CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National Cybersecurity Organisation: GERMANY

Sebastian Cymutta
NATO CCDCOE Law Researcher

National Cybersecurity Governance Series

Tallinn 2020

About this study

This publication is part of a series of reports offering a comprehensive overview of national cybersecurity governance by a nation. The aim is to improve awareness of cybersecurity management in the varied national settings, support nations in enhancing their cybersecurity governance, encourage the spread of best practice and contribute to the development of interagency and international cooperation.

Primarily focusing on NATO nations that are sponsoring nations to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), each country report outlines the division of cybersecurity roles and responsibilities between agencies, describes their mandates, tasks and competences and the coordination between them. In particular, it covers the mandates of political and strategic management; operational cybersecurity capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and management. It offers an introduction to the broader digital ecosystem of the country and outlines national cybersecurity strategy objectives to clarify the context for the organisational approach in a particular nation.

CCDCOE

The CCDCOE is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 29 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the *Tallinn Manual*, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring in Tallinn the Centre hosts the International Conference on Cyber Conflict, CyCon, a unique event bringing together key experts and decision-makers of the global cyber defence community. The Centre is also responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations, currently Austria, Belgium, Bulgaria, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO command structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

This publication is a product of the NATO CCDCOE. It does not necessarily reflect the policy or the opinion of the Centre, NATO, or any of its member countries. The Centre may not be held responsible for any loss or harm arising from the use of the information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation.

Reports in this series

National Cybersecurity Organisation in Czechia

National Cybersecurity Organisation in Estonia

National Cybersecurity Organisation in France

National Cybersecurity Organisation in Germany

National Cybersecurity Organisation in Hungary

National Cybersecurity Organisation in Italy

National Cybersecurity Organisation in Lithuania

National Cybersecurity Organisation in the Netherlands

National Cybersecurity Organisation in Poland

National Cybersecurity Organisation in Romania

National Cybersecurity Organisation in Spain

National Cybersecurity Organisation in Slovakia

National Cybersecurity Organisation in Turkey

National Cybersecurity Organisation in the United Kingdom

National Cybersecurity Organisation in the United States

China and Cyber: Attitudes, Strategies, Organisation

National Cybersecurity Organisation in Israel

Series editor: Kadri Kaska (CCDCOE)

Information in this document has been checked for accuracy as of December 2020.

Table of Contents

1. Digital society and cybersecurity assessment 5
   1.1. Infrastructure availability and take-up 5
   1.2. Digital public services 7
   1.3. Digitalisation in business 8
2. National cybersecurity framework 8
   2.1. National cybersecurity strategy 8
   2.2. National cybersecurity legislation 9
      2.2.1. BSI act 10
      2.2.2. BSI kritis regulation 10
      2.2.3. IT-security law 2.0 11
3. National cybersecurity governance 11
   3.1. Cybersecurity policy coordination 11
      3.1.1. National Cybersecurity Council 11
      3.1.2. IT Planning Council 12
      3.1.3. IT Council 12
   3.2. Cyber incident management and coordination 13
   3.3. Military cyber defence 15
      3.3.1. Federal Ministry of Defence 16
      3.3.2. Cyber and Information Domain Service 17
      3.3.3. Cyber Agency 17
      3.3.4. Cyber Innovation Hub 18

References 19
   Policy 19
   Law 19
   Other 19

Acronyms 21

1. Digital society and cybersecurity assessment

Country indicators

Population: 80,1 million[1]

Internet users: 66,4 million[2]

Area: 357.581[3] km[2]

GDP per capita: €42,637[4] EUR

International rankings*

ICT Development Index (ITU 2017):[5] 12

E-Government Development Index (UN 2018):[6] 12

Digital Economy and Society Index (EU 2020):[7] 12

Global Cybersecurity Index (ITU 2018):[8] 22

National Cybersecurity Index (eGA 2019):[9] 13

1.1. Infrastructure availability and take-up

As a nation with a history of industrial achievement and a wide range of products advertised with the iconic 'made in Germany', it might come as a surprise that amongst the citizens of the Federal Republic of Germany, there is a common perception that the federal government (*Bundesregierung*) has missed important trends and developments concerning internet, e-government and everything else commonly associated with the term 'cyber'. [10] Giving Germany's international reputation and its standing as one of

[1] https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Bevoelkerungsstand/_inhalt.html.
[2] https://de.statista.com/themen/2033/internetnutzung-in-deutschland/.
[3] https://www.destatis.de/DE/Themen/Laender-Regionen/Regionales/Gemeindeverzeichnis/Administrativ/02-bundeslaender.html.
[4] https://de.statista.com/statistik/daten/studie/161330/umfrage/entwicklung-des-bruttonationaleinkommens-bne-in-deutschland-pro-kopf/.
[5] ICT Development Index 2017: Germany. ITU, 2017. https://www.itu.int/net4/ITU-D/idi/2017/#idi2017economycard-tab&DEU.
[6] Annexes 2018. UN Division for Public Institutions and Digital Government, [2018]. https://drive.google.com/file/d/1FZT5zDfTa-ejvPh9c1Zu1w51DoMOefw1/view.
[7] Germany: Digital Economy and Society Index (DESI). European Commission, 2020. https://ec.europa.eu/digital-single-market/en/scoreboard/germany.
[8] Global Cybersecurity Index (GCI) 2018. ITU Publications, 2019. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
[9] Germany, National Cybersecurity Index (NCSI), version 2 April 2019. eGovernance Academy, 2019. https://ncsi.ega.ee/country/de/.
[10] https://m.faz.net/aktuell/politik/inland/digitalisierung-darum-liegt-deutschland-im-eu-vergleich-hinten-15480625.html

the most developed countries in the world,[11] German officials and governmental agencies have made it a priority to speed up the digitalisation of every aspect of private and public life and to put Germany at the front of economic developments and trends again.[12]

