Federal Ministry
of the Interior, Building
and Community

Cyber Security Strategy for Germany 2021

Federal Ministry
of the Interior, Building
and Community

Publication data

Published by
Federal Ministry of the Interior, Building and Community

Contact information
Federal Ministry of the Interior, Building and Community
Alt-Moabit 140
10557 Berlin, Germany
Telephone: +49 (0)30 18 681-0
Email: CSS2021@bmi.bund.de

Last updated
August 2021

1 Contents

2 Executive summary

The Cyber Security Strategy for Germany 2021 creates a strategic framework for Federal Government policy on cyber security for the next five years, subject to the availability of budgetary funds.

The strategy begins with an assessment of the threat situation, which is currently marked by a considerable quantitative and qualitative increase in cyber attacks, an expansion in the potential scope for attacks, and a wealth of entirely new threat scenarios. In addition, the potential damage caused by cyber attacks is also increasing.

The strategy then looks at those institutions which contribute to providing cyber security in Germany. The cyber security landscape includes initiatives and stakeholders from civil society, the research community, the private sector, and government.

Following its analysis of the starting point, the 2021 Cyber Security Strategy sets out four cross-cutting guiding principles:

1. Establishing cyber security as a joint task for government, private industry, the research community and society.
2. Reinforcing the digital sovereignty of government, private industry, the research community and society.
3. Making digital transformation secure.
4. Setting measurable, transparent objectives.

These guiding principles touch on elements of all four of the following action areas of the Cyber Security Strategy. The strategic objectives within the action areas are based on the guiding principles, ensuring consistency and synthesis.

Action Area 1 – "Remaining safe and autonomous in a digital environment" – focuses on citizens and society. The ten strategic objectives of this action area are intended to enable citizens to make the most of the opportunities provided by digital technologies while remaining safe and autonomous in a digital environment. To achieve this, the strategic objectives aim to raise awareness among citizens, to improve cyber literacy, and to reinforce consumer protection in the digital world. The objectives also outline planned new regulations which will strengthen the framework for autonomous action.

Action Area 2 is "Government and private industry working together". The 13 strategic objectives in this action area aim to strengthen cyber security in private industry in general, but also focus on critical infrastructures. The action area also looks specifically at small and medium-sized enterprises. The objectives are intended to enhance the way in which government and industry work closely together on the basis of mutual trust, while also further developing the regulatory framework for the private sector. Objectives which promote emerging and key enabling technologies are also intended to foster the digital sovereignty and the competitiveness of companies in the cyber security field.

Action Area 3 – "Strong and sustainable cyber security architecture for every level of government" – focuses on government stakeholders involved in cyber security and looks at necessary developments in this field. The objectives in Action Area 3 come into three categories: 1. Cooperation between and distribution of competences among the relevant authorities. 2. Enhancement of skills and powers within the authorities. 3. New challenges facing state actors in cyberspace. The 14 strategic objectives of this action area aim in particular to reduce barriers to effective cooperation among the authorities and to highlight the constantly evolving challenges associated with cyberspace; the authorities must have the skills and powers necessary to overcome these challenges.

Providing high levels of cyber security in Germany is contingent on Germany's active role in European and international cyber security policy. This is addressed in Action Area 4, which has a total of 7 strategic objectives. Germany's participation in the European Union (EU) and the North Atlantic Treaty Organization (NATO) is key. While matters relating to harmonising regulations within Community law appear in every action area, the objectives of this action area focus on enhancing the foundations and instruments of cyber security policy within these organisations. In addition, the action area aims to strengthen international law in cyberspace for states and to step up the international fight against cyber crime. Action Area 4 also promotes bilateral cooperation and confidence-building measures.

The Cyber Security Strategy concludes by outlining a transparent method for its implementation, reporting and strategic controlling. Effective implementation is to be continually tracked and reviewed and systematic preparation is put in place for future evaluations.

3 Introduction

We live in an age that is defined by the new opportunities of the digital world. Technologies like artificial intelligence (AI), connected electronic devices and new, innovative means of communication are changing everything. Many of our everyday tasks, whether in our private lives, our professional lives or when dealing with the authorities, are simplified and speeded up by the use of new technologies. Growing numbers of processes take place virtually. The COVID-19 pandemic gave this trend a further boost.

But these new opportunities can also cause the risks we face in cyberspace to multiply or change. If we want to benefit in full from the opportunities, advantages and necessities that digital transformation brings with it, we must protect ourselves from these risks. Government has an obligation to work with private industry, the research community and civil society to assess this rapid technological development and to guide and influence its progress in the public interest, making sure that the general conditions are in place for high levels of protection and security in cyberspace.

Individuals must be able to use these technologies safely and autonomously at all times. We cannot view cyber and information security simply as a necessary inconvenience – it is our guarantee that the digital transformation will be a success in the long term.

The Federal Government's Cyber Security Strategies for Germany adopted in 2011[1] and 2016[2] provided important outlines for forward-looking cyber security policy.

For example, the strategies laid the foundations for the National Cyber Security Council (NCSR), the National Cyber Response Centre (Cyber-AZ) and the Central Office for Information Technology in the Security Sector (ZITiS). The strategies initiated work towards objectives such as "Promoting digital literacy among all users", "Securing critical infrastructures", "Intensifying law enforcement in cyberspace" and "Shaping international cyber security".

The 2021 Cyber Security Strategy takes up where the earlier strategies left off. The guiding principles, measures and objectives it sets out provide the basis for Germany's security in cyberspace in the coming years.

Cyber and information security is important for government, private industry, the research community and society in equal measure. The strategy is therefore aimed at and seeks to involve all stakeholders.

Cyber security is a task for the present, but it is also one of our most important tasks for the future. The 2021 strategy therefore prioritises emerging and key enabling technologies.

---

[1] Available at: https://www.cio.bund.de/Web/DE/Strategische-Themen/IT-und-Cybersicherheit/Cyber-Sicherheitsstrategie-fuer-Deutschland/cyber_sicherheitsstrategie_node.html

[2] Available at: https://www.bmi.bund.de/cybersicherheitsstrategie/

The German economy will have to move increasingly into cyberspace in the future. Transformation processes are already under way, as evidenced by Industry 4.0 and the Work 4.0 dialogue, and these processes must be safeguarded in the long term by cyber and information security. To achieve this, the strategy continues to encourage government and industry to work closely together, fostering cooperation through more in-depth dialogue, improved protection and the promotion of secure products and services.

The state must also examine and upgrade government cyber security architecture to ensure it can keep pace.

The Federal Government additionally intends to expand its involvement at European and international level, with a stronger focus on cooperating and coordinating action with its partners.

Alongside this development of topic areas, changes have also been made to the structure of the Cyber Security Strategy. A comprehensive evaluation was carried out in conjunction with the federal ministries and the authorities in their remits; the federal states; and representatives of private industry and civil society. This evaluation found that the four action areas, “Remaining safe and autonomous in a digital environment”, “Government and private industry working together”, “Strong and sustainable cyber security architecture for every level of government” and “Germany’s active role in European and international cyber security policy” had proved useful and remained relevant. The action areas apply across disciplines and have a bearing on every area of society, encompassing all of the necessary measures. At the same time, multidisciplinary issues were identified which must be addressed across all action areas, such as digital sovereignty. This updated Cyber Security Strategy defines guiding principles which run through the strategy, ensuring synthesis among the individual strategic objectives and measures.

Another change since the last Cyber Security Strategy is that the strategy’s implementation is to be continually tracked and reviewed. To facilitate this, the strategy includes specific indicators for each of the strategic objectives. This will allow transparent monitoring of the strategy’s success.

4 Objectives of the 2021 Cyber Security Strategy

The Cyber Security Strategy for Germany 2021 replaces the Cyber Security Strategy for Germany 2016. It provides the strategic interministerial framework for Federal Government action on cyber security over the next five years. The strategy builds on the tried and tested aspects of the strategies of 2011 and 2016, while also incorporating new priority areas.

The strategy sets forth the essential long-term direction of the Federal Government's cyber security policy, broken down with the help of guiding principles, action areas and strategic objectives. It seeks to actively shape policy and aims to facilitate the target-oriented, coordinated involvement of all stakeholders. The Cyber Security Strategy for Germany and the cyber security strategies of the federal states are complementary to each other, fostering closer cooperation within the federal system. As part of the EU's Cybersecurity Strategy for the Digital Decade,[3] the Cyber Security Strategy for Germany also helps shape Europe's digital future.

The governance framework in line with the NIS Directive[4] is part of the strategy. As set forth in the Directive, the strategic objectives reflect the Federal Government's priorities. In addition, section 6, "The cyber security landscape in Germany", lists the actors in the cyber security landscape.

The Cyber Security Strategy

- sets out the framework for Federal Government cyber security activities;
- creates transparency and comprehensibility for all stakeholders in government, private industry, the research community and society;
- facilitates the active, target-oriented involvement of all these stakeholders;
- takes into account EU specifications;
- enshrines reporting and controlling at the strategic level; and
- systematically prepares for future evaluations and the ongoing refinement of the strategy.

Implementation of the objectives of the Cyber Security Strategy is subject to the availability of allocated budgetary resources. The principles of economy and efficiency (see section 7 of the German Federal Budget Code) also apply to the EU budget, when resources come from this source.

Cyber and information security is closely related to numerous other fields, and in some cases overlaps with them. The Federal Government has published its own strategies for some of these issues. Where this is the case, these strategies are referenced in the Cyber Security Strategy with a brief explanation, to help with general understanding.

---

[3] Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020JC0018

[4] According to the NIS Directive, member states must create a governance framework in their strategy (see Art. 7 (1) (b) of Directive (EU) 2016/1148) which must address (i) how to achieve the objectives and priorities of the national strategy and (ii) which government or private bodies are responsible for attaining these objectives and priorities. The Directive is available at: https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:32016L1148

The matters of hybrid threats and data protection have particularly large areas of overlap with cyber and information security and must therefore always be taken into account. Section 5, "The cyber threat situation", zooms in on the topic of hybrid threats.

The overlap between data protection and cyber and information security is evidenced by the fact that numerous data protection objectives are also important for cyber and information security. Since 2018, the General Data Protection Regulation[5] and the Directive on data protection for police and criminal justice authorities[6] have been the central data protection regulations at European level, with the Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG)[7], serving the same function at national level. The objectives of data protection regulations and of cyber and information security are largely consistent and in some cases identical (for example, the objectives of integrity and confidentiality). However, in certain cases there is tension between individual objectives. One example would be that data protection regulation calls for data minimisation, whereas logging access to data is relevant for information security. In such cases, a solution must be found that allows the different interests to be balanced as effectively as possible.

[5] Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679

[6] Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0680

[7] Available at: http://www.gesetze-im-internet.de/bdsg_2018/

5 The cyber threat situation

Information technology (IT) has become an integral part of life in our society today. There are very few technical products that do not include IT components. Early in the 21st century, process automation using IT was at the cutting edge. Today's IT systems create value in particular as part of connected devices and through their use of "intelligent" algorithms.

However, connected IT systems are much more vulnerable to attacks, particularly because they are generally accessible from anywhere in the world using the internet. At the same time, the growing complexity of IT systems and algorithms increasingly leads to unintended behaviour by and security gaps in systems, known as vulnerabilities. Attackers exploit the global accessibility of systems together with these vulnerabilities to carry out criminal acts.

The aim of ensuring and improving the security of IT systems conflicts with the market-driven, dynamic ongoing development of IT. The race to market means vulnerabilities still occur regularly. In addition, specifications and established standards for the secure operation of IT systems are not always implemented as they should be. Manufacturers have a particular responsibility in this regard, but user, operator and administrator behaviour is also key for secure IT systems. Cyber attacks can only be reliably detected and their consequences successfully prevented or minimised if all those involved cooperate effectively.

It is the role of government to create suitable framework conditions for secure IT systems. Advisory services provided by the Federal Office for Information Security (BSI), government-funded research, and prevention measures by a range of security authorities ensure that minimum standards for providing IT security are created and met, that cyber attacks are detected and resolved, and that perpetrators are investigated and prosecuted by law enforcement authorities. The international nature of such crimes means that this last step is often particularly challenging.

Despite major efforts to provide cyber security, we are facing a considerable increase in the number of cyber attacks. We can see a growing mix of "classic" cyber attacks as defined in this strategy with other areas of criminal activity such as blackmail, spreading false information, fraud and insults. The methods used by perpetrators are increasingly sophisticated. It has become the norm for cyber attacks and malware to be the work of extremely specialised individuals. This can only be combated effectively if all cyber security measures are regularly reviewed and adapted. This strategy is one of the building blocks in achieving this.

Germany is committed to a free, open, safe global internet, where constitutional rights are protected. Cyber security is also a building block in safeguarding these values.

5.1 Attack vectors – what are the gateways which allow attacks?

IT systems that are not secure, whether because of their hardware or their software, are a central gateway for cyber attacks. The larger and more complex software projects become, and the more people who are involved in their programming, the more often there are errors in the software which can be exploited as vulnerabilities by attackers. Many manufacturers do now provide regular or ad hoc updates (patches) to fix vulnerabilities, but not all vulnerabilities can be overcome

this way. In addition, the sheer number of vulnerabilities makes clear the need to improve quality assurance processes so that the quantity of vulnerabilities can at least be reduced before software is released.

Other causes of security problems in IT systems are incorrect configuration, a lack of protection mechanisms, and incorrect operation by users. These factors also enable unauthorised third parties to gain entry to systems and to compromise them.

In addition, the Internet of Things (IoT) means a rapidly growing number of devices have internet connections. Connecting devices such as speakers, refrigerators, doorbells, lifts, machine tools and medical devices increases the potential for cyber attacks. This is all the more problematic because many IoT devices have very low levels of cyber security. The fast-moving nature of this market often leads to poor-quality software with major security flaws. Coupled with this, patches are often not available for a sufficient period of time or at all, or are released with considerable delays. In some cases, they may lack the necessary functions or interfaces to enable them to be installed at all.

Exploiting the majority of vulnerabilities generally requires active cooperation on the part of the user. Attacks through vulnerabilities sometimes also make use of users' lack of information. A brief click on an insecure, faulty link, installing software from unknown sources or thoughtlessly opening an email attachment are typical everyday scenarios that can compromise an IT-based device. Even a high level of cyber security is therefore unlikely to help without greater awareness among users.

There is also a growing trend for supply chain attacks. In these cases, attackers modify software or hardware during the manufacturing or maintenance process. The attacker's work is then delivered by the actual manufacturer along with the product. For example, in December 2020 it came to light that attackers had manipulated an update provided by a software manufacturer. The update was installed automatically. Users often trust update mechanisms, which means that many systems can often be affected by a single attack. This type of attack poses a particular risk. Manipulated software of this kind is often installed or operated with administrator rights and is therefore not detected by protection mechanisms like virus scanners. Customers and consumers are frequently completely unsuspecting and therefore defenceless.

