Teka Komisji Prawniczej PAN Oddział w Lublinie, vol. XV, 2022, no. 2, pp. 61–72
https://doi.org/10.32084/tkp.4793

GERMANY'S CYBERSECURITY POLICY

Dr. Agnieszka Brzostek

War Studies University, Poland
e-mail: a.brzostek@akademia.mil.pl; https://orcid.org/0000-0002-7444-0186

Abstract. The German Federal Republic is one of the states whose state policy in the field of cybersecurity is considered to be coherent and effective. However, even Germany is a country exposed to numerous attacks. Ubiquitous technology in every aspect of our lives, and in addition the COVID-19 pandemic, introducing widespread mobile work and online education, have created even greater threats. By adapting internal legislation, indicating strategic and specific goals, Germany is part of the EU cybersecurity policy in its cybersecurity strategies. Prior to the adoption of the NIS 2 directive, Germany had already created a legal basis that would effectively and efficiently protect German cyberspace. In order to strengthen the effectiveness of their cybersecurity policy, Germany is strengthening cooperation between federal authorities, business, science and strengthening digital sovereignty.

Keywords: cybersecurity; cybersecurity competent authorities; Germany; cybersecurity strategy

INTRODUCTION

Nowadays, presenting cybersecurity as an important element of state policy is already a truism. Cybersecurity has become our everyday life in almost every aspect of our lives. Many of our daily tasks, regardless of whether they concern private, economic or social life, depend on modern technologies. The COVID-19 pandemic has further accelerated this process. In the report on cybersecurity published by BSI in 2021 in Germany, threats in the form of malware and ransome attacks posed the greatest threat, and as indicated in the report, the pandemic increased the threat to cybersecurity and attacks became more frequent and more expensive (ANSSI and BSI report). Professionalization of criminal groups and the growth of network systems caused by the transition to mobile work contributed to an increase in the attack surface through the provided and used communication services and devices, which made it possible to take advantage of the gaps in network security systems.

In order to take full advantage of all the possibilities, advantages and needs of digitization, it is necessary to protect against these threats. It is the state's responsibility to assess the rapid development of digitization in the

ISSN 1899-7694
e-ISSN 2719-7379

interests of citizens together with business, science and civil society, and actively shape the necessary framework for a high level of security and protection in cyberspace is guaranteed. The protection of the critical and civil infrastructure network has become a priority in Germany's policy. Since the adoption in 2005 of the National Plan for the Reconstruction of Information Protection Infrastructure, the National Information Protection Plan and the adoption of further cybersecurity strategies for Germany in 2011, 2016 and 2021 were aimed at building and then extending the cyberspace protection system, focusing on technical and preventive measures [Schallbruch and Iskierka 2018, 15].

The aim of the article is to analyze the legal solutions and the adopted policy set by the federal government in the field of cybersecurity in the international context, especially within the EU policy and the obligations of the NIS directive. The question is, what is this policy like? Is it effective and efficient, also bearing in mind the upcoming changes in the form of the NIS 2 Directive?

1. LEGAL BASIS OF CYBERSECURITY IN GERMANY

The literature recognizes that the beginning of the federal government's activities in the field of IT systems protection was the establishment in 1990 of the BSI (Bundesamt für Sicherheitin der Informationstechnik – Federal Information Security Office) [ibid., 16]. This was due to the fact that BSI was granted the competence to coordinate the security of the government and the economy. Solutions adopted in other countries in the field of cybersecurity and the international situation, especially after the attacks of September 11, 2001, contributed to the intensified cooperation in this area [Guitton 2013, 22] which resulted in the presentation of the Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) in 2005. It was introduced as a comprehensive umbrella strategy for IT protection. Created by the Ministry of the Interior with the support of BSI. The government has set three basic goals: to harmonize the appropriate protection of the IT structure, to be ready to respond effectively to incidents related to IT control, and to increase competences in the field of IT security. These goals were to be achieved through prevention, preparedness and sustainable development. According to these solutions, two plans were to be implemented, compulsory for federal administration and public-private for critical infrastructure (KRITIS) [Schallbruch and Iskierka 2018, 18]. This the last Umsetzungsplan KRITIS Plans zum Schiutz der Informationsinfrastrukturen (KRITIS Implementation Plan – National Information Infrastructure Protection Plan) developed by the Ministry of the Interior in 2007 was addressed to private entrepreneurs who operated in key sectors of the economy for the state

[Oleksiewicz 2019, 121]. The plan was developed in an IT security management schema through the following cycle: plan, implement, check, improve.[1] Changes in the law strengthened the position of BSI in the field of cybersecurity (Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes Vom 14. August 2009). This intensified the work of the government in the field of increasing the level of security through cooperation with international organizations and internal stakeholders, which led to the creation in 2011 of the Cybersecurity Strategy.