The Federal Ministry for Economic Affairs and Energy (*Bundesministerium für Wirtschaft und Energie*, BMWi) published a whitepaper in 2017 entitled *Digital Platform* [13] which outlines the German government's plans to improve the Information and Telecommunications (ITC) infrastructure and harness the trend of blending traditional industries and the opportunities of artificial intelligence into one another while making sure that every member of society will participate in the anticipated overhaul of European (and national) society.

The federal government recently updated its implementation strategy for the digitalisation of Germany (*Digitalisierung gestalten – Umsetzungsstrategie der Bundesregierung*), giving a comprehensive overview of the challenges and the designated projects at hand in the main focus areas:[14]

- Digital competence;
- Infrastructure and facilities;
- Innovation and digital transformation;
- Digital change of society; and
- A modern state.

In recent years the federal government has adopted a holistic approach to digitalisation and has stepped up its efforts, especially at the strategical level.[15]

Within the German government, the lead agency for digitalisation is the **Federal Ministry of Transportation and Digital Infrastructure** (*Bundesministerium für Transport und Digitale Infrastruktur*, BMVI).

The overhaul of digital infrastructure is the most pressing issue for Germany in this area. For internet broadband connectivity, Germany is amongst the last in Europe, trailing the OECD average of 30.3% with only 3.2% broadband connectivity.[16] Given that a fast internet broadband connection is commonly perceived as a major requirement for successful business ventures or start-ups, the German government has made it a top priority to improve and expand the existing infrastructure and reach the ambitious goal of providing a sufficient internet-infrastructure by 2025.[17]

A big part of providing this fast internet relies on the availability of 5G internet throughout Germany. In 2019, the 5G-Frequencies were auctioned by the **Federal Network Agency for Electricity, Gas, Telecommunication, Post and Railway** (*Bundesnetzagentur*, BNetzA). Four network providers[18] took

---

[11] Ranking at a respectable fifth place in the Human Development Index, published by the United Nations Development Programme; http://hdr.undp.org/en/composite/HDI.
[12] Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, p. 37.
[13] Weissbuch Digitale Plattformen – Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe, März 2017, available under: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.html
[14] https://www.bundesregierung.de/breg-de/suche/digitalisierung-gestalten-1605002.
[15] An overview of the different kinds of steering- and advisory panels tasked with supporting the federal government can be found here: https://www.bundesregierung.de/breg-de/themen/digitalisierung/steuerungs-und-beratungsgremien-im-ueberblick-1548450.
[16] https://de.statista.com/infografik/3553/anteil-von-glasfaseranschluessen-in-ausgewaehlten-laendern/
[17] Digitalisierung Gestalten – Umsetzungsstrategie der Bundesregierung, 09.2019, p. 31.
[18] Drillisch Netz AG, Telefonica Germany GmbH & Co. OHG, Telekom Deutschland GmbH, Vodafone GmbH.

part in the auction, with their bids amounting to around €6.5 billion.[19] These funds are exclusively designated for improving and expanding the digital infrastructure of Germany. A separate estate was created with the formation of a fund for digital infrastructure, and the money is to be dedicated to investing in the direct support of digital infrastructure in rural areas, investing in expanding the reach of telecommunication and aiding regional entities in investing in digital infrastructure for the educational sector.[20] While the last priority is a challenge for German federalism, the digitalisation of the educational sector (especially, providing devices to schools) has been highlighted as insufficient by the 2020 COVID-19 pandemic and the subsequent shutdown of school and the subsequent necessity of continuing schoolchildren's education via electronic means.

1.2. Digital public services

In June 2019, the German Parliament subdivision entrusted with rendering scientific services (*Unterabteilung Wissenschaftliche Dienste des Deutschen Bundestages*) published a report concerning e-government in Germany at both the federal and regional levels.[21] It found the necessary legislation in place to create functioning e-government-services in Germany. With the '**E-Government Act**'[22] (*Gesetz zur Förderung der elektronischen Verwaltung – E-Government-Gesetz*) stipulating the e-government agenda passed in July 2013, the German government recently enhanced its efforts with passing the **Online Accessibility Act**.[23] (*Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen – Onlinezugangsgesetz – OZG*) which obligates federal and regional governments to offer their administrative services via electronic administrative portals no later than 2022.[24]

German federalism is a challenge to the implementation of a functioning e-government system. Besides the federal government, there are 16 states and more than 10,000 communities in Germany providing administrative services. This makes the creation of a single point of contact for e-government services both a necessity and a constitutional challenge at the same time, as the division between federal and state jurisdiction is one of the pillars of the German Constitution. To overcome the obstacles, the German parliament found it necessary to change the Constitution, the *Basic Law* (*Grundgesetz*, GG). The introduction of Article 91c GG sets the stage for the cooperation of the different jurisdictional layers in Germany, effectively lowering the obstacles of German federalism to digitalisation.

