit for corresponding arrests within Germany. 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 use of the digital radio operated by the BDBOS. The

161 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, Abteilung „Cybercrime" (CC).
Federal Criminal Police Office, Cybercrime.
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 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.

CERT BPol is a guest of the CERT-Verbund. The BPol will participate in the GeKoB for the federal level, among others.[162]

- **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 in dialog formats. 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. It also provides an irregularly updated overview of national cybersecurity initiatives on the part of the state and the economy.

  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).[163]

- **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.

  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.[164]

162 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, GSG 9: Aufgaben im Inland.
Federal Police, Startseite.
Federal Police, Unterstützung anderer Bundesbehörden.
German Bundestag (Drucksache18/13555), Antwort der Bundesregierung auf die Kleine Anfrage: Aktuelle Situation und Ausrichtung der Bundespolizei.

163 Bundesverband der deutschen Industrie, Bündnis für Cybersicherheit: Industrie und Innenministerium intensivieren Kooperation.
Federal Ministry of the Interior and Community, Industrie und BMI etablieren Bündnis für Cybersicherheit.

164 Federal Office for the Protection of the Constitution, Initiative Wirtschaftsschutz.
Federal Office for the Protection of the Constitution, Initiative Wirtschaftsschutz. Das Informationsportal.

- **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 BMI is responsible for the IT Council. The IT Council is chaired by the head of the BKAmt and the CIO Bund. All federal ministries (including the AA, BMBF, BMDV, BMF, BMG, BMJ, BMVg, BMWK, BMAS, BMUV, and BMZ) are represented on the IT Council by their respective state secretaries responsible for IT.[165]

- **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, 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. ZITiS participates with the BKA in the EC-funded project OVERCLOCK. 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. Other project partners of the EU-HYBNET project include the Hybrid CoE, DG 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 constituted the establishment of a joint development center for the purpose of IT surveillance together with the BKA. ZITiS maintains exchanges with the Cyberagentur.[166]

165 Der Beauftragte der Bundesregierung für Informationstechnik, IT-Rat.
166 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 and Community, Online Kompendium Cybersicherheit in Deutschland: Zentrale Stelle für Informationstechnik im Sicherheitsbereich.
Florian Flade, Mysterium ZITiS. Was macht eigentlich die "Hackerbehörde"?.

Bundesministerium für Arbeit und Soziales (German Ministry of Labour and Social Affairs, BMAS, official translation)

The Federal Ministry of Labor and Social Affairs has departmental responsibility for labor market policy, labor law, protection and medicine, pensions and social security, the integration of people with disabilities, and labor and social jurisdiction. As part of its responsibility for occupational health and safety, it is also responsible for the cybersecurity of work equipment and systems requiring monitoring via the Ordinance on Industrial Safety and Health (BetrSichV). The BMAS obligates the operators of these facilities to keep them permanently resilient to occupational safety risks. Cybersecurity incidents must also be adequately prevented within this framework. Operators must assess cybersecurity risks as part of a risk assessment of their facilities and take appropriate protective measures. The risk assessment and any protective measures are regularly reviewed.

When issuing technical rules for operational security in the context of cybersecurity for the BetrSichV, the BMAS is guided by sets of rules and standards issued by the BSI. It is also represented on the IT Council.[167]

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 NCSR, the IT Council, as well as the Administrative Board of the ITZBund and supports the Competence and Research Centers for IT Security Research. It has launched the Research Framework Program on IT Security "Digital. Secure. Sovereign." and is supervising it. The BMBF is involved in the NCC-DE, with support from the DLR. 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. It was involved in the funding of the Cybersecurity Navigators, which was

167 Ausschuss für Betriebssicherheit, Technische Regel für Betriebssicherheit, TRBS 1115 Teil 1, Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen.
Bundesministerium für Arbeit und Soziales, Betriebssicherheitsverordnung.

developed by the DKE and others. In the context of Horizon Europe, the BMBF has a coordinating office and an initial information center for interested parties.[168]

Bundesministerium für Digitales und Verkehr (Federal Ministry for Digital and Transport, BMDV, official translation)

The BMDV 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 BMDV also develops crisis scenarios regarding possible cyber operations on digital infrastructure. The BMDV's Department for Digital and Data Policy also assumes responsibilities for European and international digital policy, among other issues. The Federal Government's Digital Strategy was being developed under the leadership of the BMDV.

The BSH falls within the BMDV's purview. It assumes subject-specific supervision over certain areas of responsibilities of the BNetzA. It is represented on the NCSR, the IT Council, as well as ITZBund's Administrative Board. The BMDV participates in the ACS and cooperates with DsiN. A representative of the BMDV is represented in the Steering Committee of the German IGF (IGF-D) and the ICANN's Governmental Advisory Committee. The ITU lists the BMDV and the BNetzA as participating member state institutions from Germany.[169]

- **Bundesamt für Seeschifffahrt und Hydrographie (Federal Maritime and Hydrographic Agency, BSH, official translation)**

  The BSH is responsible for, among other things, averting dangers to maritime waters and relevant surveying tasks. In the context of navigation and communication systems, the BSH's "Navigation Division" also deals with cyber risks and aims to contribute to the prevention of malicious cyber operations within its area of responsibility.

  The BSH falls within the purview of the BMDV and has signed an administrative agreement with the BSI to strengthen cyber security in maritime navigation.[170]

168 Federal Ministry of the Interior 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.

169 Federal Ministry for Digital and Transport, Krisenmanagement.
Federal Ministry for Digital and Transport, Organisationsplan des Bundesministerium für Digitales und Verkehr.

170 Federal Maritime and Hydrographic Agency, BSH unterzeichnet Vereinbarung zur Verbesserung der Cyber-Sicherheit auf See.
Federal Maritime and Hydrographic Agency, Leitung und Abteilungen.
Federal Maritime and Hydrographic Agency, Wir über uns.
Federal Office for Information Security, Mehr Cyber-Sicherheit auf See: BSI unterzeichnet Verwaltungsvereinbarung.

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 NCSR and the IT Council. 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 Board of Trustees of the BAKS, and the Foundation Board of the SWP. The establishment of the German counterpart to the ECB's TIBER-EU, TIBER-DE, is the result of a joint decision by the D BBk and the BMF.[171]

- **Bundesanstalt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority, BaFin, official translation)**
  The task of the 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 area of banking supervision, a dedicated directorate deals with IT supervision/ cyber security. Cyber risks are among the focus risks identified by the BaFin. The BaFin can, among other measures, carry out corresponding examinations at the institutions it supervises, for example, with regard to aspects of IT security and compliance with supervisory IT requirements.

  In the event of a cyber intrusion or malicious cyber activity, an exchange of information with the BSI takes place. BaFin falls under the purview of the BMF and is represented as a partner in the Cyber-AZ. The BaFin analyzes information from the Cyber-AZ daily. On this basis, the BaFin notifies the financial industry of any potential operational patterns. The implementation framework of TIBER-DE of the D BBk was developed with the involvement of the BaFin.[172]

- **Informationstechnikzentrum Bund (Federal Information Technology Centre, ITZBund, official 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

171 Federal Ministry of Finance, Grundelemente zur Cyber-Sicherheit. (Website deleted)
Federal Ministry of Finance, Themen.
172 Federal Financial Supervisory Authority, Aufgaben & Geschichte der BaFin.
Federal Financial Supervisory Authority, BaFinPerspektiven. Ausgabe 1 2020: Cybersicherheit.
Federal Financial Supervisory Authority, Jahresbericht der BaFin 2021.
Federal Financial Supervisory Authority, Organigramm der BaFin.
Federal Financial Supervisory Authority, Risiken im Fokus der BaFin.
Federal Financial Supervisory Authority, "Risiken im Fokus der Bankenaufsicht: Was tut die BaFin?".

to consolidate and bundle the Federal Government's IT capacities. The ITZBund's portfolio of tasks also includes ensuring and maintaining the highest possible level of IT security. In this context, the ITZBund provides the federal administration with the "Zentraler Dienst für Informationssicherheit" (Central Service for Information Security, ZeDIS, own translation), which enables them to implement their corresponding security concepts in accordance with "IT-Grundschutz" (IT basic protection, own translation) requirements. To this end, the ITZBund also coordinates closely with the BSI, for example, to strengthen the dissemination of security by design, inter alia in software used by the federal administration. It is also planned to set up a service for improved detection of cyber operations (Detection as a Service) for the federal administration in the framework of the "Bundescloud" (Federal Cloud, own translation).

The ITZBund falls under the purview of the BMF. The ITZBund's Administrative Board is composed of state secretaries from all federal ministries (including the AA, BMBF, BMDV, BMI, BMJ, BMUV, BMVg, BMWK, BMZ, and BKAmt) under the chairmanship of a state secretary from the BMF. The ITZBund is commissioned by the BMI and the BMF to implement measures towards the "IT-Konsolidierung Bund" (Federal IT Consolidation, own translation). The ITZBund and the BSI a "Lenkungskreis Informationssicherheit" (Steering Committee for Information Security, own translation) to create closer cooperation between both institutions. It also participates in the BSOC Network. The BfDI regularly reviews the data and information processing of the ITZBund. As part of a BMG grant, the ITZBund provides, among other things, data centers for the operation of SORMAS (Surveillance Outbreak Response Management and Analysis System), an IT solution for the identification and tracking of contacts in the context of the SARS-CoV-2 pandemic.[173]

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

  The ZKA is a specialized directorate within the "Generalzolldirektion" (General Customs Directorate, GZD, own translation), which is subordinate to the BMF and

173 Federal Information Technology Centre, ITZBund und BSI intensivieren Zusammenarbeit für mehr IT-Sicherheit.
Federal Information Technology Centre, IT-Sicherheit.
Federal Information Technology Centre, Organisation und Verwaltungsrat.
Federal Information Technology Centre, Über uns.
Federal Information Technology Centre, Unsere Kunden.
Federal Information Technology Centre, Zentraler Dienst für Informationssicherheit (ZeDIS).

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).[174]

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. This also includes the reform of the German healthcare system. 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's division dealing with cybersecurity and interoperability is responsible, among other issues, for the "Krankenhauszukunftsgesetz" (Hospital Future Act, official translation) and other healthcare-specific IT projects such as SORMAS. In the context of the Hospital Future Act, a dedicated "Krankenhauszukunftsfond" (Hospital Future Fund) is intended to improve the digital infrastructure of hospitals – at least 15 percent of the funding must be used to strengthen information security. In addition, the BMG also supports pilot projects addressing the implementation of IT security awareness programs in medical care facilities.

It is represented in the NCSR and the IT Council. The BMG has commissioned gematik to develop an electronic data transmission infrastructure, which is the prerequisite for secure interconnection of the health care system. Within the framework of a BMG grant, the ITZBund provides, among other things, data centers for the operation of SORMAS.[175]

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (Federal Ministry for the Environment and Consumer Protection, BMUV, official translation)

Within the federal government, the BMUV is also responsible for consumer protection, which includes digital consumer protection. In this context, a division in the corresponding department also deals with cybersecurity issues and trustworthy artificial intelligence. Digital consumer protection also includes topics such as the protection of consumers from fake sales platforms or dark patterns on the Internet, as well as consumer data protection.

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

175 Federal Ministry of Health, Aufgaben und Organisation.
Federal Ministry of Health, E-Health-Gesetz.
Federal Ministry of Health, Öffentliche Bekanntmachung des Bundesministeriums für Gesundheit (BMG) zum Thema „Förderung von Vorhaben zur Umsetzung von IT-Security–Awareness-Programmen in Einrichtungen der medizinischen Versorgung".
Wegweiser, Thomas Süptitz (BMG).

The BMUV is represented in the NCSR, the IT Council, and the Administrative Board of the ITZBund.[176]

Bundesministerium für Wirtschaft und Klimaschutz (Federal Ministry for Economic Affairs and Climate Action, BMWK, official translation)
The BMWK 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 and the cybersecurity of medium-sized businesses.

The BMWK is represented in the NCSR, the IT Council, and the Administrative Board of the ITZBund and participates in the NCC-DE with the support of the DLR. Operationalized via the DLR, it is responsible for the German ESA participation. It is also involved in the NCC-DE. 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. Representatives of the BMWK 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 BMWK funds the KITS of the DIN. The BMWK chairs the BSIKT and provides its office. The BSIKT can act in an advisory capacity vis-à-vis the BMWK. The BMWK can participate in meetings of the MAG of the IGF and supports the IGF Trust Fund financially. A representative of the BMWK 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 BMWK's purview, chairs the UNECE's Working Group 6 (ECOSOC).[177]

- **Beirat für Standardisierung in der Informations- und Kommunikationstechnologie (Advisory Board for Standardization in Information and Communication Technology, BSIKT, own translation)**
  The BSIKT is composed of accredited experts from public authorities, science, industry, and associations. Its objective is to develop common positions on essential and strategic issues of standardization in information and communication technologies.

176 Federal Ministry for the Environment and Consumer Protection, Die digitale Souveränität von Verbraucherinnen und Verbrauchern stärken.
Federal Ministry for the Environment and Consumer Protection, Digitaler Verbraucherschutz.
Federal Ministry for the Environment and Consumer Protection, Organigramm.
177 Federal Ministry for Economic Affairs and Climate Action, Cybersicherheit im Mittelstand.
Federal Ministry for Economic Affairs and Climate Action, IT-Sicherheit.
Federal Ministry for Economic Affairs and Climate Action, IT-Sicherheit für die Industrie 4.0.

The BSIKT can act in an advisory capacity towards the BMWK and the BNetzA. It deals with developments in national, European, and international standardization organizations/bodies, including DIN, DKE, ETSI, CEN, CENELEC, ITU, ISO, IEC, ISO/IEC JTC1, or the IETF. The BSIKT is chaired by the BMWK, which also provides the BSIKT office.[178]

- **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, regarding 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 BMWK. BKartA and BSI cooperate in the area of digital consumer protection. It is also a member of the ACS.[179]

- **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. The BNetzA publishes security requirements for all network providers and operators of energy facilities in the electricity and gas sector, which have been designated as critical infrastructures in accordance with the "BSI-Kritisverordnung" (Regulation on the designation of Critical Infrastructures according to the BSI Act, own translation). The requirements are prepared in line with Section 11 (1a) and (1b) of the "Energiewirtschaftsgesetz" (Energy Industry Act, official translation). Furthermore, the BNetzA verifies compliance with the requirements.

  The BNetzA falls under the purview of the BMWK. The BMDV assumes subject-specific supervision over certain of its areas of responsibilities. The BNetzA prepares the requirements in accordance with §11 (1) a and b of the Energy Industry Act in consultation with the BSI. The BSIKT can, among other things, act in an advisory capacity vis-à-vis the BNetzA. The ITU lists the BNetzA as a participating German member state institution.[180]

178 Federal Ministry for Economic Affairs and Climate Action, Standards und Wettbewerb.
Federal Ministry for Economic Affairs and Climate Action, Geschäftsordnung des Beirates für Standardisierung in der Informations- und Kommunikationstechnologie (BSIKT).
German Bundestag (Drucksache 20/1667), Antwort der Bundesregierung auf die Kleine Anfrage: Einführung des Mobilfunkstandards neuer Generation (6G).

179 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.

180 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.

- **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 BMWK 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 BMWK, the BSI, and the DsiN. The latter was established as part of the initiative[181].

  – **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 BMWK. 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 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.[182]

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.

The BMZ is represented in the NCSR, the IT Council, as well as the Administrative Board of the ITZBund. It 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.[183]

181 Federal Ministry for Economic Affairs and Climate Action, Erste Berufsschulen in Niedersachsen setzen auf Bottom-Up für mehr IT-Sicherheit im Mittelstand.
Federal Ministry for Economic Affairs and Climate Action, Steuerkreis.

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

183 Federal Ministry for Economic Cooperation and Development, Digitalisierung in der Entwicklungszusammenarbeit.
Federal Ministry for Economic Cooperation and Development, Grundsatzfrage: Warum brauchen wir Entwicklungspolitik?.

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 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 activities include digital communication and services, such as the protection of privacy in digital space, net neutrality, and copyright law. In the area of IT security, it inter alia calls for a legal obligation for "security by design" as well as "security by default" and comments on legislative proposals at both the national and European levels.

As much as 97% of the core work of the vzbv is financed by the BMJ. The vzbv and the BSI have a general agreement regarding their cooperation.[184]

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, the BfDI, and the IM NRW 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.[185]

184 Federal Ministry of Justice, Verbraucherzentralen.
Federal Office for Information Security, BSI und Verbraucherzentrale stärken digitalen Verbraucherschutz.
Verbraucherzentrale Bundesverband, Häufige Fragen (FAQ). (Website deleted)
Verbraucherzentrale Bundesverband, IT-Sicherheit.
Verbraucherzentrale Bundesverband, IT-Sicherheit für vernetzte Geräte und digitale Dienste. Vorschläge des Verbraucherzentrale Bundesverbandes zur Konsultation zu einem europäischen Gesetz über Cyberresilienz.
Verbraucherzentrale Bundesverband, IT-Sicherheit im Verbraucheralltag stärken. Stellungnahme zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0) in der Fassung vom 16. Dezember 2020.
Verbraucherzentrale Bundesverband, Über Uns.

185 Federal Office for Information Security, Liste von Multiplikatoren der Allianz für Cyber-Sicherheit.
Cyber Security Cluster Bonn, Über uns.
Cyber Security Cluster Bonn, Wechsel im Beirat des Vereins.
Cyber Security Cluster Bonn, Weisenrat für Cyber-Sicherheit.
Email exchange with representatives of the Cyber Security Cluster Bonn in November 2019.

Deutsche Bundesbank (D BBk)

As Germany's central bank, the Deutsche Bundesbank inter alia works in the area of monetary policy as well as banking supervision, and to ensure the stability of the financial and monetary system. The Bundesbank also performs functions to strengthen the resilience of key financial market infrastructures and relevant other actors against threats from cyberspace. To this end, the Bundesbank has, among other things, implemented the European framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU) at the German level (TIBER-DE). For this purpose, a national competence center (TIBER Cyber Team, TCT) has been established at the Bundesbank's General Payments and Settlement Systems Directorate, which supports companies in conducting a voluntary TIBER-DE test.

The D BBk is supervised by the ECB, and the President of the D BBk is a member of the ECB's Governing Council. The establishment of TIBER-DE is based on a joint decision with the BMF. The implementation framework of TIBER-DE was developed with the participation of the BaFin and the BSI. The D BBk participates in meetings of the ECRB.[186]

Deutsche Akkreditierungsstelle (German Accreditation Body, DAkkS, official 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 concerning the realms of cybersecurity and IT security.

The Federal Republic of Germany (represented by the BMWK), the federal states of Bavaria, Hamburg, and North Rhine-Westphalia are shareholders of the DAkkS. The supervision of the DAkkS in matters relating to cybersecurity is assumed by the BMI. In addition to members from industry and representatives of the federal states, the DAkkS Supervisory Board also includes representatives of the BMWK and BSI. Within the framework of an administrative agreement, the BSI and the DAkkS have also agreed on increased cooperation, including a focus on accreditation procedures for cybersecurity testing. The DAkkS is a member of the EA.[187]

186 Deutsche Bundesbank, Implementierung von TIBER-DE.
Deutsche Bundesbank, TIBER-DE macht das deutsche Finanzsystem sicherer.

187 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. Also, one representative of the GIZ is a member of the IGF's MAG.[188]

Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (German Commission for Electrical, Electronic & Information Technologies of DIN and VDE, DKE, official translation)
As a competence center for electrotechnical standardization, the DKE also works on agreeing standards in the field of information technology in order to contribute to improved interoperability as well as standardization of systems and networks, among other things. With regard to cyber and information security, these are also intended to increase the general internal as well as external security level and thereby reduce potential dangers. The DKE was involved in the development of a *Cybersecurity Navigator*, which aims at facilitating the search for relevant legal regulations and corresponding norms and standards in the form of a database.

The DKE is the German member of IEC, CENELEC, and ETSI. It coordinates with DIN in the framework of the DIN/DKE Joint Committee "Cybersecurity". The Cybersecurity Navigator is funded, among others, by the BMBF. DKE-related developments are also dealt with in the BSIKT.[189]

Deutsches Institut für Normung (German Institute for Standardization, DIN, official translation)
As Germany's standardization organization, DIN also established a "Koordinierungsstelle IT-Sicherheit" (IT Security Coordination Office, KITS, own translation). Among other things, the KITS performs coordination and advisory tasks and organizes an annual conference. In the past, DIN has also taken a stance on European legislative projects and has, for example, published a statement on the EU Cybersecurity Act or the NIS 2 Directive.

188 Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH, Bundesregierung.
Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH, Startseite.
189 Background Conversation, 2018.
Cybersecurity Navigator, Research.
German Commission for Electrical, Electronic & Information Technologies of DIN and VDE, Cybersecurity Navigator bietet Rechtsvorschriften und Standards für Kritische Infrastrukturen an.
German Commission for Electrical, Electronic & Information Technologies of DIN and VDE, Organisation.
German Commission for Electrical, Electronic & Information Technologies of DIN and VDE, Sichere und innovative Informationssysteme.
German Commission for Electrical, Electronic & Information Technologies of DIN and VDE, Über Uns.

DIN is the German member of CEN and ISO. The CSCG secretariat is located at DIN, which also participates in the CSCG on behalf of Germany. DIN also provides the secretariat of ISO/IEC JTC 1/SC 27. Together with the DKE, the DIN/DKE Joint Committee "Cybersecurity" exists at the German level. DIN-related developments are also dealt with in the BSIKT. It is among the network partners of the DAB. The KITS is funded by the BMWK.[190]

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. Every year, DsiN publishes a security index that examines the digital security situation of German Internet users as a representative study. It is based on four security factors: the threat situation (security incidents and feelings of insecurity) and the level of protection (security knowledge and security behavior). DsiN also implements the "Politiker:innen sicher im Netz" (Politicians Secure in the Internet, own translation) project, which implements lectures and workshops for politicians and employees on various political levels.