The first cybersecurity strategy was adopted by the federal government in 2011. The strategy focused mainly on the civilian aspects of cybersecurity. They are complemented by measures taken by the Bundeswehr to protect its capabilities and measures necessary to make cybersecurity part of Germany's preventive security strategy. The strategy recognizes the necessity of international coordination and the creation of appropriate networks focusing on aspects of foreign and security policy. This was to include cooperation not only in the United Nations, but also in the European Union, the Council of Europe, NATO, G8, OSCE and other multinational organizations [Chałubińska-Jentkiewicz and Brzostek 2021, 129]. As goals and means, the Strategy identified the protection of critical IT infrastructure, construction of secure IT systems in Germany, strengthening IT security in public administration, establishment of the National Cybersecurity Council, development and implementation of the effectiveness of crime control in cyberspace, development of human resources in federal administration and international cooperation.[2] As a result of adopting the strategy, work on the adoption of the IT security law was initiated, which should improve the protection of critical infrastructure by regulating critical infrastructure operators.

In June 2015, the federal government adopted one of the first laws on IT security in Europe (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, IT-Sicherheitsgesetz). IT security discussions mechanisms for critical infrastructure operators have been operating at the European level for several years, and the Directive NIS (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems in the territory of the Union, Journal of Laws of the EU, L 194/1) was introduced only a year later, in 2016 [Schallbruch and Iskierka 2018, 22-23].

The IT Security Act imposed a number of obligations on critical infrastructure operators in seven sectors (energy, health, information and telecommunications technologies, transport, water, food, and the financial and

[1] Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen, Bundesministerium des Innern, Berlin 2007, p. 10-11.

[2] Cybersecurity Strategy Germany, 2011, p. 6-7.

insurance sectors). Government administration as well as media and culture are classified as: critical infrastructure, but already regulated by other legal acts, and therefore not covered by the IT Security Act. The law creates mandatory reporting requirements requiring Critical Infrastructure Operators to report potential and actual IT relevant security incidents to BSI. In addition, critical infrastructure operators must implement mandatory minimum IT security standards. [ibid.].

Due to the fact that the most important NIS solutions were already included in the German legislation in the IT Act, this meant that the federal government changed the federal law only to a small extent. The NIS Directive was implemented by the Act of 27 April 2017 on measures to ensure a high level of common network and information security in the Union (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) BSI and some safety management provisions. Critical infrastructure, CISIRT regulations and special regulations for digital service providers, included in the BSI or on the Military Counterintelligence Service [Adamiec, Branna, Dziewulak, et al. 2021, 301-302]. In Germany's Cybersecurity Strategy in 2016, the federal government planned to focus its cybersecurity policy in four areas in the coming years: safe and independent operation in the digital environment, joint cybersecurity mission of the state and business, powerful and sustainable cybersecurity architecture throughout the state, and active positioning Germany in the European and international cybersecurity policy.[3] Mobile incident response teams (MIRT) have been established at the Federal Information Security Authority (BSI) [Schallbruch and Iskierka 2018, 26], which analyzed and removed cyber incidents in institutions. A specific feature of German solutions is entrusting BSI with control over the implementation of detailed protective procedures in those sections of the critical infrastructure that determine the way the society functions. The following systems were considered to be: banking, energy, water (drinking water supply), food, telecommunications and information technology. Due to the fact that the tasks relate to teleinformation network operators and institutions using them in the field of data protection, forms of security in the event of their digitization and attempts to hack into personal accounts in the system, it was decided to divide the competences of federal institutions in such a way [Mickiewicz 2017, 76]. The BSI was expected to play the role of a national CERT in administration and for critical infrastructure operators, the economy and citizens, as well as a central point of contact for foreign and international CERTs. The 2016 strategy is broader than the

[3] Cyber-Sicherheitsstrategie für Deutschland, 2016, p. 9.