Hardware vulnerabilities that are created deliberately make it particularly clear that cyber security is also a matter of digital sovereignty, as a domestic manufacturing process can be better supervised and regulated. Dependence on systems where it is not possible to monitor trustworthiness opens up opportunities for cyber threat actors.

There is no doubt that technologies such as AI and quantum computing offer huge potential. But this comes along with new risks. For example, AI-based processes often hinge on training the systems involved. Their behaviour is not always fully comprehensible. This means that the skilled selection of input models or training data by potential attackers could compromise the integrity of these algorithms. Clever manipulation of traffic signs has led to false results in traffic-sign recognition systems, for example. Further research is needed and new technologies must be developed to help counter risks in new information technologies.

5.2 Threats – what are the new trends in cyber attacks?

The widespread integration of IT into life in our society has brought a whole spectrum of new threats with it. Online media provision creates new opportunities to manipulate public opinion. The fact that social media can be used both easily and anonymously has resulted, among other things, in higher volumes of fake news and hate speech. Online dissemination of illegal content such as child sexual abuse images and copyrighted materials continues to increase, aided in particular by the use of anonymisation and encryption services.

However, this strategy does not focus on phishing crimes or on threat situations in which IT is used to disseminate illegal content. Instead, it focuses on cyber attacks that directly and substantially compromise the availability, integrity and confidentiality of IT systems. This frequently includes data protection violations to collect personal data. Cyber attacks can also be used as a part of hybrid threats. In addition, cyber attacks are a typical element of cyber crime, cyber terrorism, cyber espionage and cyber sabotage, all of which can target critical infrastructures in ways that can cause considerable financial and social impact.

5.2.1 Cyber crime

In the field of cyber crime, the use of ransomware to prevent access to data or systems is currently one of the greatest threats. Perpetrators attack wherever they find unprotected vulnerabilities, regardless of whether these involve companies, government agencies or private users. The cyber attack itself is followed by attempts to blackmail the victim, with threats ranging from publishing customer data online to revealing sensitive information to competitors. Ransomware has developed to a point where it can cause considerable damage, particularly because those affected are often part of global networks. This means that whole divisions of companies, or entire infrastructure areas, can be affected by outages caused by this type of attack. The danger posed by what is known as “big game hunting” should also be taken seriously. In this type of attack, perpetrators target particularly wealthy or potentially lucrative victims so they can demand very high ransoms.

Distributed denial-of-service (DDoS) attacks generally lead to IT systems overloading with network traffic, and are also often threatened as part of blackmail attacks. Attacks of this type often use botnets. In a botnet attack, perpetrators hijack several IT systems which they then control remotely, or they misappropriate publicly accessible systems which may be configured wrongly or in some cases cannot be secured, in order to overload the system they are targeting. The malware used for this type of attack has developed considerably over the years, often enabling perpetrators not just to carry out DDoS attacks, but at the same time to access the data in the bots, which means they can then collect victims’ personal data. This is a typical gateway for obtaining access data. Another sphere of activity for DDoS attacks is unwelcome online content. This can be used to obstruct political party events, for example. The potential motives for attacks like this, such as hacktivism or government influence, are becoming increasingly blurry.

5.2.2 State-sponsored cyber attacks

Government and non-government organisations and private companies alike are increasingly faced with strategic activity on the part of cyber threat actors carrying out state-sponsored cyber attacks such as cyber espionage and cyber sabotage. The threat actors most commonly active in this field, known as advanced persistent threat (APT) groups, are characterised by their access to sometimes substantial resources, their tenacity, and their comprehensive technical expertise.

Their activities are therefore often ascribed to intelligence services or groups acting on behalf of intelligence services.

These groups use complex long-term strategies to try and infiltrate IT systems undetected. As well as the use of these intrusions for cyber espionage purposes such as stealing sensitive information, an increase has recently been observed in activities to lay the groundwork for cyber sabotage, known as pre-positioning. As more and more state governments are developing their cyber expertise, it is likely that cyber attacks by APT groups will remain a major threat for the foreseeable future. In some cases, a developing symbiosis is visible between threat actors in the areas of cyber crime and cyber espionage/cyber sabotage. Military actors are also working continually on expanding their cyber capabilities. This means that any assessment of the cyber threat situation must also take into account the military component.

5.2.3 Cyber attacks as a component of hybrid threats

The term hybrid threat means targeted activity by government actors and their non-government upstream entities (proxies) and can encompass a broad range of concealed and open means of carrying out this activity. This means that attacks in cyberspace can affect broader areas (for example the information domain), can take place in conjunction with activities in other areas, or can serve as preparation for other activities with the aim of exerting illicit influence.

There is a close relationship between cyberspace and the information domain, given that the information domain is increasingly based on information technology and is characterised by high levels of connectivity. One example of attacks resulting from hybrid threats are cyber espionage attacks which illegally obtain sensitive information from IT systems and then disseminate this information to manipulative ends, causing damages in the information domain by discrediting the victim or spreading disinformation.

Cyber sabotage can also aim to cause damages in other areas, such as private industry, and can focus on critical infrastructures, subsequently exploiting the effects of these damages in the information domain for the purpose of manipulation. Critical infrastructures are essential for the provision of basic services. Outages of critical infrastructures can have a very destabilising effect, which makes them a potential goal for attackers. This type of infrastructure therefore needs a high level of protection. The methods used in hybrid threat situations often make it relatively easy for the perpetrators to conceal or deny their responsibility and their motives for carrying out such attacks. One example of this would be the cyber attack carried out in 2017 with a sabotage tool in the guise of ransomware (NotPetya), which is presumed to have been carried out by or on behalf of a government.

Propaganda and disinformation can be particularly dangerous if they are disseminated as a result of cyber attacks on credible platforms. Media companies' online outlets therefore need extensive protection against cyber attacks.

Cyber attacks as a component of hybrid threats are for the time being no different in technical terms from other cyber attacks provided for in this strategy. The general use of digital media to spread disinformation or for other illicit purposes is, on the other hand, not a cyber security matter.

5.3 Which assets are at risk?

Given that IT is part of almost every area of our lives, cyber attacks can affect every area of life. An IT outage resulting from a cyber attack could lead to supply shortages, for example. Data are an

increasingly valuable asset, for instance when sensitive financial or health data are accessed as a result of cyber attacks so that they can then be used for blackmail or sold on the darknet. The scope and variety of online information portals allow false information to be disseminated from seemingly legitimate sources. This can cause considerable uncertainty among the general public. Ultimately, cyber attacks can affect central assets and values in our society, such as security, prosperity, autonomy and democracy.

Whether we look at communication with family and friends, online shopping and banking, the use of government services or the democratic opinion-forming process, digital technology is intrinsic to our everyday lives. Cyber attacks that aim to steal data or identities or to disseminate disinformation therefore affect users' ability to remain safe and autonomous in cyberspace.

Germany's industry depends to a great extent on functional, reliable IT infrastructure of which the integrity is guaranteed. The complex supply links and supply chains which characterise global production mean that cyber attacks on companies both in Germany and around the world can have a far-reaching domino effect with massive financial consequences. Digital economic espionage is both a direct threat to the business success of our companies and also an indirect threat to the competitiveness and stability of our whole economy.

Critical infrastructures like electricity and telecommunication networks, networks of hospitals and financial systems are essential to the functioning of private, economic and public life and are increasingly dependent on IT infrastructure with guaranteed integrity operating without disruption. Disruption or outages caused by IT security incidents can lead to supply-chain bottlenecks with long-term effects and can have a considerable impact on public security and order, or other extremely serious consequences.

The growing level of digital technology used in public administration means that alongside the danger posed to sensitive data by espionage, cyber attacks on state institutions constitute a fundamental threat to the functionality and integrity of government service provision. Attacks on parliamentary systems are attacks on the democratic formation of political will and the free democratic basic order.

5.4 The bottom line

It is hard to say whether the threat situation in cyberspace has objectively worsened, or if the threat has only increased in proportion to the growing importance of IT in every area of life. However, the increasingly all-pervasive nature of IT, combined with the speed of the market, a lack of standards, and in some cases poor design, has increased the risk of cyber attacks causing large-scale damage or disruption, the effects of which could be further reaching than simply the IT systems themselves. This has to be prevented. The number of cyber attacks recorded has increased continually in recent years.

New technologies are regularly accompanied by new risks. The more often these technologies are used, the more the danger of cyber attacks increases. Cyber security provision must therefore be just as dynamic as the development of the IT it seeks to protect.

Constant vigilance and appropriate adjustments to cyber security measures are an important element of solving the problem. At the same time, security must be incorporated at the design stage when developing and using new technology. This strategy is a building block for achieving this. Another important pillar of cyber security provision is a combination of awareness-raising among users and knowledge exchange in regard to cyber threats. When these are considered

alongside the proven excellent work of our security authorities, including in cyberspace, Germany is in a good position to respond to the constantly evolving cyber threat situation.

6 The cyber security landscape in Germany

Providing cyber security in Germany is a task for society as a whole. A broad range of stakeholders from government, private industry, the research community and wider society play an essential part in this. But every single member of society is in some way responsible for cyber security. A comprehensive list of key stakeholders can be found in the online cyber security compendium for Germany (*Online-Kompendium Cybersicherheit in Deutschland*), which is regularly updated.[8]

The stakeholders and initiatives involved in providing cyber security in Germany generally come into the following categories, although they often work together on an interdisciplinary basis:

1. Civil society initiatives and stakeholders
2. Research community initiatives and stakeholders
3. Private industry initiatives and stakeholders
4. Government initiatives and stakeholders

6.1 Civil society initiatives and stakeholders

The majority of civil society stakeholders active in the field of cyber security in Germany are associations and foundations. Numerous independent voluntary experts also play a part. The work of these stakeholders includes compiling political analyses and recommendations for action, raising awareness among the general public of cyber security issues, providing training in media literacy and technology, and serving as a network among different groups within society. The breadth of different civil society initiatives and actors involved means tailored options can be offered to a wide range of different target groups.

6.2 Research community initiatives and stakeholders

The research community makes a key contribution to improving cyber security in Germany in particular through basic research and applied theoretical, experimental and industrial research. The resulting findings and innovation in the form of analyses, recommendations for action, training content and technologies are a vital basis for specific use cases in government, industry and society.

6.3 Private industry initiatives and stakeholders

Stakeholders and initiatives in private industry are involved in many different facets of cyber security, including developing innovative technical solutions, contributing to advancing development of standards and norms that have a bearing on cyber security, and creating topic-specific working groups as a driving force for networking and skills development. Cyber security can be a key factor in the competitiveness and choice of location for private industry stakeholders.

---

[8] Available in German at: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/online-kompendium-nationaler-pakt-cybersicherheit.pdf?__blob=publicationFile&v=4

Networks such as the Alliance for Cybersecurity, the UP KRITIS public-private partnership and the Economic Security Initiative therefore help raise Germany's profile as an attractive location for business.

6.4 Government initiatives and stakeholders

It is the state's responsibility to play a leading role in ensuring high levels of cyber security. Government tasks in this regard range from drawing up threat situation reports, preventing, detecting and defending against threats, managing incidents when they occur, and carrying out law enforcement activities, through defending against espionage and gathering intelligence for prevention purposes, to cyber defence and international cyber policy. Numerous stakeholders at federal and state level are therefore closely involved in responding to threats from cyberspace on the basis of their respective competences. Federal Government activities are divided between the strategic and the operational level.

6.4.1 Strategic level

The different ministries are responsible for the strategic orientation of their cyber security policy and monitoring its implementation. The ministries are responsible for managing the activities in their remits independently, based on the principle of ministerial autonomy. At federal level, the Federal Ministry of the Interior, Building and Community is responsible for coordinating domestic cyber security policy and the Federal Foreign Office is responsible for coordinating international cyber security policy. The Federal Ministry of Defence is responsible for cyber defence.

The NCSR is the Federal Government's strategic advisory body. It was created on the basis of the Cyber Security Strategy for Germany 2011 and was further developed in the Cyber Security Strategy for Germany 2016. Consisting as it does of representatives from federal, state and local governments and from private industry, the NCSR serves as the fulcrum for the relevant stakeholders in the German cyber security landscape. A permanent scientific working group was set up in 2018 to advise the NCSR from a research perspective on the developments and challenges associated with secure, reliable digital transformation.

Responsibility for the strategic orientation of federal IT security management and the implementation of the cabinet decision on the guideline for information security in the public administration (UP Bund) lies with the CIO Council and its working group on information security. The office of Federal Government Commissioner for Information Technology is within the Federal Ministry of the Interior, Building and Community. Among other things, the Commissioner is responsible for steering information security management on the basis of the UP Bund guideline for information security.

6.4.2 Operational level

The strategic guidelines and objectives are implemented at operational level primarily by the subordinate authorities of the Federal Chancellery and of the ministries. The following task areas and stakeholders are especially important in this context.

The BSI is the central federal cyber security authority. The Federal Security Operations Centre (BSOC), the Computer Emergency Response Team for federal agencies (CERT-Bund) and the National IT Situation Centre come under the auspices of the BSI. In specific cases, the National IT Situation Centre becomes a national crisis response centre. The BSI is additionally responsible for the security and protection of the Federation's network and its information technology, and it influences information security for digital transformation by providing testing, standardisation, certification, authorisation and advisory services for government, industry and society, working closely with stakeholders from all relevant areas.

The Federal Office for the Protection of the Constitution (BfV) is responsible for upholding internal security. It reports to the Federal Government and the public on the security situation. It is responsible for collating and evaluating information on cyber attacks that have extremist or terrorist motivation or that are initiated by foreign intelligence services. The Military Counterintelligence Service (MAD) protects the Bundeswehr from espionage and sabotage and from extremism and terrorism in cyberspace in every situation, including during deployment, not just in defensive cases or states of tension. The Federal Intelligence Service (BND) is tasked with collating and evaluating the information required to gain intelligence that is relevant to German foreign and security policy, including 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 threat prevention. The Federation 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. This jurisdiction extends to the cyber domain. The tasks associated with this special jurisdiction 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 the state criminal police offices and police authorities and from the BKA and the BPOL as 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, which was established in 2011 as the central information and coordination platform for such matters and which has been further developed since.

The Central Office for Information Technology in the Security Sector (ZITiS) is mainly a service provider for the security authorities within the remit of the Federal Ministry of the Interior, Building and Community, aiming to strengthen their cyber capabilities and digital sovereignty.

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 operator of Germany's IT abroad.

6.4.3 Cooperation between the Federation and the states

The broad range of government tasks required in cyberspace can only be carried out with a joint effort by the Federation and the states. Activities at federal and state level must be closely interlinked with the aim of ensuring cooperation and complementary efforts.

The Standing Conference of the Interior Ministers of the Länder in the Federal Republic of Germany, with its cyber security working group at state level, and the IT Planning Council, with its information security working group, are the key committees for coordinating cooperation between federal and state level. The IT Planning Council and its working group are also responsible for information security management between federal and state level.