The BMI, BMWK, BMJ, BSI, BKA, BfDI, and CODE are represented on the DsiN Advisory Board. The Federal Minister of the Interior assumes the patronage over the DsiN. The DsiN is funded by the BMI and BMWK. DsiN cooperates with "Initiative IT-Sicherheit in der Wirtschaft. Other cooperations exist, among others, with the ACS, the BMDV, the BMJ, the BKA, the BSI as well as the StMD [BY]. It leads the consortium of TISiM.[191]

DIN/DKE Gemeinschaftsgremium "Cybersecurity" (DIN/DKE Joint Committee "Cybersecurity", own translation)

The Joint Committee pools German activities in the field of cybersecurity standardization and consolidates a German position for standardization undertakings at the European level.

As a "nationales Spiegelgremium" (national mirror committee, own translation), the Joint Committee of DIN and DKE coordinates and steers, for example, the German participation in the CEN/CENELEC JTC 13 and the TC Cyber of ETSI.[192]

190 German Institute for Standardization, Gesetze und Normen zur Cybersicherheit.
German Institute for Standardization, Koordinierungsstelle IT-Sicherheit.
German Institute for Standardization, Statement on the Proposal for Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS 2).
191 Deutschland sicher im Netz, DsiN Sicherheitsindex 2022.
Deutschland sicher im Netz, Politiker:innen sicher im Netz (PolisiN).
Deutschland sicher im Netz, Presse.
Deutschland sicher im Netz, Über Uns.
192 German Institute for Standardization, Cybersecurity: DIN und DKE gründen Gemeinschaftsgremium.

Deutsches Zentrum für Luft- und Raumfahrt (German Aerospace Center, DLR, official translation)

The German Aerospace Center conducts research and development in aeronautics, space, energy, transport, security and digitization on behalf of the Federal Republic of Germany. As part of this mission and thematic areas, DLR conducts research on a wide range of cybersecurity projects on behalf of the government. This includes both civilian and military projects. DLR hosts the German Space Agency, which is responsible for planning and implementing German space activities. This results in a focus on the cyber security of space infrastructures. Through so-called DLR project executing agencies, DLR assumes management for various government research and funding projects of the federal government, including extensive cybersecurity projects.

DLR participates in the NCC-DE on behalf of the BMWK and the BMBF. In addition, there are links with BMI and BMDV. There is close cooperation with the BSI, DLR prepared the "IT-Grundschutzprofil" for space infrastructures of the "IT-Grundschutz" compendium. DLR works closely with the Bundeswehr (BMVg) in the areas of cyber security, space, aeronautics, earth observation, communications and navigation, and increasingly with CIR and UniBW. As the German space agency, there are extensive links with ESA.[193]

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 brings 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.

193 Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium-Edition2023.
Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzprofil für Weltrauminfrastrukturen.
Deutsches Zentrum für Luft- und Raumfahrt, Cyber-Sicherheit.
DLR-Projektträger, Cyber-Sicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G.
Deutsches Zentrum für Luft und Raumfahrt, DLR und Inspekteur des Cyber- und Informationsraums der Bundeswehr tauschen sich zu sicherheitsrelevanten Themen aus.

The research framework program was introduced by the BMBF and is being supervised by it.[194]

Föderale IT-Kooperation (Federal IT Cooperation, FITKO, own translation)
The FITKO was established as a coordination and networking body for digitization projects of the German public administration. Its purpose is to pool competencies and resources to advance the digitization of public administration in coordination with the IT Planning Council and cooperation with other stakeholders – for example, by promoting collaboration between all federal levels and developing new implementation strategies. FITKO's tasks also include providing strategic and organizational support to the IT Planning Council and its committees, managing its projects and products as well as their operational implementation, and managing the joint digitization budget of the federal level and federal states. The FITKO has also been mandated by the IT Planning Council to develop and refining the "föderale IT-Architektur" (federal IT architecture, own translation), for example, to increase the dissemination of common standards.

The FITKO is an independent institution established under public law borne by all federal states (BW, BY, BE, BB, HB, HH, HE, MV, NI, NW, RP, SL, SN, ST, SH, and TH) and the federal government. FITKO is the operational substructure of the IT-PLR, and the president of FITKO is an advisory member of the IT-PLR. A municipal committee of the IT Planning Council was established in 2020 under the chairmanship of FITKO. The FITKO is a member of the IT-PLR's AG InfoSic.[195]

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. The gematik operates its own CERT (gematik CERT).

194 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.

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

gematik is supported by various shareholders. The BMG, for example, holds 51% of the shares. Its Advisory Board includes, among others, a representative of the BfDI, as well as the BSI and the BMWK. The gematik CERT is listed as a participating team at TI.[196]

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 a daily exchange of information between official cooperation partners and members.

The G4C cooperates with the BKA and the BSI.[197]

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. Among others, the ministers of the IM BW, the StMI [BY], the MIK [BB], the MIBD MV, the MI [NI], the IM NRW as well as the senator of the SenInnDS [BE] participate in the IMK on behalf of the federal states. On a regular basis, the IMK receives reports from the NCSR. The CISO [SN] is represented in federal state working group of the IMK.[198]

IT-Planungsrat (IT Planning Council, IT-PLR, official translation)
The IT Planning Council was created as a political steering body between the federal level and federal states on issues relating to information technology and the

196 Federal Ministry of Health, E-Health-Gesetz.
Gematik, Datensicherheit.
Gematik, Die elektronische Gesundheitskarte. (Website deleted)
Gematik, Telematikinfrastruktur.
Gematik, Themen. (Website deleted)
Gematik, Über uns.
197 German Competence Centre against Cyber Crime e.V. (G4C), Über uns.
198 Bundesrat, Innenministerkonferenz.
CISO der niedersächsischen Landesverwaltung, Cybersicherheit in der Landesverwaltung. (Website deleted)
Email exchange with representatives of the BSI in February 2020.
Innenministerkonferenz, 213. Sitzung der Innenministerkonferenz.
Secupedia, Nationales Cyber-Abwehrzentrum.

digitization of public administration in Germany. Its decisions provide the federal government and 16 federal states with a binding foundation for joint federal digitization activities. The IT Planning Council defines overarching IT interoperability and IT security standards, manages e-government projects assigned to it, and coordinates the "Verbindungsnetz" (connection network, own translation) between the federal and federal state IT networks. The federal level and federal states alternate annually in the chairmanship (in alphabetical order). The committees of the IT Planning Council include the "Arbeitsgruppe Informationssicherheit" (Working Group on Information Security, AG InfoSic, own translation). This working group is responsible for monitoring the implementation of the guidelines for information security in public administration and for further developing goals and strategies for information security.

The CIO Bund (BMI) chairs the IT-PLR. The BfDI, representatives of the Central Municipal Associations, and the president of FITKO, as well as a representative of the 16 data protection authorities in the federal states 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 [SH], CIO [SL], CIO [SN], CIO [ST], and CIO [TH] are members. Brandenburg is represented by a state secretary of the MIK and Hamburg by the head of the SK [HH]. Other persons, including the points of contact of the respective ministerial conferences, may also participate if the decisions of the IT-PLR affect their remit. The BSI participates in the AG InfoSic in an advisory capacity. The FITKO is subordinate to the IT-PLR. The municipal committee is a body of the IT Planning Council to exchange information with municipalities. The head of the BKAmt and its respective federal state counterparts take note of the activity report of the IT Planning Council each year and inform themselves about further developments of the National E-Government Strategy.[199]

IT Security made in Germany (ITSMIG)

The trust mark ITSMIG was jointly launched by the BMI, the BMWK, 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 BMWK provided support in establishing ITSMIG. Both ministries are represented in the Advisory Board of the working group.[200]

199 IT-Planungsrat, Aufgaben des IT-Planungsrats.
IT-Planungsrat, Besprechung des Chefs des Bundeskanzleramtes mit den Chefinnen und Chefs der Staats- und Senatskanzleien der Länder. (Website deleted)
IT-Planungsrat, IT-Planungsrat.
IT-Planungsrat, Umsetzung Leitlinie InfoSic. (Website deleted)
IT-Planungsrat, Zusammensetzung des IT-Planungsrates.

200 TeleTrust, IT Security made in Germany.

Kompetenz- und Forschungszentren für IT-Sicherheitsforschung (Competence and Research Centers for IT Security Research, 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 in the field of cybersecurity and privacy protection.

The three competency and research centers for IT security are funded by the BMBF.[201]

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 that 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.[202]

Nationaler Cyber-Sicherheitsrat (National Cyber Security Council, NCSR, official translation)
As a strategic advisor to the Federal Government, the NCSR aims to identify requirements for long-term action as well as trends in cybersecurity to stimulate appropriate impulses. In accordance, the NCSR shall make proposals for the further development of national regulations for more cyber security and identify areas for public-private cooperation. The NCSR 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, BMWK, BMJ, BMF, BMUV, BMDV, BMG, BMZ, and BMBF, the BSI, as well as representatives of the federal states of Lower-Saxony and Hesse, are represented in the NCSR. In addition, also UP KRITIS and municipalities (currently represented by the Association of German Cities, KSV) are represented in the NCSR. It is chaired by the CIO Bund. In the past, representatives of ENISA, the BfV, and the SWP have also been invited to special meetings of the NCSR. In addition to scientific representatives, the scientific working group also includes a representative of the BSI.

201 Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.
202 Deutscher CERT-Verbund, Überblick.
Federal Ministry of the Interior and Community, Online Kompendium Cybersicherheit in Deutschland: CERT-Verbund.

The Cyber-AZ sends its annual report to the NCSR. Besides the federal government, the NCSR is also to provide impetus for the IMK.[203]

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 is a cooperation platform between the BSI, BPol, BKA, BfV, BBK, BND, KdoCIR, and BAMAD. The BaFin is involved on an associated basis as a partner. At the federal state level, partners of the Cyber-AZ are the Cyber Defence Bavaria, Hessen3C, the Central Office Cybercrime Bavaria as well as the Central and Contact Office Cybercrime North Rhine-Westphalia. It sends its annual report to the NCSR. 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 from CIR and cooperates with the LZ.[204]

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 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

203 Der Beauftragte der Bundesregierung für Informationstechnik, Der Nationale Cyber-Sicherheitsrat (NCSR).
Federal Ministry of Defence, Cyber-Sicherheitsrat.
Federal Ministry of the Interior and Community, Cyber-Sicherheitsstrategie für Deutschland 2016.
Federal Ministry of the Interior and Community, Sondersitzung des Nationalen Cyber-Sicherheitsrates.
Fraunhofer-Institut für Sichere Informationstechnologie, Beratung aus der Forschung. Wissenschaftliche Arbeitsgemeinschaft Nationale Cyber-Sicherheit.

204 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.

cybersecurity, developing common positions, and offering network opportunities that all contribute to the mutual exchange of information.

The BMI, BSI, and BBK cooperate within the framework of UP KRITIS, which is 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 and is represented in the NCSR.[205]

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 EC are among the SWP's third-party donors. Its Foundation Board is composed of representatives from BKAmt, BMBF, BMZ, BMI, AA, BMF, BMWK, and BMVg, for example. In the past, a representative of the SWP has been invited to a special meeting of the NCSR.[206]

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.

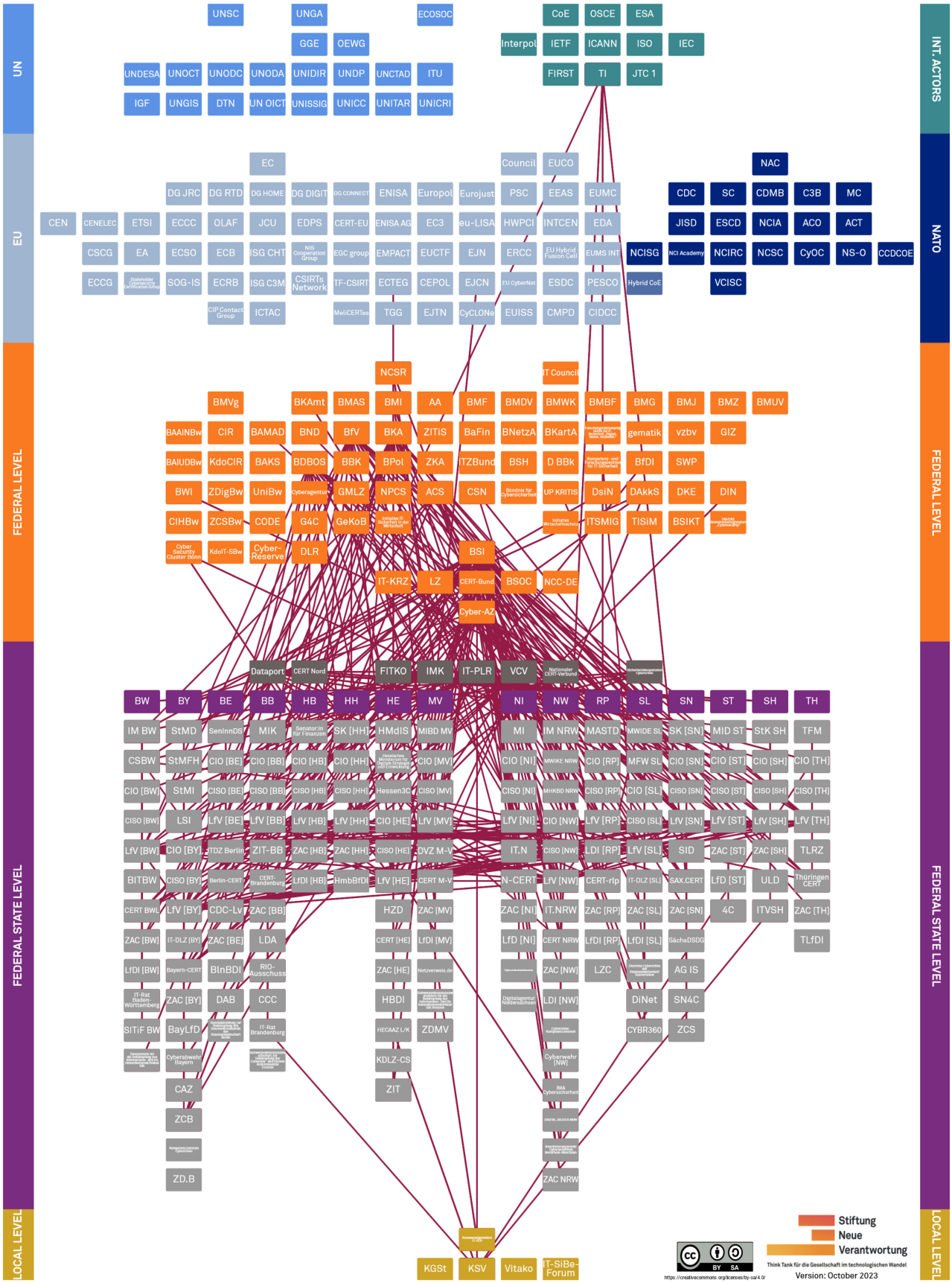
The BSI, CERT-Bund, CERTs on the federal state level, and the LSI are involved in the VCV. The members of the VCV receive the daily "Lagebericht IT-Sicherheit" (IT security status report, own translation) of the LZ as well as the "Cyber-Lage" (cyber situation report, own translation) of the Cyber-AZ. Working relations exist with the Hessen3C. The CISO [MV] represents Mecklenburg-Western Pomerania in the VCV.[207]

205 Bundesamt für Sicherheit in der Informationstechnik. Geschäftsstelle UP KRITIS, UP KRITIS. Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland.
Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, UP KRITIS. Organisation.
Internetplattform zum Schutz Kritischer Infrastrukturen, UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen.
Internetplattform zum Schutz Kritischer Infrastrukturen, Zusammenarbeit im Rahmen des UP KRITIS.

206 Stiftung Wissenschaft und Politik, Cyber-Sicherheit.
Stiftung Wissenschaft und Politik, Cluster »Digitalisierung – Cyber – Internet«.
Stiftung Wissenschaft und Politik, Organe der Stiftung.
Stiftung Wissenschaft und Politik, Unterstützerinnen und Unterstützer.
Stiftung Wissenschaft und Politik, Über uns.

207 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)

9. Explanation – Actors at Federal State Level



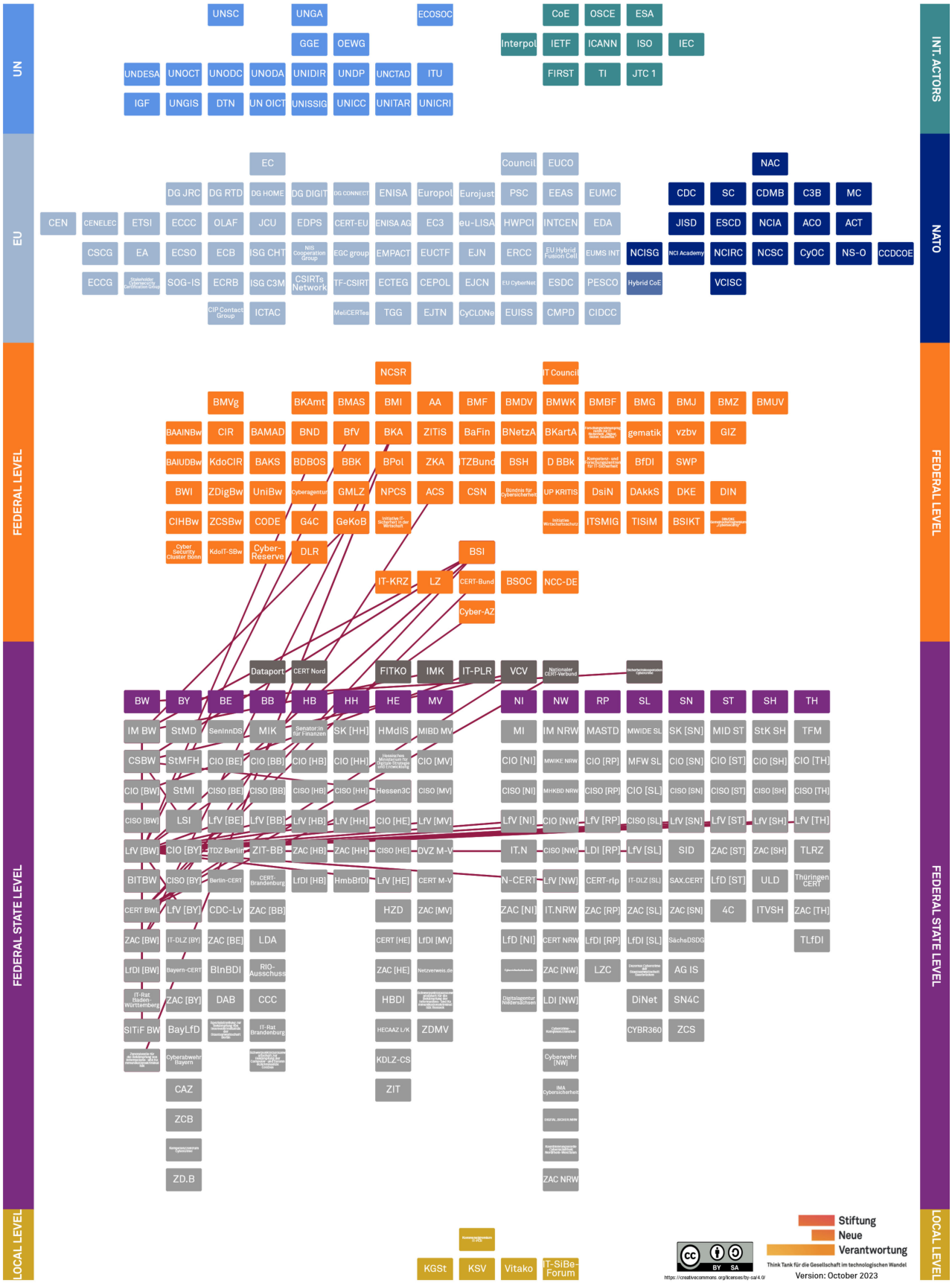
Policy Overview

Year	Federal State	Name
2023	HB	Bremische Cybersicherheitsstrategie (in German, "Cybersecurity Strategy of the City Municipality of Bremen", own translation)
2023	HE	Hessisches Gesetz zum Schutz der elektronischen Verwaltung, Hessisches IT-Sicherheitsgesetz, HITSIG (in German, "Hessian Act on the Protection of Electronic Administration, Hessian IT Security Act", own translation)
2022	BY	Gesetz über die Digitalisierung im Freistaat Bayern, Bayerisches Digitalgesetz – BayDiG (in german, „Bavarian Digital Act", own translation")
2022	MV	Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung Mecklenburg-Vorpommern, ZDMVG (in german, „Law on the Establishment of the Mecklenburg-Western Pomerania State Office Center for Digitization", own translation)
2021	BW	Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026 – (in German, "Cybersecurity Strategy Baden-Württemberg – Perspective 2026 –", own translation)
2021	BW	Gesetz für die Cybersicherheit in Baden-Württemberg (in German, "Law for Cybersecurity in Baden-Württemberg", own translation)
2021	HE	Informationssicherheitsleitlinie für die hessische Landesverwaltung (in German, "Information security guideline for the Hessian state sdministration", own translation)
2021	NW	Cybersicherheitsstrategie des Landes Nordrhein-Westfalen (in German, "Cybersecurity strategy of the state of North Rhine-Westphalia", own translation)
2020	BB	Richtlinie für die Organisation des E-Government und des Einsatzes der Informationstechnik in der Landesverwaltung Brandenburg (in German, "Directive for the organization of e-government and the use of information technology in the state administration of Brandenburg", own translation)
2020	HE	Förderrichtlinie Cybersicherheitsforschung in Hessen (in German, "Funding guideline for cybersecurity research in Hesse", own translation)
2020	RP	Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz (in German, "Law for the promotion of electronic administration in Rhineland-Palatinate", own translation)
2019	NI	Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (in German, "Law on digital administration and information security Lower Saxony", own translation)