Still, meeting the 2022 deadline seems a rather ambitious goal considering that Germany is ranked 24th out of the 28 European Union (EU) member states for e-government services.[25] The DESI Report 2019 identified e-government as the single biggest challenge for Germany in the area of digitalisation.[26] The implementation strategy for the digitalisation of Germany concurs in this, calling the digitalisation of the German administration a focal point.[27]

---

[19] Detailed information about the auction can be found here: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/MobilesBreitband/Frequenzauktion/2019/Auktion2019.html.
[20] § 2, Gesetz zur Errichtung des Sondervermögens „Digitale Infrastruktur" (Digitalinfrastrukturfondgesetz – DIFG), https://www.gesetze-im-internet.de/difg/BJNR252500018.html.
[21] Sachstand E-Government in Deutschland. 2019.
[22] Gesetz zur Förderung der elektronischen Verwaltung, https://www.gesetze-im-internet.de/egovg/
[23] Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen, http://www.gesetze-im-internet.de/ozg/
[24] Vgl. § 1 Abs. 1 OZG.
[25] Index für die digitale Wirtschaft und Gesellschaft (DESI). Länderbericht 2019. Deutschland. p 14.
[26] Index für die digitale Wirtschaft und Gesellschaft (DESI). Länderbericht 2019. Deutschland. p 3.
[27] Digitalisierung Gestalten – Umsetzungsstrategie der Bundesregierung, 09.2019, p. 157 ff.

1.3. Digitalisation in business

In Germany, there are around 137 million mobile network connections[28] and around 84% of Germans are connected to the internet[29] and Germans eagerly engage in a wide variety of e-commerce. Internet usage of Germans is above the EU average.[30]

2. National cybersecurity framework

2.1. National cybersecurity strategy

In 2011, the Federal Ministry of the Interior (*Bundesministerium des Inneren*, BMI) published its '**Cybersecurity Strategy for Germany** (Cyber-Sicherheitsstrategie für Deutschland 2011)'.[31] In this document, the government acknowledged that the accessibility of cyberspace, its integrity, authenticity and confidentiality have become an existential question of the 21st century.[32] The Cybersecurity Strategy for Germany was updated in 2016.[33] Following up on the first edition, the now renamed **Federal Ministry of the Interior, Building and Community** (*Bundesministerium für Inneres, für Bau und Heimat*) highlights the most important areas in which the government tries to engage and acknowledges the importance of providing security in an ever-evolving cyber environment.

The document identifies four major spheres of activity for the German government:

- Secure and self-determined actions in a digitalised environment;
- The common mission of government and economy;
- Capable and sustainable governmental cybersecurity architecture; and
- Active positioning of Germany within the European and international cybersecurity policy.[34]

In mid-2020, the BMI started a process of evaluating the cybersecurity strategy, beginning by sending out a questionnaire to cyber-practitioners and actors[35] to evaluate the situation and gather opinions on how to make the next version of the Cybersecurity Strategy more accountable.[36] As deduced from the questionnaire, the drafting process for the updated Cybersecurity Strategy will likely take until 2021 and hopefully involve a wide variety of subject matter experts. In the meantime, the document still serves as

---

[28] https://de.statista.com/statistik/daten/studie/3907/umfrage/mobilfunkanschluesse-in-deutschland/
[29] https://de.statista.com/statistik/daten/studie/13070/umfrage/entwicklung-der-internetnutzung-in-deutschland-seit-2001/
[30] Index für die digitale Wirtschaft und Gesellschaft (DESI). Länderbericht 2019. Deutschland, p 10.
[31] Cyber-Sicherheitsstrategie für Deutschland 2011.
[32] ibid. p. 2.
[33] Cyber-Sicherheitsstrategie für Deutschland 2016; available Under http://www.bmi.bund.de/cybersicherheitsstrategie/.
[34] Cyber-Sicherheitsstrategie für Deutschland 2016, p. 10, 11.
[35] https://www.stiftung-nv.de/de/publikation/evaluation-der-cyber-sicherheitsstrategie-fuer-deutschland-2016#collapse-newsletter_banner_bottom.
[36] See Question 1 of the questionnaire: "Which focal points and goals of the CSS 2016 have been proven to be probate. Which agreements, structures and procedures have been proven to be advantageous for target achievement, cited from: https://www.stiftung-nv.de/de/publikation/evaluation-der-cyber-sicherheitsstrategie-fuer-deutschland-2016.

an anchor inside the complex German cybersecurity architecture,[37] providing a guideline for assessing developments.

2.2. National cybersecurity legislation

From a national legal perspective, 'cyber' is a cross-subject matter, mostly dominated by public law. Cybersecurity provisions can be found in areas like police law (especially on the federal level) and the law regulating telecommunications.

One of the biggest challenges for the implementation of the German national cybersecurity strategy stems from one of the German constitutional core principles; federalism.[38] Germany is a federal state with a strong and clear division between central ('*Bund*') and regional ('*Länder*') jurisdiction. Matters of internal security (policing) are devolved, while the federal police (*Bundespolizei, BPol*) only has limited jurisdiction (primarily border control). Military defence is obviously under the exclusive jurisdiction and control of the federal government.

This makes cybersecurity an area of law of great scope as it falls foul of the traditional pitfalls of German federalism in which it is often difficult to determine which governmental body and at what level is responsible for a certain issue.

Considering that cyber is a relatively new issue for German authorities, it comes as no surprise that over the last couple of years numerous governmental bodies, agencies and offices have been set up dealing with cyber issues. Unfortunately, there is often no certainty of where lines between jurisdictions are drawn and sometimes even without a clear understanding of what task has to be accomplished.