There are also numerous formats for cooperation between the Federation and the states at operational level. A small selection of examples would be the trusting cooperation between the federal and state intelligence authorities within the community of the German domestic civil intelligence services, the in-depth dialogue that takes place in the Federal Administration CERT Group (VCV), and the close coordination between state criminal police offices and the BKA as the hub for police information and intelligence services and for the criminal police. A growing number of states have set up their own central cyber security coordination offices, and these are also closely involved in this cooperation at operational level. The BSI's national liaison division forges relationships between the BSI and national partners and serves as the point of contact at regional level for the states.

7 Guiding principles of the Cyber Security Strategy

The strategic objectives and operational measures which are set forth for the first time in the Cyber Security Strategy for Germany 2021 are considered, reviewed and implemented on the basis of guiding principles. The guiding principles are derived from interests and concerns that span all of the action areas. Their purpose is to consolidate and focus the issues covered, ensuring synthesis among the individual strategic objectives and measures.

7.1 Guiding principle: Establishing cyber security as a joint task for government, private industry, the research community and society

Cyber threats and cyber crime do not just affect the state; they also affect companies, research institutions, associations and the general public. To provide a high level of security in this context, all stakeholders must contribute to overcoming cyber threats. The Federal Government therefore considers cyber security a joint task for government, private industry, the research community and society as a whole. This calls for a cooperative approach in a spirit of trust, so that all those involved can work together to find answers to cyber threats.

Threats in cyberspace do not stop at national borders. As in many other areas, in the field of cyber security Germany is part of a European and international cooperation network. This means that cyber security is only possible if we work together with our European and international partners.

7.2 Guiding principle: Reinforcing the digital sovereignty of government, private industry, the research community and society

The topic of digital sovereignty has grown considerably more visible and more relevant since 2016. Digital sovereignty is defined in this strategy (from the perspective of the Federal Government) as "the capabilities and options of individuals and institutions to exercise their role(s) in the digital world independently, autonomously and safely".[9] This means that digital sovereignty is also an intrinsic part of cyber and information security – secure technologies and solutions, alongside the ability to recognise and assess the opportunities and potential risks associated with digital technologies, are a key requirement for digital sovereignty. In this way, a high level of cyber security helps enhance the digital sovereignty of citizens, private industry, government and the research community. At European level, digital sovereignty requires closer networking with strategically important partners on business and security policy matters to minimise dependency and safeguard the ability to plan and take political action.

Digital sovereignty is therefore a central guiding principle of the 2021 Cyber Security Strategy, and is a reason for action in each of the four action areas. The focus areas include

- applied research and development and the transfer of research (Action Area 1),

[9] See the strategy for improving digital sovereignty in public administration IT (*Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung*), available in German at: https://www.it-planungsrat.de/beschluesse/beschluss/ag-cloud-computing-und-digitale-souveraenitaet

- cyber security "made in Germany" as a quality label (Action Area 2),
- government capabilities for assessing new technologies, commissioning European providers and ensuring the self-protection of the public administration (Action Area 3),
- a common EU vision and strategy for cyber security and European digital sovereignty (Action Area 4).

A closer look reveals that, depending on stakeholder and context, the focus falls on different aspects and dimensions of digital sovereignty. This shows that the topic of digital sovereignty is extremely broad and complex. It is therefore dealt with differently in each action area.

Federal Government initiatives and concerns

The aim of the new Strategy Paper of the Federal Government on Strengthening the Security and Defence Industry,[10] which was adopted on 12 February 2020, is to maintain and promote key industrial competences and strategically relevant development capacity in Germany and the EU. The strategy paper provides the framework for Federal Government policy in regard to the security and defence industry, which makes it a key guiding principle for the protection of digital sovereignty. The Federal Government has already listed relevant measures in five areas in this regard:

- strengthening research, development and innovation,
- creating the basic conditions for efficient production,
- optimising the procurement system,
- providing political support for and responsible control of exports, and
- protecting security interests.

In regard to protecting security interests, digital sovereignty and resilience in the face of hybrid threats is to be achieved and dependence on foreign information technologies is to be reduced. Alongside the verification methods of the Foreign Trade and Payments Act (*Außenwirtschaftsgesetz*, AWG) and the Foreign Trade and Payments Ordinance (*Außenwirtschaftsverordnung*, AWV), the Federal Government is working on flexible instruments that can be employed strategically as needed to respond to the risk of selling off future key enabling technologies in security and defence. As part of this, progress is to be made on establishing an IT security fund to actively counteract unwanted takeovers.

In the area of strengthening research, development and innovation, the Agentur für Innovation in der Cybersicherheit GmbH (Agency for Innovation in Cybersecurity), which was set up in summer 2020, plans to commission and fund ambitious research projects with considerable potential for innovation in the field of cyber security and associated key enabling technologies, with the aim of meeting Germany's domestic and foreign security needs.

The Federal Government has also launched the "StartUpSecure" initiative, to enable the quicker implementation of ideas in IT security with market potential. The initiative provides funding

[10] Available at: https://www.bmwi.de/Redaktion/DE/Artikel/Branchenfokus/Industrie/branchenfokus-sicherheits-und-verteidigungsindustrie.html

for starting new businesses in the IT security branch. Business incubators have been set up at the national centres of excellence for IT security research ATHENE (Darmstadt), CISPA (Saarbrücken) and KASTEL (Karlsruhe), and at Ruhr University Bochum, to support the newly founded businesses.

In the field of research into the cutting-edge topic of 6G, the Federal Government has stated that its aim is for Germany to become a leading supplier in the global market of trustworthy communication technology, and to play a key role in shaping technological change from the outset. As a first step, the Federation has established four 6G research hubs and a platform for future communication technologies and 6G.

In regard to the public administration, in March 2021 the IT Planning Council adopted its strategy for improving digital sovereignty in public administration IT. As well as the strategic objectives "option to switch providers", "ability to plan" and "influence on providers", the strategy also includes a range of potential solutions and measures aimed at strengthening digital sovereignty in the public administration. These include putting in place the necessary legal framework and building skills and expertise, and also diversifying through needs-based open-source IT solutions.

As part of the QuNET[11] initiative, which is funded by the Federal Government, since late 2019 the Fraunhofer-Gesellschaft, the Max Planck Society and the German Aerospace Center have been developing technology for a pilot network for quantum communication in Germany. The aim of this network is to allow data transmission that is safe from eavesdropping and manipulation.

7.3 Guiding principle: Making digital transformation secure

Since 2016, the digital transformation of government (e.g. the E-Government Act (*E-Government-Gesetz*, EGovG), the Online Access Act (Onlinezugangsgesetz, OZG), IT consolidation, mobile work, etc.), industry (e.g. security requirements for 5G networks) and society (e.g. electronic ID) has gained significant momentum. In addition, the COVID-19 pandemic meant that 2020 saw the demands and expectations surrounding digital products and services skyrocket.

Cyber and information security is a basic requirement if the digital transformation is to succeed in Germany. If digitalisation is not secure, then free and autonomous navigation in a digital environment will not be possible. A high level of cyber security, on the other hand, allows us to fully exploit the potential of the digital age and to approach risks confidently and autonomously. For this reason, the 2021 Cyber Security Strategy features the topic "Making digital transformation secure" as a guiding principle and addresses it in the strategic objectives across all action areas.

Federal Government initiatives and concerns

[11] Available in German at: https://www.qunet-initiative.de/

The Federal Government has advanced a range of initiatives and measures aiming to guide the digital transformation in Germany. The current implementation strategy, Shaping Digitalization,[12] outlines several key policy objectives for shaping the digital transformation, including in the areas of digital competence, infrastructure, the digital transformation of government and society, and ethics in a digital society.

For example:

- the cyber cluster at the Universität der Bundeswehr München in Munich not only carries out research in the CODE Research Institute, but also provides basic, advanced and further training for officers and Federal Government employees, with a focus on cyber security.
- The Federal Government has launched a new research framework programme on IT security, *Digital. Sicher. Souverän.*
- The Agency for Innovation in Cybersecurity was founded to make interministerial research projects with considerable potential for innovation in the field of cyber security and associated key enabling technologies possible, with the aim of meeting Germany's domestic and foreign security needs.

The network strategy 2030 for the public administration (*Netzstrategie 2030 für die öffentliche Verwaltung*)[13] reworked and built on the Federal Government's network strategy from 2013. This new strategy responds to the growing demands regarding the ability to communicate of Germany's public administration as a whole, new technical developments, and increased security requirements. The aim is to establish an information network for Germany's public administration (IVÖV) which would be operated by the federal network operator (BDBOS). The following strategic objectives were defined:

- national digital sovereignty,
- a high-performance network infrastructure,
- information security, data protection and security of classified material,
- future-readiness and flexibility, and
- digital cooperation based on a whole-of-government approach.

The following action areas were drawn up to implement these strategic objectives, and a catalogue for implementation was compiled:

- strategic configuration of the vertical range of manufacture,
- further development of active vendor management,
- consolidation of wide area networks,
- internet resources and standardisation,

[12] Available at: https://www.bundesregierung.de/breg-de/service/publikationen/digitalisierung-gestalten-1605002

[13] Available in German at: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/Moderne-Verwaltungskommunikation/netzstrategie_2030_fuer_die_oeffentliche_verwaltung.html?nn=4624892

- provision of information security, data protection, and security of classified material in the public administration's network infrastructure,
- advancement of requirements management, user management and service development, and
- promotion of innovations and key enabling technologies for a citizen-focused, modern public administration.

The network strategy 2030 for the public administration is therefore an important building block for Germany's cyber security.

7.4 Guiding principle: Setting measurable, transparent objectives

Government activity must be transparent if citizens are to trust the state. The benefits and impact of government initiatives must therefore be comprehensible to everyone. The 2021 Cyber Security Strategy therefore addresses the issue of making objectives transparent and measurable for the first time, enabling systematic preparation for implementation and future updates.

To assess the success of the 2021 Cyber Security Strategy, target achievement will be measured on an ongoing basis throughout the term of the strategy and finally when the strategy ends. To make this possible, the objectives in each action area have been formulated to be measurable. Indicators are given for each strategic objective so that its achievement can be assessed.

The 2021 Cyber Security Strategy differentiates between strategic objectives and operational measures:

Strategic objectives

The strategic objectives are SMART (specific, measurable, actionable, realistic and time-bound) objectives within an action area that are to be achieved as part of the implementation of the Cyber Security Strategy. They address the challenges in the action area and outline the state of affairs which is to be reached by implementing the strategy. Strategic objectives are formulated in a way that is specific and concrete, so that they are verifiable. In addition, indicators are defined for each strategic objective so that its achievement can be measured. Generally, it should be possible to attain the strategic objectives in a period of five years.

Measures

Measures are the means by which the strategic objectives are to be achieved. Together, the measures must enable each strategic objective to be attained in full within the term of the 2021 Cyber Security Strategy. They can consist of individual projects or ongoing measures. The measures are not part of the strategy; they are planned and implemented subsequently as ongoing activities (see section 9, Cyber Security Strategy: implementation, reporting, strategic controlling and evaluation).

8 Action areas of the Cyber Security Strategy

This section describes the strategy's action areas, relating them to the strategic objectives. On the understanding that cyber security can only be ensured as a joint task (see section 7.1 Guiding principle: Establishing cyber security as a joint task for government, private industry, the research community and society), the tried and tested action areas of

1. Remaining safe and autonomous in a digital environment
2. Government and private industry working together
3. Strong and sustainable cyber security architecture for every level of government
4. Germany's active role in European and international cyber security policy

have been taken up again in this strategy. The strategic objectives have been allocated to action areas based on their focus topic. The necessary stakeholders, the key points for implementation or the desired impact mean that some objectives have more than one focus topic. It is important for all the relevant stakeholders to be involved at the implementation stage, and for action to be multidisciplinary.

8.1 Action Area 1: Remaining safe and autonomous in a digital environment

If citizens are to make the most of the opportunities provided by digital technologies, they must be able to remain safe and autonomous in a digital environment. They must be able to recognise and assess both the opportunities and potential risks associated with digital technologies, and overcome the associated challenges effectively and independently.

One important factor in supporting users' ability to assess these things are products and services that certify their conformity with IT security standards.

The Federal Government has numerous options to increase the population's cyber security literacy: it can take measures and offer products that raise awareness among users; it can take classic consumer protection measures; and it can use regulatory measures to create a framework supporting safety and autonomy in a digital environment. The following objectives work towards these things.

8.1.1 Promoting digital literacy among all users

Why is the objective relevant?

An awareness of safety in cyberspace among all users, from the general public and small and large companies right up to government agencies, is a fundamental requirement for protection against cyber risks and digital carelessness.

What is our current position?

Achieving digital literacy is an ongoing process that must evolve in parallel with new technologies and trends. Awareness of the relevance of IT security among all actors has increased greatly in recent years. Numerous state and non-government projects are carrying out good outreach work, which must be continued and stepped up. However, targeted action is required in school education and vocational training settings to further increase knowledge on the topic of IT security.

The Federal Ministry of Education and Research is responding to these challenges by providing targeted research funding, for example with its funding priority aiming to help citizens with their private IT security needs (*Unterstützung von Bürgerinnen und Bürgern bei der privaten IT-Sicherheit*),[14] through funding guidelines like those aiming to achieve secure Industry 4.0 *(Sichere Industrie 4.0 in der Praxis*),[15] and in the form of the privacy forum (*Forum Privatheit*),[16] which takes an interdisciplinary approach to matters of privacy protection and undertakes ongoing outreach work to raise awareness of cyber risks and data protection issues.

The nationwide information and awareness-raising campaign on IT security organised by the Federal Ministry of the Interior, Building and Community and the BSI, #einfachaBSIchern, which has been running since March 2021, and the consumer protection pages provided by the BSI,[17] aim to foster digital literacy by raising awareness and providing information on risks in cyberspace.

Since 2006, the initiative Deutschland sicher im Netz e.V. (Germany secure on the internet, DsiN) has offered a broad spectrum of support to the public and small businesses. This support includes the digital neighbourhood (*Digitale Nachbarschaft*) scheme promoting online security for associations and volunteers,[18] PolisiN – *Politiker:innen sicher im Netz*,[19] an initiative aimed at keeping professional and volunteer politicians safe online, and BottomUp – *Berufsschulen für IT-*

[14] Available in German at: https://www.bmbf.de/foerderungen/bekanntmachung-3160.html

[15] Available in German at: https://www.bmbf.de/foerderungen/bekanntmachung-2019.html

[16] Available in German at: https://www.bmbf.de/foerderungen/bekanntmachung-2547.html

[17] Available in German at: https://www.bsi.bund.de/VerbraucherInnen

[18] Available in German at: https://www.digitale-nachbarschaft.de/

[19] Available in German at: https://polisin.de/

Sicherheit,[20] which is an initiative to promote digital protection skills in dual vocational education. Through the transfer point *IT-Sicherheit im Mittelstand* (IT security for medium-sized businesses), which is funded by the Federal Ministry for Economic Affairs and Energy, DsiN works in association with other partners from industry and the research community to provide 80 contact offices throughout Germany, which provide support in particular to small companies, self-employed individuals and freelancers to help them implement IT security measures.