Year	Federal State	Name
2019	SL	Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes (in German, "Law on the defense against threats to data in the country's information and communications infrastructure", own translation)
2019	SN	Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (in German, "Law for ensuring information security in the Free State of Saxony", own translation)
2019	SN	Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen (in German, "Law for the promotion of electronic administration in the Free State of Saxony", own translation)
2019	ST	Gesetz zur Förderung der elektronischen Verwaltung im Land Sachsen-Anhalt (in German, "Law for the promotion of electronic administration in the state of Saxony-Anhalt", own translation)
2018	All	Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung (in German, "Guideline for information security in the public administration", own translation)
2018	BB	Gesetz über die elektronische Verwaltung im Land Brandenburg (in German, "Law on electronic administration in the state of Brandenburg", own translation)
2018	HB	Gesetz zur Förderung der elektronischen Verwaltung in Bremen (in German, "Law for the promotion of electronic administration in Bremen", own translation)
2018	HE	Hessisches Gesetz zur Förderung der elektronischen Verwaltung (in German, "Hessian Law for the promotion of electronic administration", own translation)
2018	TH	Thüringer Gesetz zur Förderung der elektronischen Verwaltung (in German, "Law for the promotion of electronic administration Thuringia", own translation)
2017	BW	Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (in German, "Administrative regulation of the Ministry of the Interior on information security", own translation)
2017	HB	Informationssicherheitsleitlinie der Freien Hansestadt Bremen (in German, "Information security guideline of the Free Hanseatic City of Bremen", own translation)
2017	SL	Gesetz zur Förderung der elektronischen Verwaltung im Saarland (in German, "Law for the promotion of electronic administration in Saarland", own translation)
2016	BE	Gesetz zur Förderung des E-Government (in German, "Law for the promotion of e-government", own translation)

Year	Federal State	Name
2016	MV	Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (in German, "Law for the promotion of electronic administrative activities in Mecklenburg-Western Pomerania", own translation)
2016	NW	Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen (in German, "Law for the promotion of electronic administration in North Rhine-Westphalia", own translation)
2015	BW	Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg (in German, "Law for the Promotion of Electronic Administration in Baden-Württemberg", own translation)
2015	BY	Gesetz über die elektronische Verwaltung in Bayern (in German, "Law on electronic administration in Bavaria", own translation)
2014	MV	Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (in German, "Guideline for ensuring information security in the state administration of Mecklenburg-Western Pomerania", own translation)
2010	All	Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG (in German, "Treaty on the establishment of the IT Planning Council and on the principles of cooperation in the use of information technology in the federal and federal state administrations – Treaty on the implementation of Article 91c of the German Constitution", own translation)
2009	SH	Gesetz zur elektronischen Verwaltung für Schleswig-Holstein (in German, "Law on electronic administration in Schleswig-Holstein", own translation)

9.1 Baden-Württemberg (BW)



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

Overview

- **Relevant policy documents:**
  - 2021: Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026 – (in German, "Cybersecurity Strategy Baden-Württemberg – Perspective 2026 –", own translation)
  - 2021: Gesetz für die Cybersicherheit in Baden-Württemberg (in German, "Law for Cybersecurity in Baden-Württemberg", own translation)
  - 2017: Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit (in German, "Administrative regulation of the Ministry of the Interior on information security", own translation)
  - 2015: Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg (in German, "Law for the Promotion of Electronic Administration in Baden-Württemberg", own translation)

- **Ministerial responsibility(ies) for cyber and IT security topics:** "Ministerium für Inneres, Digitalisierung und Kommunen" (Ministry of the Interior, Digitalization and Municpalities, IM BW, own translation), "Abteilung 7: Digitalisierung" (Department 7: Digitization, own translation), "Referat 74: Informations- und Cybersicherheit" (Division 74: Information and Cybersecurity, own translation).

  The BSI and Baden-Württemberg have agreed to intensify their cooperation. The interior minister of Baden-Württemberg participates in the IMK.[208]

- **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-Württemberg in the IT-PLR.[209]

- **Chief Information Security Officer of the State Administration (CISO [BW]):** In Baden-Württemberg, the CISO is appointed by the IM BW. *The CISO is responsible for defining and updating information security guidelines for the state administra-*

208 Ministerium des Inneren, für Digitalisierung und Kommunen, Organigramm.
Wim Orth, BSI und BaWü kooperieren eng bei Cyber-Sicherheit. (Website deleted)
209 CIO Baden-Württemberg, Stefan Krebs.

tion, 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].[210]

- **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.*[211]

- **Computer Emergency Response Team (CERT):** The CERT BWL is part of the **CSBW**.

  It cooperates with ZAC [BW] and is represented in the CERT-Verbund.[212]

- **State Authority for the Protection of the Constitution**[213] **(LfV [BW])**: Within the Baden-Württemberg 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). If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[214]

- **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**[215]**):** "Landeskriminalamt Baden-Württemberg" (State Criminal Police Office Baden Württemberg, 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.

210 Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg, Verwaltungsvorschrift des Innenministeriums zur Informationssicherheit.
211 Landesoberbehörde IT Baden-Württemberg, Über BITBW.
212 Landtag von Baden-Württemberg, Stellungnahme des Ministeriums für Inneres, Digitalisierung und Migration: Verhinderung und Aufklärung von Cybercrime-Straftaten.
Natalie Zibolz, Baden-Württemberg bündelt Cybersicherheits-Angebote.
Staatsministerium Baden-Württemberg, Systeme des Landesamtes für Geoinformation wieder in Betrieb.
213 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").
214 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.
215 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.

The LKA BW is participating in the ACS as a multiplier.[216]

- **State Data Protection Authority:** "Landesbeauftragte:r für den Datenschutz und die Informationsfreiheit Baden-Württemberg" (State Commissioner for Data Protection and Freedom of Information Baden-Württemberg, LfDI [BW], own translation).[217]

Other actors in Baden-Württemberg:

Cybersicherheitsagentur Baden-Württemberg (Cybersecurity Agency Baden-Württemberg, CSBW, own translation)

The tasks of the CSBW 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-Württemberg'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, and 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. In addition, the CSBW offers the "Cyber-Ersthilfe BW" (Cyber First Aid BW, own translation), a telephone consultation in case of IT security incidents.

The IM BW is responsible for the official and technical supervision of the CSBW, to which it is subordinate. The CSBW is supervised by the respective subject-matter division of the IM BW – currently headed by the person who also acts as the CISO [BW]. At the operational level, the CSBW cooperates with the SITiF, the ZAC [BW], the BITBW, and the LfV [BW]. It reports to the CIO [BW] and once a year to the LfDI [BW]. The CSBW has taken over the CERT BWL operationally and thus became a member of the VCV. It has already been working with the VCV and the BSI before. The CSBW reports to the IM BW and the IT Council Baden-Württemberg at least once a year in the form of a report.

216 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.

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

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-Württemberg's point of contact for cybersecurity issues for other actors at the federal state (including Hessen3C and LSI), federal, EU, and international levels.[218]

IT-Rat Baden-Württemberg (IT Council Baden-Württemberg, own translation)
The IT Council decides on Baden-Württemberg'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-Württemberg. 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.[219]

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-Württemberg'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).[220]

218 Landesrecht BW Bürgerservice, Gesetz für die Cybersicherheit in Baden-Württemberg (Cybersicherheitsgesetz – CSG).
Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg, Cybersicherheitsagentur Baden-Württemberg.
219 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).
220 Staatsministerium Baden-Württemberg, Sicherheitszentrum IT in der Finanzverwaltung vorgestellt.

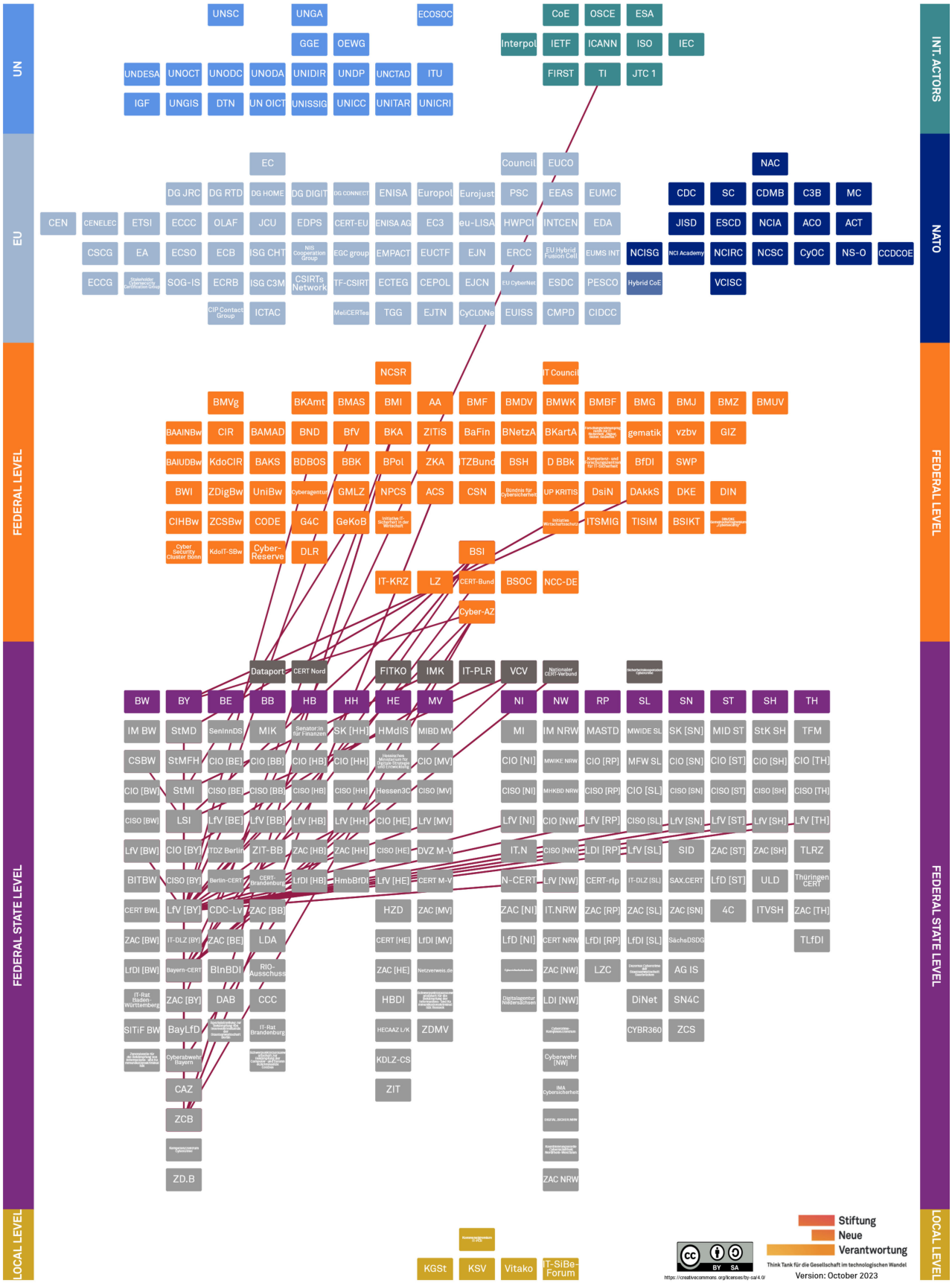
ZentralstellefürdieBekämpfungvonInformations-undKommunikationskriminalität (Central Office for the Fight against Information and Communication Crime, own translation)

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 BW.[221]

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

9.2 Bavaria (BY)



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

- **Relevant policy documents:**
  - 2022: Gesetz über die Digitalisierung im Freistaat Bayern, Bayerisches Digitalgesetz – BayDiG (in German, „Bavarian Digital Act", own translation")
  - 2015: Gesetz über die elektronische Verwaltung in Bayern (in German, "Law on electronic administration in Bavaria", own translation)

- **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).

    The StMD cooperates with DsiN.[222]

  - "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).[223]

  - "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).

    Bavaria's interior minister participates in the IMK.[224]

222 Bayerisches Staatsministerium für Digitales, Organisationsplan.
223 Bayerisches Staatsministeriums der Finanzen und für Heimat, Organisationsplan.
224 Bayerisches Staatsministerium des Innern, für Sport und Integration, Organigramm.
Bayerisches Staatsministerium des Innern, für Sport und Integration, Schutz vor Cybergefahren.

- **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.[225]

- **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.

  He or she is based in the StMFH and is responsible for the technical supervision of the Bavarian CERT.[226]

- **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.*[227]

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

  It participates in the National CERT Network and TI.[228]

- **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]. If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[229]

225 Bayerisches Staatsministerium für Digitales, IT-Beauftragte der Bayerischen Staatsregierung.
226 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.
227 Bayerisches Staatsministerium der Finanzen und für Heimat, Behörden und Staatsbetriebe im Ressort.
Landesamt für Digitalisierung, Breitband und Vermessung, IT-Dienstleistungszentrum des Freistaats Bayern.
228 Landesamt für Sicherheit in der Informationstechnik, Staatsverwaltung.
229 Landesamt für Verfassungsschutz Bayern, Organisation.
Landesamt für Verfassungsschutz Bayern, Spionageabwehr / Wirtschaftsschutz.

- **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.[230]

- **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.[231]

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.[232]

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 coor-

230 Bayerische Polizei, Zentrale Ansprechstelle Cybercrime – Kontakt für Unternehmen.
Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: Initiativen der Landespolizeien.
Cyberabwehr Bayern, Cybersicherheit für bayerische Unternehmen und Behörden.
231 Der Bayerische Landesbeauftragte für den Datenschutz, Cybersicherheit.
232 Bayernkurier, Bayern stärkt die Cyber-Abwehr.
StMI Bayern, Bayern stärkt Cyberabwehr und Digitalfunk.
Tagesspiegel, Cyberabwehr: Neues Lagezentrum in Bayern geplant.
Verfassungsschutz Bayern, Cyberabwehr Bayern.

dination 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].[233]

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 authorities 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.[234]

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 can award the seal "Municipal IT Security" to municipalities.

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.[235]

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 cy-

233 Bayerisches Landesamt für Verfassungsschutz, Cyber-Allianz-Zentrum Bayern (CAZ).
234 Bayerische Staatsregierung, Cyber-Kompetenzzentrum im Landeskriminalamt.
235 Bayerische Staatskanzlei, Gesetz über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz – BayEGovG).
Landesamt für Sicherheit in der Informationstechnik Bayern, Startseite.
Landratsamt Kitzingen, Kommunale IT-Sicherheit.

bercrime 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. The unit is made up of prosecutors and IT forensic experts specializing in cybercrime. In the past, building on the work of the ZCB, Bavaria introduced a application in the Bundesrat on the use of leeway in the storage of IP addresses.

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.[236]

Zentrum Digitalisierung.Bayern (Center for Digitization Bavaria, ZD.B, own translation)

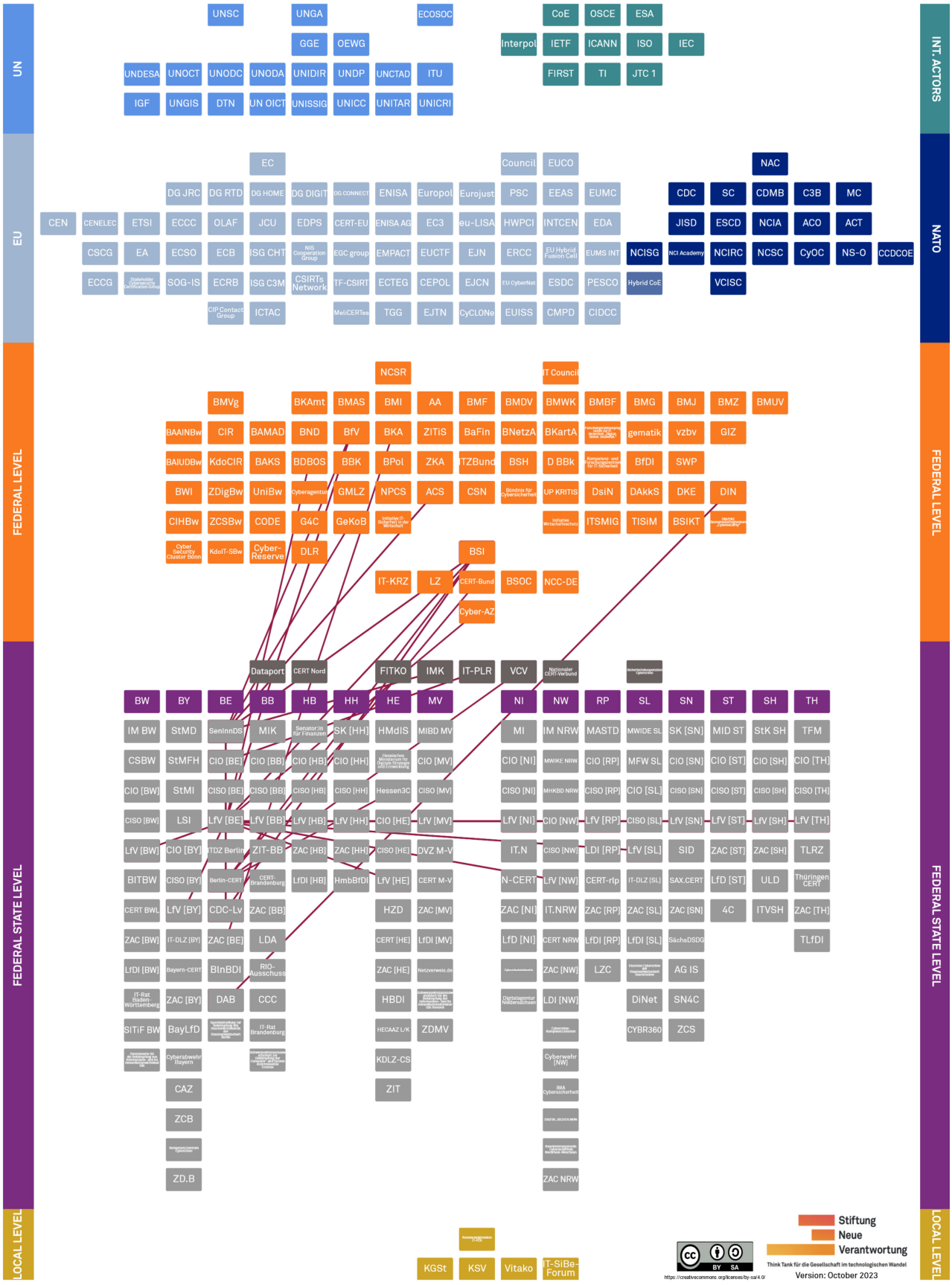
The ZD.B is intended to serve as a cross-regional research and cooperation platform in Bavaria and promote cooperation between industry and science, help shape societal dialog, and support the promotion of young people and researchers. As one of a total of 11 platforms, the ZD.B also has a thematic platform 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.[237]

236 Federal Office for Information Security, Teilnehmerliste der Allianz für Cyber-Sicherheit.
Generalstaatsanwaltschaft Bamberg, Zentralstelle Cybercrime Bayern (ZCB).

237 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.

9.3 Berlin (BE)


UN
EU
FEDERAL LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
INT. ACTORS
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
UNISSIG
UNICC
UNITAR
UNICRI
CoE
OSCE
ESA
Interpol
IETF
ICANN
ISO
IEC
FIRST
TI
JTC 1
EC
Council
EUCO
DG JRC
DG RTD
DG HOME
DG DIGIT
DG CONNECT
ENISA
Europol
Eurojust
PSC
EEAS
EUMC
CEN
CENELEC
ETSI
ECCC
OLAF
JCU
EDPS
CERT-EU
ENISA AG
EC3
eu-LISA
HWPCI
INTCEN
EDA
CSCG
EA
ECSO
ECB
ISG CHT
NIS Cooperation Group
EGC group
EMPACT
EUCTF
EJN
ERCC
EU Hybrid Fusion Cell
EUMS INT
ECCG
SOG-IS
ECRB
ISG C3M
CSIRTs Network
TF-CSIRT
ECTEG
CEPOL
EJCN
EU CyberNet
ESDC
PESCO
CIP Contact Group
ICTAC
MeliCERTes
TGG
EJTN
CyCLONe
EUISS
CMPD
CIDCC
NAC
CDC
SC
CDMB
C3B
MC
JISD
ESCD
NCIA
ACO
ACT
NCISG
NCI Academy
NCIRC
NCSC
CyOC
NS-O
CCDCOE
Hybrid CoE
VCISC
NCSR
IT Council
BMVg
BKAmt
BMAS
BMI
AA
BMF
BMDV
BMWK
BMBF
BMG
BMJ
BMZ
BMUV
BAAINBw
CIR
BAMAD
BND
BfV
BKA
ZITiS
BaFin
BNetzA
BKartA
gematik
vzbv
GIZ
BAIUDBw
KdoCIR
BAKS
BDBOS
BBK
BPol
ZKA
TZBund
BSH
D BBk
BfDI
SWP
BWI
ZDigBw
UniBw
Cyberagentur
GMLZ
NPCS
ACS
CSN
UP KRITIS
DsiN
DAkkS
DKE
DIN
CIHBw
ZCSBw
CODE
G4C
GeKoB
ITSMIG
TISiM
BSIKT
Cyber Security Cluster Bonn
KdoIT-SBw
Cyber-Reserve
DLR
BSI
IT-KRZ
LZ
CERT-Bund
BSOC
NCC-DE
Cyber-AZ
Dataport
CERT Nord
FITKO
IMK
IT-PLR
VCV
Nationaler CERT-Verbund
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
MIBD MV
MI
IM NRW
MASTD
MWIDE SL
SK [SN]
MID ST
StK SH
TFM
CSBW
StMFH
CIO [BE]
CIO [BB]
CIO [HB]
CIO [HH]
CIO [MV]
CIO [NI]
MWIKE NRW
CIO [RP]
MFW SL
CIO [SN]
CIO [ST]
CIO [SH]
CIO [TH]
CIO [BW]
StMI
CISO [BE]
CISO [BB]
CISO [HB]
CISO [HH]
Hessen3C
CISO [MV]
CISO [NI]
MHKBD NRW
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]
CIO [NW]
LfV [RP]
CISO [SL]
LfV [SN]
LfV [ST]
LfV [SH]
LfV [TH]
LfV [BW]
CIO [BY]
TDZ Berlin
ZIT-BB
ZAC [HB]
ZAC [HH]
CISO [HE]
DVZ M-V
IT.N
CISO [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
LfV [NW]
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]
IT.NRW
ZAC [RP]
ZAC [SL]
SN
4C
ITVSH
ZAC [TH]
ZAC [BW]
IT-DLZ [BY]
ZAC [BE]
LDA
CERT [HE]
LfDI [MV]
LfD [NI]
CERT NRW
LfDI [RP]
LfDI [SL]
SächsDSDG
TLfDI
LfDI [BW]
Bayern-CERT
BlnBDI
RIO-Ausschuss
ZAC [HE]
Netzverweis.de
LZC
AG IS
IT-Rat Baden-Württemberg
ZAC [BY]
DAB
CCC
HBDI
DiNet
SN4C
SiTiF BW
BayLfD
IT-Rat Brandenburg
HECAAZ L/K
ZDMV
CYBR360
ZCS
Cyberabwehr Bayern
KDLZ-CS
Cyberwehr [NW]
CAZ
ZIT
IMA Cybersicherheit
ZCB
ZAC NRW
ZD.B
KGSt
KSV
Vitako
IT-SiBe-Forum
Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel
Version: October 2023

Overview

- **Relevant policy documents:**
  - 2016: Gesetz zur Förderung des E-Government (in German, "Law for the promotion of e-government", own translation)

- **Ministerial responsibility(ies) for cyber and IT security topics:** "Senatsverwaltung für Inneres, Digitalisierung und Sport" (Senate Department for the Interior, Digitization 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). This division also 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 BSI have signed a declaration of intent to strengthen their cooperation. Division III of the SenInnDS is a member of the ACS. Berlin's Senator of the Interior is among the participants of the IMK.[238]

- **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.[239]

- **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 of 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.*[240]

238 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.
239 CIO, Sabine Smentek wird CIO vom Land Berlin.
240 Senatsverwaltung für Inneres und Sport Berlin, Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin.

