Authorities Competent for Cybersecurity in Germany

AGNIESZKA BRZOSTEK

Abstract In Germany, the federal states are generally responsible for the prevention of threats in cyberspace. The Federal Government has special jurisdiction over threat prevention in certain areas, such as international terrorism, security in the territory belonging to the federal railways, border protection, and national self-protection, where jurisdiction extends to the cyber domain. Cooperation between the Federal Government and Länders is essential. Germany's new Cybersecurity Strategy, adopted by the Federal Government on 8 September 2021, provides a framework for government action for the next five years. Germany was one of the first countries to respond to cyber threats in Europe. The Strategy announced the setting up of an institution, within the remit of the Federal Ministry of the Interior, whose task would be to provide technical support to federal security and technical authorities, including intelligence services, in their operational cyber capabilities. The German Federal Government's cybersecurity policy is consistent and in line with the European Union's cybersecurity policy. The multiplicity of tasks requires the involvement of multiple actors who, in a decentralised form, carry out tasks at both strategic and operational levels.

Keywords: • Germany • cybersecurity strategy • critical infrastructure • federal government

CORRESPONDENCE ADDRESS: Agnieszka Brzostek, Ph.D., Lecturer, War Studies University in Warsaw, Institute of Law, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: brzostek.agnieszka@gmail.com.

https://doi.org/10.4335/2022.2.17 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

Germany's new Cybersecurity Strategy, adopted by the Federal Government on 8 September 2021, provides a framework for government action for the next five years. The Strategy is in line with the European Union's cybersecurity policy. The NIS Directive (EU 2016/1148) requires Member States to create a steering framework in the Strategy, to identify objectives and priorities, and to designate the authorities that will be responsible for achieving these objectives. The effective implementation of the Strategy requires the adoption of legal and organisational solutions. Hence, the purpose of this paper is to analyse the legal and administrative forms of action of the federal authorities established for the implementation of cybersecurity tasks. An issue of major importance is the legal and formal way of organising the system that would take into consideration the form of action of the authorities.

It should be noted that Germany was one of the first countries to respond to cyber threats in Europe. As pointed out in 2005, cybersecurity must be part of national security. In 2011, the government adopted its first Cybersecurity Strategy (The 2011 Strategy, p. 3-4). According to C. Guitton, Germany adopted the Cybersecurity Strategy as a form of preventive policy, unsupported by any incidents concerning critical information infrastructure. The level of threat was significantly influenced by unverifiable data supplied by cybersecurity providers and the impact which events taking place in other countries had on them, e.g., in the USA (C. Guitton, p.22). The adoption of the Strategy resulted in establishing the National Cybersecurity Council, whose task was to oversee the implementation of the Strategy's objectives and, if necessary, to adapt strategies and measures to the specific requirements and framework conditions arising from it (The 2011 Strategy, p. 7). In 2011, the Ministry of the Interior of the Federal Republic of Germany set up the National Cyber Response Centre (Nationale Cyber-Abwehrzentrum – NCAZ), which was supposed to become the first link in the fight against cyber threats and to provide a platform for cooperation between the competent authorities of the German administration. The Germans decided not to institutionalise the work of the Centre due to the order for the separation (*Trennungsgebot*) of special services from police services (Sacewicz, pp. 129-130). Currently, the Centre consists of the following bodies the Federal Office for Military Counterintelligence, the Federal Criminal Police Office, the Federal Office for Information Security (*BSI – Bundesamt für Sicherheit in der Informationstechnik*), the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz – BfV*); the Federal Office of Civil Protection and Disaster Assistance (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK*); the Federal Criminal Police Office (*Bundeskriminalamt – BKA*); the Federal Intelligence Service *(Bundesnachrichtendienst – BND*); the Federal Police (*Bundespolizei – BPol*), and the cyberspace and information space of the Command of Bundeswehr (the armed forces of the Federal Republic of Germany). Included as external partners are the Bavarian Cyber Defence, cyber specialist prosecutors from Bamberg and Cologne and the Federal Financial Supervisory Authority.