What do we want to achieve?

Our aim is to promote the necessary awareness and understanding among small and medium-sized enterprises, training and social institutions, federations, associations and consumers when dealing with increasingly complex technologies, service provision and business models.

Teaching digital literacy will be part of broad-based training provided in schools, colleges, universities and the workplace. In addition, users will be able to access target group-specific information and support options for all matters relating to information and cyber security. They will also be able to gain certification of their literacy level with the DsiN digital driving licence,[21] funded by the Federal Ministry of the Interior, Building and Community. These options are being fleshed out and expanded.

These offerings will help users gain digital literacy, allowing them to benefit from the digital revolution. Users will be aware of the problems related to cyber risks and will be in a position to assess the security of applications and services and to act with full awareness of potential risks.

What impact are we expecting?

Private industry, especially SMEs, the research community and society as a whole will be more resilient in the face of risks in cyberspace. They will make full use of the benefits of the digital transformation, will be able to deal with the challenges associated with it, and will be able to protect themselves.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The digital driving licence, funded by the Federal Ministry of the Interior, Building and Community, is in high demand among the population and is contributing to increasing digital literacy among citizens in both the private and professional context.
- Consumers are making increasing use of the BSI's information services.
- Consumers are aware and well informed. They take more active interest in cyber security matters and are better equipped to assess and counter cyber risks.
- The number of private individuals affected by cyber attacks is falling.

[20] Available in German at: https://www.dsin-berufsschulen.de/

[21] Available in German at: https://www.sicher-im-netz.de/dsin-digitalfuehrerschein

8.1.2 Increasing the user-friendliness of security solutions

Why is the objective relevant?

In IT security solutions, which in some cases must fulfil very specific requirements, user-friendliness is often given second billing. However, it is key for the acceptance, and therefore the active use, of such products. The (failure) safety and solidity of a product, in terms of its protection against malfunctions or cyber attacks, are key elements of user experience which are gaining in importance in light of the increasing dependency of IT systems.

What is our current position?

A wide range of IT security measures that are now implemented as standard show that information security and user-friendliness are not mutually exclusive. Examples of this are end-to-end encryption and two-factor authentication, which are so widely used precisely because they are so user friendly.

However, price is generally an extremely important factor in invitations to tender for security solutions. Users generally have no alternative available, and user experience is usually of secondary importance in implementation. As a result, current security solutions are often not user friendly at all and are therefore simply not used.

The current difference in user numbers of messenger services and other security solutions (such as VPN services) makes plain that the specialised suitability of a security product is not enough in itself to enable users to make sensible use of it or to facilitate its scalable provision by IT service providers. The desired security gain can only take place when all three dimensions – security, user-friendliness and management – are taken into account at the development stage.

What do we want to achieve?

Our aim is to review the extent to which invitations to tender for the security solutions used by the federal administration can ensure that the solutions are more user friendly, or the extent to which user-friendly solutions can be made more secure.

We will promote the integration of verifiable security characteristics in user-friendly, marketable IT products. Examples of best practice for this include the main messenger apps on the market, which now largely offer end-to-end encryption without this impacting their ease of use in any tangible way.

What impact are we expecting?

User-friendliness and ergonomics alongside high performance of security solutions will be the required, desirable and generally expected characteristics of marketable devices and solutions. Marketable solutions will be made safer with the integration of IT security characteristics. When the development and security approaches have been refocused, there will be greater willingness to invest in, deploy and use security solutions.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The Federal Government has incorporated user-friendliness as a criterion in its invitations to tender for security solutions.
- Research and development in the field of user-friendly security solutions has been stepped up. The topics of usable security and security by design are more closely integrated into programmes and guidelines for research funding.
- The number of marketable, user-friendly products with integrated IT security characteristics such as end-to-end encryption has increased.
- The use of products with IT security characteristics has increased.

8.1.3 Expanding government measures to protect consumers in the digital world

Why is the objective relevant?

The increasing connectivity of information and entertainment electronics, household devices and other day-to-day objects, along with the growing use of digital services, creates new risks and potential for attacks. Security in the sense of consumer protection in the digital world is therefore becoming more and more important, both for individual users and society as a whole.

What is our current position?

The Federal Government is already involved in providing information and raising awareness among consumers. For example, the Federal Ministry of Justice and Consumer Protection has a consumer portal on its homepage and provides funding for the DsiN *Digital-Kompass plus* (Digital Compass Plus) project.[22] The Federal Government also funds the *Digitalen Engel* (Digital Angels)[23] project, which aims to provide older people in rural areas with digital skills, through the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth. The BSI provides brochures and guides[24] for everyday navigation of the digital world. In conjunction with DsiN, it compiles the *Cyberfibel* (Cyber Handbook),[25] which provides comprehensive advice for those involved in the transfer of knowledge regarding consumer protection. The IT Security Act (*IT-Sicherheitsgesetz*), passed in May 2021, established consumer protection in the digital world as the responsibility of the BSI. It also provided for ongoing dialogue throughout society as a whole on the issue of cyber security.

The right of associations to take legal action and using synergies with consumer advice centres

Consumer associations can use their right to take legal action (for example the Injunctive Relief Act (*Unterlassungsklagengesetz*, UKlaG) and the Fair Trading Act (*Gesetz gegen unlauteren Wettbewerb*, UWG) to take court action to force companies to cease business practices that violate consumer protection law, without the associations themselves having to be directly affected by these practices. With its expert knowledge in the field of IT security and within its legal mandate, the BSI can indirectly support such actions by consumer advice centres by examining IT products as part of its legal duties and providing the findings of these examinations to third parties in accordance with legal provisions. The BSI can also provide general advisory services to consumer advice centres on matters of IT security. This means that the BSI can help consumer advice centres to use synergy effects to improve consumer protection in matters of IT security.

[22] Available in German at: https://www.digital-kompass.de/

[23] Available in German at: https://www.digitaler-engel.org/

[24] Available in German at: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Broschueren/broschueren_node.html

[25] Available in German at: https://www.cyberfibel.de/

What do we want to achieve?

Our aim is to expand government measures to protect consumers in the digital world with a view to strengthening the public's trust in government services which support them in the use of new technologies. The BSI will serve as point of contact and will expand its service and information options for this. Based on more extensive monitoring of the market for consumer products and services, and in consultation with the relevant providers, the BSI will provide information relevant to security.

The BSI's cooperation with consumer advice centres will lead to synergy effects in technical expertise and the right of associations to take legal action.

A digital consumer protection advisory council established at the BSI will bring together representatives from established digital consumer protection disciplines to provide independent advice to the BSI.

What impact are we expecting?

Targeted provision of information and assistance will considerably increase the level of cyber security and therefore also society's resilience to cyber risks of any type. The security characteristics of consumer products will be established as a purchase criterion. As a result, more manufacturers will take account of IT security aspects in their products.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The BSI monitors the consumer market for IT products and services and carries out its own testing.
- The BSI has created a central service centre for multichannel first-level support and general advisory services and for the collection, coordination and documentation of and response to enquiries from government, private industry and the public.
- The needs of specific target groups among citizens have been ascertained and this knowledge is used to provide tailored awareness-raising measures.
- A permanent digital consumer protection advisory council has been established at the BSI.

8.1.4 Establishing uniform European security requirements

Why is the objective relevant?

The cyber security of products and services on the market is at times unsatisfactory and can also not be transparently assessed. This situation should be countered by increasing cyber security requirements at European level. In particular, binding uniform EU-wide IT security requirements should be introduced.

What is our current position?

During Germany's Presidency of the Council of the EU, the Council conclusions on the cyber security of connected devices were drawn up. These provided key impetus for EU-wide uniform, recognised, legally binding IT security requirements. In order to ensure consumers can easily understand the cyber security characteristics of products, the IT Security Act 2.0 introduced a voluntary national IT security label.

What do we want to achieve?

Our aim is for consumers to be confident in the knowledge that products and services provide an appropriate level of cyber security and that complying with the required cyber security characteristics is governed by uniform regulation across the EU.

Conformity with EU-wide binding IT security requirements will be stated suitably and clearly on IT products. The Federal Government will launch discussions of a national voluntary IT security label as a possible approach.

What impact are we expecting?

Consumers will be protected when using labelled products and will have greater confidence in such products. The binding IT security requirements will increase the level of cyber security in the European digital single market and strengthen awareness in businesses and the research community of security issues. Infrastructure, employees, products and services will be more resilient in the face of cyber attacks. At the same time, binding IT security requirements will increase the competitiveness of European companies.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Infrastructure and capabilities for monitoring the market have been established and put into practice at the BSI, and are used in particular for the IT security label.
- The IT security label is accepted by consumers, manufacturers and service providers as a matter of course across the board and the number of IT security labels issued in Germany is continually increasing.
- Binding IT security characteristics are being introduced at EU level and will be made transparent for consumers with the help of a suitable European label (for example the CE label or a specific IT security label).

- Binding IT security requirements for IT consumer products are being drawn up and implemented as a consequence of the Council conclusions on the cybersecurity of connected devices.

8.1.5 Guaranteeing secure electronic identities

Why is the objective relevant?

Secure electronic identities (eID) are essential for many day-to-day actions in the digital age. They are relevant to industry, the research community and private users. Not only that, but they are an imperative element of government activity. This means that the state should be responsible for setting out the requirements for electronic identification procedures and their security to ensure that a uniform solution is created for every area in which this technology is used.

Trustworthy eIDs strengthen Europe's digital sovereignty and single market by enabling users to prove their identity to service providers digitally in an online process. The digitalisation of public administration, for example the implementation of the Online Access Act, requires secure, user-friendly use of electronic identities. To achieve this, and as the basis for an identity ecosystem in conjunction with business, suitable means of identification that are widely accepted by the public are required, along with the associated eID infrastructure.

Electronic identities can potentially promote national economic growth through the optimisation of processes and supply chains, the seamless, secure exchange of confidential information, time-saving for citizens and businesses, and reduced opportunities for fraud. Germany must exploit this potential to the full. A central building block in doing so is Germany's government online ID function. This form of identification, which is internationally recognised as being highly secure (notified to the EU at the highest assurance level according to the eIDAS Regulation) is the basis for official identification. However, there are many elements to identity and, depending on the situation, it can be understood as something much broader than just the information on a national identity card, an electronic residence permit or an eID card for EU citizens used for the online ID function. As well as the option of using the online ID function to prove that holders of ID cards are who they say they are, further attributes could therefore be useful for other digital identities, such as specific school or higher education qualifications.

What is our current position?

Citizens increasingly use their smartphones to deal with the authorities or carry out business tasks. In the future, they should therefore be able to save their online ID function directly on their smartphone, giving them the option to use the secure digital identification process on their smartphone in just a few seconds, with no need for an ID card.

We have set up an interministerial project group to identify the potential of eID, with the aim of making digital identities simpler and more convenient to use.

To achieve this, the BSI is designing secure eIDs by developing specifications and working as part of the team that pilots and implements new technologies, particularly those for smartphone-based online identification functions. In addition, improvements and further services are to make card-based online identification more user-friendly for citizens. Depending on their business model, private companies also use comprehensive identity management. Secure official online identification is used to some extent for this, but it is only one option for identification alongside others. The different options are not generally interoperable and they make different use of data.

In addition, the market is highly fragmented. We are in a situation where technology is penetrating more and more areas of our lives. At the same time, private companies providing identification solutions want first and foremost to protect their business interests. In the interests of digital sovereignty, the state must come up with a stronger alternative which offers users security, data protection and digital self-determination, which is user friendly and flexible, and which can be widely used.

What do we want to achieve?

Our aim is for the online ID function on a smartphone to be derived from the national ID card and to be saved in the phone's secure element. It will be possible to use this smart eID alongside an ID card to provide online proof of identity to companies and authorities. Other apps will be available from private companies for online identification and smart eID functions. The smart eID will have been notified to the European Commission, which means it will be a recognised means of identification throughout the EU.

What impact are we expecting?

The ability to use the online identification function on a smartphone will create widespread acceptance and expansion of the eID security infrastructure in Germany and will serve as an example for secure smartphone usage in the EU.

Secure, government-checked eIDs will foster trust in technology, create new opportunities for value creation, and protect against digital identity theft, among other things.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The number of downloads and installations of the Ausweis-App2 app (including the applet) on smartphones has increased.
- The number of active users of the online identification function has increased.
- The number of options for using the online identification function has increased.
- The smart eID has been notified to the European Commission, which means it has to be recognised as a means of identification throughout the EU.
- An identity ecosystem has been piloted in conjunction with private industry.
- The smart eID function is available for smartphones. A secure eID infrastructure for smartphones is available.
- Card-based online identification using a national ID card, an electronic residence permit or an eID card for EU citizens is easy to use.

8.1.6 Protecting the authenticity and integrity of algorithms, data and documents, and the electronic identities of people and things in the broader sense

Why is the objective relevant?

Even now, the ongoing digital revolution is the result of huge amounts of interconnectedness among physical objects, algorithms, data, documents and people. The number of participants in different digital networks, and the depth of connection among them, will grow continually in the future. Examples of this type of network are the IoT, connected vehicles, distributed AI systems, energy networks and digital learning platforms. Protecting the identity (people and objects) or the authenticity and integrity (data, algorithms and documents) of participants in these networks is a fundamental requirement for trust in these networks, and therefore for a successful digital transformation.

What is our current position?

Identities currently play a central role in the digital revolution. As well as a person's identity as used for the online identification function,[26] there are numerous other identities that are becoming more important by the day. Alongside non-official identities, such as school student cards and the identities of those using electronic media (media identities), these include the identities of physical objects such as vehicles or sensors. The authenticity and integrity of algorithms (for example neural networks), of documents (for example official certificates) and of data (for example flight paths and take-off and landing instructions in air traffic control) also play a major role.

With sufficient effort, these identities, or their authenticity and integrity, can be falsified. This can cause damages to finances, health and personal reputation. Vulnerabilities and appropriate defence strategies are in many cases the subject of current research. It is becoming increasingly easy to falsify media identities using AI (deep fakes), even for non-experts, and this can be used to attempt fraud or to deliberately influence opinions.

What do we want to achieve?

Our aim is to increase the security of identification of participants in digital networks in different areas of application. To achieve this, enabling technologies such as biometric processes and hardware-based identifying characteristics (physical unclonable functions) will be examined and documented, along with their resilience in the face of cyber attacks, and robust protection methods will be developed. We will have a better understanding of automated forgery of media, particularly using AI, and attacks on biometric systems by merging the biometric characteristics of several people (morphing), while detection and defence measures will be radically improved. Evaluation methods for authentication and identification processes that take into account the required assurance level will be developed and will be published in the medium term in the form of technical guidelines. The knowledge gained from these steps will then be used by national and

[26] See strategic objective 8.1.5
Guaranteeing secure electronic identities

international standardisation organisations. Public key infrastructure (PKI), which enables cryptographic key pairs to be rolled out and managed, will be made more secure, and eID interoperability infrastructure will be implemented and maintained.