Since Germany is a member state of the EU, the German legal system is highly influenced by European directives and regulations of which one of the most influential in this area is Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, commonly referred to as the 'NIS Directive'.[39] With this Directive, the EU seeks to:[40]

- Improve cybersecurity capabilities at national levels;[41]
- Increase EU-level cooperation;[42] and
- Impose risk management and incident reporting obligations for operations of essential services and digital service providers.[43]

[37] Stiftung Neue Verantwortung e.V., a German think tank, has created a mapping of the German Cybersecurity architecture, which highlights the complexity of the issue; https://www.stiftung-nv.de/de/publikation/akteure-und-zustaendigkeiten-der-deutschen-cybersicherheitspolitik

[38] Federalism is among the very few constitutional principles, which are unchangeable even by a 2/3 parliamentary vote, see Article 79(3) of the Basic Law.

[39] https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[40] See European Commission – Fact Sheet Directive on Security of Network and Information Systems.

[41] See Art. 1 II (a) of the Directive 2016/1148; member states are obligated to adopt a national strategy on the security of network and information systems.

[42] See Art. 1 II (c) of the Directive 2016/1148, where there is the creation of a computer security incident response teams network ("CSIRTs network") envisaged.

[43] See Art. 1 II (d) of the Directive 2016/1148.

The NIS Directive was domesticated into German federal law in 2017,[44] amending the **Act on the Federal Office for Information Security** and several other laws in the area of public services. This and other relevant acts are briefly examined below.

2.2.1. BSI act

The closest thing to a cybersecurity law that can be found in the German legal system is the **Act on the Federal Office for Information Security** (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, BSIG). It tasks the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) with providing information security at the national level.[45] Incorporating the NIS Directive, §3 BSIG presents a diverse portfolio of instruments to promote the security of information technology. This provision formulates a catalogue of rights assigned to the BSI to fulfil its tasks, such as:

- preventing threats to the security of federal information technology (§3 I 2 Nr. 1 BSIG);
- testing and evaluating the security of information technology systems or components and issuing security certificates (§3 I 2 Nr. 5 BSIG); and
- developing technical security standards for federal information technology (§3 I 2 Nr. 10 BSIG).

BSIG is central to the legal cyber landscape. In 2015, it was enhanced by the first IT security act[46] and recently supplemented by a regulation on critical infrastructure.[47] §7 of the Act gives the BSI the right to alert the public to security vulnerabilities in software or services and the BSI must report to the BMI, enabling it to publish an annual comprehensive overview of the IT security situation in Germany.[48]

2.2.2. BSI kritis regulation

Critical infrastructure is a tempting target for any cyber-attack. The BSI-KritisV contains provisions to help identify which infrastructure must be considered critical. The national plan for the protection of information infrastructure (*Nationaler Plan zum Schutz von Informationsinfrastruktur*) was published in 2005 and has since been superseded by the Cybersecurity Strategy.[49] It is complemented by the national strategy for the protection of critical infrastructure (*Nationale Strategie zum Schutz Kritischer Infrastruktur*, KRITIS-Strategie).[50]

---

[44] Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, BGBl. I 2017, p. 885.
[45] § 1 sentence 2 BSIG.
[46] Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, BGBl. I 2015, p. 1324.
[47] Verordnung zur Bestimmung Kritischer Infastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV).
[48] Vgl. § 13 BSIG; the 2019 edition of the annual overview on the IT-security situation in Germany can be accessed here: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7.
[49] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/cs_Strategie_node.html.
[50] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf;jsessionid=4B759134A3DE0998B6AB3DA5306225D3.1_cid364?__blob=publicationFile&v=3.

2.2.3. IT-security law 2.0

The BMI has recently published a new draft IT-Security law 2.0 (*Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme*, IT-Sicherheitsgesetz 2.0 – IT-SIG 2.0),[51] which expands the authority of the BSI, emphasising its vital role in German cybersecurity architecture. Amongst other changes, it is planned to give the BSI the following responsibilities:

- Relaying information in case of a cyber attack;
- Exercising control over the federal communications technology; and
- Function as a repository for federal cyber incidents.

It is unclear when the IT Security law 2.0 will be passed, even though the federal government has committed itself in its coalition agreement to continue its development.[52]

3. National cybersecurity governance

3.1. Cybersecurity policy coordination

The BMI is responsible for matters of internal security in Germany at the federal level including the drafting, implementation and execution of the Cybersecurity Strategy. There are also intergovernmental working groups and public-private organisations which influence the policy-making process.

3.1.1. National Cybersecurity Council

As promised in the first edition of the cybersecurity strategy for Germany, a **Cybersecurity Council** (*Cyber-Sicherheitsrat*, Cyber-SR) was implemented in 2011.[53] The goal of this intergovernmental platform was to boost cooperation within the federal government in the area of cybersecurity.[54] The 2016 update of the Cybersecurity Strategy designates the Cybersecurity Council a permanent role as a strategic advisor to the federal government.[55]

Given the rather ambiguous information on what the Cybersecurity Council actually does, it is difficult to assess its importance in the policy-making process. The sessions of the Cybersecurity Council are chaired by the Chief Information Officer of the Federal Government and, since October 2018, there has been a standing working group supporting the efforts of the Council. The Council reports to the federal government on the strategic cybersecurity subjects it is working on.[56]

Finally, it is important not to confuse the *Cyber-Sicherheitsrat* with the *Cyber-Sicherheitsrat Deutschland e.V.*, a private organization, offering advice on cybersecurity to anyone.[57]

---

[51] Referentenentwurf, Bearbeitungsstand 07.05.2020 17:13, available here: http://intrapol.org/wp-content/uploads/2020/05/200507_BMI_RefE_IT-SiG20.pdf.
[52] Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, p. 43.
[53] Cyber-Sicherheitsstrategie für Deutschland 2011, p. 9.
[54] ibid.
[55] Cyber-Sicherheitsstrategie für Deutschland 2016, p. 45.
[56] ibid.
[57] https://cybersicherheitsrat.de/.

