Bundesministerium
des Innern
und für Heimat

Cyber Security Agenda of the Federal Ministry of the Interior and Community

Objectives and measures for the 20th legislative period

Cyber Security Agenda of the Federal Ministry of the Interior and Community

Objectives and measures for the 20th legislative period

Contents

Introduction

In April 2022, the Federal Minister of the Interior and Community, Nancy Faeser, unveiled her programme entitled "2025 Digital Policy Objectives and Measures of the Federal Ministry of the Interior and Community" (*Digitalpolitische Ziele und Maßnahmen bis 2025 des Bundesministeriums des Innern und für Heimat*). It outlines the projects she intends to implement, for example in relation to the digitalisation of public administration, data policy and cyber security, in order to ensure that the country makes progress in those regards between now and 2025. This Cyber Security Agenda of the Federal Ministry of the Interior and Community (*Bundesministerium des Innern und für Heimat*, BMI) is designed to flesh out the cyber security aspects of that digital programme.

The war in Ukraine is yet another prime example of why cyber security is so essential for modern, high-tech and digitalised developed countries such as Germany: targeted attacks on critical infrastructures (CIs), activities of cyber criminals (including state-sponsored cyber criminals), "collateral damage" resulting from attacks on companies which support the local economy, targeted disinformation and attacks on and/or sabotage of government structures are designed to have a huge, lasting negative effect on our society and our economy in terms of their ability to function or even bring them to their knees.

Bolstering the cyber resilience of the federal authorities, other government and civil infrastructures and, in particular, critical infrastructures is therefore of immediate and paramount importance, as are modernising the cyber security architecture, further developing secure infrastructures, safeguarding digital consumer protection and ensuring the availability of trustworthy technology. Citizens rightly expect their government to plan ahead, ensure that these structures work and protect society from digital threats. This also includes bolstering the cyber capabilities of the security authorities and expanding in-house development capacity. This is essential for our police forces and intelligence services to be able to fulfil their legal mandates confidently.

The following measures are therefore designed to ensure that we benefit from effective and efficient arrangements in cyberspace and maximum cyber security protection.

1. Modernising and harmonising the cyber security architecture

We will strive to achieve a clearer and more efficient allocation of responsibilities within the cyber security architecture and will bring all stakeholders involved closer together using a logical approach. As such, we will assess the effectiveness of all stakeholders' current performance and examine the effectiveness of the current division of powers as well as cooperation among the various different authorities. This applies both to cooperation between the federal authorities and to collaborative efforts between the Federal Government and the *Länder*.

Objectives and measures for the 20th legislative period:

- Development of the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) into a hub for cooperation between the Federal Government and the *Länder*
- Adaptation of the division of powers with regard to the prevention of threats in cyberspace
- Further development of the Cyber Security Strategy for Germany 2021 (*Cybersicherheitsstrategie für Deutschland 2021*)
- Further development of the National Cyber Response Centre (*Nationales Cyber-Abwehrzentrum*)
- Strengthening of the National Cyber Security Council (*Nationaler Cyber-Sicherheitsrat*)
- Establishment of greater independence for the Federal Office for Information Security (BSI)

2. Strengthening the cyber capabilities and digital sovereignty of the security authorities

By further developing and strengthening the technical investigation and analysis capabilities and tools of the security authorities, we will be able to ensure that the authorities can keep pace with technological changes in the digital domain and continue to fulfil their legal mandates with regard to threat prevention and law enforcement in line with requirements. Expanding the Central Office for Information Technology in the Security Sector (*Zentrale Stelle für Informationstechnik im Sicherheitsbereich*, ZITiS) will ensure that the security authorities are supported with technical solutions specifically to help improve their investigation and analysis capabilities, while reducing the security authorities' dependence on manufacturers from outside Europe. At the same time, the police forces and intelligence services will benefit from the expansion of in-house national development capacities and the centralised pooling of investments and development capacities within the Central Office for Information Technology in the Security Sector.

Objectives and measures for the 20th legislative period:

- Creation of a comprehensive digitalisation strategy for the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*, BfV)
- Modernisation of the IT infrastructure within the Federal Office for the Protection of the Constitution
- Further development of the cyber capabilities of the Federal Office for the Protection of the Constitution and their deployment within the community of the German domestic civil intelligence services, in particular, the modernisation of:
  - research tools for gathering intelligence on extremism on social media; and
  - data filing and analysis systems and tools for the gathering of intelligence on and early detection of state-sponsored cyber attacks
- Better powers for gathering intelligence on the technical aspects of cyber attacks carried out by foreign powers
- Strengthening and expansion of the central role played by the Federal Office for the Protection of the Constitution within the community of the German domestic civil intelligence services