The integrity protection, proof of authenticity and, where necessary, the long-term digital preservation of documents and data from different areas of application such as intelligent transport systems, smart metering, Industry 4.0, electronic recording systems and digital education will be advanced with the help of various different technologies. Where it makes sense and is possible, existing standards should be taken into account.

What impact are we expecting?

Increasing the security of digital networks will make them more robust and will increase trust in them. A follow-on effect will be greater use of them, speeding up the digital transformation.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Evaluation methods for authentication and identification processes that take into account the required assurance level have been developed and established as standard. For example, the security requirements for identification and authentication methods for access to digital education provision have been standardised.
- In biometrics, the aspects of different attack methods have been examined in detail and documented, and their prevention and detection has been systematically improved and implemented in practice. The relevant technical guidelines have been published or developed further.
- Methods for the reliable identification of wireless devices using physical fingerprinting (individual characteristics of their electronic components) have been developed and demonstrated.
- The security of PKI, which is needed for the rollout and management of cryptographic key pairs, has been further developed, as have eID technologies and PKI itself, while secure eID interoperability infrastructure has been established. These things undergo regular maintenance. A PKI toolkit has been established for digital transformation projects by modularising PKI standards and implementing uniform standards for secure elements.
- The security of integrity protection processes and long-term digital preservation technology has improved significantly on the basis of the BSI's technical guidelines. The relevant technical guidelines have been further developed accordingly.
- A secure server has been implemented to ensure the verifiability of the origins and integrity of electronic documents. Digital seals and signed barcodes to protect the integrity and to prove the authenticity of paper documents and data have been developed for new areas of application.

8.1.7 Creating the conditions for secure electronic communication and safe web offerings

Why is the objective relevant?

Secure, interoperable communication and safe web offerings are essential requirements for successful digital transformation across the spectrum of areas of application, such as in vehicle-to-vehicle and vehicle-to-cloud communication, email, health care and the implementation of the Online Access Act.

What is our current position?

In regard to the implementation of the Online Access Act, the BSI has drawn up specifications in the form of technical guidelines on operating interoperable user accounts (citizen accounts) as components of identification for online government services, which it has coordinated with federal and state governments and has published. The requirements are yet to be implemented in federal and state government solutions. In parallel to this, a pilot project is to formulate and implement specifications for the mail boxes of interoperable user accounts.

The BSI is currently discussing the planning of the Telematics Infrastructure 2.0 with gematik GmbH. The consultation is expected to be complete by the end of 2021.

What do we want to achieve?

Our aim is to (further) develop application-specific cryptographic standards for the secure and interoperable use of communication protocols, and to incorporate these into proposed legislation as the latest technology. Application-specific cryptographic standards, test criteria and profiles will be expanded to include other use cases, for example mobility, health care, public administration and Industry 4.0.

What impact are we expecting?

Appropriate implementation of the measures is expected to increase trust in digital technology in key areas of use, leading to greater use of associated products.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- In regard to mobility, the IT security of communication between vehicles and of the connection of vehicles to the cloud has increased.
- In the ongoing development of telematics infrastructure, the use of both stationary applications and new mobile options for telematics infrastructure applications by patient and provider is secure at all times.
- In addition to De-Mail, the mailboxes of interoperable user accounts provide a further secure communication route for the public administration. The security of these mailboxes is ensured through a BSI technical guideline compiled in cooperation with federal and state governments. A technical guideline has been drawn up for the secure implementation of the Online Access Act.

8.1.8 Responding responsibly to vulnerabilities – promoting coordinated vulnerability disclosure

Why is the objective relevant?

Fixing known vulnerabilities quickly in systems, products and service provision is a cornerstone of cyber security. A user who discovers a vulnerability should contact the manufacturer of the product in question or the provider of the service in question immediately and in confidence, so that vulnerabilities that are detected can be fixed with a patch or update within a reasonable time period. There must be careful consideration of whether the vulnerability should be made public knowledge before the relevant updates or patches are available. Putting these factors into practice in a coordinated process is known as coordinated vulnerability disclosure (CVD).

What is our current position?

In practice, there is currently no general framework setting out which stakeholder, to what extent, and using which methods and instruments, is permitted to find vulnerabilities and report these to the manufacturer. The question of how to approach vulnerabilities is therefore left up to the companies themselves. This means that some companies use methods such as bug bounty programmes to offer a financial incentive for a coordinated approach (CVD), while other companies take legal measures to prevent the discovery of bugs as they see this as an infringement of their rights. This leads to uncertainty, with the result that certain software products are no longer examined for vulnerabilities, or knowledge of critical vulnerabilities is not reported to manufacturers immediately.

What do we want to achieve?

Our aim is for the Federal Government to develop a framework to ensure that those reporting bugs have legal certainty if they approach companies to inform them that they have become aware of vulnerabilities, with a view to fostering proactive vulnerability governance. There will be reliable points of contact for them to report their findings. These can take the form of internal contact points which companies themselves are obligated to set up, or the BSI as a public liaison office.

The legislator will obligate the companies affected to provide points of contact and processes to enable them to fix reported vulnerabilities in a suitable time frame. The extent to which the rights and duties are set out on both sides of the CVD process will be examined. These rights and duties could include a holdback period before making vulnerabilities public or a binding deadline for patches or updates. A coordinated process will be put in place between the BSI and manufacturers which extends beyond the simple exchange of information. This will also apply to vulnerabilities in the IT supply chains of products and services (supply chain security).

IT security vulnerabilities will be reported to the companies in question as quickly as possible. At the same time, companies will have internal processes in place enabling the rapid checking and fixing of reported vulnerabilities in the form of a patch or an update.

The BSI will be involved in the exchange of information on the basis of its CVD process. It will support the reporting of vulnerabilities as a neutral specialist liaison body. It will also issue high-profile public warnings and will incorporate its knowledge of the vulnerability landscape into the

national cyber threat situation report and into the general and industry-specific overview of the threat situation (in particular regarding critical infrastructures). Users will be warned of vulnerabilities as quickly as possible and will be given information on potential protection measures.

Action will be taken to ensure that unauthorised third parties do not have access to confidential details of vulnerabilities before the necessary patches or updates are available. The specific interests of the security authorities are addressed in strategic objective 8.3.10 Fostering responsible handling of zero-day vulnerabilities and exploits.

What impact are we expecting?

Users, critical infrastructures and institutions of special public interest will be better protected from cyber attacks, as IT vulnerabilities in systems, products and service provision will be communicated and remedied quickly, suitable protective measures will be taken, and confidential details of IT vulnerabilities will not fall into the hands of malicious cyber actors before the problem is resolved.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- There is legal certainty surrounding seeking and finding vulnerabilities.
- The Federal Government regulates the involvement of the BSI in CVD events and publishes a coordinated process for the responsible public announcement of vulnerabilities (CVD process).
- Vulnerabilities that are discovered are increasingly reported.
- Incentives for manufacturers and service providers to remedy reported vulnerabilities in a suitable time frame have been increased.

8.1.9 Using encryption – a prerequisite for self-determined, autonomous action – across the board

Why is the objective relevant?

Encryption guarantees the confidentiality, integrity and authenticity of digital information, making it a cornerstone of cyber and information security. Encryption processes effectively protect government, industry and individual users from the theft, espionage or sabotage of personal, business or official digital information and communication. They create trust, which in turn increases acceptance of the use of new technologies. However, encryption processes face continually evolving threats, making their continuous evaluation and development essential.

Ongoing developments in quantum technology exacerbate this problem, as many encryption processes that are currently used will no longer be secure in the future. This objective focuses on the interests of society and industry. The specific interests of the security authorities are addressed in strategic objective 8.3.9 Providing security through encryption, and security despite encryption.

What is our current position?

Since the last cyber strategy was published in 2016, there has been an upturn in the use of encryption processes, particularly in businesses and organisations. This is a positive development from a cyber and information security perspective. Businesses protect their company networks using VPNs, or make increasing use of encrypted IT services.

Private users benefit from the secure options offered by messenger services with end-to-end encryption, the now widely adopted TLS protocols used for communication on the internet, and the increasing use of encryption by cloud service providers.

Yet it should be noted that the majority of users in Germany (except users of messenger services) rarely use encryption solutions such as VPN apps, leaving the safeguarding of their data to commercial providers. In the rapidly growing IoT market in particular, encrypted products make up the minority. This is worrying, as IoT products will be a huge part of everyday life in the future yet will not themselves provide security for the resultant data. This broadens the scope for attack hugely. Encryption can make the use of IT considerably safer.

What do we want to achieve?

Our aim is for the Federal Government to help users to have confidence in the digital transformation and consider it dependable. It will do so by continuing to promote the comprehensive use of secure encryption technologies and by actively encouraging the removal of legal, financial and technical hurdles hampering the use of encryption solutions.

To achieve this, the Federal Government will continue to argue on the international stage against the prohibition of encryption technologies and will refrain from such prohibitions itself.

The Federal Government will also promote the development of new encryption solutions, particularly in the field of post-quantum cryptography, by funding cryptography as a research discipline, creating market incentives for product development, actively initiating its own

development projects and participating in other such projects, and scrutinising the trustworthiness of products on the market in approval and certification processes.

What impact are we expecting?

The consistent encryption of digital communication and storage will prove a barrier to access to and exploitation of data by unauthorised third parties. Government, industry and society will be better protected against cyber risks. In addition, secure communication options will create trustworthiness and dependability of digital environments. This will open up opportunities for the increased use of digital technology in other areas of life, for new business models, and for further technical innovation.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Initiatives have been launched to promote the use of encryption which target industry, individual users and the research community, as well as international bodies which have the same aim.
- Other initiatives have been established along the same lines as the implementation of post-quantum cryptography in open-source products.
- Funding for basic and applied research into cryptography has increased.
- The number of encryption solutions that are either certified or examined and approved has increased.
- Citizens and businesses use more secure, encrypted communication methods.

8.1.10 Guaranteeing IT security through AI and for AI

Why is the objective relevant?

AI is one of the central key enabling technologies of the 21st century and is the driving force behind the increasing digitalisation of products, services and processes. Even now, AI influences critical security processes and decisions, for example in biometrics, health care and mobility.

The growing use of AI provides new opportunities for cyber security, but also brings new risks. AI systems can help identify vulnerabilities and can rapidly detect and ward off attacks. AI can also be used to make existing tools for defending against cyber attacks more efficient and to help develop new tools.

At the same time, greater use of AI-based systems to automate processes and decision-making brings with it new security risks that established IT security standards do not consider.

Germany's Artificial Intelligence Strategy

As a key enabling technology, AI offers vast potential for economic growth and productivity increases. In its Artificial Intelligence Strategy, the Federal Government developed a framework for action and adopted extensive measures to promote and use this potential in the interest of the population and the environment, responsibly, safely and for the common good.

This strategy, which was adopted in 2018 and updated in 2020, underscores the Federal Government's commitment to AI as a technology of the future. The strategy increases the Federation's investments in AI funded from the Stimulus Package and/or the Future Package from three million euro to five million euro by 2025.

The strategy is available at https://www.ki-strategie-deutschland.de/home.html.

What is our current position?

The use of AI-based systems is increasing. These systems are used in a whole spectrum of scenarios. There are currently no uniform criteria, methods or tools available for the evaluation of AI systems. However, the proposal for a European Commission Artificial Intelligence Act[27] which is currently in negotiation at European level develops harmonised rules on artificial intelligence and sets out assessment criteria for them which Germany would also have to apply. The Federal Government is funding a range of research and industry measures related to AI. It also provides expert input to national and international standardisation processes, actively contributing to the design of standards and norms.

What do we want to achieve?

Our aim is to attain the highest possible level of IT security for AI systems, regardless of the purpose they are used for, while also deploying AI systems to provide a high level of IT security (IT security

[27] Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206

through and for AI). To this end, the opportunities for using AI systems to protect (government) IT systems will be examined continually.

The regulatory framework for IT security requirements will include the security of AI systems. There will be clearly defined IT security requirements for AI systems which take into account the special characteristics of such systems. It will be possible to evaluate the security characteristics of AI-based systems using effective, efficient assessment criteria and methods. These will, in particular, take into account new methods of attack that exploit the specific characteristics of AI systems. These must be considered in particular in the European Artificial Intelligence Act so that high IT security standards are in place for AI applications that are considered high risk.

IT security will be one of the key components taken into account when developing AI systems (security by design). AI systems will attain a high level of IT security regardless of the purpose they are used for.

In addition to the protection of AI-based systems (IT security for AI), AI-based systems will also be used to achieve improved analysis and reporting formats and better protection measures (IT security through AI). IT security through AI will be used in particular to detect attacks on networks and as a tool for the security authorities in their law enforcement activities. It should be noted, though, that in regard to online hate speech, an analysis of context is essential and this is beyond the capabilities of AI.

In a collective process involving partners from research, industry and the public administration, the Federal Government will develop the basic technological principles for assessing systems of this type and will then apply these in practice. In doing this, the Federal Government will play an active part in pushing forward the adoption of European standards for AI products around the globe.

What impact are we expecting?

Providing verifiable security for AI will be an important foundation for the acceptance and success of this key enabling technology, which is essential to digital transformation. Only when AI is accepted and successful will government, industry and society be able to fully reap the benefits it offers. This is also the way to establish and maintain user trust in AI-based systems.

At the same time, the use of AI for IT security applications, coupled with the improved security of AI systems, will improve security for government, industry and society. This will in turn bolster the national and the European economy, strengthening digital sovereignty in a global AI market.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- There has been a considerable increase in the number and quality of academic publications discussing AI-specific attack vectors and the associated countermeasures, and the use of these in relevant areas of application.

- The Federal Government has contributed to ensuring that IT security aspects be suitably taken into account in the upcoming AI Act at EU level and in its implementation at national level.
- Assessment criteria, tools and methods have been developed to evaluate cyber security aspects of AI-based systems. Suitable technical guidelines have been published in relevant, particularly critical areas of application, and now form the basis for standardisation projects.
- AI systems are increasingly used successfully to detect and prevent attacks.

8.2 Action Area 2: Government and private industry working together

Businesses in Germany are often targeted in cyber attacks. Considerable damages are caused by ransomware attacks alone. This type of attack prevents victims from accessing their data or systems. The number of new types of malware is also increasing, and critical vulnerabilities are discovered time and again in widely used software products.

Critical infrastructures in particular are crucial to the functioning of society. Their failure or disruption would cause serious supply shortages which would pose a threat to public security. The protection of critical infrastructures is therefore set down in law in the BSI Act (*BSI-Gesetz*, BSIG).[28]

Companies based in Germany must be able protect themselves and their customers appropriately against cyber attacks. This generally includes installing updates immediately and raising awareness among employees. Depending on requirements in relation to the security concerns affecting each particular company, regular staff training should take place as a matter of course. In addition, companies should introduce and operate an information security management system (ISMS) in line with national or international standards, such as ISO 27001 or the BSI standard for baseline IT security. It is the responsibility of manufacturers to develop their own quality assurance measures with the aim of providing quality products and to fix vulnerabilities discovered in their products promptly, providing user protection that is part of a high level of cyber security in Germany.