The most important tasks of the Centre include preventing and combating threats in cyberspace, which includes exchanging information, analysing and evaluating

information incidents, developing mechanisms for the effective protection, preventing and neutralising the outcomes of attacks, as well as assessing the effectiveness of the implementation of the cyberspace protection strategy. The Centre's affiliated authorities provide information according to their competence – the BSI evaluates incidents in technical terms, the BfV investigates whether a foreign special service is responsible for an attack, and the BBK assesses the effects of attacks on critical infrastructure. The other authorities identify new attack methods and tools. As a result, the NCAZ can provide, within a short period of time, up-to-date and comprehensive information on threats against cyberspace. As part of preventive measures, the NCAZ periodically, and additionally when necessary, provides the National Cybersecurity Council with relevant guidelines, and in emergency situations reports directly to the crisis management centre at the Ministry of the Interior (Sacewicz, pp. 129-130, Oleksiewicz, pp. 47-51).

The assumptions adopted in the Strategy for the activities of the authorities were criticised by experts. It was argued that the composition of the National Cybersecurity Council was indicated in a manner that was too general. As noted in a confidential report prepared by the Federal Office for Control, the Council is not an appropriate institution for repelling an attack because it does not have a sufficient number of staff and its area of activity is not clearly defined (S. Steller, pp. 52-53). There were also expert opinions that Germany's involvement in foreign cooperation, as indicated in the Strategy, should be described more precisely and in more detail, i.e., how exactly this cooperation should look (Steller, p. 53).

Germany's Cybersecurity Strategy adopted in 2016 identified the need to build a sustainable cybersecurity system (The 2016 Strategy, p. 9). The National Cyber Response Centre (NCAZ) organised its structure at the federal level in such a way that the various actors could cooperate in their activities. An important objective was to intensify cooperation with Länders (federal states) and to make them more involved. As part of the NCAZ, the federal authorities responsible for cybersecurity issues exchange information on cyber incidents in the Cyber-AZ and share their assessments and analyses. In order to strengthen cyber defence capabilities, the Cyber-AZ has been appropriately configured and organisationally strengthened within a nationwide cybersecurity architecture, and as a departmental institution it will develop into a central platform for cooperation and coordination under the directorship of the Federal Ministry of the Interior (the 2016 Strategy, pp. 27-28).

The implementation of the NIS Directive in Germany required legislative changes. The Implementing Act to the NIS Directive of June 2017 established the basis for setting up Mobile Incident Response Teams (MIRTs) at the BSI. Meanwhile, options for detecting and blocking cyber-attacks were broadened in telecommunications law. Mobile Incident Response Teams (MIRTs) were established at the BSI to analyse and clear up cyber incidents in institutions. Upon the request of the MIRT, the BSI will be able to provide support to constitutional authorities, federal authorities and operators of critical infrastructures, as well as similarly important institutions. This assistance is intended to

rapidly restore the safe technical operations of the institutions concerned (The 2016 Strategy, p. 29). A specific feature of the German solution is that the BSI is entrusted with control over how to implement detailed protection procedures in those departments of critical infrastructure that determine the way society functions. The following systems have been identified as such: banking, energy, water supply (drinking water delivery), food, telecommunications and information technology. As the tasks refer to the operators of ICT networks and institutions using them in terms of data protection, forms of security in case of their digitisation and attempts to hack personal accounts in the system, it was decided to distribute the competences of federal institutions in this way. The BSI is authorised to implement procedures on critical infrastructure elements of information systems, whose procedures refer both to the way they are used and to the changes introduced, and investments made in order to secure their functionality (Mickiewicz, p. 76).

Cyber-attacks might also require action by local federal security agencies. To this end, the Federal Criminal Police Office (BKA) set up a specialised investigative unit, the Quick Reaction Force (QRF), which, in consultation with the responsible public prosecutor's office or the Office of the Federal Prosecutor, conducts the first criminal procedure for law enforcement agencies (The 2016 Strategy, p. 29). "Mobile Cyber Teams" were set up within the BfV itself, which are made up of IT specialists, intelligence specialists experienced in analysing cyber-attacks and, if necessary, staff with foreign language skills. These cyber teams will travel to the scene of cyber-attacks with an intelligence or extremist/terrorist background (The 2016 Strategy, p. 29).