2011 strategy, it is a work program for individual federal government agencies, it is not a strategic program. He defined goals and directions for action, without specific and measurable ways of achieving them [Schallbruch and Iskierka 2018, 27]. The assumptions of the bodies' activities adopted in the strategy have been criticized by experts. It was argued that the composition of the National Cyber Security Council was too general. It was noted in a confidential report of the Federal Audit Office that the council was not an appropriate institution to counter the attack because it did not have enough staff and its area of operation was not clearly defined [Steller 2017, 52-53]. There were also opinions of experts that the involvement of Germany in foreign cooperation indicated in the strategy should be described in more detail and precisely, is exactly what this cooperation should look like [ibid., 53].

The introduction of the new cybersecurity strategy was preceded by the adoption of the ICT network security act on May 7, 2021 (I IT-Sicherheitsgesetz 2.0). The act substantially strengthened the competences of BSI as the competent authority in the field of cybersecurity. In addition to the abovementioned competences, BSI has broadened its scope of activity in five key areas of activity. The first is to indicate that BSI is the national authority competent for cybersecurity certification, in accordance with §9a para 1, within the meaning of Article 58(1) of the EU Regulation 2019/881. The BSI is responsible in particular for the monitoring and enforcement of European cybersecurity certification schemes. Another one is threat detection and defense against cyber attacks. As a central cybersecurity competence center, BSI can design digital security strategies by setting binding standards for federal authorities and monitoring them effectively. The next area concerns the security of cellular networks and the certification of key components. Another area is consumer protection, which has become a BSI task. It has become an independent IT consumer advice center at federal level and the competent authority to introduce uniform, transparent IT certification. In the field of corporate security, BSI will monitor the implementation of IT security measures and information exchange.[4]

The cybersecurity strategy of September 8, 2021 created the framework for the federal government to operate for the next five years. The NIS Directive required the Member States to create a steering framework in the strategy and to identify goals and priorities, and to designate the bodies that would be responsible for achieving these goals. The implementation of the specifications and strategic goals is carried out primarily by the departmental bodies of the Federal Chancellery and ministries. As part of activities at

[4] IT-Sicherheitsgesetz 2.0, p. 11.

the federal level, two levels of action have been identified: strategic and operational [Chałubińska-Jentkiewicz and Brzostek 2021, 139].

2. INSTITUTIONS COMPETENT IN CYBERSECURITY

The activity of institutions competent in the field of cybersecurity in Germany is based on the structure of the division of the level of their operation into political, strategic and operational. Politically and strategically, responsibility for shaping cybersecurity policy lies with the federal government, internal cybersecurity policy is the responsibility of BMI (Bundesministeriums des Innern und für Heimat) and the Federal Office of Foreign Affairs (Auswärtiges Amt – AA) in the area of foreign policy cybersecurity. The BMVg (Federal Ministry of Defense – Bundesministerium der Verteidigung) is responsible for cyber defense. At the operational level, however, the system is structured around the BSI. The Federal Office for Security and Information (Bundesamt für Sicherheit in der Informationstechnik – BSI) is the central federal authority for security, within the Ministry of the Interior. Established in 1991 (Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik) and as a result of several amendments to the law in 2009, 2015 and 2017, the legislator successively extended the scope of tasks and BSI currently serves as the central authority for cybersecurity in Germany. According to § 3 of the BSI Act, its main task is to promote information technology security in order to ensure the availability, integrity, confidentiality and processing of information. BSI is responsible for shaping information security through testing, standardization, certification, approval and consulting services for the state, business and society, and closely cooperates with entities from all areas of the economy.[5] BSI is both the federal government's central reporting office on information technology security and the central reporting office for critical infrastructure operators on information technology security issues. It is responsible for collecting and assessing the information necessary to counteract security threats in information technology, analyzing their potential impact on the availability of critical infrastructure in cooperation with the competent supervisory authorities, and constantly updating the situation report on IT security of critical infrastructure or companies of special public interest (section 8b of the BSI Act) [Mollers 2020, 6]. BSI is also the central accreditation and certification body for IT security in Germany. BSI is also empowered to investigate the IT security of products and services on the market and may publish alerts when it detects an IT security failure of products or services. Only in

[5] Cybersicherheitsstrategie für Deutschland, 2021, p. 8.

the years 2013-2017, 45 additional laws and regulations were adopted that entrusted BSI with such tasks [Schallbruch and Iskierka 2018, 32].