- Further development and modernisation of the investigation capabilities and tools of the Federal Criminal Police Office (*Bundeskriminalamt*, BKA) and the Federal Police (*Bundespolizei*, BPOL) in the digital domain in regard to automotive IT, the Internet of Things (IoT) and encryption as well as the police's use of artificial intelligence
- Establishment of an effective vulnerability management (vulnerability equities) process, including the introduction of official processes
- Creation of a legal basis for the Central Office for Information Technology in the Security Sector
- Expansion of the Central Office for Information Technology in the Security Sector as a central service provider for the security authorities as well as creation and further improvement of in-house national development capacities and assessment expertise within the Central Office for Information Technology in the Security Sector

3. Combatting cyber crime and illegal online content

Criminals are increasingly shifting their focus towards the digital domain. The ever-increasing number of cases recorded and the ever-increasing amounts of loss and damage incurred mean that effective measures need to be deployed in order to win the fight against cyber crime. This is especially true with regard to the issue of blackmail using ransomware. Furthermore, protecting children and minors from sexual abuse is a top priority. As such, we will adopt a robust stance by implementing a national strategy and will deploy targeted measures in order to take firm action against perpetrators, their networks and their dissemination tactics. In particular, we will establish processes for consistently reporting, prosecuting and removing child sexual abuse material. This will rely heavily on close cooperation between the digital sector, civil society and the authorities.

Combatting hate crime is another key focus. We will not tolerate people feeling unable to voice their opinions freely online out of fear of threats or violence, and we will ramp up our efforts to ensure that perpetrators are swiftly identified and prosecuted.

In order to fulfil these tasks, our security authorities need to have the best capabilities and tools at their disposal in the digital domain. We will therefore ensure that these are consistently enhanced and upgraded.

Objectives and measures for the 20th legislative period:

- Further expansion of the Cyber Crime Division of the Federal Criminal Police Office
- Expansion of the central skills and services of the Federal Criminal Police Office for combatting cyber crime
- Strengthening of international cooperation on the part of the Federal Criminal Police Office in the fight against cyber crime, including as part of international counter-ransomware initiatives
- Promotion of an EU-wide legal framework for preventing and combatting child sexual abuse, aimed in particular at preventing the dissemination of online child sexual abuse material
- Development of a national strategy for combatting child sexual abuse
- Creation of an annual overview of the national situation entitled “Child Sexual Abuse”
- Strengthening of the Federal Criminal Police Office’s human and technical resources for combatting child sexual abuse
- Creation of a nationwide process for the reporting and removal of online child sexual abuse material centrally coordinated by the Federal Criminal Police Office
- Stepping-up of efforts to combat illegal online content, in particular right-wing extremist content, for example by strengthening existing structures within the Federal Criminal Police Office
- Further development of the investigation capabilities of the Federal Police in the area of cyber crime by strengthening human and technical resources
- Consistent expansion of the Central Office for Information Technology in the Security Sector in order to develop digital investigation tools for the security authorities with a view to improving assessment and analysis capabilities in the fight against cyber crime

4. Strengthening the federal authorities' cyber security

In the light of the current escalation in Europe's security situation, even the federal authorities urgently need to reconsider their own self-protection measures. Germany is facing an ever-increasing number of cyber threats. Government structures' own self-protection measures are essential for ensuring that the government can continue to function and carry out its work. As such, the Federal Government is required, as a matter of priority, to ensure a significant increase in the federal authorities' cyber resilience. The Federal Government must immediately adapt the protection measures in its IT security architecture in line with the increased threat situation. The reinforcement measures set out below are essential.

Objectives and measures for the 20th legislative period:

- Establishment of a stronger legal basis regarding information security as well as implementation of a programme to strengthen the cyber security of the Federal Government with the appointment of a Chief Information Security Officer for the Federal Government (CISO BUND) and the establishment of a centre of excellence for federal operational security advisory services (*Kompetenzzentrum zur operativen Sicherheitsberatung des Bundes*)
- Establishment of the principle of "security by design and by default" in the federal administration
- Provision of advanced IT products and systems for the federal authorities for secure communications as well as investment in quantum computing and post-quantum cryptography
- Investment in quantum computing at the BSI in order to ensure secure government communications
- Improvement in the high availability of the Federal Government's data centres
- Advancements in terms of the Federal Government's information security management

5. Strengthening the cyber resilience of critical infrastructures

Critical infrastructure operators' dependence on availability in IT supply chains can be of immediate, vital importance in the event of loss or damage, or in a crisis situation. Therefore, in addition to the assessment of manufacturers' trustworthiness, which is already a requirement, measures need to be taken to help ensure the availability of resources such as software licences, cloud services, maintenance services and replacement parts (e.g. network components) in the future.

In order to ensure that they are able to take swift action in the event of cyber security incidents, critical infrastructure operators should maintain close ties with the BSI's National IT Situation Centre. A sector-specific Computer Emergency Response Team (CERT) should therefore be set up for each critical infrastructure sector by the critical infrastructure operators.