In the defence sector, these tasks were carried out by the Military Counterintelligence Service (MAD). The Federal Intelligence Service (BND) could monitor attacks as they were being prepared and carried out. Information flows resulting from attacks are also registered. The Bundeswehr may also contribute, as much as they are allowed by the Constitution, to security preparedness with its Incident Response Teams and other relevant units. Setting up MAD is widely regarded by experts as a paradigm shift from defensive to offensive cyber defence (Bendik 2016, p. 13).

In the case of foreign intelligence services, cyber-attacks on governmental IT systems, and those of businesses, research institutes and their employees, are monitored by the BfV Directorate-General for Counterintelligence. Its scope of activity concerns cyber espionage, the evaluation of attacks on federal agencies and other targets which are thought to be the work of intelligence services. In line with its scope of activity, the BND monitors cyber spying and other cyber-attacks from abroad targeting government and/or critical infrastructures in Germany. The BND could send potential targets an early warning to take any necessary defensive action (Signals Intelligence Support to Cyber Defence (SSCD)). In this way, the BND was using IT specialists and experienced analysts to create an early-warning system for cyber-attacks (The 2016 Strategy, p. 32).

The Strategy announced the setting up of an institution, within the remit of the Federal Ministry of the Interior, whose task would be to provide technical support to federal security and technical authorities, including intelligence services, in their operational cyber capabilities. In 2017, the Centre for Information Technology of Security Authorities (*Zentrale Stelle für Informationstechnik im Sicherheitsbereich – ZITiS*) was established. The ZITiS itself has no operational powers (The 2016 Strategy, p. 32).

In Germany, the BSI acts as the national CERT for administration and for operators of critical infrastructure, the private sector and individual users, as well as a single point of contact for foreign and international CERTs. CERTs act as computer emergency response teams, which are an important component of any sustainable cybersecurity architecture, as single points of contact for technical prevention and response in the field of IT security. There are also independent CERTs at other federal agencies and in Länders, as well as in some businesses and research institutions (The 2016 Strategy, p. 34; Mickiewicz, p. 75).

The introduction of the new Cybersecurity Strategy was preceded by the IT Security Act 2.0 adopted on 7 May 2021 (I IT-Sicherheitsgesetz 2.0). The Act essentially strengthened the competences of the BSI as the competent authority for cybersecurity. In addition to the afore-said competences, the BSI has broadened its scope of action in five key areas of activity. The first is the indication that the BSI is the national cybersecurity certification authority, pursuant to §9a (1), within the meaning of Article 58(1) of EU Regulation 2019/881. In particular, the BSI is responsible for monitoring and enforcing the provisions of law under European cybersecurity certification schemes. Another area is the detection of threats and defence against cyber-attacks. As a major competence centre for cybersecurity, the BSI can design digital security strategies by setting binding standards for federal authorities and monitoring them effectively. The next area concerns mobile network security and the certification of key components. Another area is consumer protection, which has become one of the BSI's tasks. It has become an independent consumer IT advice centre at the federal level and the authority competent for the introduction of uniform, transparent IT certification. In the area of business security, the BSI will monitor the implementation of IT security measures and the exchange of information (IT-Sicherheitsgesetz 2.0, p. 11).

The Cybersecurity Strategy was adopted by the Federal Government on 8 September 2021. The starting point of the Strategy is an assessment of the threat situation. This is marked by a considerable quantitative and qualitative increase in cyber-attacks, an expansion in the potential scope for attacks and new threat scenarios. The cybersecurity landscape includes civil society, initiatives and research institutions, business entities and governmental bodies. The objectives of the Strategy are identified in 4 areas:

1. Establishing cybersecurity as a joint task for the government, private industry, the research community and society.
2. Reinforcing the digital sovereignty of the government, private industry, the research community and society.
3. Making digital transformation secure.