The law implementing the NIC Directive of June 2017 created the basis for the establishment of mobile MIRT incident response teams at BSI. On the other hand, the telecommunications law has expanded the options for detecting and blocking cyber attacks. Mobile Incident Response Teams (MIRTs) are established at BSI to analyze and remove cyber incidents in institutions. At the request of MIRT, BSI will be able to provide support to constitutional bodies, federal authorities and operators of critical infrastructure and similarly important local facilities, in order to quickly restore the technical efficiency of a given facility.[6] A specific feature of German solutions is entrusting BSI with control over the implementation of detailed protective procedures in those sections of the critical infrastructure that determine the way the society functions. The following systems were considered to be: banking, energy, water (drinking water supply), food, telecommunications and information technology. Due to the fact that the tasks relate to ICT network operators and institutions using them in the field of data protection, forms of security in the event of their digitization and attempts to break into personal accounts in the system, it was decided to allocate such competences of federal institutions. BSI is entitled to implement procedures regarding the way of using IT systems by elements of the critical infrastructure, relating both to the way they are used, as well as to changes and investments made in order to secure their functionality [Mickiewicz 2017, 76]. BSIs have CERT as one of the specialized units under the national cybersecurity umbrella unit [Backman 2015, 9-26]. The BSI includes the Security Operations Center (BSOC), the Federal Computer Emergency Response Team (CERT-Bund) and the National Center for IT Situations. The IT Security Act contains many provisions to strengthen the role of BSI. The main task was to evaluate reports on potential cyber attacks on critical infrastructure and in this respect he cooperates with the Federal Intelligence Service (BND), the Federal Office for the Protection of the Constitution (BfV) and the National Center for Counteracting Cyber Threats (NCAZ, also known as Cyber A-Z) [Oleksiewicz 2019, 131].

The NCAZ operates within the BSI structure. Established in 2011, it is a platform for cooperation and operation of the federal level and the competent authorities of individual federal states. At the time of its establishment, it was to become the first link in the fight against cyber threats and a platform for cooperation between the relevant German administration bodies. The Germans decided not to institutionalize the Centre's work due to the order in force in Germany to separate (Trennungsgebot) the secret services

[6] Strategy 2016, p. 29.

from the police services [Sacewicz 2012, 129-30]. Currently, the Center consists of, among others from the Federal Office for Military Counterintelligence, the Federal Criminal Police Office, the Federal Office for Teleinformation Security (BSI – Bundesamt für Sicherheit in der Informationstechnik), the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz – BfV); Federal Office for Civil Protection and Emergency Response (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 cybernetic and information space of the Bundeswehr command. The following were added as external partners: cyber defense of Bavaria, prosecutors of cyber protection specialists from Bamberg and Cologne and the Federal Office of Financial Supervision [Oleksiewicz 2017, 48-49].

The Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz – BfV) protects internal security and informs the federal government and the public about the state of security. The BfV is responsible for gathering information and assessing it about extremist or terrorist-motivated cyber attacks. The Federal Intelligence Service (Bundesnachrichtendienst-BND) is responsible for providing the necessary information. Acquiring knowledge about other countries that are important for Germany from the point of view of foreign and security policy, also for the purpose of collecting and assessing them in cyberspace. The cybernetic and information domain service (Kommando Cyber- und Informationsraum – KdoCIR) coordinates cyber defense in the Bundeswehr.[7] In the defense sector, these tasks are performed by the Military Shield Service (MAD). The Federal Intelligence Service (BND) can observe an attack in both the preparation and implementation phases, and information outflows resulting from attacks are also recorded. The Bundeswehr may also use its organizational components (including incident response teams) to contribute to general security measures within constitutional limits. In the opinion of experts, the creation of MAD is considered to be a change of the paradigm from defensive to offensive cyber defense [Bendiek 2016, 13].

The strategy emphasizes that the federal government has specific tasks resulting from the provisions on risk prevention in certain areas (for example, in the area of international terrorism, as well as security in the area of federal railroad facilities, border protection or self-security), which also includes cyberspace. These tasks are carried out by the Federal Criminal Police Office (BKA), the Federal Police (BPOL) and the BSI. The judiciary is responsible for prosecution in cyberspace with the support of state

[7] Cybersicherheitsstrategie für Deutschland, 2021, p. 20.