3.1.2. IT Planning Council

The IT Planning Council (*IT-Planungsrat*) is a cooperative unit comprised of government entities from the federal government, the *Länder,* the Association of German counties, the Association of German cities and the German Association of Town and Municipalities. It is a forum for considering the opinions of the different levels of government to create a holistic cyber vision which transcends jurisdictional matters and tackles the federal complexity[58] and is enabled by a constitutional provision, Article 91c(1) GG, which allows for cross-federal cooperation.[59]

The work of the Council is governed by the State Treaty on the establishment of the IT Planning Council and on the principle of cooperation underlying the use of information technology in the administration of the Federation and the *Länder* (*Vertrag zur Ausführung von Artikel 91c GG*, IT-Staatsvertrag).[60] §1 I Nr. 3 of the Treaty states that the management of the ICT-supported governance and administration projects (e-government) are amongst the most important issues the IT Planning Council is tasked with. In 2020, the German Parliament passed a law to create an institution that will effectively conduct all non-subject tasks like human resource management and administration for the Council. Known as the Federal IT Coordination, (*Föderale IT-Kooperation,* FITKO) it will be based in Frankfurt am Main. According to the parliamentary documents, the establishment of FITKO was necessary to unburden the Council from these tasks.[61] While the budget allocation to the IT Planning Council is impressive,[62] it remains to be seen if FITKO can be an asset in helping the IT Planning Council with its day-to-day business.

3.1.3. IT Council

The **IT-Council** (*IT-Rat*) serves as a strategic board for fostering the digitalisation of the administration at the federal level.[63] Board members are recruited from amongst the undersecretaries of state of federal ministries, and they convene around three times a year.[64] These meetings are chaired by the Minister of the Chancellery.[65] While not the most prominent organisation within the German cybersecurity architecture, it is the only organisation besides the National Cybersecurity Council which recruits its members directly from federal ministries. Therefore, it could play an important part in the policymaking process.

Lastly, the IT Council serves to illustrate the complexity of the German Cybersecurity Architecture, as it is not to be confused with the above-mentioned IT *Planning* Council, which has a cross-jurisdictional perspective on Cybersecurity.

---

[58] https://www.it-planungsrat.de/DE/Home/home_node.html.
[59] Gesetz zur Änderung des Grundgesetzes (Artikel 91c, 91d, 104b, 109, 109a, 115, 143d) vom 29. Juli 2009, BGBl. I 2009, p. 2248.
[60] https://www.it-planungsrat.de/DE/ITPlanungsrat/RechtlicheGrundlagen/rechtliche_grundlagen_node.html, available in German and in English.
[61] BT-Drs. 19/9737, p. 6.
[62] BT-Drs. 19/9737, p. 1: up to 180 Million Euro tor the time period of 2020 – 2022.
[63] https://www.cio.bund.de/Web/DE/Politische-Aufgaben/IT-Rat/IT-Rat_node.html.
[64] Ibd.
[65] https://www.bundesregierung.de/breg-de/themen/digitalisierung/steuerungs-und-beratungsgremien-im-ueberblick-1548450.

3.2. Cyber incident management and coordination

Improving state and non-state Computer Emergency Response Teams (**CERT**s) has been one of the main goals of the Cybersecurity Strategy for Germany 2016.[66] It seeks to increase the resilience of the German cybersecurity landscape and therefore serve as one of the cornerstones of a viable cyber defence.

Federal Office for Information Security

The **Federal Office for Information Security** (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) executes the government's cybersecurity agenda, bundling the strategic insight of the federal ministry with the hands-on knowledge of experts and practitioners. Located in Bonn and staffed by around 1,400 civilians,[67] the BSI can be seen as the working muscle of the BMI in the area of cyber defence. The BSI is a key (if not the main) organisation when it comes to matters of cybersecurity in Germany and contains four of the most important cyber defence units:

- the National Cyber Defence Centre,
- the Alliance for Cybersecurity,
- the federal Computer Emergency Response Team and
- the IT Situation Centre.

With the passing of the IT-Security-Act 2.0, the importance of the BSI as the centre of German cyber defence will grow as its responsibilities, duties and powers will be expanded. This could lead to a reduction in the complexity of the German cybersecurity architecture.

Probably the most important task of the BSI is formulated in §5 BSIG which makes it responsible for protecting the federal ICT against harmful software and threats. The BSI publishes an annual report concerning the state of the IT security in Germany[68].