- **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.[241]

- **CERT:** The Berlin-CERT is operated by the ITDZ Berlin.[242]

- **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 SenInnDS has transferred tasks of cyber defense to the BfV in the framework of an administrative agreement. If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[243]

- **Institutional location of the ZAC [BE]:** "Landeskriminalamt Berlin" (State Criminal Police Office Berlin, own translation).[244]

- **State Data Protection Authority:** "Berliner Beauftragte:r für Datenschutz und Informationsfreiheit" (State Commissioner for Data Protection and Freedom of Information Berlin, BlnBDI, own translation).[245]

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.

241 Berliner Vorschriften- und Rechtsprechungsdatenbank, Gesetz über die Anstalt des öffentlichen Rechts IT-Dienstleistungszentrum Berlin.
ITDZ Berlin, Profil.
242 ITDZ Berlin, Sicherheit.
243 Senatsverwaltung für Inneres und Sport Berlin, Organigramm.
Senatsverwaltung für Inneres und Sport Berlin, Verfassungsschutzbericht 2019.
244 Polizei Berlin, Zentrale Ansprechstelle Cybercrime für die Wirtschaft im LKA Berlin.
245 Berliner Beauftragte für Datenschutz und Informationsfreiheit, Über uns.

The CDC-Lv reports via the Berlin-CERT to Berlin's (CISO [BE]). At the working level, there is an exchange with the Berlin liaison office of the BSI.[246]

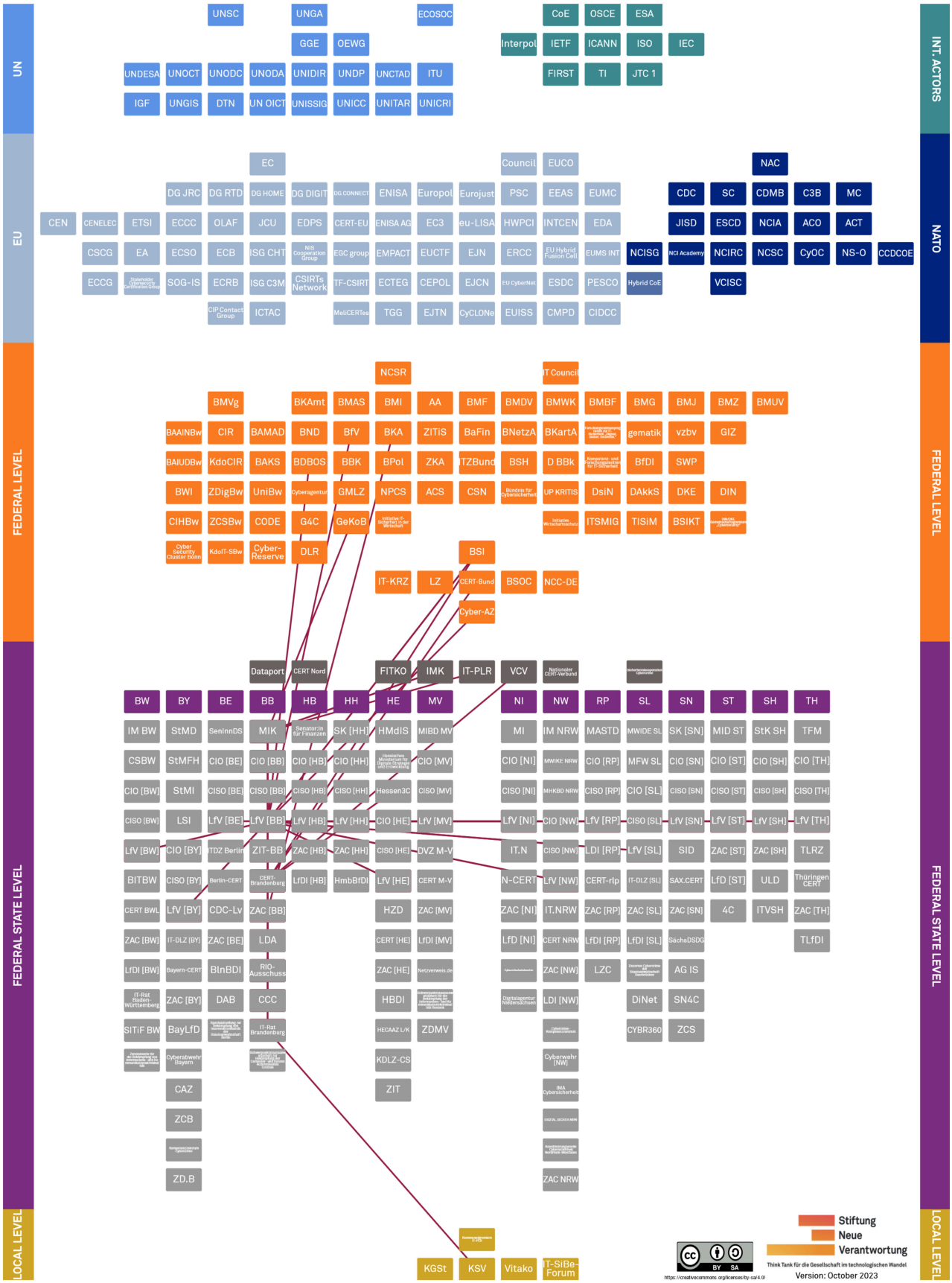
Digitalagentur Berlin (Digital Agency Berlin, DAB, own translation)
The Digital Agency Berlin provides support services for Berlin-based companies. Its portfolio also includes a "Cyberhotline" and webinars on IT security for its addressed audience. The "Cyberhotline" acts as a point of contact for companies in Berlin in the event of IT and cybersecurity-related emergencies, with "first responders" on the other end of the line. If necessary, the hotline can also refer the caller to private IT security companies from its network.

The state of Berlin supports and finances the DAB. Its network partners include the DIN.[247]

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.[248]

246 Background Conversation, 2021.
ITDZ Berlin, Innovationsmanagement im ITDZ Berlin.
247 Digitalagentur Berlin, IT-Sicherheit.
Digitalagentur Berlin, Netzwerk.
248 Diana Nadeborn, Berliner Staatsanwaltschaft rüstet auf gegen Cyberkriminalität.

9.4 Brandenburg (BB)



Overview

- **Relevant policy documents:**
  - 2020: Richtlinie für die Organisation des E-Government und des Einsatzes der Informationstechnik in der Landesverwaltung Brandenburg (in German, "Directive for the organization of e-government and the use of information technology in the state administration of Brandenburg", own translation)
  - 2018: Gesetz über die elektronische Verwaltung im Land Brandenburg (in German, "Law on electronic administration in the state of Brandenburg", own translation)

- **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).

  The interior minister of Brandenburg participates in the IMK.[249]

- **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.[250]

- **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.[251]

249 Ministerium des Innern und für Kommunales Brandenburg, Organigramm.
250 CIO, Die IT-Chefs der Bundesländer.
251 Brandenburgisches Vorschriftensystem, Leitlinie zur Gewährleistung der IT-Sicherheit in der Landesverwaltung Brandenburg.

- **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.*[252]

- **CERT**: The CERT-Brandenburg is being operated by the ZIT-BB.[253]

- **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 a "Verfassungsschutzbericht" (Report on the protection of the constitution, own translation) of Brandenburg, it inter alia referred to current developments in so-called "cyber-extremism".

  If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[254]

- **Institutional location of the ZAC [BB]**: Cyber-Competence-Center (CCC), actor description see below.[255]

- **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).[256]

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.

252 Brandenburgischer IT-Dienstleister, Start.
253 Brandenburgischer IT-Dienstleister, CERT-Brandenburg.
254 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.
255 Polizei Brandenburg, Internetkriminalität.
256 Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht, Über uns.

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.[257]

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.[258]

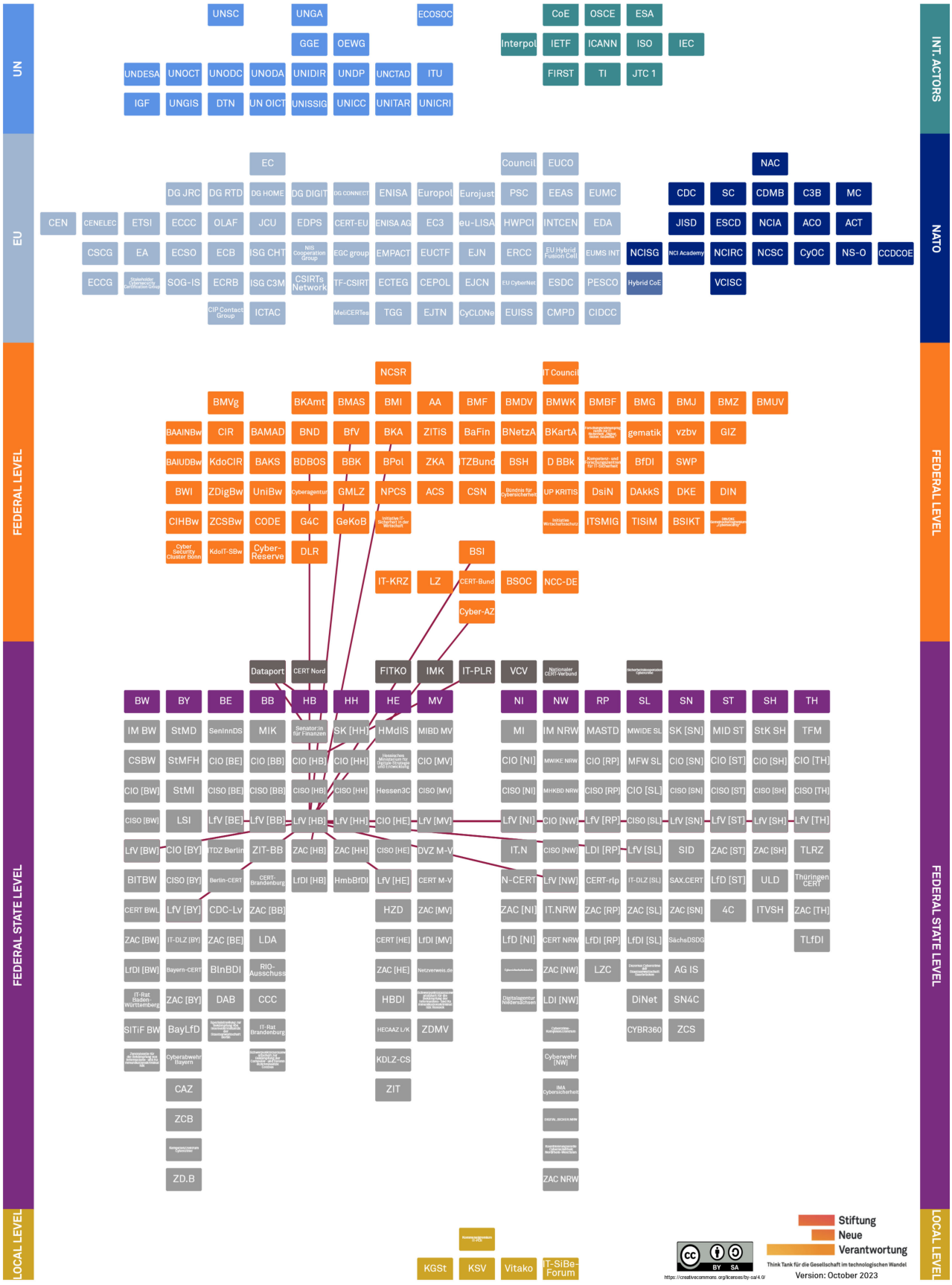
IT-Rat Brandenburg (IT Council Brandenburg, own translation)
The IT Council Brandenburg has been set up to permit the strategic coordination and joint management of information technology matters relating to cross-level cooperation between the federal state and its municipalities. Among other things, 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.[259]

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".[260]

257 Landesregierung Brandenburg, Richtlinie für die Organisation des E-Government und des Einsatzes der Informationstechnik in der Landesverwaltung Brandenburg (E-Government- und IT-Organisationsrichtlinie).
258 Polizei Brandenburg, Cyber-Competence-Center im Landeskriminalamt.
259 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.
260 Staatsanwaltschaft Cottbus, Schwerpunktstaatsanwaltschaft. (Website deleted)

9.5 Bremen (HB)


UN
EU
FEDERAL LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
INT. ACTORS
NATO
UNSC
UNGA
ECOSOC
GGE
OEWG
UNDESA
UNOCT
UNODC
UNODA
UNIDIR
UNDP
UNCTAD
ITU
IGF
UNGIS
DTN
UN OICT
UNISSIG
UNICC
UNITAR
UNICRI
CoE
OSCE
ESA
Interpol
IETF
ICANN
ISO
IEC
FIRST
TI
JTC 1
EC
Council
EUCO
DG JRC
DG RTD
DG HOME
DG DIGIT
DG CONNECT
ENISA
Europol
Eurojust
PSC
EEAS
EUMC
CEN
CENELEC
ETSI
ECCC
OLAF
JCU
EDPS
CERT-EU
ENISA AG
EC3
eu-LISA
HWPCI
INTCEN
EDA
CSCG
EA
ECSO
ECB
ISG CHT
NIS Cooperation Group
EGC group
EMPACT
EUCTF
EJN
ERCC
EU Hybrid Fusion Cell
EUMS INT
ECCG
SOG-IS
ECRB
ISG C3M
CSIRTs Network
TF-CSIRT
ECTEG
CEPOL
EJCN
EU CyberNet
ESDC
PESCO
CIP Contact Group
ICTAC
MeliCERTes
TGG
EJTN
CyCLONe
EUISS
CMPD
CIDCC
NAC
CDC
SC
CDMB
C3B
MC
JISD
ESCD
NCIA
ACO
ACT
NCISG
NCI Academy
NCIRC
NCSC
CyOC
NS-O
CCDCOE
VCISC
Hybrid CoE
NCSR
IT Council
BMVg
BKAmt
BMAS
BMI
AA
BMF
BMDV
BMWK
BMBF
BMG
BMJ
BMZ
BMUV
BAAINBw
CIR
BAMAD
BND
BfV
BKA
ZITiS
BaFin
BNetzA
BKartA
gematik
vzbv
GIZ
BAIUDBw
KdoCIR
BAKS
BDBOS
BBK
BPol
ZKA
TZBund
BSH
D BBk
BfDI
SWP
BWI
ZDigBw
UniBw
Cyberagentur
GMLZ
NPCS
ACS
CSN
UP KRITIS
DsiN
DAkkS
DKE
DIN
CIHBw
ZCSBw
CODE
G4C
GeKoB
ITSMIG
TISiM
BSIKT
Cyber Security Cluster Bonn
KdoIT-SBw
Cyber-Reserve
DLR
BSI
IT-KRZ
LZ
CERT-Bund
BSOC
NCC-DE
Cyber-AZ
Dataport
CERT Nord
FITKO
IMK
IT-PLR
VCV
Nationaler CERT-Verbund
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
MIBD MV
MI
IM NRW
MASTD
MWIDE SL
SK [SN]
MID ST
StK SH
TFM
CSBW
StMFH
CIO [BE]
CIO [BB]
CIO [HB]
CIO [HH]
CIO [MV]
CIO [NI]
MWIKE NRW
CIO [RP]
MFW SL
CIO [SN]
CIO [ST]
CIO [SH]
CIO [TH]
CIO [BW]
StMI
CISO [BE]
CISO [BB]
CISO [HB]
CISO [HH]
Hessen3C
CISO [MV]
CISO [NI]
MHKBD NRW
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]
CIO [NW]
LfV [RP]
CISO [SL]
LfV [SN]
LfV [ST]
LfV [SH]
LfV [TH]
LfV [BW]
CIO [BY]
TDZ Berlin
ZIT-BB
ZAC [HB]
ZAC [HH]
CISO [HE]
DVZ M-V
IT.N
CISO [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
LfV [NW]
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]
IT.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]
CERT NRW
LfDI [RP]
LfDI [SL]
SächsDSDG
TLfDI
LfDI [BW]
Bayern-CERT
BlnBDI
RIO-Ausschuss
ZAC [HE]
Netzverweis.de
LZC
AG IS
IT-Rat Baden-Württemberg
ZAC [BY]
DAB
CCC
HBDI
DiNet
SN4C
SiTiF BW
BayLfD
IT-Rat Brandenburg
HECAAZ L/K
ZDMV
CYBR360
ZCS
Cyberabwehr Bayern
KDLZ-CS
Cyberwehr [NW]
CAZ
ZIT
IMA Cybersicherheit
ZCB
ZAC NRW
ZD.B
KGSt
KSV
Vitako
IT-SiBe-Forum
Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel
Version: October 2023

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

Overview

- **Relevant policy documents:**
  - Bremische Cybersicherheitsstrategie (in German, "Cybersecurity Strategy of the City Municipality of Bremen", own translation)
  - 2018: Gesetz zur Förderung der elektronischen Verwaltung in Bremen (in German, "Law for the promotion of electronic administration in Bremen", own translation)
  - 2017: Informationssicherheitsleitlinie der Freien Hansestadt Bremen (in German, "Information security guideline of the Free Hanseatic City of Bremen", own translation)

- **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.[261]

- **State Commissioner for Information Technology ([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.[262]

- **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.[263]

- **IT Service Provider of the Federal State Administration:** Dataport, actor description see below (Chapter 9.17).

261 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.
262 Freie Hansestadt Bremen, Staatsrat Dr. Martin Hagen.
263 CISO Bremen, Vorlage für die Sitzung des Senats am 14.7.2020. Jahresbericht zur Informationssicherheit in der bremischen Verwaltung.

- **CERT**: CERT Nord, actor description see below (Chapter 9.17).

- **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.