Future and key enabling technologies such as IoT, KI, Blockchain, big data and quantum technology bring about leaps forward in innovation and change the fundamental conditions for cyber security in Germany. They create new potential for improving existing cyber security tools, but they can also cause new cyber risks to emerge. To protect users, the security of key enabling technologies must therefore be incorporated as a central component right from the development process, with security by design becoming the default.

Top-class IT security research and well-trained IT security professionals are key to ensuring cyber security provision in the long term.

The Federal Government will draw up measures for continuing the existing close, trusting cooperation between government and industry. The basis for IT security is a strong German IT industry, fostered through modern economic policy.

Stronger cyber security in industry therefore calls for cooperation between government and industry; at the same time, the Federal Government must also ensure that the necessary conditions are created. The following objectives focus on both of these approaches.

[28] Available in German at: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

8.2.1 Reinforcing the coordination function of the NCSR in the cyber security landscape

Why is the objective relevant?

There are no areas of life or sectors of the economy that are not affected by the digital revolution. Ensuring high levels of cyber security is therefore of growing importance for society. To keep pace with this development, the NCSR needs to bring together the different perspectives from the private sector and society as a whole in the strategic advice it gives the Federal Government, and to give this advice a more formal status.

What is our current position?

The NCSR, which was founded in 2011 to serve as a driving force and strategic adviser, is the highest-level body on the German cyber security landscape. The 2016 Cyber Security Strategy extended its remit to include identifying long-term trends and need for action, and drawing up recommendations for action. With this in mind, an advisory council was set up in 2017. Its recommendations were collated in a final report. One of these recommendations was ongoing support for the work of the NCSR by an academic working group which would compile and publish discussion papers at regular intervals.

What do we want to achieve?

Our aim is for the NCSR to play a heightened role in the future in raising cyber security questions. With this in mind, its role as strategic adviser to the Federal Government will be expanded and given a formal needs-based structure. It will attain significant reach in industry, the research community and society, and will provide ongoing support for the implementation and further development of cyber security strategy.

To achieve this, we will look at how cooperation and reporting to the Federal Cabinet, introduced as part of the 2016 Cyber Security Strategy, can be made more binding. In addition, we will examine possibilities for greater public impact and increased involvement of industry, the research community and civil society in the work of the NCSR.

What impact are we expecting?

We expect the NCSR to provide a more comprehensive perspective on cyber security topics. The expanded consultation process should provide all stakeholders with a deeper understanding of the respective positions of those involved. One of the aims of the increased ability of the NCSR to influence the private sector and society by providing tangible ideas is to enhance the consistency of activities in the cyber security landscape.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criterion:

- A concept paper has been drawn up by the Federal Government in consultation with the NCSR. It lists measures that will enable the NCSR to provide the Federal Government with

a more targeted advisory process, and offers a more comprehensive overview of the cyber security landscape for decision-makers in all of the relevant bodies.

8.2.2 Improving cooperation between government, private industry, the research community and civil society on matters of cyber security

Why is the objective relevant?

Cyber security in Germany can only be strengthened on a lasting basis if government, the private sector, civil society and the research community work together.

Society as a whole must improve the way it works together, strengthening this work through new types of cooperation. This will increase knowledge of cyber security risks and dangers among consumers, the research community, and decision-makers in government and the private sector, and will support them in preventing these risks. Targeted, practical government provision and feasible standards can also be developed.

What is our current position?

Representatives of private industry are already involved in many areas and processes. There is close cooperation between government and the private sector, in particular in regard to critical infrastructures and economic protection. Established forums for this include the UP KRITIS public-private partnership, the Alliance for Cyber Security, the BSI's Dialogue for Cyber Security, and the Economic Security Initiative.[29]

The Federal Ministry for Economic Affairs and Energy supports SMEs in matters of digital transformation and IT security. It provides users with easy-to-understand, impartial, practical information and helps them design and implement their strategies.

In April 2021 the National Pact on Cyber Security was published. This is a joint declaration on cyber security with the involvement of government, private industry, the research community and civil society. The final declaration lists 13 action areas on which all groups within society are to work together to implement.[30]

This dialogue depends on a diverse range of participants. It is still at the early stages, however, and will be reinforced on the basis of the findings from the National Pact on Cyber Security.

---

[29]The Economic Security Initiative (www.wirtschaftsschutz.info) is coordinated by the Federal Ministry of the Interior, Building and Community. Its aim is to implement the National Economic Security Strategy, to work with experts from the security authorities (BfV, BKA, BND and BSI) and with national business and security associations (Federation of German Industries, Association of German Chambers of Commerce and Industry, ASW Bundesverband (the German association for security in industry and commerce) and BDSW, the German association for the security industry) to analyse the risk situation and develop action plans for comprehensive economic security.

[30] Available in German at: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/nationaler-pakt-cybersicherheit/gesamtgesellschaftliche-erklaerung/gesamtgesellschaftliche-erklaerung-artikel.html

What do we want to achieve?

Our aim is to actively involve the private sector, the research community and society as a whole in planning cyber security by means of initiatives offered by the responsible government agencies. There should be room within the discussion process to work together to develop long-term solutions and possibilities for action related to cyber security. The issues and needs affecting different groups will be noted early and will be incorporated into the work of government stakeholders.

IT security service providers will implement standards for IT security products and systems and will be able to detect challenges and trends at an early stage based on their direct contact with users. Government agencies will therefore involve them early when defining legal standards for IT security products and will work with them to find feasible ways to implement these standards.

What impact are we expecting?

Pushing forward a dialogue on IT security involving every area of society will lead to increased acceptance of government institutions. This will facilitate cooperation and will help promote the consideration of cyber security topics at all levels of IT usage.

Cooperation models will allow stakeholders to work more closely together, bringing about a strong multiplier effect in the transfer of knowledge. Established cooperation relationships will mean that communication can take place at the very start of development projects, when processes are at the definition stage. This will allow findings to be presented in a way that is more user friendly and will save time and maximise synergies.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The number of members of the Alliance for Cybersecurity has increased.
- The dialogue organised by the BSI and involving the whole of society on the topic of IT security has moved forward, with representatives from every area of society contributing to the discussion of acute IT security topics.
- The Federal Government is actively working to implement the 13 action areas from the joint declaration in the National Pact on Cyber Security, while at the same time bringing new stakeholders on board and documenting this implementation in a way that is transparent.
- Government support provision, which includes a range of cooperation options and information via social media and newsletters, has been expanded and the number of people making use of this provision has increased.
- The proportion of major surges in ransomware attacks that are detected by technical sensors has increased.
- The Economic Security Initiative has increased its offering for companies, research institutions and local government.

- The Federal Ministry for Economic Affairs and Energy's *Mittelstand Digital* (medium-sized companies go digital) network and its IT security options are used by private industry, particularly SMEs.

8.2.3 Establishing a cooperative platform for government, private industry, the research community and society to enable communication about cyber attacks

Why is the objective relevant?

Organisations in government, the private sector, the research community and society as a whole that are affected by cyber attacks need usable technical information if they are to detect these attacks. Such information is based on analyses of cyber attacks. These analyses are carried out by federal authorities and IT security service providers, for example. If the organisations affected can be provided with this information effectively and efficiently, it can lead to a significant reduction in or even the prevention of damages resulting from cyber attacks.

What is our current position?

Cyber attacks are fended off by a wide range of actors. This means that the information required for effective defence against cyber attacks is often fragmented and is not always available quickly and in full to the organisations affected. There has been a stronger focus on working with providers, as set forth in the Cyber Security Strategy for Germany 2016. However, that is only one component of the necessary exchange of information.

What do we want to achieve?

If cyber security is to succeed, all organisations involved in cyber threat prevention must provide as much information from their area of responsibility as data protection and confidentiality obligations permit. Our aim is to improve detection of cyber attacks in public communication networks by involving service providers. As a neutral intermediary among stakeholders, the state will create the necessary basis for a cooperative information-sharing portal. Candid discussion among all of the organisations involved will allow the pool of information on cyber attacks to be expanded, which will improve cyber threat prevention for all those organisations.

General information on cyber attacks, and in particular technical specifications for detecting attacks, will be exchanged efficiently through the information-sharing platform among organisations affected and organisations involved in evaluating such attacks (e.g. the BSI, the security authorities, IT security service providers and major corporations) with a view to facilitating detection. This will enable improved threat analysis and targeted cyber threat prevention. Information will be shared efficiently, using automated systems where this is legally and technically possible, and will reach a large number of target recipients. Information will also be adapted to suit the expertise of the user group in question, for example SMEs. Sensitive information will be effectively protected during the exchange of information.

What impact are we expecting?

Voluntary participation by as many organisations affected by cyber attacks as possible in the exchange of information via the information-sharing portal will make the detection of cyber attacks more successful and enable quicker defence against and attribution of such attacks. Improved networking will lead to greater awareness, in particular for businesses and the research community. Damages from cyber attacks will be reduced or prevented.

As far as data protection and confidentiality obligations allow, the organisations affected by cyber attacks will provide information from their cyber attack detection activities to IT security service providers and government agencies responsible for cyber threat prevention. These entities will then create a pool of information on cyber attacks and exchange this information with each other to achieve better analytical results. Consequently, it will be possible to continually improve the analysis of cyber attacks and to draw up new, more targeted technical specifications for detection. This will strengthen cyber defence in company and public networks.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The new cooperative information-sharing portal for the voluntary exchange of information on cyber attacks has been established.
- Sensitive, detailed information is handled confidentially, in line among other things with applicable legal regulations and current provisions affecting the transmission of information, which means it is effectively protected from misuse.
- Incentives for participating in the exchange of information and for sharing information have been increased.
- The amount of information and technical specifications regarding cyber attacks shared among the organisations affected has increased, and protection against damages resulting from cyber attacks has improved.

8.2.4 Protecting businesses in Germany

Why is the objective relevant?

Businesses in Germany face wide-ranging, constantly evolving risks in the form of cyber attacks. A lack of resources and expertise means that SMEs in particular are not adequately equipped for the challenges posed by cyber attacks. They therefore need suitable support to ensure they are properly protected against cyber attacks. This type of business is in the majority in the private sector in Germany.

What is our current position?

A wide range of initiatives have been put in place to allow the exchange of information and knowledge between government and private industry on cyber security matters. Some of these are the Federal Ministry for Economic Affairs and Energy's initiative for IT security in the private sector,[31] the Alliance for Cybersecurity, and the public-private cyber alliance Cyberbündnis mit der Wirtschaft, founded by the Federal Ministry of the Interior, Building and Community and the Federation of German Industries.

The Economic Security Initiative, established since 2016, also continually includes the risks to businesses in the digital world in its work. In addition, companies can approach the intelligence services, for example case recording by the BfV and the cyber intelligence division of the BND, and police authorities as trustworthy points of contact. These options are supplemented by the central cyber crime contact offices of the federal and state police, which were set up as expert points of contact for businesses and public and private institutions to report IT security incidents. When such incidents are reported, the cyber crime contact offices are in a position to rapidly instigate initial measures and then to refer the incidents to the responsible investigation office.

What do we want to achieve?

Our aim is to expand public-private cooperation. Platforms for dialogue and information exchange between the state and the private sector will be strengthened. These platforms include UP KRITIS, the Alliance for Cybersecurity, the National Pact on Cyber Security, the public-private cyber alliance Cyberbündnis mit der Wirtschaft, and the Economic Security Initiative.

Interaction between business and the responsible bodies in the cyber security sub-areas of prevention, detection and reaction will be bolstered, which means that businesses will contribute more to the detection and investigation of cyber security threats. Cyber security will be an integral part of comprehensive economic security.

Measures will be taken together with and in coordination with federal and state governments to protect businesses, particularly SMEs, the arms industry and companies providing German key enabling technology. The economic security network of the community of the German domestic civil intelligence services will also be involved. The measures set forth in the initiative for IT security in the private sector, including the transfer point for IT security for medium-sized

[31] Available at: https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Navigation/DE/Home/home.html

businesses (TISiM), will be implemented, and funding programmes such as go-digital[32] and *Digital Jetzt* (digital now)[33] will be further developed as needed. The network of *Mittelstand Digital* centres will be extended, with a particular focus on the cross-cutting topic of IT security.

More information will be provided to support businesses, in line with existing needs. Businesses, particularly SMEs, will be aware of IT security. They will have a strong sense of potential cyber risks and will have the skills needed to assess these risks and find solutions. There will be support for IT security measures implemented by businesses, particularly SMEs. To achieve this, support provided by the BSI for private industry will be expanded, particularly within the Alliance for Cybersecurity.

What impact are we expecting?

Businesses, particularly SMEs and businesses in the crafts sector, will be offered more targeted support to implement IT security measures, taking into account the specific cyber risk they face, and will have the knowledge to instigate organisational, technical and staffing measures efficiently. This means they will be able to protect themselves effectively against cyber attacks. This will increase the competitiveness of German industry.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The services provided by the *Mittelstand Digital* centres are used by private-sector companies.
- The TISiM is well known among SMEs and businesses in the crafts sector in particular, and there is demand for its services.
- Assistance programmes with aims including support for IT security in SMEs, including craft businesses and the self-employed, are well known and there is demand for them. These include in particular go-digital and *Digital Jetzt*.
- The number of members of the Alliance for Cybersecurity has increased. The Alliance has expanded its offerings.
- There has been a recorded increase in the number of those using the support options offered by the BSI.
- The implementation of recommended cyber security precautions has increased.
- The percentage of businesses which have reacted to warnings from the BSI by fixing their vulnerabilities has increased.
- The Economic Security Initiative has established projects intended to provide comprehensive protection against know-how and information drain in the value chain.

[32] Available in German at: https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/foerderprogramm-go-digital.html

[33] Available in German at: https://www.bmwi.de/Redaktion/DE/Dossier/digital-jetzt.html

8.2.5 Strengthening Germany's digital economy

Why is the objective relevant?

German industry has a wide range of innovations and success stories on which to build. However, at the same time it is faced with stiff international competition. Alongside new areas of application like smart home and smart city, the digital transformation of long-established industries is also particularly important. Targeted measures are needed to ensure that German industry continues to play a leading role in the digital future, to enable its success in other branches, and to strengthen digital sovereignty. The associated supply chains must also be taken into account.

What is our current position?

On the one hand, foreign companies dominate important fields in the digital economy, particularly those that are data-driven. On the other hand, Germany and Europe are world leaders in many areas of research associated with the digital transformation, and are known for their high standards. We must create the conditions that will allow German companies to use the advantages they have to remain or to become competitive.

What do we want to achieve?