investigation and investigation offices and state police authorities or by the BKA and BPOL within their respective competences. Coordination between these and other competent authorities at the operational level takes place, *inter alia*, at Cyber A-Z (within the BSI structure), which serves as a central information and coordination platform. The Central IT Security Sector (ZITiS) works to strengthen cyber skills and digital sovereignty as a service provider to the security authorities of the Federal Ministry of the Interior. In addition, the federal government agencies entrusted with securing the federal IT infrastructure are of particular importance. These include the Federal Agency for Digital Radio for Authorities and Organizations with Security Tasks (Bundesanstalt für den Digitalfunk der Behörden und Organizationen mit Sicherheitsaufgaben – BDBOS) – federal network operator, the Federal Center for Information Technology (Informationstechnikzentrum Bund – ITZBund), as well as the Ministry of Foreign Affairs - operator of his international IT.

3. STRATEGIC GOALS OF THE POLICY AND ITS FUTURE

There has been a clear shift in the stated strategic goals that the federal government wanted to achieve. In the strategy of 2010, the goals were indicated most extensively, in as many as 10 points, i.e. protection of critical infrastructure as the main priority, security of IT systems (i.e. security of state documents provided – identity card or e-mail), strengthening of IT security of public administration by creating a uniform and secure network infrastructure, establishment of the NCAZ and the National Cyber Security Council, effective control of digital crime and international cooperation in the field of cyber security, development of human resources and creation of a coordinated and comprehensive set of tools to respond to cyber attacks.[8]

In the 2016 cybersecurity strategy, the federal government already planned to concentrate its policy in four main areas: safe operation in a digitized world, joint cooperation in the field of government and business security, building a sustainable cybersecurity architecture and active participation of Germany in European and international cybersecurity policy.[9]

In turn, the 2021 strategy defines the goals in four areas, i.e. cybersecurity as a joint task of the state, business, science and public participation, strengthening the digital sovereignty of the state, business, science and society, ensuring safe digitization and making the indicated goals measurable and transparent.[10]

---

[8] Cyber-Sicherheitsstrategie, 2011, p. 3-7.

[9] Cyber-Sicherheitsstrategie für Deutschland, 2016, p. 9.

[10] Cybersicherheitsstrategie für Deutschland, 2021, p. 8.

By reviewing only the goals that the federal government set in subsequent cybersecurity strategies, one can see the evolution of not only issues related to the perception of cybersecurity, but also changes that took place in international and European policy, the construction of the cybersecurity system (as a result of the IT 2.0 Act and the NIS Directives), the role of society and business in shaping a coherent and effective cybersecurity policy. Education in each area remains a separate issue, the first strategy focuses on the education of clerical staff, while the next ones recognize the need to educate the society from an early age. The fastest changes came with the COvid-19 pandemic. Remote work, remote education and interrupted supply chains in the economy made the federal administration aware that the most expedient is to focus on cooperation, i.e. to identify four actors as the goal of this policy: the state, business, science and society. Achieving this goal requires secure digitization and digital sovereignty. The federal government has decided that the implementation of the strategy is to be constantly monitored and verified.

At the same time, work was underway on a new European cybersecurity policy package. Already in December 2020, the European Commission presented a proposal for the NIS 2 Directive [Schmitz-Berndt and Chiara 2022]. This concerned the enactment of the IT 2.0 Act in May 2021, which significantly changed the existing national cybersecurity law, tightening the obligations in the field of NIS security. The upcoming changes concern, *inter alia*, the scope of the Directive, revised cybersecurity risk management measures and reporting obligations, the strengthening of supervisory powers and the introduction of harmonized administrative sanctions. As noted by S. Schmitz-Berndt, P.G. Chiara adopted by the German state legislation is in line with the NIS2 legal standard and already covers, *inter alia*, waste management sector. Nevertheless, it requires changes in relation to, *inter alia*, postal and courier services, chemicals, food production, processing and distribution. The NIS 2 provisions also correspond to the indicated cybersecurity management measures and reporting obligations. This applies, *inter alia*, to cybersecurity risk management in the supply chain, internal rules introducing a manufacturer credibility assessment that reflects an EU-coordinated risk assessment of critical supply chains in accordance with Article 19 of the NIS2 project. Minor adjustments concern the notification timeframe which, according to the NIS2 proposal, will be adjusted to the uniform notification procedure. Regarding the role of supervisory authorities, the German legislators considered it appropriate to strengthen and extend the mandate of the BSI. It will be the national competent authority and single point of contact for the NIS and the national cybersecurity certification authority. Progress with ITSiG 2.0 ahead of the vote on the NIS2 directive means that entities in Germany will face the adoption of a new law in the