We will also launch "Cyber Security Awareness and Cyber Resilience" projects developed in advance by the BSI for small and medium-sized enterprises (SMEs) which will be provided via service providers of the Alliance for Cyber Security. SMEs often form the backbone of the value chain and also act as service providers for many critical infrastructure operators. However, at the same time, cyber resilience is often not a priority for SMEs, as their core competence lies in operations, and cyber security aspects are generally viewed as cost drivers.

Objectives and measures for the 20th legislative period:

- Encouragement of SMEs involved in the critical infrastructure sector to invest in cyber resilience measures
- Establishment of Cyber Security Awareness and Cyber Resilience projects to be provided by the BSI and external service providers
- Provision for the security of IT supply chains as part of the legal regulation of critical infrastructures
- Verification of the establishment of sector-specific CERTs for critical infrastructure operators and establishment of close ties with the BSI's National IT Situation Centre

6. Protecting civil infrastructures from cyber attacks

In addition to companies involved in critical infrastructures, other civil digital infrastructures are becoming increasingly important. We already encourage information sharing, for example with more than 6,000 companies and institutions involved in the Alliance for Cyber Security. We are setting up a cooperative communications platform at the BSI to ensure that information regarding cyber attacks can be shared effectively and efficiently (BSI Information-Sharing Portal – BISP). This is designed to ensure, for example, that any loss or damage on account of ransomware is significantly reduced.

As a first step, we will pool the information currently provided by the BSI and associated institutions and make it available to a wider community of users, in particular SMEs, via a centralised platform, namely the BSI Information-Sharing Portal (BISP). As a second step, this platform should be expanded to form a civil cyber defence system (ZCAS) containing key "civil network defence" components designed to actively and automatically respond to cyber attacks.

Objectives and measures for the 20th legislative period:

- Creation of a BSI Information-Sharing Portal (BISP)
- Design and initial development of a civil cyber defence system (ZCAS)

7. Strengthening digital sovereignty in the cyber security field

Cyber threats are also changing as digitalisation gathers pace. We are confronted with new types of attacks on an almost daily basis. Cyber security standards, in particular of critical infrastructure companies, therefore need to be adapted, as part of a holistic approach, to new threat situations as digitalisation and connectivity evolve. The same applies for new and disruptive fields of technology such as automated driving, telemedicine and smart-city solutions. To this end, ensuring that untrustworthy manufacturers are not involved in the expansion of underlying infrastructures is of paramount importance.

We therefore need to step up our cyber security research efforts. We need to promote research, development and market access of cyber security-focused products and services as a whole, but in particular modern communication technologies for 5G/6G networks. The awarding of research contracts by the Agency for Innovation in Cyber Security (*Agentur für Innovation in der Cybersicherheit GmbH*) and the utilisation of the results obtained will also contribute to strengthening digital sovereignty.

Objectives and measures for the 20th legislative period:

- Stepping-up of German cyber security research efforts in order to increase resilience in the face of existential threats
- Promotion of digital sovereignty, in particular with regard to 5G/6G communication technologies
- Enhancement of the BSI's ability to assess the trustworthiness of manufacturers which provide "critical components" for critical infrastructure operators (e.g. in the energy, health care and finance sectors)
- Increased commissioning of innovative research projects on the basis of the security authorities' (predicted) applications and cyber defence

8. Creating resilient communication capabilities and enhancing network security

The successful implementation of the public administration's digitalisation projects will require a modern communications platform. Reliable and secure networks form the basis of any cooperation within the public administration. In the process, the network infrastructures must keep pace with innovation cycles and the public administration's increasing digitalisation needs. They will therefore need to be continuously enhanced not only from a technical point of view but also, and most importantly, from a strategic point of view with regard to national digital sovereignty.

The "Network Strategy 2030 for Public Administration" (*Netzstrategie 2030 für die öffentliche Verwaltung*) sets out a comprehensive programme for constructively pooling network modernisation requirements and for establishing an information network for public administration (*Informationsverbund der öffentlichen Verwaltung*) at the federal, state and local government levels.

Communication is the most important management tool available to public safety agencies and the Bundeswehr. There is an urgent need to provide users of the public safety digital radio with nationwide, secure and high-availability broadband data communication in addition to the TETRA radio. The modernisation of both the network infrastructure and the public safety digital radio will therefore provide a solid foundation for administrative modernisation.

Objectives and measures for the 20th legislative period:

- Modernisation of the wide area networks in accordance with the "Network Strategy 2030 for Public Administration"
- Centralised support for authorities when introducing IPv6
- Introduction of a centralised video-conferencing system for the federal administration
- Modernisation of the digital radio network for public safety agencies
- Creation of broadband communication in the digital radio network

Publication data

Published by

Federal Ministry of the Interior and Community, 11014 Berlin

Website: www.bmi.bund.de

Last updated

June 2022

Design by

KOMPAKTMEDIEN Agentur für Kommunikation GmbH

Torstraße 49, 10119 Berlin

Photo credits

Michael Traitov – stock.adobe.com

Article no. BMI22020