National Cyber Defence Centre

One recommendation of the first edition of the Cybersecurity Strategy was the implementation of a national cyber defence agency.[69] Consequently, the **National Cyber Defence Centre** (*Nationales Cyber-Abwehrzentrum*, Cyber-AZ) was founded in June 2011 as a cooperative effort between different German federal services dealing with various aspects of cybersecurity. This Centre serves as a platform for police agencies, intelligence services and the **Federal Office of Civil Protection and Disaster Assistance** (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe*, BBK) to effectively share information concerning cyber threats and to synchronise government efforts to prevent and counter cyber-attacks.

There have been some concerns expressed that there are members of the intelligence services, the police and the military working on the same platform, as those actors are bound by different objectives, jurisdictions and legal rights and obligations. The federal police organisations (*Bundeskriminalamt*, BKA, *Zollkriminalamt*, ZKA and BPol) are tasked with the prevention and investigation of crime. The intelligence services gather intelligence, have next-to-no operational mandate and are restricted to very different jurisdictions: the **Foreign Intelligence Service of Germany** (*Bundesnachrichtendienst*, BND) gathers information outside Germany; the **Federal Office for the Protection of the Constitution** (*Bundesamt für Verfassungsschutz*, BfV) is the domestic intelligence service of the Federal

[66] German Cyber-Security-Strategy, 2011, p. 34.
[67] For further information: https://www.bsi.bund.de/DE/Presse/BSI-Kurzprofil/kurzprofil_node.html.
[68] https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.
[69] German Cyber-Security-Strategy, 2011, p. 10.

Government; and the **Federal Armed Forces Counterintelligence Office** (*Bundesamt für den Militärischen Abschirmdienst*, BAMAD) is responsible for military counterintelligence.

To simplify things, each of the National Cyber Defence Centre's member organisations sticks to their respective legal regime to preclude any jurisdictional violation. According to Cyber-AZ's website, the BSI will assess a cybersecurity threat from an information security point of view, the BfV, the MAD and the BND from an intelligence point of view and the BKA, the ZKA and the BPol from a police point of view.[70]

This also highlights the main tasks of the Cyber-AZ: analysing information and sharing it. Thus, despite carrying 'defence' in its name, no active or operational duties are assigned to the Cyber-AZ, which could therefore be more clearly described as an 'Information- and Cooperation Hub'.[71] This would align with §4 I BSIG, according to which the BSI shall be the central clearinghouse for cooperation among federal authorities in matters related to the security of information technology.

The German Military Cyber Command recently joined the Cyber-AZ. [72]

Alliance for Cybersecurity

The **Alliance for Cybersecurity** (*Allianz für Cyber-Sicherheit*, AfCS) was jointly initiated by the BSI and Germany's digital association (*Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.*, BITKOM).[73] As stipulated in the Cybersecurity Strategy, cyber is a subject which needs to be addressed by the government and representatives of the business world together.[74] Calling on the business world seems right given the insight and competencies it has, although declaring cybersecurity a public-private effort seems to be going too far. Today, around 4,000 companies contribute to the AfCS, an increase from 2,500 2018,[75] suggesting that the awareness of cybersecurity has risen in recent years.

Membership of the Alliance gives access to specific information regarding cybersecurity and allows the use of the 'Alliance for Cybersecurity-logo', showing a company's active support for cybersecurity.[76]

CERT-Bund

The **CERT-Bund** is the federal Computer Emergency Response Team.[77] The BSI describes it as the 'central point of contact for preventive and reactive measures regarding security-related computer incidents'.[78]

As a service provider for the federal administration, CERT-Bund offers:

- Creation of best practices for damage prevention;
- Information about security vulnerabilities; and

---

[70] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/Cyber-Abwehrzentrum/cyberabwehrzentrum_node.html.
[71] See Stiftung Neue Verantwortung e.V., Cybersicherheitspolitik in Deutschland, im Fokus: Das Cyber Abwehrcenter, p. 9, stressing that the name of the N-CAZ is misleading and could therefore lead to expectations, which are unaccomplishable.
[72] https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html.
[73] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Ueber_uns/ueber_uns.html;jsessionid=E1CE1B0E4863E3D414AAEE40036E61C4.1_cid341.
[74] Cyber-Sicherheitsstrategie für Deutschland 2016, p. 4.
[75] Infobroschüre Allianz für Cybersicherheit, p. 7.
[76] Infobroschüre Allianz für Cybersicherheit, p. 12.
[77] https://www.cert-bund.de/.
[78] https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/cert-bund_node.html.

- Recommendations and best practices.

CERT Bund is also active in networking with other national CERTs in Germany and is part of the European Governmental CERT Group (EGC), an informal association of European governmental CERTs.[79]

IT-Situation Centre

The IT-Situation Centre (*Nationales IT-Lagezentrum*) was first mentioned in the National Plan for Information Infrastructure Protection under the name IT Crisis Reaction Centre (*Krisenreaktionszentrum IT*).[80] It was envisaged that the Centre should be part of the BSI, closely cooperating with existing Situation Centres.[81]

The Cybersecurity Strategy 2016 did not explicitly name the IT-Situation Centre, but mentioned that the National Cyber Defence Centre will – in case of a cybersecurity incident – transform into an **IT Crisis Reaction Centre**, stressing the need for a coordinated response in case of a cybersecurity incident.[82] According to the BSI, the role will be performed by the IT-Situation Centre in such an incident.[83]

3.3. Military cyber defence

While the BMI is responsible for ensuring the internal security of Germany and its society, external security is traditionally provided by the German armed forces (*Bundeswehr*). With cybersecurity, the line between internal and external security tends to be blurred, which is acknowledged by the Cybersecurity Strategy 2016.[84] It describes cyber defence as an integral part of national defence and references the white paper on Security Policy and the Future of Bundeswehr 2016 (*Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016*).[85]

This white paper describes the pillars of the German military security policy and puts a special emphasis on the *Bundeswehr* and its need to be revised and updated to cope with the threats of the 21st century like hybrid warfare and cyber attacks.