Our aim is to strengthen Germany's digital economy through targeted support for key enabling technologies[34] and through advisory services, grants, joint projects and networking with relevant researchers. Cooperation with the relevant bodies on the joint development of recommendations for action and standards for key areas of application, such as electromobility and smart home products, will also strengthen the country's digital economy.

Specifically, targeted measures will be taken to strengthen the following sectors and supply chains by increasing the IT security of their products and/or by developing products aimed at improving IT security: the mobility and automotive industry, the energy sector, smart home, IoT and smart cities, Industry 4.0, health care, finance, and the IT security industry in the fields of biometrics, long-term digital preservation and quantum technologies.

The PKI for smart metering, which is a key infrastructure component for digitalising the energy transformation, will be operated successfully for growing user numbers. The Federal Ministry for Economic Affairs and Energy/BSI roadmap for developing technical cornerstones for the areas of application smart grid, smart mobility and smart or sub metering (intelligent energy use measurement, including in multiple-dwelling buildings) will be implemented through several standardisation projects.

What impact are we expecting?

Suitable implementation of the measures mean we can expect products with improved IT security, together with innovative products that themselves increase IT security. This will lead to these

[34] See strategic objectives 8.1.10 Guaranteeing IT security through AI and for AI and 8.2.9 Providing IT security through quantum technologyProviding IT security through quantum technology.

products enjoying greater competitiveness, greater acceptance and wider circulation. Innovation resulting from research and networking will make the German digital economy a global leader.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Data transmission to and from mobility data rooms and autonomous driving functions have been secured. Resilience against attacks on vehicle sensors has increased and the associated technical guidelines have been published. To ensure cyber security, the type approval and market monitoring of motor vehicles and motor vehicle components has been designed by the BSI in conjunction with the Federal Motor Transport Authority.
- The PKI for smart metering, which is a key infrastructure component for digitalising the energy transformation, is operated successfully for growing user numbers. The Federal Ministry for Economic Affairs and Energy/BSI roadmap for developing technical cornerstones for the areas of application smart grid (controlled consumption and production facilities), smart mobility (integration of the charging infrastructure of electric vehicles), and smart/sub metering (cross-sector measurement for electricity, gas, water, and heating or heat) has been implemented through several standardisation projects. In the smart home/consumer IoT sector, standards, norms, technical guidelines and inspection criteria (for example the TR-Router inspection specification) for use, among other things, in conjunction with national and international labelling and certification processes (such as within the Cybersecurity Act) have been developed in cooperation with key stakeholders from government, private industry and society.
- In the smart cities sector, existing municipal IoT infrastructure has been analysed and recommendations for its secure expansion and operation, technical guidelines, and standards for key enabling technologies and platforms have been drawn up in cooperation with key stakeholders from government, private industry and society. In addition, the legal framework for a binding obligation to implement the measures for improving IT security in critical areas of application has been put in place.
- Regarding Industry 4.0, a concept for trust infrastructure for constructing digital value-creation networks has been agreed in the international context and recommendations for action (best practices) for implementing important components of trust infrastructure have been compiled for SMEs. Additionally, service interfaces for secure digital transformation and Industry 4.0 have been created.
- In health care, a catalogue of security requirements for digital health care applications has been established as part of the approval process, and digital activities to combat the pandemic have continued. Initiatives in health care have been expanded to include rescue activities.
- In the finance sector, security analyses of online payment processes have been communicated and updated, and the security requirements for biometrics applications for two-factor authentication have been established.

8.2.6 Creating a uniform European regulatory framework for businesses

Why is the objective relevant?

The regulatory framework for the cyber security of products and services is inconsistent at national and international level. It is distributed among a wide range of standards, norms and laws. Binding standards in some cases do not exist or are insufficient. Moreover, ascertaining the relevant regulation can be time-consuming and error-prone.

Current EU regulations on surveillance technology are causing manufacturers to move their headquarters from EU member states to non-EU countries, because it is considerably easier to import into the EU from there than to export from the EU to non-EU countries. One result of this is technology drain in the fields of telecommunications surveillance, digital forensics and big data analysis, for example. In addition, it works against the objective of digital sovereignty.

What is our current position?

The aim of only bringing devices into circulation that guarantee protection against fundamental cyber security risks cannot be reached at EU level. The European Commission therefore intends to impose standards on connected devices as a requirement for offering them on the market. This move would considerably improve the situation in the short to medium term, as there would be no need to propose draft legislation, meaning the effects would be felt more quickly. Germany therefore expressly supports this intention.

What do we want to achieve?

Our aim is to have uniform legal requirements throughout the EU, including market access regulations and norms and standards, for businesses in the cyber security industry. Double regulation will be avoided. The Federal Government will coordinate its approach in national, European and international standardisation organisations, striving to ensure that uniform norms and standards be developed and introduced for companies in the EU. It will actively help shape the EU's NIS Directive 2.0[35] and German concerns will be included in the subsequent legislative act. The Federal Government will also actively engage with sector-specific legislative proposals, such as the proposed DORA act for the finance sector.[36]

International cooperation will be intensified, as will work in standardisation committees. National and European standardisation and certification offices will become more competitive on the international stage and their processes will remain world leading.

Germany will participate in European and international standardisation committees with digital sovereignty in mind. A policy of strategic standardisation is particularly necessary in regard to information and communications technology (ICT), software and AI. To achieve this, an interministerial committee on information and communications technology standardisation will

[35] Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020PC0823

[36] Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020PC0595

be set up. The aim of the committee will be to promote cyber security and to participate in European and global standardisation bodies. The stakeholders relevant to the main technology areas (federal ministries, private industry, researchers and standards organisations) will be involved.

Negotiations will be initiated at EU level for a horizontal, uniform legal framework for the placing on the market or the use of connected devices within the EU. Where necessary, this framework will be supplemented with special sectoral regulations. The Federal Government will play a key role in initiating these negotiations and will actively support the process. This will ensure that connected products brought into circulation in the EU will be sufficiently secure.

What impact are we expecting?

The creation of a uniform European regulatory framework for businesses will lead, among other things, to improved market access, as it will make products and services more easily comparable. Businesses will benefit from uniform EU-wide standards that reduce red tape and increase their competitiveness.

Standardised product quality and security will increase consumer trust. Interoperability between products and services can be improved by standardisation. Standardisation will also open doors to exports to the EU single market or other countries around the world.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Double regulation for businesses is kept to a minimum.
- Germany is actively contributing to drawing up an EU-wide standard, horizontal legal framework for cyber security and sectoral cyber regulations.
- An interministerial committee has been set up for ICT standardisation in cyber security.
- The number of stakeholders and areas of technology represented in the interministerial committee for ICT standardisation in cyber security has increased.

8.2.7 Promoting research and development into more resilient, more secure IT products, services and systems for the EU single market

Why is the objective relevant?

Today's IT security research is tomorrow's innovation. This type of research is essential for strengthening digital sovereignty and the resilience of IT systems. While objective 8.2.6 Creating a uniform European regulatory framework for businesses aims to foster targeted cooperation between government and industry experts, this objective will affect the general public.

What is our current position?

Germany and Europe have a strong scientific foundation in IT security research. The Federal Government's research framework programme on IT security, Self-determined and secure in the digital world 2015–2020, set a course for this in the early days. The follow-up research programme on IT security, *Digital. Sicher. Souverän.* was launched in 2021, driving IT security research in Germany resolutely and systematically forward.

The Federal Ministry of Education and Research provides funding to the ATHENE National Research Center for Applied Cybersecurity, the CISPA Helmholtz Center for Information Security and the KASTEL Institute of Information Security and Dependability, all of which are world leaders in IT security research. Other German institutions carrying out excellent research into IT security are the Fraunhofer Institute for Applied and Integrated Security (AISEC), the Fraunhofer Institute for Secure Information Technology (SIT), the Max Planck Institute for Security and Privacy, the CODE research institute at the Universität der Bundeswehr München in Munich and numerous other internationally visible research groups at universities and other institutions.

The Agency for Innovation in Cybersecurity is active on an interministerial basis, commissioning and funding ambitious research projects with considerable potential for innovation in the field of cyber security and associated key enabling technologies, with the aim of meeting Germany's domestic and foreign security needs.

Alongside the research community and major corporations, SMEs and start-ups are both the backbone of Germany's important *Mittelstand* (a core of medium and small firms) and are key innovators. The Federal Ministry of Education and Research supports research and transfer of knowledge in this important economic sector with the very successful programmes StartUpSecure[37] and KMU-innovativ (Innovative SMEs).[38]

Investment by security companies in developing existing and new products and services is often very limited due to the very small business eco system (the collection of companies working on

[37] Available in German at: https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/startup-secure

[38] Available in German at: https://www.bmbf.de/bmbf/de/forschung/innovativer-mittelstand/kmu-innovativ/kmu-innovativ_node.html

the same value creation chain), in particular for high-security products. This decreases still further as classification levels increase.

What do we want to achieve?

Our aim is for IT security research on emerging technologies and on cyber threats to deliver important, relevant findings. To achieve this, targeted funding will be provided to universities and other higher education and research institutions, as well as to businesses and public facilities carrying out research. At the same time, efforts will be made to attract and train new IT security professionals, and joint federal and state cooperation in research will be reinforced.

Fundamental IT security technologies will be made accessible as open technologies, making them transparent, comprehensible and easier to use.

A "networks protect networks" approach will be pursued, promoting networking among stakeholders in industry, the research community and civil society. The transfer of knowledge to industry will be guaranteed. Cooperation relationships among industry, the research community and government institutions will be promoted to help turn knowledge into marketable products or practical applications. With this in mind, incentives will be provided for spin-off companies. This will generate additional research findings and will allow synergies to be exploited.

It is strategically important to develop and roll out advanced technologies (for example fifth and sixth generation mobile communications networks) to maintain digital sovereignty both in Germany and the European Union. To this end, government will actively promote open basic technologies, especially open and secure standards for hard and software, and interoperable interfaces, and will introduce suitable regulatory approaches. This will establish a stronger technology basis for the entire value chain in the long term.

The Federal Government's IT security research programme, *Digital. Sicher. Souverän.* will continue to resolutely drive forward IT security research in Germany.

What impact are we expecting?

The risks that new threat situations and technologies pose for private industry, government and society will be reduced, and resilience to a constantly evolving threat situation will be bolstered.

The transfer of research findings, as recommendations for action and technologies, for example, and the commercial availability of IT security solutions will reinforce the IT security of private industry, citizens and the state. Achieving cyber security will be simpler and more economical for all.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The number of projects and businesses in research and the scope of funding for the Federal Government's research framework programme have increased.

- Standards and norms for open basic technologies have been developed with the help of funding and have been successfully field tested. They have, where appropriate, been recognised by standards or certification organisations. One example of this is Open RAN.
- IT security research in Germany is internationally renowned.
- Innovations resulting from our IT security research are increasingly used in practice and/or marketed by businesses and start-ups.
- Recommendations for action have been made on the basis of research findings.

8.2.8 Strengthening the security of future technologies and key enabling technologies through security by design

Why is the objective relevant?

Future technologies and key enabling technologies like AI, IoT and robotics are driving the ongoing digitalisation of products, services and processes. To ensure that the resulting push for innovation is not weakened by IT security risks, it is essential to take security considerations into account from the very start of the development process. Security by design systematically ascertains these considerations at the start of the development process and includes them in the design. This prevents or minimises the need to resolve security vulnerabilities at a later stage.

What is our current position?

The Federal Government has promoted security-by-design approaches for a number of years in its research funding. This support has been intensified recently with the promotion of trustworthy microelectronic and IT systems. Industry and the research community are focusing in particular on advancing suitable solutions for security-critical applications such as autonomous vehicles and Industry 4.0. However, the security-by-design approach has not yet been incorporated to a sufficient level in the development of digital hard and software products and services, particularly in the user environment. Security is still frequently seen as a secondary or peripheral characteristic of products and services, and is seldom used as a selling point. Higher quality standards for security in production and operation make products and services more expensive and thus less able to compete with products and services that are not secure. This leads to average or even poor IT security in many products and services.

What do we want to achieve?

Our aim is for a security-by-design approach to be used from the start in the development of products and solutions based on emerging and key enabling technologies.

To achieve this, we want the security-by-design approach to be well known to hardware and software developers. The security-by-design approach will be further reinforced in projects funded or commissioned for production by the state. Work will continue systematically on the planning and design of a comprehensive security architecture.

When new technologies are introduced as part of projects commissioned for productive implementation or funded by the state, the body responsible will in each case promote suitable risk reduction through security by design and a cyber security impact assessment. This will enable potential risks to be detected and reduced at an early stage in the development process. In this way, the Federal Government will promote the development and production of trustworthy IT systems.

Information on the manufacture and use of trustworthy IT will be available throughout the value creation chain in a way that fosters competitiveness. In addition, communication will be established with private sector stakeholders on research into and the development, production and operation of trustworthy IT. The private sector stakeholders involved will form a network and will discuss questions of technology, development tools and business models.

The finishing touch to the competitive provision of the required information will be infrastructure for the quality management of trustworthy IT, based on secure open-source hardware and software. This will promote the competitiveness of trustworthy IT systems.

What impact are we expecting?

By firmly establishing security characteristics as a design criterion in the development of hardware and software solutions based on emerging and key enabling technologies, system faults will be avoided from the outset and the scope for potential attack will be minimised. This will guarantee security in the use of key enabling technologies.

Enhancing the competitiveness of trustworthy IT solutions will in turn increase their market share, improving the general level of cyber security.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Security by design is increasingly included as a component of competitive tendering processes for projects funded or commissioned for production by the state.
- Requirements, criteria and standards have been set out that IT systems must meet to be considered trustworthy (including trustworthy electronics).
- Organisation, quality assurance and communication infrastructure has been established the length of the value creation chain for trustworthy IT systems. Work is under way on projects in a range of technology fields within the network for trustworthy IT that has been created by private sector stakeholders.
- The number of stakeholders involved in the network for trustworthy IT has increased.
- Trustworthy IT products are successfully placed on the market.

8.2.9 Providing IT security through quantum technology

Why is the objective relevant?

Development in the field of quantum technology is making rapid progress. This implies vast potential, but also new challenges, for cyber security.

Quantum technology exploits the special physical effects of single particles or groups of few particles. Quantum computers use this to create a new computing architecture, which can enable many complex problems to be solved much more efficiently. This can be helpful in optimisation problems, but it also poses a risk to certain cryptographic processes that are currently in use, and therefore to cyber security. Quantum key distribution uses the effects of quantum mechanics to enable two parties to communicate using cryptographic keys. This type of communication is theoretically protected from interception.

Quantum computers can solve a range of optimisation problems more efficiently than standard computers. However, they also have the potential to crack fundamental mathematical hypotheses on which cryptographic algorithms are based, which are currently widely used and which form the basis of our IT security. It is therefore necessary to develop cryptographic processes that cannot be cracked even by quantum computers (post-quantum cryptography) and to promote crypto-agility, which is the ability to replace modular cryptographic processes in operations with other processes.