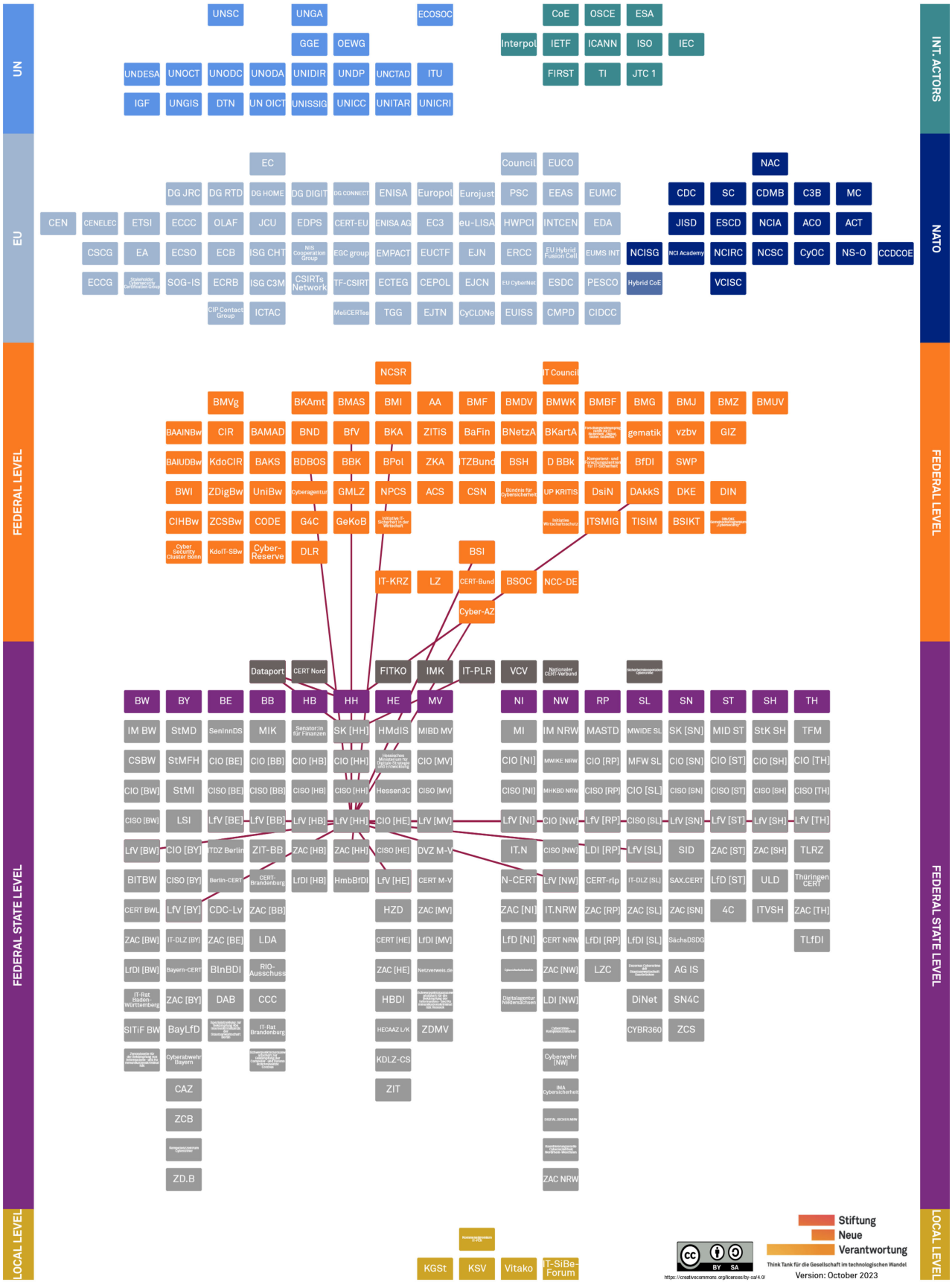
  If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[264]

- **Institutional location of the ZAC [HB]**: "Polizei Bremen" (Bremen Police, own translation). There, police department K13 deals with cybercrime and digital traces.[265]

- **State Data Protection Authority: "**Landesbeauftragte:r für Datenschutz und Informationsfreiheit" (State Commissioner for Data Protection and Freedom of Information, LfDI, own translation)[266].

264 Landesamt für Verfassungsschutz Bremen, Über Uns.
Freie Hansestadt Bremen, Verfassungsschutzbericht 2019.
265 Polizei Bremen, Organigramm Direktion Kriminalpolizei / untere Ebene.
266 Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen, Wir über uns.

9.6 Hamburg (HH)



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

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.[267]

- **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.[268]

- **Chief Information Security Officer of the State Administration (CISO [HH])**: Hamburg's CISO has been established within the ITD of the SK [HH].[269]

- **IT Service Provider of the Federal State Administration:** Dataport, actor description see below (Chapter 9.17).

- **CERT**: CERT Nord, actor description see below (Chapter 9.17).

- **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, it also refers to threats from cyber espionage, cyber sabotage, and cyber operations.

  If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[270]

- **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 de-

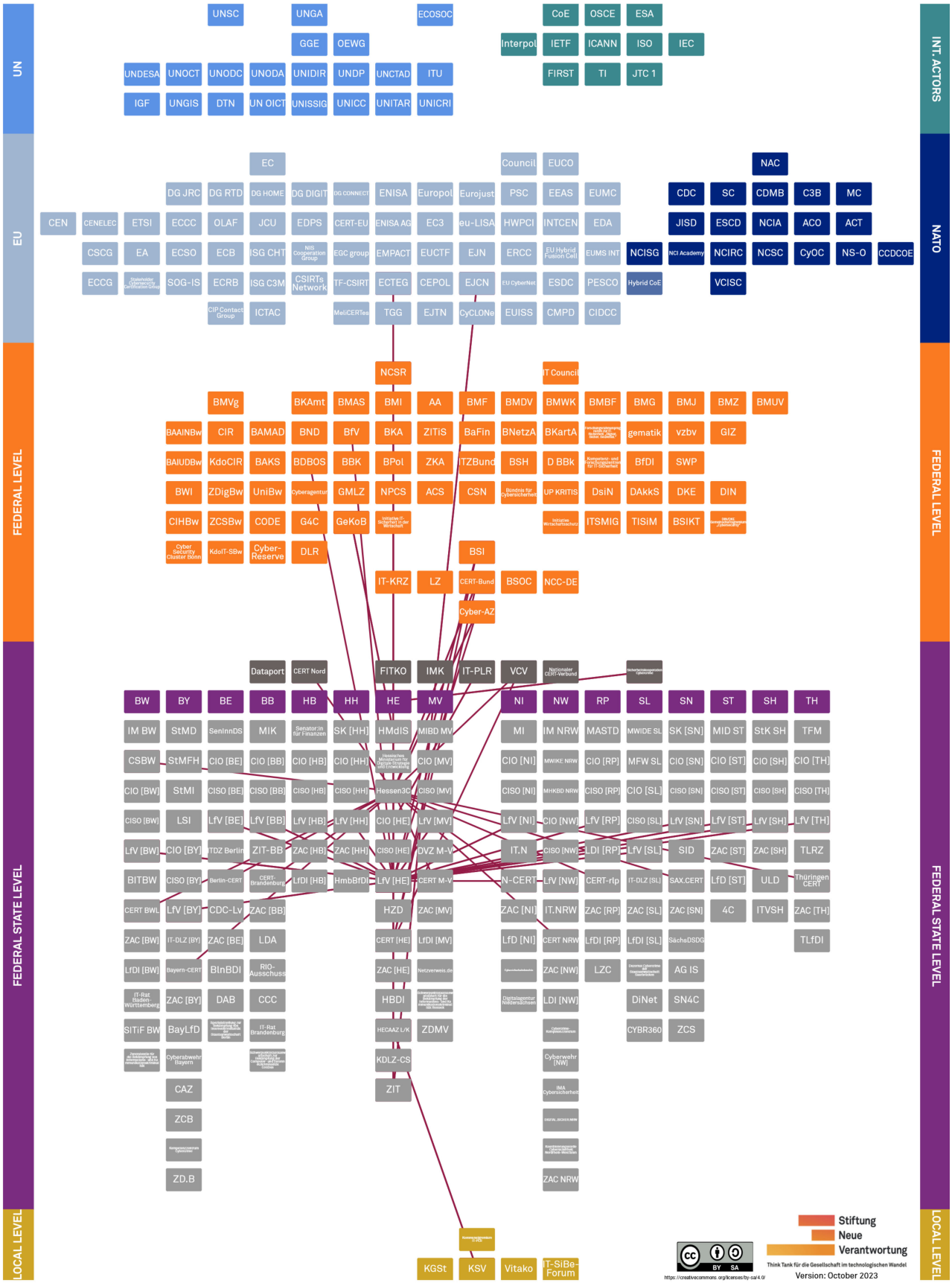
267 Senat der Freien und Hansestadt Hamburg Senatskanzlei, Arbeitsstrukturen des Amtes für IT und Digitalisierung (ITD). (Website deleted)
268 Senatskanzlei Hamburg, Senatskanzlei Amt für IT und Digitalisierung.
269 Freie Hansestadt Hamburg, Rahmen-Sicherheitskonzept.
270 Landesamt für Verfassungsschutz Hamburg, Organigramm des Landesamtes für Verfassungsschutz. Behörde für Inneres und Sport Freie Hansestadt Hamburg, Verfassungsschutzbericht 2019.

partment that pools the competencies of criminal investigators and computer scientists to combine technological and police knowledge. IT security and cybercrime are also an area of activity of the "Netzwerk Standortsicherheit Hamburg" (Hamburg Site Safety Network, own translation) coordinated by the Hamburg police.[271]

- **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).[272]

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

9.7 Hesse (HE)


UN
EU
FEDERAL LEVEL
FEDERAL STATE LEVEL
LOCAL LEVEL
INT. ACTORS
NATO
UNSC
UNGA
ECOSOC
GGE
OEWG
CoE
OSCE
ESA
Interpol
IETF
ICANN
ISO
IEC
FIRST
TI
JTC 1
UNDESA
UNOCT
UNODC
UNODA
UNIDIR
UNDP
UNCTAD
ITU
IGF
UNGIS
DTN
UN OICT
UNISSIG
UNICC
UNITAR
UNICRI
EC
Council
EUCO
NAC
DG JRC
DG RTD
DG HOME
DG DIGIT
DG CONNECT
ENISA
Europol
Eurojust
PSC
EEAS
EUMC
CDC
SC
CDMB
C3B
MC
CEN
CENELEC
ETSI
ECCC
OLAF
JCU
EDPS
CERT-EU
ENISA AG
EC3
eu-LISA
HWPCI
INTCEN
EDA
JISD
ESCD
NCIA
ACO
ACT
CSCG
EA
ECSO
ECB
ISG CHT
NIS Cooperation Group
EGC group
EMPACT
EUCTF
EJN
ERCC
EU Hybrid Fusion Cell
EUMS INT
NCISG
NCI Academy
NCIRC
NCSC
CyOC
NS-O
CCDCOE
ECCG
SOG-IS
ECRB
ISG C3M
CSIRTs Network
TF-CSIRT
ECTEG
CEPOL
EJCN
EU CyberNet
ESDC
PESCO
Hybrid CoE
VCISC
CIP Contact Group
ICTAC
MeliCERTes
TGG
EJTN
CyCLONe
EUISS
CMPD
CIDCC
NCSR
IT Council
BMVg
BKAmt
BMAS
BMI
AA
BMF
BMDV
BMWK
BMBF
BMG
BMJ
BMZ
BMUV
BAAINBw
CIR
BAMAD
BND
BfV
BKA
ZITiS
BaFin
BNetzA
BKartA
gematik
vzbv
GIZ
BAIUDBw
KdoCIR
BAKS
BDBOS
BBK
BPol
ZKA
ITZBund
BSH
D BBk
BfDI
SWP
BWI
ZDigBw
UniBw
Cyberagentur
GMLZ
NPCS
ACS
CSN
UP KRITIS
DsiN
DAkkS
DKE
DIN
CIHBw
ZCSBw
CODE
G4C
GeKoB
ITSMIG
TISiM
BSIKT
Cyber Security Cluster Bonn
KdoIT-SBw
Cyber-Reserve
DLR
BSI
IT-KRZ
LZ
CERT-Bund
BSOC
NCC-DE
Cyber-AZ
Dataport
CERT Nord
FITKO
IMK
IT-PLR
VCV
Nationaler CERT-Verbund
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
MIBD MV
MI
IM NRW
MASTD
MWIDE SL
SK [SN]
MID ST
StK SH
TFM
CSBW
StMFH
CIO [BE]
CIO [BB]
CIO [HB]
CIO [HH]
Hessisches Ministerium für Digitale Strategie und Entwicklung
CIO [MV]
CIO [NI]
MWIKE NRW
CIO [RP]
MFW SL
CIO [SN]
CIO [ST]
CIO [SH]
CIO [TH]
CIO [BW]
StMI
CISO [BE]
CISO [BB]
CISO [HB]
CISO [HH]
Hessen3C
CISO [MV]
CISO [NI]
MHKBD NRW
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]
CIO [NW]
LfV [RP]
CISO [SL]
LfV [SN]
LfV [ST]
LfV [SH]
LfV [TH]
LfV [BW]
CIO [BY]
TDZ Berlin
ZIT-BB
ZAC [HB]
ZAC [HH]
CISO [HE]
DVZ M-V
IT.N
CISO [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
LfV [NW]
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]
IT.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]
CERT NRW
LfDI [RP]
LfDI [SL]
SächsDSDG
TLfDI
LfDI [BW]
Bayern-CERT
BlnBDI
RIO-Ausschuss
ZAC [HE]
Netzverweis.de
LZC
AG IS
IT-Rat Baden-Württemberg
ZAC [BY]
DAB
CCC
HBDI
Digitalagentur Niedersachsen
DiNet
SN4C
SiTiF BW
BayLfD
IT-Rat Brandenburg
HECAAZ L/K
ZDMV
ZAC [NW]
CYBR360
ZCS
KDLZ-CS
Cyberwehr [NW]
Cyberabwehr Bayern
ZIT
IMA Cybersicherheit
CAZ
ZCB
ZAC NRW
ZD.B
KGSt
KSV
Vitako
IT-SiBe-Forum
Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel
Version: October 2023

The state of Hesse is represented in the NCSR 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

- **Relevant policy documents:**
  - Hessisches Gesetz zum Schutz der elektronischen Verwaltung, Hessisches IT-Sicherheitsgesetz, HITSIG (in German, "Hessian Act on the Protection of Electronic Administration, Hessian IT Security Act", own translation)
  - 2021: Informationssicherheitsleitlinie für die hessische Landesverwaltung (in German, "Information security guideline for the Hessian state sdministration", own translation)
  - 2020: Förderrichtlinie Cybersicherheitsforschung in Hessen (in German, "Funding guideline for cybersecurity research in Hesse", own translation)
  - 2018: Hessisches Gesetz zur Förderung der elektronischen Verwaltung (in German, "Hessian Law for the promotion of electronic administration", own translation)

- **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).

    The KDLZ-CS is a municipal support service provided by the HMdIS.[273]

  - "Hessisches Ministerium für Digitale Strategie und Entwicklung" (State Ministry for Digital Strategy and Development, own translation).[274]

- **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.

  He or she is supported by a Co-CIO and represents Hesse on the IT-PLR.[275]

- **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.

273 Hessisches Ministerium des Innern und für Sport, Organisationsplan des Hessischen Ministerium des Innern und für Sport.
274 Hessische Staatskanzlei: Organisationsplan.
275 Hessische Ministerin für Digitale Strategie und Entwicklung, CIO.
Hessische Ministerin für Digitale Strategie und Entwicklung, Drei Fragen an Roland Jabkowski.

A representative of the Hessen3C acts as his or her deputy.[276]

- **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).[277]

- **CERT**: Upon the founding of Hessen3C, the Hessian CERT was integrated into its cybersecurity portfolio and now performs all tasks of the CERT.[278]

- **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.

  If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[279]

- **Institutional location of the ZAC [HE]**: "Landeskriminalamt Hessen" (State Criminal Police Office Hesse, own translation).[280]

- **State Data Protection Authority:** Hessische:r Beauftragte:r für Datenschutz und Informationsfreiheit (Hessian Commissioner for Data Protection and Freedom of Information, HBDI, own translation)[281].

Other actors in Hesse:

Hessisches Cyberabwehrausbildungszentrum Land/Kommunen (Hessian Cyber Defense Training Center Federal State/Municipalities, HECAAZ L/K, own translation)
The HECAAZ L/K seeks to improve the IT and cyber security of Hessian municipalities through on-site exercises, among other things. Their offer for municipal decision-makers in Hesse also includes, for example, the development of corresponding strategies or emergency plans.

The HECAAZ L/K was developed by Hessen3C in cooperation with a municipal IT service provider, with the latter being responsible for the operational implementation of

276 Ministerium des Innern und für Sport Hessen, Der zentrale Informationssicherheitsbeauftragte der Landesverwaltung.
Hessischer Landtag (Drucksache 20/1520), Antwort auf Kleine Anfrage: Umsetzung Informationssicherheitsrichtlinie.
277 Hessische Zentrale für Datenverarbeitung, Organisation.
278 Hessisches Ministerium des Innern und für Sport, Der Bereich Cybersecurity im Hessen3C.
279 Landesamt für Verfassungsschutz Hessen, Organigramm.
Landesamt für Verfassungsschutz Hessen, Wirtschaftsschutz. Was ist Cyberspionage?.
280 Bundeskriminalamt, Polizei – Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen.
281 Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Über uns.

the training elements. The training courses take place in coordination with and with the support of KSV.[282]

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 governments and those affecting SMEs. As part of Hessen3C's warning and information service, Hessian municipalities can inter alia receive daily vulnerability reports. If necessary, a Mobile Incident Response Team (MIRT) is also available to municipalities.

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. The HECAAZ L/K was developed by Hessen3C in cooperation with a municipal IT service provider. Working relationships exist with the VCV, the CERT-Bund, as well as the other CERTs of the federal states. Hessen3C is also represented in the Cyber-AZ.[283]

Kommunales Dienstleistungszentrum Cybersicherheit (Municipal Cyber Security Service Center, KDLZ-CS, own translation)

The KDLZ-CS offers municipalities the conduct of free individual analyses of their IT and cybersecurity status quo and the development of a corresponding action plan based on this analysis in order to develop and strengthen municipal cyber resilience in Hesse. Thereby, the KDLZ-CS is intended to contribute to the attainment and implementation of the "BSI IT-Grundschutzprofil 'Basis-Absicherung Kommunalverwaltung'" (BSI IT Basic Protection Profile "Basic Protection Local Administration", own translation) on the part of Hessian municipalities.

282 Hessisches Ministerium des Innern und für Sport, Innenministerium erweitert Beratungsangebot für Kommunen.

283 Hessischer Landtag (Drucksache 20/8039), Antwort auf Kleine Anfrage: Interkommunale Zusammenarbeit bei der Digitalisierung.
Hessisches Ministerium des Innern und für Sport, Cybersecurity: Hessen ist Partner im Nationalen Cyber-Abwehrzentrum.
Hessisches Ministerium des Innern und für Sport, Der Bereich Cybersecurity im Hessen3C.
Hessisches Ministerium des Innern und für Sport, Hessen3C.
Email exchange with representatives of Hessen3C in November 2019.

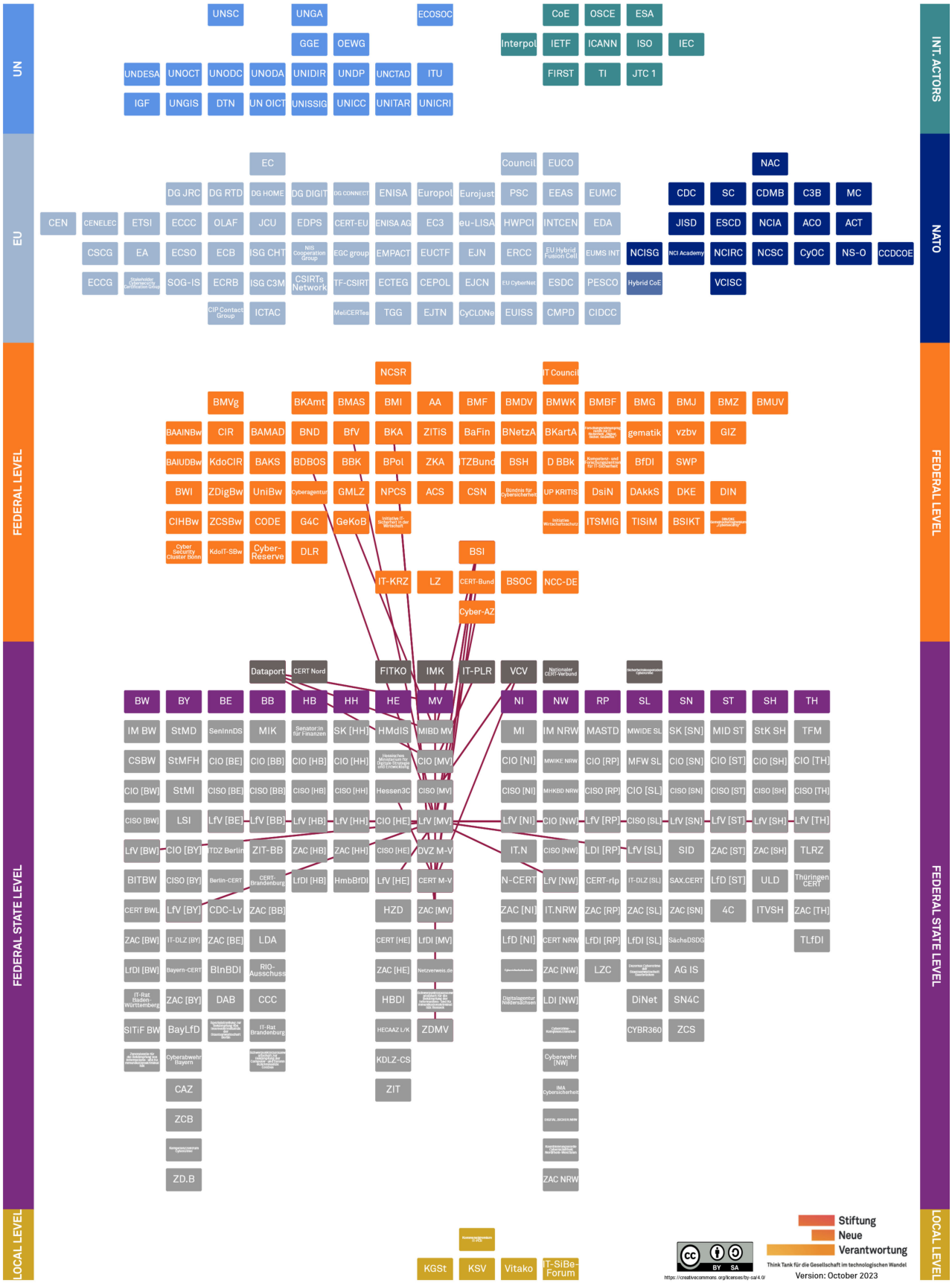
The KDLZ-CS is a municipal support service provided by the HMdIS.[284]

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.[285]

284 Hessischer Landtag (Drucksache 20/8039), Antwort auf Kleine Anfrage: Interkommunale Zusammenarbeit bei der Digitalisierung.
Hessisches Ministerium des Innern und für Sport, Innenministerium erweitert Beratungsangebot für Kommunen.
285 Staatsanwaltschaften Hessen, Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT).