The 'challenges of the cyber and information domain'[86] are outlined by the white paper as follows:

- Increase of danger (for example) through advanced persistent threats;[87]
- Possibility of (severe) cyber-attacks by non-state actors;[88]
- The danger of cyber-attacks against critical infrastructures;[89] and

---

[79] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/CERT-Bund/Zusammenarbeit/zusammenarbeit_node.html;jsessionid=D40ACCC6329C15C7776D487DFBD3BC23.1_cid502.
[80] Nationaler Plan zum Schutz der Informationsinfrastrukturen, p. 14.
[81] Ibid.
[82] German Cyber-Security-Strategy, 2016, p. 28.
[83] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/IT-Krisenreaktionszentrum/itkrisenreaktionszentrum_node.html.
[84] Cyber-Sicherheitsstrategie für Deutschland, 2016, p. 22.
[85] Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016, https://www.bmvg.de/de/themen/weissbuch.
[86] Subheading Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016, p. 36.
[87] Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016, p. 36.
[88] *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* ibid
[89] Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016, p. 37.

- Hybrid warfare as a means to influence public opinions (or the outcome of elections).[90]

Published in 2016, the last four years have seen those challenges become reality. It was therefore accurate of the white paper to call on the *Bundeswehr* to provide solutions in this area.[91]

Military defence is largely regulated by the German Constitution in Chapter 10a, dealing with the state of defence. Article 115a(1) sentence 1 of the Basic Law defines the state of defence (*Verteidigungsfall*) as a situation in which the territory of the Federal Republic of Germany is under an armed attack (or such an attack is imminent).

Recently, there has been much debate over whether or not there needs to be the introduction of a 'digital state of defence'.[92] The following paragraphs introduce some aspects of the German military cyber-landscape.

3.3.1. Federal Ministry of Defence

The **Federal Ministry of Defence** (*Bundesministerium der Verteidigung,* BMVg) is led by the Minister of Defence, who serves as the supreme commander of the German armed forces during times of peace.[93] In this capacity, the Minister has complete control over every aspect concerning the armed forces and defence administration. It is only in times of war (after the promulgation of the above-mentioned state of defence) that command over the armed forces is transferred to the Federal Chancellor.[94]

To reflect the importance of 'cyber' and its interdisciplinary nature, the division 'Cyber- and Information technology' (*Abteilung Cyber- und Informationstechnik*, CIT) was founded within the Federal Ministry of Defence in 2016,[95] consisting of two sub-divisions:

- CIT I: Methods and Digitalisation.
- CIT II: Capabilities Cyber/IT.

The division manager, holding the rank of Lieutenant-General, also serves as the Chief Information Officer of the Federal Ministry of Defence.

The CIT-division is complemented by three organisations, which are annexed to it:

- Central Tasks and Controlling (CITZ);
- Strategical steerage BWI (CIT BWI); and
- Staff for the set-up of the Cyber Agency (*Aufstellungsstab Cyberagentur*[96]).

---

[90] Ibid.
[91] Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016, p. 95.
[92] https://augengeradeaus.net/2019/06/bundeswehr-plaediert-fuer-digitalen-verteidigungsfall-zur-besseren-cyber-abwehr/.
[93] Article 65a Basic Law.
[94] Article 114b(1) Basic Law.
[95] Erster Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung, Berlin, Oktober 2019, October 2019, p. 9, see also Organisationsplan BMVg – Stand: November 2020, available here: https://www.bmvg.de/resource/blob/11902/dd851907987b144dd53fffe499a57b75/a-03-download-organigramm-data.pdf
[96] See 3.3.3.

3.3.2. Cyber and Information Domain Service

One of the most notable developments in recent German military history has been the establishment of a new military branch named the **Cyber and Information Domain Service** (*Cyber- und Informationsraum*, CIR) in 2017, following a ministerial recommendation.[97]

In establishing the CIR, the *Bundeswehr* acknowledged the importance of cyberspace as a new and unique battlefield besides the traditional land, sea and air domains of warfare. Led by the Chief of Cyber and Information Domain Service, CIR is supposed to reach full operating capability by the end of 2021.[98] According to the Ministry of Defence's first report on digital transformation, CIR is already comprised of around 11,600 civilian and military personnel,[99] mostly incorporating existing units. This leads to a decentralised structure, in which you can find battalions and specialised centres under the umbrella of CIR all over Germany.

Command wise, CIR is structured around the **Cyber and Information Domain Command** (*Kommando Cyber- und Informationsraum*, KdoCIR), which is located in Bonn. This Command is supported by three sub organisations:

- Strategic Reconnaissance Command (*Kommando Strategische Aufklärung*, KSA) in Gelsdorf;
- Bundeswehr Geoinformation Centre (*Zentrum für Geoinformationswesen der Bundeswehr*, ZGeoBw) in Euskirchen; and
- Information Technology Command (*Kommando Informationstechnik der Bundeswehr,* KdoITBw) in Bonn.