4. Setting measurable and transparent objectives (The 2021 Strategy, p.6).

The presented objectives of the Strategy point to ensuring the security of citizens as the main users of IT networks. To this end, the strategic objectives envisage sensitising citizens and increasing their cyber competence. The next objective is to be achieved by strengthening, in general, cybersecurity in private industry, focusing on the protection of critical infrastructures, specifically on the operations of small and medium-sized enterprises. In this case, fostering digital sovereignty and the competitiveness of companies in the cybersecurity field is essential. Under the next objective, the following three main areas of action can be identified: 1. The distribution of competences and cooperation among the relevant authorities; 2. The enhancement of skills and powers within the authorities; and 3. New challenges facing state actors in cyberspace. As for the last objective, the Federal Government intends to achieve it through "Germany's active role in European and international cybersecurity policy" and through Germany's participation in the European Union (EU) and the North Atlantic Treaty Organization (NATO) (The 2021 Strategy, pp. 6-7).

The 2021 Cybersecurity Strategy is based on the development of the afore-said 2011 and 2016 Strategies and, above all, on the foundations laid down for the National Cybersecurity Council (NCSR), the National Cyber Response Centre (NCAZ, Cyber-AZ) and the Central Office for Information Technology in the Security Sector (ZITiS). The implementation of the specifications and strategic objectives are carried out, in particular, by the departmental bodies of the Federal Chancellery and the ministries. Federal activities are divided between two levels of action: strategic and operational.

Ministries are responsible for the strategic orientation of their cybersecurity policy and monitoring its implementation. They are in charge of managing the activities in their remits independently, based on the principle of ministerial autonomy. At the federal level, the Federal Ministry of the Interior, Building and Community (BMI) is responsible for coordinating domestic cybersecurity policy, and the Federal Foreign Office is responsible for coordinating international cybersecurity policy. Finally, the Federal Ministry of Defence (BMVg) is responsible for cyber defence (The 2021 Strategy, p. 19).

The Strategy highlights the important role of the NCS as a coordinator that needs to bring together different perspectives from the private sector and society as a whole in the strategic advice it provides to the Federal Government. The 2016 Cybersecurity Strategy set out its specific remit as the authority competent for the identification of long-term action needs and trends, and for the development of recommendations for action. Recognising the importance of the NCSR, the current Strategy emphasises its role as the Federal Government's strategic advisory body by extending and formalising its powers. The Government expects the NCSR to provide a more comprehensive perspective on cybersecurity topics by enabling information sharing aimed at providing all stakeholders with a deeper understanding of the respective positions of those involved (The 2021 Strategy, pp. 55-56).

The operational level primarily includes the activities of the BSI as the Federal Government's central agency for information security. The BSI comprises the Federal Government, the Federal Security Operations Centre (BSOC), the Computer Emergency Response Team for federal agencies (CERT-Bund), and the National IT Situation Centre. The BSI is additionally responsible for the security and protection of the Federation's network and information technology, as well as for national critical infrastructure. The BSI is further in charge of shaping information security by providing testing, standardisation, certification, authorisation and advisory services for the government, industry and society, working closely with stakeholders from all relevant areas (The 2021 Strategy, pp. 19-20).

The Federal Office for the Protection of the Constitution (BfV) is responsible for upholding internal security, and it reports to the Federal Government and the public on security situations. It is responsible for collating and evaluating information on cyber-attacks that have extremist or terrorist motivations or that have been initiated by foreign intelligence services. The Military Counterintelligence Service (MAD) protects the Bundeswehr from espionage and sabotage as well as from extremism and terrorism in cyberspace. The Federal Intelligence Service (BND) is responsible for providing any necessary information. Gaining knowledge of other countries is relevant to the German foreign and security policy, which is included for the purpose of collating and evaluating security in cyberspace. The Bundeswehr's Cyber and Information Domain Service Headquarters (KdoCIR) coordinates cyber defence within the Bundeswehr.

In Germany, the federal states are generally responsible for the prevention of threats in cyberspace. The Federal Government has special jurisdiction over threat prevention in certain areas, such as international terrorism, security in the territory belonging to the federal railways, border protection, and national self-protection, where jurisdiction extends to the cyber domain. These tasks are carried out by the Federal Criminal Police Office (BKA), the Federal Police (BPOL) and the BSI. The judiciary is responsible for law enforcement in cyberspace, with support from state criminal police offices and police authorities, as well as from the BKA and the BPOL, as and when necessary, in line with their respective jurisdiction. The agencies listed, as well as any others involved, are coordinated at operational level in the Cyber-AZ (within the BSI structure), which serves as the central information and coordination platform.