9.8 Mecklenburg-Western Pomerania (MV)



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

Overview

- **Relevant policy documents:**
  - Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung Mecklenburg-Vorpommern, ZDMVG (in german, „Law on the Establishment of the Mecklenburg-Western Pomerania State Office Center for Digitization", own translation)
  - 2016: Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (in German, "Law for the promotion of electronic administrative activities in Mecklenburg-Western Pomerania", own translation)
  - 2014: Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (in German, "Guideline for ensuring information security in the state administration of Mecklenburg-Western Pomerania", own translation)

- **Ministerial responsibility(ies) for cyber and IT security topics: "**Ministerium für Inneres, Bau und Digitalisierung" (Ministry of the Interior, Building and Digitalisation of Mecklenburg-Western Pomerania, MIBD MV, official translation), "Abteilung 2 Digitale Verwaltung, digitale Infrastruktur und Geoinformation" (Department 2: Digital Administration, Digital Infrastructure and Geoinformation, own translation).

  MIBD MV cooperates with the BSI in the field of cybersecurity. The interior minister of Mecklenburg-Western Pomerania participates in the IMK.[286]

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

  He or she represents Mecklenburg-Western Pomerania in the IT-PLR and is a member of Dataport's Board of Directors[287].

- **Chief Information Security Officer of the State Administration (CISO [MV]):])**: In Mecklenburg-Western Pomerania, the state's CISO is based in the MIBD MV.

286 Ministerium für Energie, Infrastruktur und Digitalisierung Mecklenburg-Vorpommern, Verstärkte Kooperation zwischen Bund und Land bei IT-Sicherheit.
Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern, Organigramm.
287 Regierung Mecklenburg-Vorpommern, Staatssekretärin Ina-Maria Ulbrich.

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.[288]

- **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 MIBD MV assumes the function as Chairman of DVZ M-V's Supervisory Board.[289]

- **CERT**: The CERT M-V is located in the MIBD MV.

- **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 MIBD MV, Department 5. Counterintelligence and economic protection as its fields of work include threats from cyber operations and industrial espionage.

  If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[290]

- **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.[291]

- **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).[292]

288 DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH, DVZ.info 02/14.
Ministerium für Inneres und Sport Mecklenburg-Vorpommern, Stellenausschreibung Beauftragte/Beauftragter der Landesverwaltung für Informationssicherheit.
289 DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern, Über uns.
290 Verfassungsschutz Mecklenburg-Vorpommern, Spionageabwehr und Wirtschaftsschutz.
291 Landeskriminalamt Mecklenburg-Vorpommern, Cybercrime in M-V. Aktuelle Aspekte. (Website deleted)
Landespolizei Mecklenburg-Vorpommern, LKA-MV: Internationaler Ermittlungserfolg gegen Kinderpornografieplattform im Darknet.
292 Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Behörde.

Other actors in Mecklenburg-Western Pomerania:

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.[293]

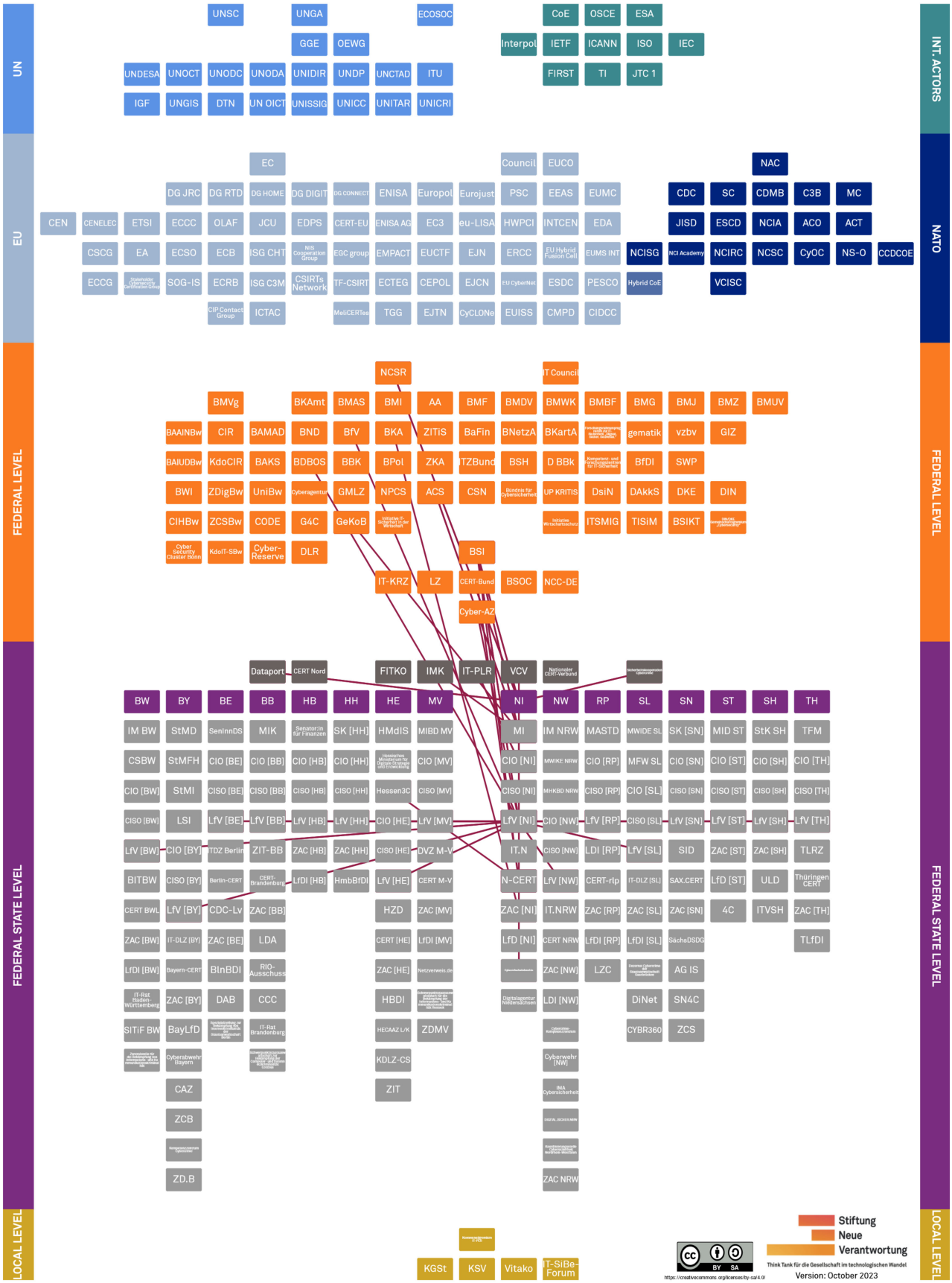
Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock (Special Prosecutor for Combatting Information and Communication Crimes of Rostock, own translation)
With statewide jurisdiction, the "Staatsanwaltschaft Rostock" (Public Prosecutor's Office of Rostock, own translation) is concurrently the "Schwerpunktstaatsanwaltschaft für die Bekämpfung der Informations- und Kommunikationskriminalität Rostock," thus also covering the area of cybercrime.[294]

Zentrum für Digitalisierung Mecklenburg-Vorpommern, ZDMV (Center for Digitization Mecklenburg-Western Pomerania, own translation)
The Center for Digitization Mecklenburg-Western Pomerania (ZDMV) is an upper state authority. The center is to bundle expertise on IT and digitization as well as on operational information security and data protection management centrally in a state office, thus relieving the state authorities of these tasks. Among other things, it will guarantee the provision of uniform and standardized IT services in the future.

The ZDMV operates under the umbrella of the MIBD MV and is controlled by the MIBD MV and the CIO [MV]. It cooperates with the DVZ M-V. The center is also to provide the CERT M-V as well as information security and data protection officers for the state authorities.[295]

293 Netzverweis, Online-Meldestelle.
Regierung Mecklenburg-Vorpommern, Landesregierung.
294 Justiz Online in Mecklenburg-Vorpommern, Zuständigkeit.
295 Landtag Mecklenburg-Vorpommern, Gesetz zur Errichtung des Landesamtes Zentrum für Digitalisierung Mecklenburg-Vorpommern.
Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern, Landtag gibt grünes Licht: Zentrum für Digitalisierung kann kommen.

9.9 Lower Saxony (NI)



The state of Lower Saxony is represented on the NCSR. It has signed a cooperation agreement with the BSI. 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

- **Relevant policy documents:**
  - 2019: Niedersächsisches Gesetz über digitale Verwaltung und Informationssicherheit (in German, "Law on digital administration and information security Lower Saxony", own translation)

- **Ministerial responsibility(ies) for cyber and IT security topics: "**Niedersächsisches Ministerium für Inneres und Sport" (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.[296]

- **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.[297]

- **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.*[298]

296 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.
297 Niedersächsisches Ministerium für Inneres und Sport, Neuer CIO in Niedersachsen: Dr. Horst Baier ist IT-Bevollmächtigter der Landesregierung.
298 Ministerium für Inneres und Sport Niedersachsen, Informationssicherheit.
Ministerium für Inneres und Sport, Informationssicherheit in Niedersachsen.

- **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).[299]

- **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 cybersecurity situation picture. More than 100 municipalities in Lower Saxony rely on support services offered by N-CERT.[300]

- **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.

  If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[301]

- **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.[302]

- **State Data Protection Authority:** Landesbeauftragte:r für den Datenschutz Niedersachsen (State Commissioner for Data Protection Lower Saxony, LfD, own translation).[303]

299 Landesbetrieb IT.Niedersachsen, Das Organigramm von IT.Niedersachsen.
300 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.
301 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.
302 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?.
303 Die Landesbeauftragte für den Datenschutz Niedersachsen, Die Behörde.

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.

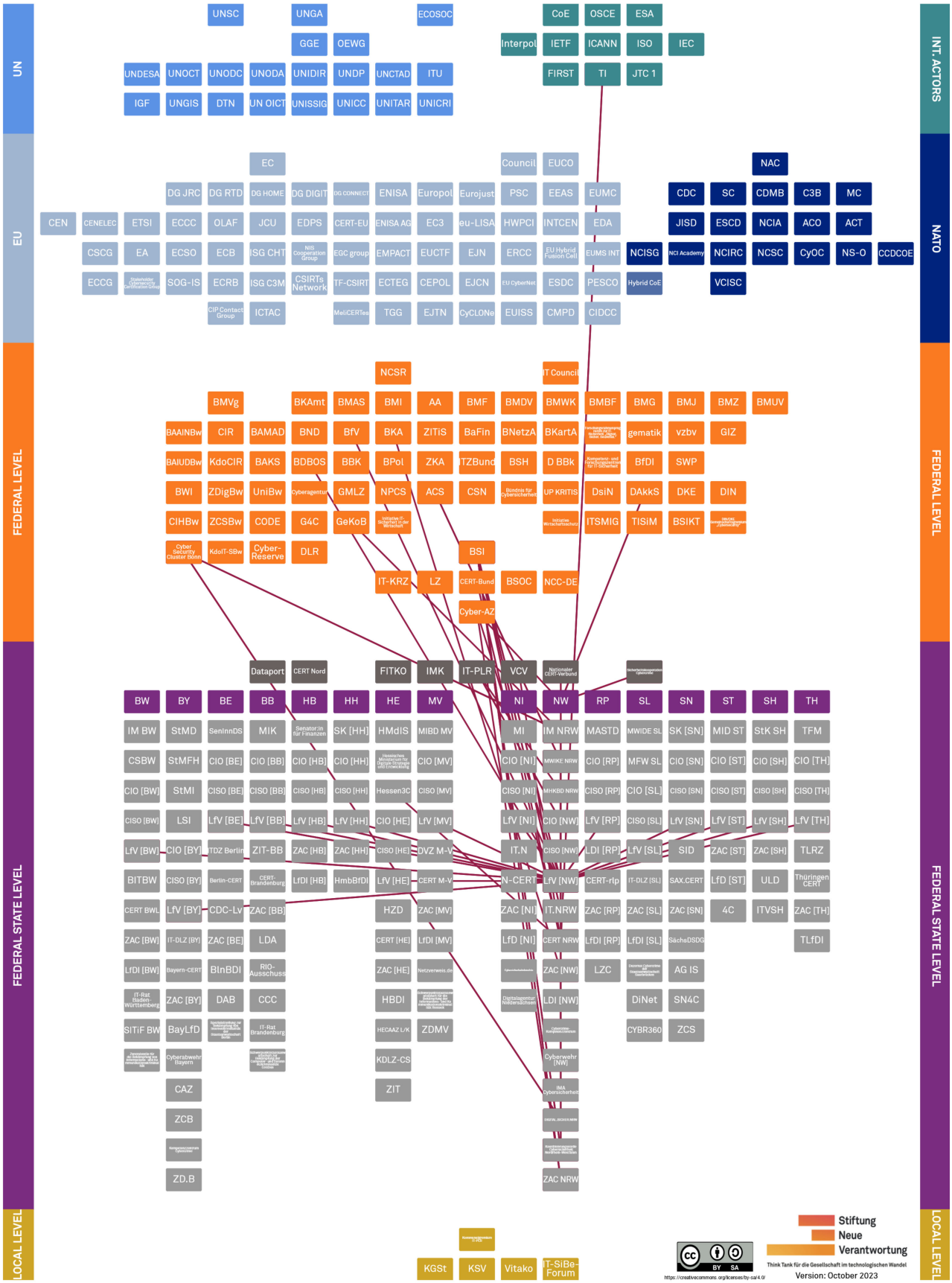
Moreover, municipalities can make use of services provided by the N-CERT.[304]

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).[305]

304 Niedersächsisches Ministerium des Innern und für Sport, Sicherheit in der digitalen Welt.
305 Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: Digitalagentur Niedersachsen.
Digitalagentur Niedersachsen, IT-Sicherheit für Niedersachsen.
Niedersächsisches Ministerium für Wirtschaft, Arbeit, Verkehr und Digitalisierung, Digitalagentur und weitere Angebote zur Unterstützung.

9.10 North Rhine-Westphalia (NW)



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

- **Relevant policy documents:**
  - 2021: Cybersicherheitsstrategie des Landes Nordrhein-Westfalen (in German, "Cybersecurity strategy of the state of North Rhine-Westphalia", own translation)
  - 2016: Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen (in German, "Law for the promotion of electronic administration in North Rhine-Westphalia", own translation)

- **Ministerial responsibility(ies) for cyber and IT security topics:**
  - "Ministerium des Innern des Landes Nordrhein-Westfalen" (Ministry of the Interior of the State of North Rhine-Westphalia, IM NRW, own translation), "Abteilung 3: Gefahrenabwehr, Vermessung Referat 32: Staatliche Krisenvorsorge, Krisenmanagement der Landesregierung, Schutz Kritischer Infrastruktur, Zivile Verteidigung" (Department 3: Hazard Prevention, Surveying, Division 32: State Crisis Preparedness, State Government Crisis Management, Critical Infrastructure Protection, Civil Defense, own translation) and "Abteilung 7: Digitalisierung im IM und im Geschäftsbereich, Referat 73: Koordinierungsstelle für Cybersicherheit NRW, Informationssicherheit im IM und Geschäftsbereich" (Department 7: Digitization in IM and its organizational area, Division 73: NRW Cyber Security Coordination Office, Information Security in IM and its organizational area, own translation).

    The interior minister of North Rhine-Westphalia participates in the IMK. The IM NRW is represented on the Advsory Board of the Cyber Security Cluster Bonn.[306]

  - "Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen" (Ministry of Home Affairs, Municipal Affairs, Building and Digitalization of the State of North Rhine-Westphalia, MHKBD NRW, own translation) "Abteilung 2: Digitalisierung der Landesverwaltung, Referat 224: Informationssicherheit in der Landesverwaltung" (Department 2: Digitalization of the State Administration, Division 224: Information Security in the State Administration, own translation).[307]

306 Ministerium des Innern des Landes Nordrhein-Westfalen, Geschäftsverteilungsplan.
307 Ministerium für Heimat, Kommunales, Bau und Digitalisierung des Landes Nordrhein-Westfalen, Geschäftsverteilungsplan.

- "Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen" (Ministry of Economic Affairs, Industry, Climate Action and Energy, MWIKE NRW, official translation), "Abteilung I: Zentralabteilung" (Department I: Central Department, own translation), "Referat 115: IT, Informationssicherheit, Open.NRW" (Division 115: IT, Information Security Open. NRW, own translation), „Abteilung 4: Innovation und Märkte, Referat 414: IKT, Mobilfunk und Cybersicherheit in der Wirtschaft" (Department 4: Innovation and Markets, Division 414: ICT, Mobile Communications and Cybersecurity in the Economy, own translation) and „Abteilung 8: Digitalisierung, Startups und Dienstleistungen, Referat 811: digitale Kompetenzen" (Department 8: Digitization, Startups and Services, Division 811: Digital Competencies).

  The MWIKE NRW participates in the ACS. The Cyberwehr [NW] draws on funding from the MWIKE NRW (Regio Call EFRE.NRW).[308]

- **State Commissioner for Information Technology (CIO [NW])**: The CIO of North Rhine-Westphalia is based in the MHKBD 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.[309]

- **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 MHKBD NRW.[310]

- **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 MHKBD NRW.

  The BSI and IT.NRW are cooperating.[311]

308 Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen, Geschäftsverteilungsplan.
309 Die Landesregierung Nordrhein-Westfalen, Prof. Andreas Meyer-Falcke neuer CIO.
310 Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie Nordrhein-Westfalen, Geschäftsverteilungsplan.
311 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.

- **CERT**: The CERT NRW is operated by IT.NRW. Via the CERT NRW, IT.NRW operates a "Kommunaler Warn- und Informationsdienst" (Municipal Warning and Information Service, KWID, own translation), which is available to municipalities in North Rhine-Westphalia

  It takes part in the National CERT Network and TI.[312]

- **State Authority for the Protection of the Constitution (LfV [NW])**: Das IM NRW beherbergt die Verfassungsschutzbehörde des Landes. Dort (Abteilung 6, Gruppe 61) befinden sich Zuständigkeiten für ein Cyber-Zentrum für Analysen, Prototyping und Internetaufklärung (Referat 611) sowie Spionageabwehr, Wirtschaftsschutz und Cyberabwehr (Referat 613).

  If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[313]

- **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).[314]

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 "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.

312 Information und Technik Nordrhein-Westfalen, Informationssicherheit für die Landesverwaltung NRW.
Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie Nordrhein-Westfalen, Nordrhein-Westfalen stärkt Cybersicherheit in den Kommunen mit neuem Warn- und Informationsdienst.
313 Ministerium des Innern Nordrhein-Westfalen, Organisationsplan.
314 Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Über uns.

The ZISC is also home to the ZAC [NW] for the economy.[315]

Cyberwehr (Cyber Defence [NW], own translation)
The Cyberwehr is a pilot project which provides a point of contact for SMEs in the cities of Bochum, Essen, and Gelsenkirchen. These can contact the Cyberwehr free of charge by telephone in case of emergencies. After an initial assessment by telephone and depending on the scope of the incident, a partner of the Cyberwehr can be commissioned to provide "first aid" free of charge, either on-site or remotely, for example, by taking stock or making recommendations for action. Further system reconstruction or other services by these or other companies will continue to be subject to a charge for the SME. In the long-term, the pilot project is to be extended to North Rhine-Westphalia as a whole.

The Cyberwehr is supported by funding from MWIKE NRW (via Regio Call EFRE.NRW).[316]

Interministerieller Ausschuss Cybersicherheit (Interministerial Cybersecurity Committee, IMA Cybersicherheit, own translation)
In North Rhine-Westphalia, cybersecurity topics are exchanged, and measures for increased cybersecurity are coordinated within a dedicated interministerial committee. The IMA was also involved in the development of the North Rhine-Westphalian cybersecurity strategy and the state report on cybersecurity.

All departments of the North Rhine-Westphalian state government, including the IM NRW and the MWIKE NRW, are represented in the IMA Cybersecurity under the chairmanship of the Coordination Office for Cybersecurity.[317]

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.

315 Polizei Nordrhein-Westfalen, Das Cybercrime-Kompetenzzentrum beim LKA NRW.
Polizei Nordrhein-Westfalen, Lagebild Cybercrime.
316 Cyberwehr, Über Uns.
eurobits, Pilotprojekt für das Ruhrgebiet: eurobits baut Cyberwehr für den Mittelstand auf.
317 Ministerium des Innern des Landes Nordrhein-Westfalen, Bericht zur Cybersicherheit in Nordrhein-Westfalen.
Ministerium des Innern des Landes Nordrhein-Westfalen, Cybersicherheitsstrategie des Landes Nordrhein-Westfalen.

DIGITAL.SICHER.NRW was established by the MWIKE NRW. The Cyber Security Cluster Bonn is a partner of the competence center.[318]

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.