Members of the Cyber and Information Domain Service are involved in almost all military operations in which the *Bundeswehr* is taking part.[100]

3.3.3. Cyber Agency

One of the biggest issues in dealing with a cyber threat is that they transcend the classical distinction between internal and external security and the jurisdictional divisions between the police and the military. The German government has therefore committed to the implementation of a **Cyber Agency** (*Agentur für Innovation in der Cybersicherheit,* Cyberagentur)[101] run jointly by the Ministry of the Interior and the Ministry of Defence[102] to enable creative and innovative projects with an emphasis on foreign, defence and security policy. The first applications for research assignments are to be expected in 2020.[103] The Agency will be located in Halle/Saale[104] and, according to the BMVg, will take the form of

---

[97] Abschlussbericht Aufbaustab Cyber- und Informationsraum, April 2016.
[98] Erster Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung, Berlin, Oktober 2019, p. 13.
[99] Erster Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung, Berlin, Oktober 2019, p. 13.
[100] https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/cir-im-einsatz.
[101] See overview: https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/agentur-fuer-innovation-in-der-cybersicherheit-1546892.
[102] Erster Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung, Berlin, Oktober 2019, p. 18.
[103] https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/agentur-fuer-innovation-in-der-cybersicherheit-1546892
[104] See Absichtserklärung zwischen BMVg, BMI, dem Freistaat Sachsen und dem Land Sachsen-Anhalt über den zukünftigen Standort der Agentur für Innovation in der Cybersicherheit (Cyberagentur).

a limited liability corporation (*Gesellschaft mit beschränkter Haftung*, GmbH). Some €352.5 million has already been allocated to its budget.[105]

3.3.4. Cyber Innovation Hub

The **Cyber Innovation Hub** (CIH)[106] tries to build a bridge between *Bundeswehr* and the start-up scene, seen as key to developing tools and strategies for being on the winning side of cyber conflicts. Therefore, the CIH appeals to the young and creative minds, offering them an environment to develop disruptive products and smart solutions in a lean and supportive atmosphere. The CIH is an organisational branch of the limited liability company which is the IT service provider for the German military (BWI-GmbH), but it is only a platform for the development of products. Whether or not those products are procured by the German military will still be decided by the *Bundeswehr* procurement agency (*Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr*, BAAINBw).

[105] Zweiter Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung, Teil 1, Berlin, März 2020, p. 18.
[106] https://www.cyberinnovationhub.de/de/.

References

Policy

Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr, Bundesregierung, Juni 2016

Cyber-Sicherheitsstrategie für Deutschland, BMI, Berlin, 09.2016

Cyber-Sicherheitsstrategie für Deutschland, BMI, Berlin, 02.2011

Digitalisierung Gestalten – Umsetzungsstrategie der Bundesregierung, 6. Überarbeitete Ausgabe, Berlin, 09.2019

Ein neuer Aufbruch für Europa, eine neue Dynamik für Deutschland, ein neuer Zusammenhalt für unser Land, Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, Berlin, 03.2018

Nationale E-Government-Strategie Fortschreibung 2015. IT-Planungsrat. Oktober 2015

Nationaler Plan zum Schutz der Informationsinfrastrukturen, BMI, Berlin, Juli 2005

Law

Grundgesetz für die Bundesrepublik Deutschland - Grundgesetz - GG

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme - IT-Sicherheitsgesetz

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme 2.0 - IT-Sicherheitsgesetz 2.0 (Enwurf)

Gesetz zur Förderung der elektronischen Verwaltung - E-Government-Gesetz - EGovG

Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen - Onlinezugangsgesetz - OZG

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik - BSIG

Gesetz zur Errichtung des Sondervermögens „Digitale Infrastruktur' - Digitalinfrastrukturfondgesetz - DIFG

Gesetz zur Änderung des Grundgesetzes (Artikel 91c, 91d, 104b, 109, 109a, 115, 143d)

Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

Verordnung zur Bestimmung Kritischer Infastrukturen nach dem BSI-Gesetz - BSI-Kritisverordnung - BSI-KritisV

Other

Sachstand E-Government in Deutschland. 2019. WD 3 – 3000 – 134/19

Herpig, Sven / Beigel, Beigel. 2020. Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik. Oktober 2020. 5. Auflage. snv-cybersicherheitspolitik_cyberverteidigungspolitik-5.2_auflage.pdf (stiftung-nv.de)

Index für die digitale Wirtschaft und Gesellschaft (DESI). Länderbericht 2019. Deutschland. https://ec.europa.eu/digital-single-market/en/scoreboard/germany

Abschlussbericht Aufbaustab Cyber- und Informationsraum, BMVg, April 2016

Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, 2017

Erster Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung, Berlin, Oktober 2019

Zweiter Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung, Berlin, März 2020

Acronyms

AfCS	Allianz für Cyber-Sicherheit
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr
BAMAD	Bundesamt für den Militärischer Abschirmdienst
BfV	Bundesamt für Verfassungsschutz
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BMI	Bundesministerium für Inneres, für Bau und Heimat
BMVg	Bundesministerium der Verteidigung
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Bundesministerium für Wirtschaft und Energie
BND	Bundesnachrichtendienst
BNetzA	Bundesagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur)
BPol	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIR	Cyber- und Informationsraum
CIH	Cyber Innovation Hub
Cyber-AZ	Nationales Cyber-Abwehrzentrum
GG	Grundgesetz
IT-SIG	IT-Sicherheitsgesetz
OZG	Onlinezugangsgesetz
ZKA	Zollkriminalamt