near future, which will result in an adaptation of business policy and action plans in the field of cybersecurity. Legislators should take the opportunity to harmonize their national cybersecurity legislation into a single, organic, comprehensive and coherent legislative text that meets the objectives of the NIS2 Directive while taking into account specific national requirements. This will bring significant benefits to the competent national authorities, economic operators and legal practitioners and avoid overlapping and duplication of requirements under different legal acts [Schmitz-Berndt and Chiara 2022]. Reflected under national legislation, there are no administrative fines yet, which should follow the RODO sanctions model, as demonstrated in section 14 of the BSI Act.

CONCLUSIONS

Germany's cybersecurity policy is consistently built around the central authority of the Federal Office for Information Security – BSI. The Act on BSI and the Act on IT 2.0 as well as numerous regulations strengthen the position of the authority. Other federal ministries and agencies complement the cybersecurity policy in their area of operation. When assessing the effectiveness of German policy, its complexity should be taken into account. In legal and organizational terms, Germany's cybersecurity system is built coherently and effectively. It operates at the federal and local level, involving state authorities taking into account their specificities. This gives the opportunity to involve many actors, taking into account specialist solutions, information technology, protection of critical infrastructure. Germany's cybersecurity policy is also consistent in its management system. Analyzes needs such as education, cooperation between the state and business, the development of science and new technologies and manages their development. The purposefulness and effectiveness of such a policy can also be seen in the response to events in international politics. In the strategy adopted in September 221, the mere indication of strategic goals makes it possible to emphasize this. Building digital sovereignty and greater emphasis on cooperation with business and science give grounds to assume that the German state will be even more effective in its policy. Finally, it should be emphasized that the federal government has already changed the regulations, even before the adoption of the NIS 2 Directive, in order to adequately respond to the changing threat landscape.

REFERENCES

Adamiec, Danuta, Justyna Branna, Dobromir Dziewulak, et al. 2021. "Informacja na temat legislacji dotyczącej systemu cyberbezpieczeństwa w wybranych państwach

Unii Europejskiej (Belgia, Czechy, Estonia, Francja, Holandia, Niemcy, Szwecja)." *Zeszyty Prawnicze. Biuro Analiz Sejmowych Kancelarii Sejmowych* 3 (71):280-314.

Backman, Sarah. 2015. "Organising National Cybersecurity Centres." *Information & Securites: An International Journal* 32, no. 1:9-26.

Bendiek, Annegret. 2016. *Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik*. Berlin: Stiftung Wissenschaft und Politik.

Chałubińska-Jentkiewicz, Katarzyna, and Agnieszka Brzostek. 2021. *Strategie cyberbezpieczeństwa współczesnego świata*. Warszawa: Towarzystwo Wiedzy Obronnej.

Guitton, Clement. 2013. "Cyber insecurity as a national threat: overreaction from Germany, France and the UK?" *European Security* 22, no. 1:21-35.

Mickiewicz, Piotr. 2017. "System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza." *Rocznik Bezpieczeństwa Międzynarodowego* 11, no. 1:65-80.

Mollers, Norma. 2020. "Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State." *Science, Technology, & Human Values* 46, no. 1:112-38.

Oleksiewicz, Izabela. 2017. "Polityka bezpieczeństwa cybernetycznego RFN." *Studia Bobolanum* 28, no. 3:41-56.

Oleksiewicz, Izabela. 2019. *Zarys polityki cyberbezpieczeństwa Unii Europejskiej. Casus Polski i RFN*. Warszawa: Elipsa.

Sacewicz, Kamila. 2012. "Niemiecka strategia ochrony cyberprzestrzeni." *Przegląd Bezpieczeństwa Wewnętrznego* 4:129-35.

Schallbruch, Martin, and Isabel Skierka. 2018. "The Organisation of Cybersecurity in Germany." In Martin Schallbruch, and Isabel Skierka, *Cybersecurity in Germany*, 31-47. Springer.

Schmitz-Berndt, Sandra, and Pier G. Chiara. 2022. "One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive." *International Cybersecurity Law Review* 3 (2):289-311.

Steller, Stephan. 2017. "Die Cyber-Sicherheitsstrategie für Deutschland." *Arbeitspapiere zur Internationalen Politik und Außenpolitik – AIPA*. No. 1.