The Central Office for Information Technology in the Security Sector (ZITiS) acts for the strengthening of cyber capabilities and digital sovereignty as a service provider for the security authorities within the remit of the Federal Ministry of the Interior, Building and Community. The federal authorities and companies that are tasked with the secure operation of federal IT infrastructure are also extremely important. They include: the Federal Agency for Public Safety Digital Radio (BDBOS), which operates the federal public safety radio networks, the Federal Information Technology Centre, and the Federal Foreign Office, as a federal operator of Germany's IT abroad. (The 2021 Strategy, p. 20).

Cooperation between the Federal Government and Länders is essential. The central authorities coordinating federal and state cooperation at a strategic level include the Standing Conference of the Interior Ministers with its cybersecurity working group at the state level, and the IT Planning Council with its information security working group. The latter is also responsible for managing information security between the federal and state governments (the 2021 Strategy, p 21). There are many forms of cooperation between the Government and Länders. First and foremost is the cooperation within CERT (VCV) or the close coordination of the state criminal police offices with the BKA as the central criminal police office. The central cybersecurity coordination offices, which are more and more often established by the federal states and linked to the BSI, are also closely involved in the cooperation at an operational level (The 2021 Strategy, p. 21).

The German Federal Government's cybersecurity policy is consistent and in line with the European Union's cybersecurity policy. Since its first Strategy adopted in 2011, Germany has consistently identified the authorities competent for cybersecurity. Efforts connected with the establishing of the National Cybersecurity Council (NCSR) and the National Cyber Response Centre in 2011, and the Central Office for Information Technology in the Security Sector (ZITiS) in 2017, as well as the participation of individual ministries in the process of building the cybersecurity system, were reprised and further clarified in the 2016 Strategy. The implementation of the NIS Directive resulted in the creation of a more transparent cybersecurity architecture. Under the IT Security Act 2.0, the BSI has been given specific competences as the national authority competent for cybersecurity. It is the Federal Office for Information Security, equipped with more and more competences, that has become the main institution for the protection of civilian cybersecurity in Germany, without prejudice to the competences of other authorities in their action area.

It is the state that plays a leading role in shaping a high level of security in cyberspace and bears the responsibility for the implementation of this policy. The state has a significant role to play and a large responsibility in ensuring a high level of cybersecurity. The state's area of activity includes the prevention, mapping, detection and counteraction of threats, incident management and criminal prosecution, counterintelligence and advanced intelligence activities conducted by the intelligence services, as well as foreign cyber policy and cyber defence. The multiplicity of tasks requires the involvement of multiple actors who, in a decentralised form, carry out tasks at both strategic and operational levels.

References:

Bendiek, A. (2016) *Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik* (Berlin: Stiftung Wissenschaft und Politik), p. 13, available at: https://www.ssoar.info/ssoar/bitstream/handle/document/46537/2016S03_bdk.pdf?sequence=1&isAllowed=y&lnkname=2016S03_bdk.pdf (July 17, 2020).

Guitton, C. (2013) Cyber insecurity as a national threat: overreaction from Germany, France and the UK?, *European Security*, 22(1), pp. 21-35.

Mickiewicz, P. (2017) System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza, *Rocznik Bezpieczeństwa Międzynarodowego*, 11(1), pp. 65-80.

Oleksiewicz, I. (2017) Polityka bezpieczeństwa cybernetycznego RFN, *Studia Bobolanum*, 28(3), pp. 41-56.

Sacewicz, K. (2021) Niemiecka strategia ochrony cyberprzestrzeni, *Przegląd Bezpieczeństwa Wewnętrznego*, 4(7), pp. 129-135.

Steller, S. (2017) Die Cyber-Sicherheitsstrategie für Deutschland, Arbeitspapiere zur Internationalen Politik und Außenpolitik, *AIPA*, 1/2017, pp. 1-84, available at: https://jaeger.uni-koeln.de/fileadmin/templates/Allgemeines/AIPA_Die_Cyber-Sicherheitsstrategie_fuer_Deutschland_Stephan_Steller.2017.pdf (July 17, 2020).