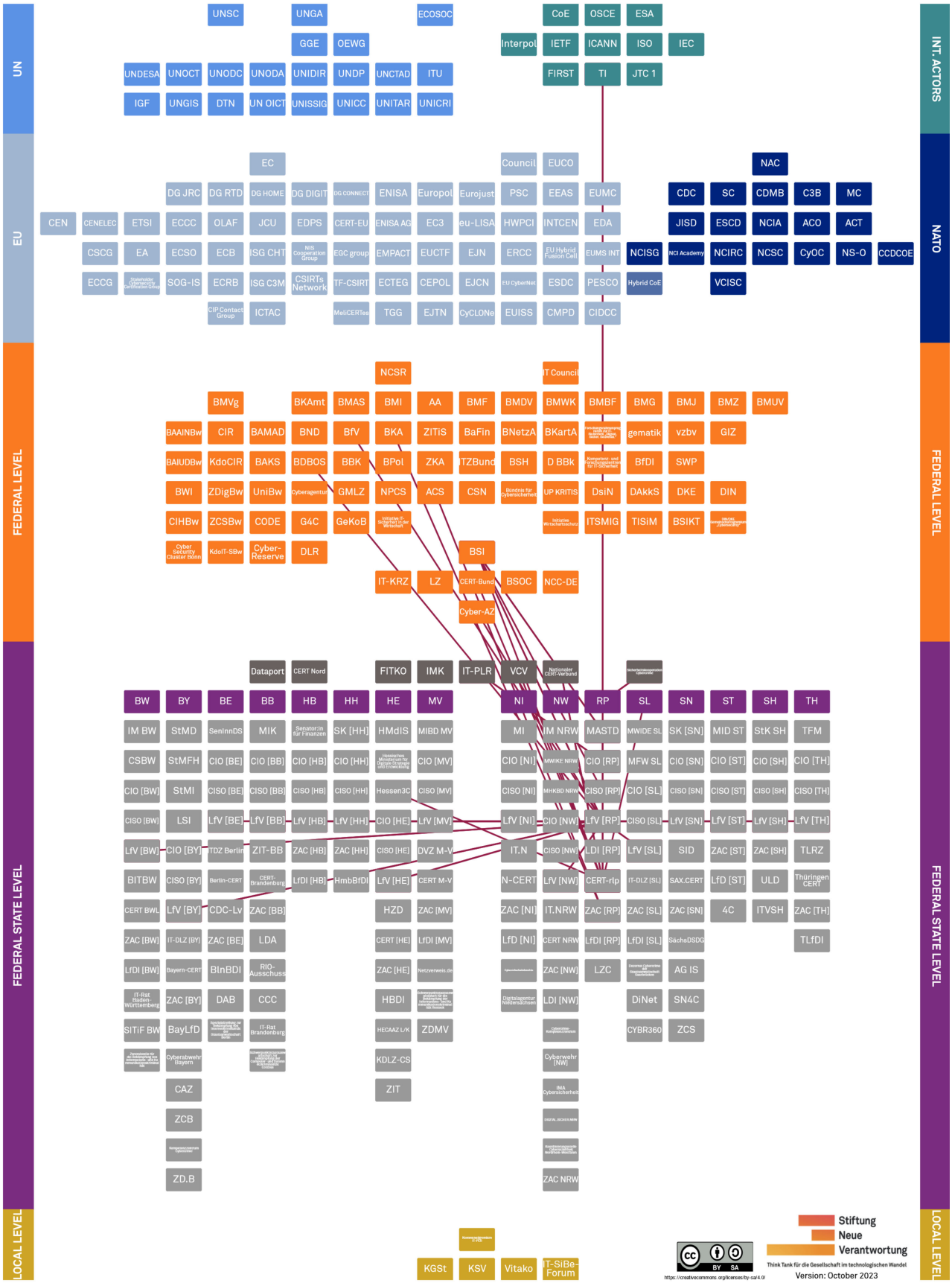
The IMA Cybersicherheit convenes under the chairmanship of the Coordination Office for Cybersecurity. Coordination Office for Cybersecurity is located within the purview of the IM NRW and is designated as the state's central point of contact vis-à-vis the BSI.[319]

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.[320]

318 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.
319 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.
320 Justiz-ONLINE, Zentral- und Ansprechstelle Cybercrime (ZAC NRW).

9.11 Rhineland-Palatinate (RP)



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

Overview

- **Relevant policy documents:**
  - 2020: Landesgesetz zur Förderung der elektronischen Verwaltung in Rheinland-Pfalz (in German, "Law for the promotion of electronic administration in Rhineland-Palatinate", own translation)

- **Ministerial responsibility(ies) for cyber and IT security topics:** "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.[321]

- **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.[322]

- **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.[323]

321 Ministerium des Innern und für Sport, Kooperationsvereinbarung zur Cybersicherheit abgeschlossen.
Ministerium für Arbeit, Soziales, Transformation und Digitalisierung Rheinland-Pfalz, Organigramm.
322 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.
323 Ministerium der Justiz Rheinland-Pfalz, Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Rheinland-Pfalz.

- **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.[324]

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

  In line with an agreement between the Saarland and Rhineland-Palatinate, CERT-rlp also provides the CERT for the Saarland (SL). It takes part in the National CERT Network and TI.[325]

- **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.

  If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[326]

- **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.[327]

- **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).[328]

324 Landesbetrieb Daten und Information, Der LDI: Der IT-Dienstleister der Landesverwaltung Rheinland-Pfalz. Landesbetrieb Daten und Information, Impressum.
325 Ministerium des Innern und für Sport Rheinland-Pfalz, CERT-rlp.
326 Ministerium des Innern und für Sport Rheinland-Pfalz, Spionageabwehr, Wirtschaftsschutz und Cybersicherheit.
327 Polizei Rheinland-Pfalz, Aufgaben des Dezernates Cybercrime.
328 Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Über uns.

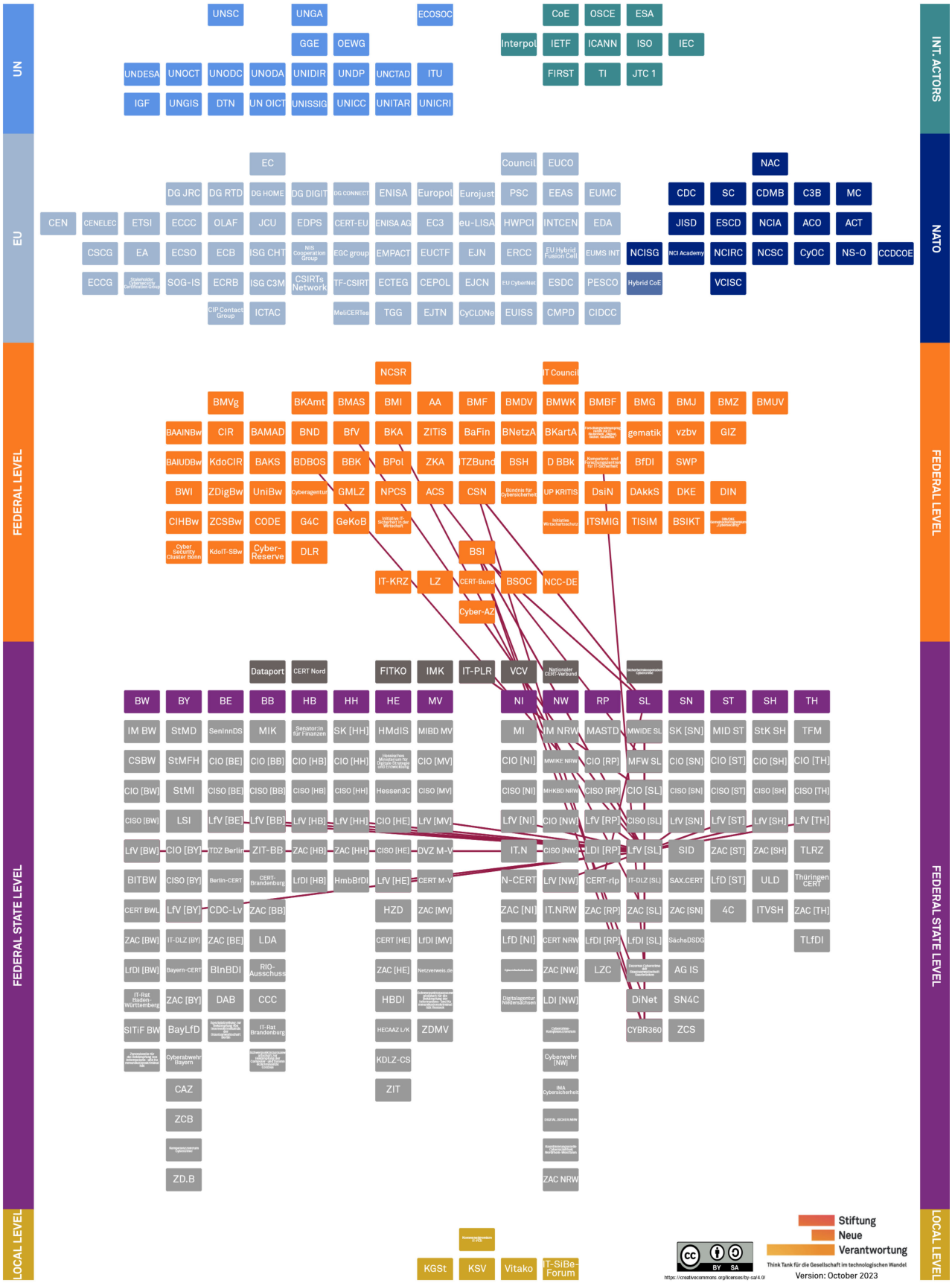
Other actors in Rhineland-Palatinate:

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.[329]

329 Generalstaatsanwaltschaft Koblenz, Landeszentralstelle Cybercrime (LZC).

9.12 Saarland (SL)



The Saarland has concluded a legally binding cooperation agreement with the BSI to intensify cooperation. In addition, the state is a pilot region of the CSN. The Saarland Ministry of Finance and Europe participates in the ACS as a multiplier.

Overview

- **Relevant policy documents:**
  - 2019: Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes (in German, "Law on the defense against threats to data in the country's information and communications infrastructure", own translation)
  - 2017: Gesetz zur Förderung der elektronischen Verwaltung im Saarland (in German, "Law for the promotion of electronic administration in Saarland", own translation)

- **Ministerial responsibility(ies) for cyber and IT security topics:**
  - "Ministerium für Wirtschaft, Arbeit, Energie und Verkehr" (Ministry of Economy, Labor, Energy and Transport, MWIDE SL, own translation), "Abteilung D: Digitalisierung in Wirtschaft und Verwaltung" (Department D: Digitization in Economy and Administration), "Referat D/6 Informationssicherheits- und Datenschutzmanagement, IT-Recht" (Division D/6 Information Security and Data Protection Management).[330]
  - "Ministerium der Finanzen und für Wissenschaft" (Ministry of Finance and Science, MFW SL, own translation), "Stabsstelle Informationssicherheitsmanagement und IT-Recht" (Administrative Department for Information Security Management and IT Law).[331]

- **State Commissioner for Information Technology (CIO [SL]**: Saarland's CIO is a state secretary of the MWIDE SL.

  He or she represents Saarland in the IT-PLR.[332]

- **Chief Information Security Officer of the State Administration (CISO [SL])**: Also Saarland's CISO is located in the MWIDE SL.

  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.[333]

330 Ministerium für Wirtschaft, Innovation, Digitales und Energie Saarland, Organigramm des Ministeriums für Wirtschaft, Innovation, Digitales und Energie.
331 Ministerium der Finanzen und für Wirtschaft, Organigramm.
332 Ministerium für Wirtschaft, Innovation, Digitales und Energie, Staatssekretärin und CIO Elena Yorgova-Ramanauskas.
333 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 MFW SL.[334]

- **CERT**: CERT Saarland is being provided by CERT-rlp in line with an agreement between the federal states of Saarland and Rhineland-Palatinate.[335]

- **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.

  If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[336]

- **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.[337]

- **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).[338]

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.[339]

334 Ministerium für Finanzen und Europa Saarland, Themen & Aufgaben.
335 Kommune 21, CERT für saarländische Kommunen.
336 Ministerium des Innern, Bauen und Sport Saarland, Lagebild Verfassungsschutz 2019.
337 sol.de, Saar-Kripo eröffnet neue "Cybercrime"-Dienststelle. (Website entfernt)
338 Unabhängiges Datenschutzzentrum Saarland, Über Uns.
339 Juristisches Internetprojekt Saarbrücken, Neues Dezernat „Cybercrime" bei der Staatsanwaltschaft Saarbrücken.

Netzwerkstelle Digitalisierung, DiNet (Digitization Network, own translation)
The Digitization Network (DiNet) is primarily intended to provide support to companies from small and medium-sized enterprises in the Saarland in their digital transformation - and to focus, for example, on topics such as the digitization of work enviroments and cybersecurity. The regional digitalization network is intended to bring relevant players into contact with one another, and to create innovation networks and strengthen knowledge exchange, among other things. The focus is not only on players from the business community, but also on networking with science and politics. Specifically, the Digitalstarter Saarland funding program is intended to support small and medium-sized enterprises in adapting to the requirements created by digitization.

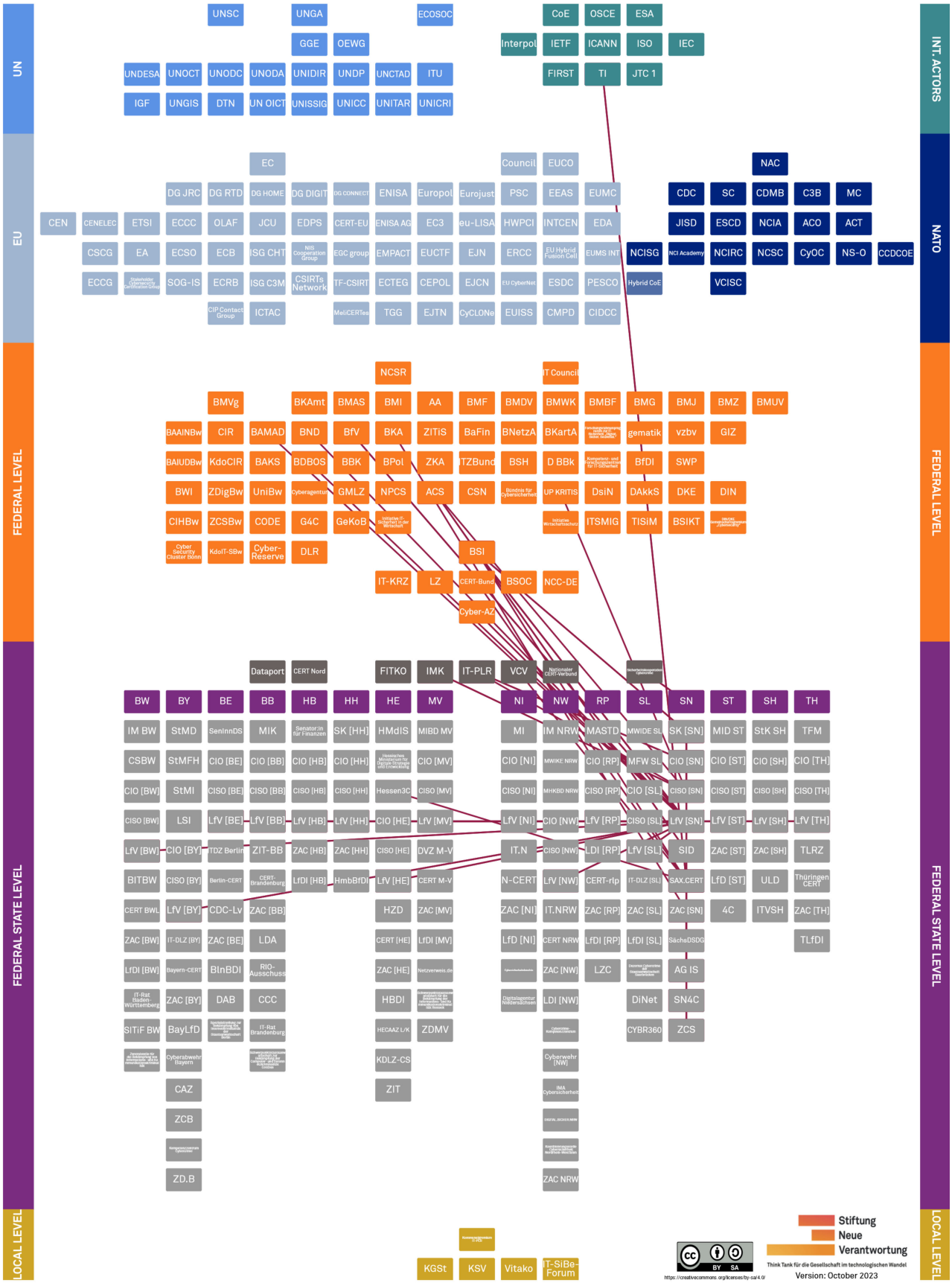
DiNet is part of MWIDE SL and is the initiator of CYBR360.[340]

Initiative für Cybersicherheit, CYBR360 (Initiative für Cybersecurity, own translation)
CYBR360 is an initiative to strengthen the cybersecurity of small and medium-sized enterprises in Saarland. With the "Digital Rescue Chain", CYBR360 provides a point of contact for small and medium-sized enterprises as an acute response to IT security incidents. With the support of the CSN, the aim here is to initiate, in addition to initial operational support, technical and institutional responses adapted to the situation, such as notifications and reports, at an early stage. CYBR360 bundles expertise from research, consulting and application and includes a network platform as well as various formats for further education and prevention.

CYBR 360 was launched as a digital security initiative by DiNet and is affiliated with MWIDE SL. Within the framework of the Saarland CSN pilot region, it works closely with the BSI and the ZAC [SL].[341]

340 Ministerium für Wirtschaft, Innovation, Digitales und Energie SL, DiNet.
341 CYBR360 Saarland, die Initiative für Cybersicherheit.
Saarland.innovation&standort, Neu: CYBR360 – Das Netzwerk für digitale Sicherheit im Saarland.

9.13 Saxony (SN)



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

Overview

- **Relevant policy documents:**
  - 2019: Gesetz zur Gewährleistung der Informationssicherheit im Freistaat Sachsen (in German, "Law for ensuring information security in the Free State of Saxony", own translation)
  - 2019: Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen (in German, "Law for the promotion of electronic administration in the Free State of Saxony", own translation)

- **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.[342]

- **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.[343]

- **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

342 Sächsische Staatskanzlei, Organisation.
Sächsische Staatskanzlei, Sachsen und Bund kooperieren bei Cyber-Sicherheit.
343 Sächsische Staatskanzlei, Staatssekretäre.

InfoSic, own translation), a state working group of the IMK, as well as the ACS and UP KRITIS.[344]

- **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.[345]

- **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.

It is listed as a participating team at TI.[346]

- **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 the working level exist with the BfV, its counterparts in all federal states (LfV's), the BND, the BAMAD, the BSI, and the Cyber-AZ. If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[347]

- **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).[348]

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 secu-

344 Sächsische Staatskanzlei, Beauftragter für Informationssicherheit des Landes (BfIS).
345 Sächsische Staatskanzlei, Nachgeordnete Behörden.
Staatsbetrieb Sächsische Informatik Dienste, Aufgaben, Leistungen.
346 Sächsische Staatskanzlei, Jahresbericht Informationssicherheit 2020 des Beauftragten für Informationssicherheit des Landes.
Staatsbetrieb Sächsische Informatik Dienste, CERT & Informationssicherheit.
347 Staatsministerium des Innern Sachsen, Sächsischer Verfassungsschutzbericht 2019.
348 Sächsischer Datenschutzbeauftragter, Über uns.

rity 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.[349]

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 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.[350]

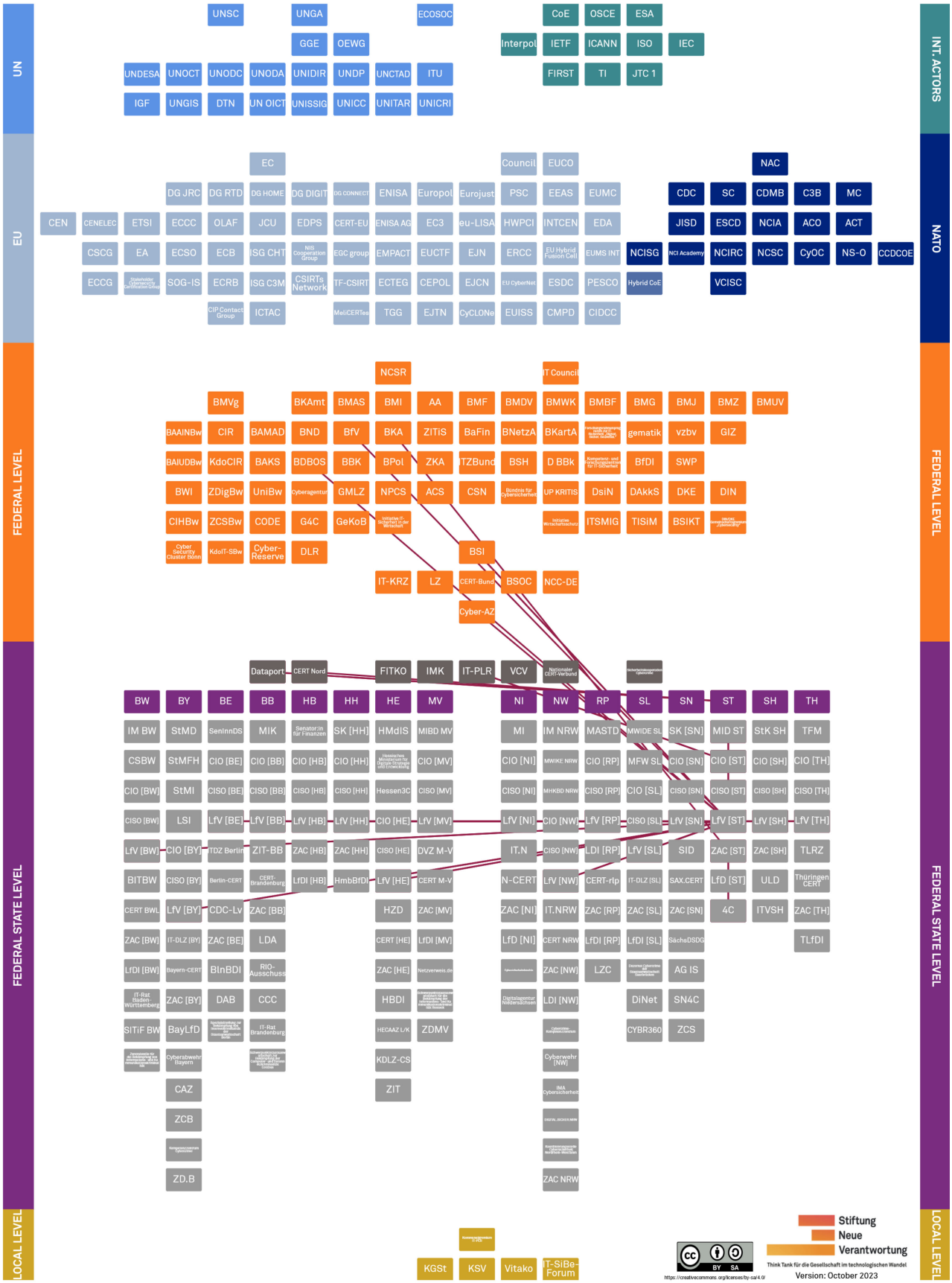
Zentralstelle Cybercrime Sachsen (Central Office Cybercrime Saxony, ZCS, own translation)

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.[351]

349 Sächsische Staatskanzlei, Arbeitsgruppe Informationssicherheit.
Sächsische Staatskanzlei, Sächsisches Informationssicherheitsgesetz.
350 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.
351 Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: Spezialisierte Einrichtungen der Justiz.
Staatsministerium der Justiz, Sächsisches Justizministerialblatt Nr. 5/2018.

9.14 Saxony-Anhalt (ST)



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

Overview

- **Relevant policy documents:**
  - 2019: Gesetz zur Förderung der elektronischen Verwaltung im Land Sachsen-Anhalt (in German, "Law for the promotion of electronic administration in the state of Saxony-Anhalt", own translation)

- **Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit:** "Ministerium für Infrastruktur und Digitales Sachsen-Anhalt" (Ministry of Infrastructure and Digital Affairs, MID ST, own translation), "Abteilung 4 Digitale Gesellschaft und Geoinformation" (Department 4: Digital Society and Geoinformation, own translation) and "Abteilung 5 Digitale Verwaltung" (Department 5: Digital Administration, own translation).[352]

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

  He or she represents Saxony-Anhalt on the IT-PLR.[353]

- **Chief Information Security Officer of the State Administration (CISO [ST])**: In addition to the federal state's CIO, the MID ST 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.[354]

- **IT Service Provider of the Federal State Administration:** Dataport, actor description see below (Chapter 9.17).

- **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

352 Ministerium für Infrastruktur und Digitales Sachsen-Anhalt, Organigramm.
353 Sachsen-Anhalt, Der Beauftragte der Landesregierung für Informationstechnik (CIO).
354 Ministerium für Justiz und Gleichstellung Sachsen-Anhalt, Leitlinie zur Informationssicherheit in der unmittelbaren Landesverwaltung Sachsen-Anhalt.

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.

If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[355]

- **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).[356]

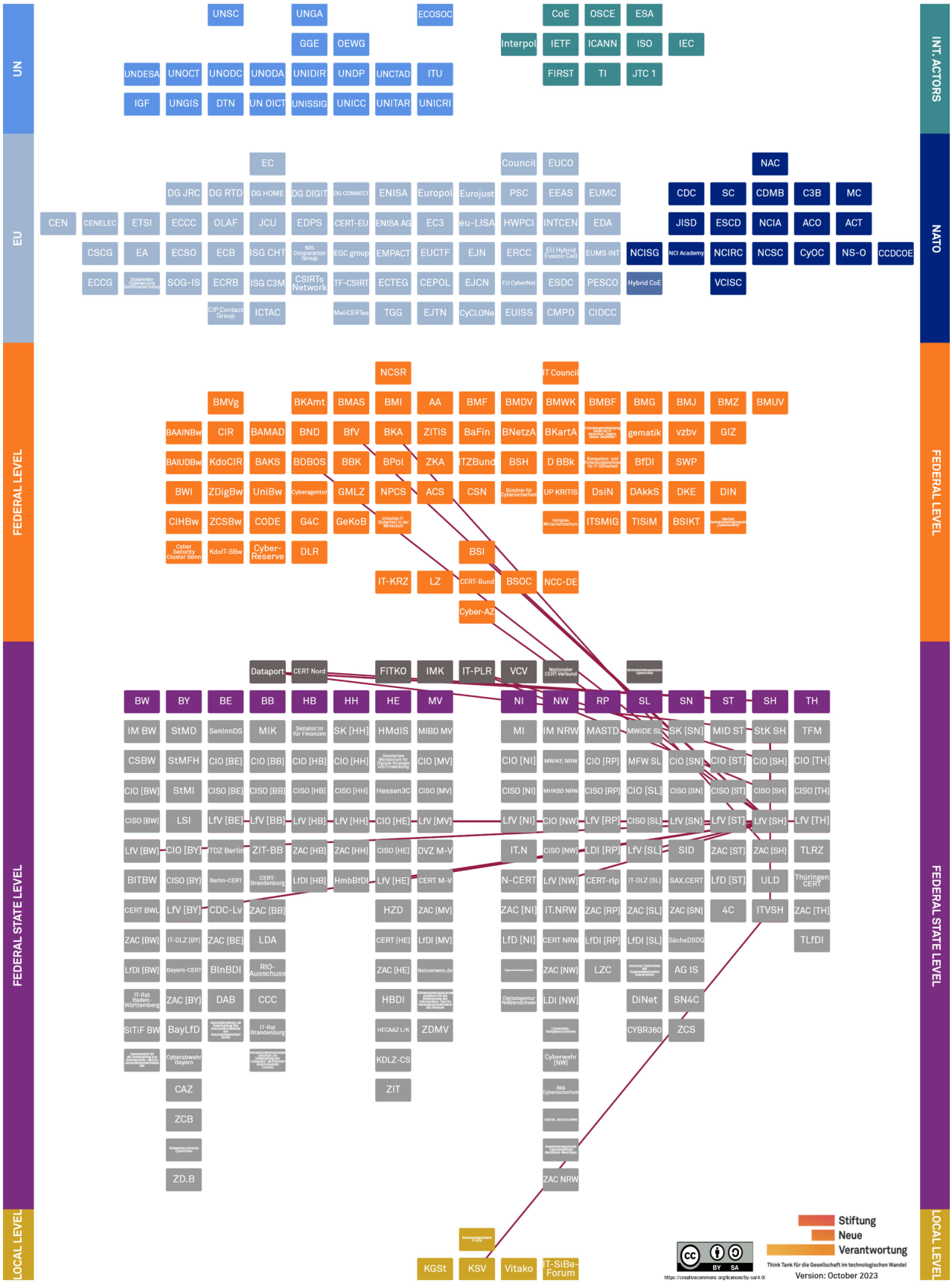
Other actors in Saxony-Anhalt:

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].[357]

355 Ministerium für Inneres und Sport Sachsen-Anhalt, Organisationsplan.
Ministerium für Inneres und Sport des Landes Sachsen-Anhalt, Verfassungsschutzbericht 2019.
356 Landesbeauftragter für den Datenschutz Sachsen-Anhalt, Gesetzliche Aufgaben und Zuständigkeiten.
357 Hallelife.de, Sachsen-Anhalt startet Kompetenzzentrum gegen Internetkriminalität.

9.15 Schleswig-Holstein (SH)



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

Overview

- **Relevant policy documents:**
  - 2009: Gesetz zur elektronischen Verwaltung für Schleswig-Holstein (in German, "Law on electronic administration in Schleswig-Holstein", own translation)

- **Ministerial responsibility(ies) for cyber and IT security topics:** "Staatskanzlei Schleswig-Holstein" (State Chancellery Schleswig-Holstein, StK SH, official translation), "Abteilung 3: Digitalisierung und Zentrales IT-Management der Landesregierung" (Department 3: Digitization and Central IT Management of the State Government, own translation).[358]

- **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 StK SH.[359]

- **Chief Information Security Officer of the State Administration (CISO [SH])**: In Schleswig-Holstein, the federal state's CISO is located within Department 3 of the StK 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.[360]

- **IT Service Provider of the Federal State Administration:** Dataport, actor description see below (Chapter 9.17).

- **CERT**: CERT Nord, actor description see below (Chapter 9.17).

- **State Authority for the Protection of the Constitution (LfV [SH])**: The State Authority for the Protection of the Constitution of Schleswig-Holstein is located

358 Staatskanzlei Schleswig-Holstein, Organisation und Ansprechpartner.
359 Schleswig-Holstein, E-Government – Steuerung und Zusammenarbeit.
360 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.

in the "Ministerium für Inneres, Kommunales, Wohnen und Sport" (Ministry of the Interior, Municipal Affairs, Housing and Sports, MIKWS SH, official translation), Department IV 7. Its fields of work include counterintelligence and economic protection. A different department (IV 76) also deals with digital work, IT, G10, and secret protection.

If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[361]

- **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.[362]

- **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).[363]

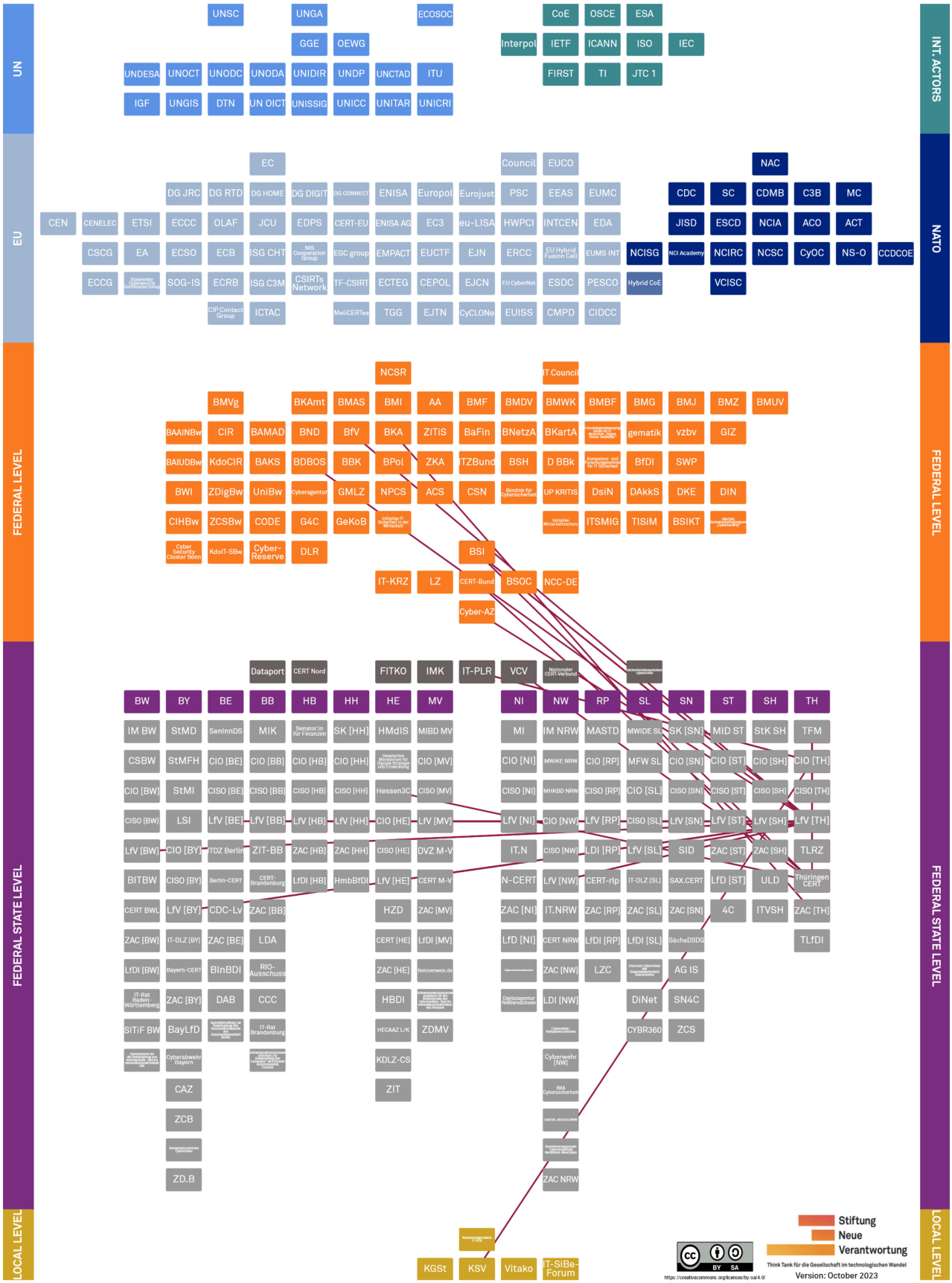
Other actors in Schleswig-Holstein:

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 StK 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.[364]

361 Der Ministerpräsident des Landes Schleswig-Holstein, Spionageabwehr und Wirtschaftsschutz.
Ministerium für Inneres, ländliche Räume, Integration und Gleichstellung, Organisationsplan.
362 Landespolizei Cybercrime, Zentrale Ansprechstelle Cybercrime (ZAC).
363 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Wir über uns.
364 Bundesministerium des Innern, für Bau und Heimat, Online Kompendium Cybersicherheit in Deutschland: IT-Verbund Schleswig-Holstein (ITVSH).
IT-Verbund Schleswig-Holstein, SiKoSH.
Landesregierung Schleswig-Holstein, Gesetz zur Errichtung einer Anstalt öffentlichen Rechts „IT-Verbund Schleswig-Holstein" (Errichtungsgesetz ITVSH).

9.16 Thuringia (TH)



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

Overview

- **Relevant policy documents:**
  - 2018: Thüringer Gesetz zur Förderung der elektronischen Verwaltung (in German, "Law for the promotion of electronic administration Thuringia", own translation)

- **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).[365]

- **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.[366]

- **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].[367]

- **IT Service Provider of the Federal State Administration:** "Thüringer Landesrechenzentrum" (Thuringian Computing Centre, TLRZ, own translation), which falls under the purview of the TFM.[368]

365 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.
366 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.
367 Finanzministerium Thüringen, Informationssicherheitsleitlinie der Thüringer Landesverwaltung.
368 Thüringer Landesrechenzentrum, Über uns.

- **CERT**: The ThüringenCERT is being operated by the TLRZ.[369]

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

  If necessary to prevent or investigate activities that compromise the security or use of information technology, the LfV can be supported by the BSI.[370]

- **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.[371]

- **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).[372]

369 Bundesamt für Sicherheit in der Informationstechnik, BSI und Thüringen: Engere Zusammenarbeit bei der Cyber-Sicherheit. (Website deleted)
Thüringer Landesrechenzentrum, ThüringenCERT.
370 Ministerium für Inneres und Kommunales Thüringen, Organigramm.
Ministerium für Inneres und Kommunales Thüringen, Wirtschaftsspionage / Wirtschaftsschutz.
371 Heise Online, Cybercrime: Neue Herausforderungen für Thüringer LKA.
Ministerium für Inneres und Kommunales Thüringen, Internetkriminellen gemeinsam mit den Unternehmen das Handwerk legen. (Website deleted)
372 Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Aufgaben.

9.17 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.[373]

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 MIBD MV (the CIO [MV]), the Ministry of Finance [ST], and the StK SH.[374]

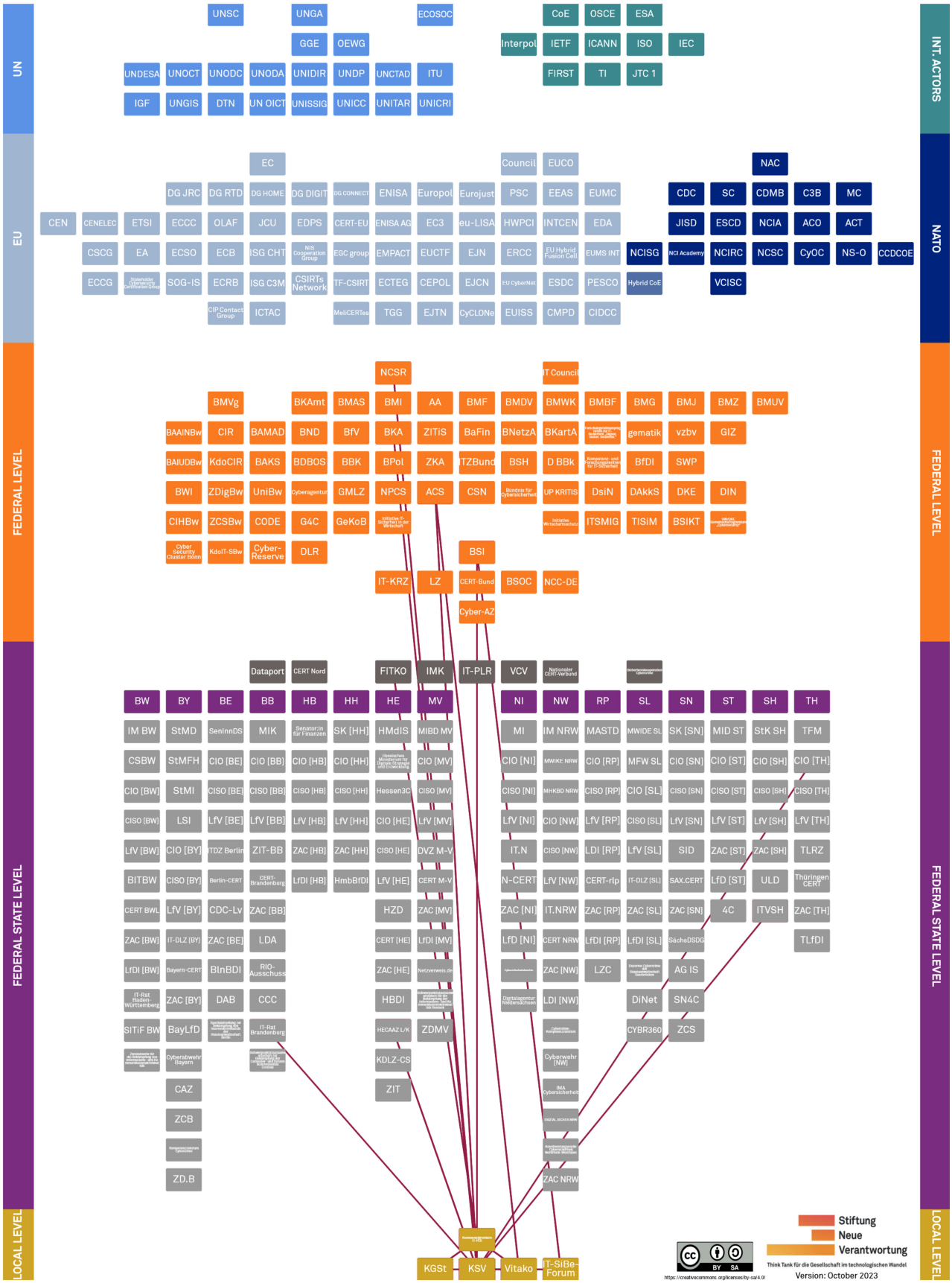
Sicherheitskooperation Cybercrime (Security Cooperation Cybercrime, own translation)

"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-Württemberg, Hesse, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate, and Saxony) and the Bitkom.[375]

373 CERT Nord, CERT Nord.
374 Bundesamt für Sicherheit in der Informationstechnik, BSI und Dataport vereinbaren engere Zusammenarbeit.
Dataport, Die Organe von Dataport.
Dataport, Dataport.Digitalisierung. Mit Sicherheit.
Dataport, Security Operations Center.
375 Sicherheitskooperation Cybercrime, Aktivitäten.
Sicherheitskooperation Cybercrime, Die Kooperation.

10. Explanation – Actors at Local Level



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

Policy Overview

Year	Name
2019	IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung (Version 2.0, in German, "IT basic protection profile: basic protection municipal administration", own translation)
2017	Handreichung: Informationssicherheits-Leitlinie in Kommunalverwaltungen (in German, "Guidance: Information security guideline in municipal administrations", own translation) Previous documents: • 2015: Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen (in German, "Guidance: Information security guideline in municipal administrations", own translation)

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 pool knowledge and know-how to aid its members regarding 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.[376]

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

376 Vitako, Gremien.
Vitako. Satzung.
Vitako, Verband.
Vitako, Verein.

translation) standards[377]. 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 is being supported by the BSI. 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 the design of the information security guideline in municipal administrations, own translation).[378]

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.[379]

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

377 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.

378 Heino Sauerbrey, Ziel und Zweck des Internetforums für IT-Sicherheitsbeauftragte der Länder und Kommunen. (Website deleted)
IT-SiBe-Forum, Grundsätze.
IT-SiBe-Forum, Kurzinformation.
IT-SiBe-Forum, Meilensteine.

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

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

The KSV (through the Association of German Cities) represents the municipalities in the NCSR. 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. The trainings of the HECAAZ L/K take place in coordination with and support of the regional KSV's.[380]

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

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 the IT Planning Council 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. The committee meets approximately every four weeks.

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.[381]

381 FITKO, Wie unterstützt die FITKO die Digitale Transformation?.
Innenministerkonferenz, Bericht zum IT-Planungsrat.
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

Dr. Sven Herpig is Director for Cybersecurity Policy and Resilience. At SNV, his focal areas include German cybersecurity policy, government hacking, vulnerability management, geopolitical responses to cyber operations, the information security of machine learning and active cyber defense.

Frederic Dutke supports the division Cybersecurity Policy and Resilience as a student assistant. His focus is the German cybersecurity architecture.

Contact the authors:

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

Frederic Dutke
Student Assistant Cybersecurity Policy and Resilience
fdutke@stiftung-nv.de

Imprint

Stiftung Neue Verantwortung e.V.
Ebertstraße 2
10117 Berlin
T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97
www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Jan Klöthe

Free Download:
www.stiftung-nv.de

ISBN 978-3-00-076311-3

This work is subject to a Creative Commons-License (CC BY-SA). The reproduction, distribution and publication, modification or translation of content of the Neue Verantwortung Foundation, which is licensed under the "CC BY-SA", as well as the creation of products derived from them, are permitted under the conditions "attribution" and "further use under the same license". Detailed information on licensing conditions can be found here: creativecommons.org/licenses/by-sa/4.0/.