In addition, quantum key distribution promises the opportunity, for example, to distribute cryptographic keys securely, enabling secure data transmission. This requires the physical technology, but also its integration into standardisation in the form of practical, secure system architecture. Digital sovereignty is also a very relevant factor in regard to quantum technology. The Federal Government should aim to ensure that it has expertise in the field of quantum technology, particularly in the key aspects of quantum computing, quantum communication and post-quantum cryptography. It is also vital that products from Germany or the EU are available.

What is our current position?

In 2020, the Federal Government resolved to invest an additional two billion euro in funding for quantum technology, and a quantum computing road map[39] was drawn up.

The Federal Ministry of Education and Research funds research and development into enabling technology, its transfer into practice, and several projects looking into developing new quantum processors. A competition for establishing hubs in the form of groups of different stakeholders and for constructing complete quantum computing systems will create new research and development structures. The Federal Ministry of Education and Research also funds research

[39] Available in German at: https://www.bundesregierung.de/breg-de/aktuelles/quantencomputing-1836542

projects into post-quantum cryptography. The BSI has published the first recommendations on algorithms for post-quantum cryptography and for the migration to quantum-safe cryptography.

What do we want to achieve?

Our aim is for systems based on quantum technology to be deployed to provide a high level of IT security, and for the use of these systems to be promoted.

Research will be carried out into the effects of quantum computing on cyber security and technological innovations will be used for greater cyber security. This includes, for example, research into the use of quantum technology (quantum computers and sensors) in side-channel analysis.

An important prerequisite for deploying quantum key distribution (QKD) in highly secure networks is the certifiable security of products. The Federal Government will develop a Common Criteria Protection Profile. It will accompany the compilation of additional necessary technical specifications with studies and will investigate quantitative and qualitative aspects of existing proofs of security.

The potential increase in security occasioned by QKD will be demonstrated not only in research prototypes, but also in real deployment situations, to show that it works in practice.

Preparation will begin for replacing algorithms that are at risk from quantum computing with new, standardised algorithms.

What impact are we expecting?

Exploiting the potential of, and minimising the risks created by, quantum technology systems will ensure a high level of IT security to the long-term benefit of government, private industry and society. In addition, Germany's technological sovereignty in the field of quantum communication will be reinforced.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- In the field of quantum computing, by 2025 computers with processors of a minimum of 100 qubits are ready to use, based on sovereign technology from Germany and Europe, and are available for application testing to check their security levels.
- In high-security fields, the changeover to quantum-safe cryptography has begun.
- The urgency of the change to quantum-safe cryptography is generally accepted by the state, private industry and society as a whole, and this change has been initiated in key areas. Pilot infrastructures are in place, involving partners from the different areas.
- Quantum communication technologies and solutions from German and European providers are available to the state, private industry and society.
- The feasibility study on quantum computers is ongoing and is updated regularly.

8.2.10 Harmonising testing and approval processes with innovation cycles (time to market)

Why is the objective relevant?

New IT products and services in the areas of smart home, automotive technology, medical technology and energy, among others, are brought to market within extremely short innovation cycles and facilitate the increasing connectivity of all areas of life, particularly in regard to IoT applications. It cannot be ruled out, particularly for new software and hardware products, that not all security aspects are taken into account or are recognisable. Criminals try to exploit potential vulnerabilities to infiltrate systems or to use them for criminal purposes. Aside from systematic law enforcement, the state should support businesses in creating products that are more secure and less vulnerable from the start.

What is our current position?

Government agencies must be in a position to understand the structure and functions of new IT products and services and to set out suitable requirements for these technologies to ensure a minimum level of security when using them. This calls for restrained action, so that we can reap the full benefit of innovation potential and manufacturers are more likely to accept new testing processes.

What do we want to achieve?

Our aim is for government agencies to be competent, trustworthy service providers which are in a position to make reliable assessments of the security of new technologies and, on that basis, to set out regulatory standards, to provide information and to make recommendations.

New testing and approval processes that take into account the rapid innovation cycles in the IT industry (time to market) will be put in place, but with no impact on the quality of the processes. There will be growing acceptance for including security characteristics.

So that alongside the appropriate certification of products and services acceptance of information security in the digital world also increases, progress will be made on developing new certification processes. Products and services will be certified appropriately, finding a balance between minimum standards and use of resources. This will ensure IT security enjoys a high level of acceptance as an integral element of digital products and services.

To ensure that this succeeds alongside official government assessments, suitable accreditation will be available for certification and conformity assessment bodies. These may be based on existing Cybersecurity Act schemes, but may also be based on the accreditation rules of the German accreditation body Deutsche Akkreditierungsstelle GmbH (DAkkS).

What impact are we expecting?

The inclusion of security characteristics will be more readily accepted with the help of new testing and approval processes.

The appropriate certification of products and services will mean that users will be better protected from cyber attacks. At the same time, the power of German and European industry to innovate

will be safeguarded and strengthened for the long term. As part of this, IT security will become established as a mark of quality for German and European providers. The range of qualitative testing and approval processes available will increase.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Technical guidelines are available for new fields of application. The content of these guidelines is quickly incorporated into the work of standardisation organisations.
- New testing, approval and certification processes (rapid security certification, IT security labels, 5G, medical products, (partially) autonomous vehicles, energy, market supervision) have been established.
- Certification has been expanded to new markets.
- The number of certificates issued has increased.
- Standards, technical guidelines and test specifications have been drawn up for the smart home and consumer IoT markets.

8.2.11 Improving the protection of critical infrastructures

Why is the objective relevant?

Critical infrastructure refers to organisations or facilities of major importance to the community. Its very definition means that securing this type of infrastructure to prevent failure or disruption is a key objective and is extremely important for the functioning of society and for the protection of individual basic rights.

What is our current position?

A legal framework for cyber security in critical infrastructures has been in place for several years in the form of the BSI Act and the ordinance defining critical infrastructures (*Verordnung zur Bestimmung Kritischer Infrastrukturen*)[40] and is continually being enhanced. In line with legal provisions, operators of critical infrastructures must regularly submit evidence to the BSI of technical and organisational measures they have taken to ensure IT security. In exchange, these companies are included in a trusting exchange of information with the BSI. At federal and state level, the critical infrastructure protection coordination offices at state level and the critical infrastructure protection coordination office working group involving federal and state governments provide important structures for dealing with critical infrastructure protection concerns including cyber security in a coordinated, networked fashion as part of an all-hazard approach.

The National Strategy for Critical Infrastructure Protection

Critical infrastructure protection focuses on those systems, institutions and facilities which are particularly important for the provision of services that are key to society. In June 2009, the Federal Cabinet passed the National Strategy for Critical Infrastructure Protection, or CIP Strategy, to create a joint framework for the activities that were already under way and to set the strategic course for coordinating tasks among the ministries. The strategy's key elements include the "all-hazard approach", which lists both cyber security and "physical protection" as partial aspects of the overall protection of critical infrastructures.

The strategy is available at https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html.

What do we want to achieve?

Our aim is for the state and the private sector to work closely together to protect critical infrastructures and to be able to react quickly to cyber security incidents. Threats from cyber sabotage will be recognised at an early stage. Relevant information concerning cyber security incidents will be available immediately to the companies to be protected and the responsible authorities.

Checking the evidence submitted and any improvements that may be called for will make it possible to infer the improvement in cyber security in the companies in question. It is important

[40] Available in German at: https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

to replace reactive measures with proactive measures, for example by maintaining a comprehensive overview of the cyber threat situation, including the possibility of detecting and warding off potential cyber attacks (or preparations for attacks) on critical infrastructures.

The requirements for protecting critical infrastructures against IT outages and cyber attacks will be tightened, and operators of critical infrastructures will be given more support in implementing these requirements. In case of cyber or IT incidents, support from the authorities for operators of critical infrastructures will be prioritised. Existing minimum requirements for critical infrastructure operators in regard to safeguarding IT systems will be based on the latest technology. In view of the constantly evolving threat situation, requirements will be under continuous review and will be adjusted as necessary. This can be assessed based on evidence submitted, with further confirmation possible using on-site checks.

Critical infrastructure operators will be included on a voluntary basis in a nationwide exchange of information. This will improve the early detection of malicious activities by cyber actors. Critical infrastructure operators will be able to react more quickly to potential cyber threats against them thanks to early warnings. The existing warning options offered by the BSI for critical infrastructure operators will also be open to other companies and institutions in the critical infrastructure sector.

What impact are we expecting?

The secure provision of critical infrastructure services, which include the supply of electricity, water, food and communication, the health care system and many others, is a fundamental prerequisite for basic services and for the functioning of government, the economy and society. The successful protection of IT components in critical infrastructures will prevent risks, ensuring stable societal and economic development.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The framework for carrying out on-site checks has been expanded. By 2026, the necessary changes have taken place or are in the pipeline.
- The Federal Government has specified the best available technology for further critical infrastructure branches where this has not already been defined based on EU-wide or international standardisation systems.
- Critical infrastructure operators can use a national exchange of information on cyber attacks to strengthen their own defence.

8.2.12 Cyber security certification

Why is the objective relevant?

Certification and conformity assessments of the security aspects of products, services and processes create trust and comparability, and promote efforts to achieve a higher level of cyber security.

What is our current position?

German IT security certification is recognised around the world.

The Cybersecurity Act[41] develops and introduces new certification schemes. The BSI has taken up position as a reliable and trustworthy partner for the verification of exacting requirements for cyber and information security. However, in the international context, it is in growing competition with other national bodies.

What do we want to achieve?

Our aim is to actively pursue the implementation of the cybersecurity certification framework provided for in the Cybersecurity Act and to push on with the drawing up of certification schemes. National standardisation and certification offices will become more competitive on the international stage so that they remain world leading. In response to the requirements of the Cybersecurity Act and national certification projects, the BSI will ensure it is equipped to provide sufficient certification options. We intend to modernise the range of certification available and to offer attractive certification options that take time to market into account. In its function as the national cyber security certification authority, the BSI will actively contribute to developing and designing certification schemes in accordance with the Cybersecurity Act.

Cybersecurity Act

The Cybersecurity Act came into force in June 2019 with the adoption of Regulation (EU) 2019/881. As well as strengthening the European Union Agency for Cybersecurity (ENISA) and further developing the agency's tasks, the Act also introduces an EU-wide cyber security certification framework. The aim of this is to harmonise regulation and the associated certification in the field of cyber security across Europe and to prevent a fragmented single market. Taking the assurance levels 'basic', 'substantial' and 'high' into account, special certification schemes are being drawn up and implemented on a step-by-step basis. These are applicable EU-wide. They are recognised by all member states, and they replace existing national and/or multilateral schemes certifying the same things. One example of this is the implementation of the SOG-IS MRA, which transfers what are known as the common criteria into a harmonised European scheme. Application of the schemes in the CSA is essentially voluntary. However, special sectoral regulation can be applied that requires relevant certification or EU statements of conformity.

[41] Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019R0881

What impact are we expecting?

The BSI will build on its outstanding reputation as a certification office and will become established as the national cyber security certification authority. Active use will be made of the certification options offered by the BSI and private providers with a view to building trust and working towards a high level of cyber security in Europe. Businesses and other potential applicants for certification will make increasing use of certification opportunities even when there is no legal requirement to do so.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The BSI remains the national certification authority with the highest number of IT security certificates issued worldwide.
- The certification schemes announced in the CSA have been adopted and are valid: Common Criteria (EUCC), Cloud Services (EUCS), IoT and 5G.
- Rapid certification has been harmonised at international level and launched as a certification scheme as part of the CSA.
- The number of certified products monitored by the national authority for cyber security certification has increased. The number of companies and organisations applying baseline IT security has increased.

8.2.13 Securing the telecommunications infrastructure of the future

Why is the objective relevant?

The current fifth generation (5G) mobile communications network and the upcoming sixth generation are characterised by virtualised network components. Central network functions are carried out entirely by software. In some cases, this software can run on generally available hardware. The aim is to keep the broader scope for attack resulting from virtualisation as small as possible, and to control residual risks.

European manufacturers of network technology face stiff competition. Many mobile phone technology providers today are increasingly based in Asia and the USA, with a growing trend towards oligopoly markets. Established providers in Germany and Europe must be strengthened or expanded so as to ensure that the further loss of expertise does not force Germany and Europe to become dependent on providers in Asia and the USA. Using open basic technologies such as Open RAN, a vendor-neutral mobile communications architecture, can help to reduce dependence on a few dominant network equipment providers; to facilitate entry onto the market of new European vendors, including smaller ones; to foster innovation; and to provide greater security of networks due to increased transparency and control. Open RAN therefore directly contributes to strengthening the digital sovereignty of telecommunications networks and ensuring their cyber security.[42]

What is our current position?

Mobile communications networks are already critical infrastructure according to the BSI ordinance defining critical infrastructures. There is also a catalogue of security requirements for telecommunications networks. The Federal Government wants to implement a technology- and vendor-neutral approach in order to increase the security of the communications network considerably without shutting specific network component providers out of the 5G network build-out in advance. Regulation to this end was included in the Second Act to Increase the Security of Information Technology Systems, IT Security Act 2.0 (*Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*) in regard to components termed critical (products that are used in certain critical infrastructures).

Germany is well placed to carry out research and development in the telecommunications field and has a good reputation in this area. However, there is room for improvement in terms of translating this research into products that can be marketed by German companies.

What do we want to achieve?

Our aim is to use a holistic approach to continuously monitor the security and controllability of telecommunications networks – in particular 5G, future 6G and space-based infrastructure, which are the backbone of digital transformation –, adapting them to new threats. As regards 6G

[42] See strategic objective 8.2.7 Promoting research and development into more resilient, more secure IT products, services and systems for the EU single market.

technology, early and intensive efforts will be made to achieve a high level of security. The Federal Government will support research into and development of a comprehensive 6G system. This is intended to create a foundation for stakeholders from Germany from which to exert a strong influence on 6G standardisation and to bring associated technologies to market. Government will actively promote suitable open basic technologies, especially open and secure standards for hard and software, and interoperable interfaces, and will introduce suitable regulatory approaches.[43]

German and European network infrastructure and cloud providers will be supported, as will the analysis and investigation of new cyber security risks in these networks.

Mechanisms will be developed and implemented for German companies to transfer research results to marketable products that will be manufactured in Germany on a long-term basis. This will give security standards that are "made in Germany" a position on the global market.

What impact are we expecting?

Promoting German and European providers and developing Germany's expertise in investigating new cyber security risks will safeguard Germany's capacity for self-determined action in cyberspace.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The availability of the telecommunications network and its resilience to disruption and attacks have increased.
- Telecommunications are confidential apart from those exceptions provided for by law; the secrecy of telecommunications is actively protected.
- The integrity of the telecommunications network is assured.
- Software and hardware of critical components are checked before deployment to ensure that vulnerabilities can be recognised and resolved.
- German and European companies are represented in the relevant standardisation organisations and have a considerable influence on the standardisation of future telecommunications systems, with an increased number of contributions to standards.
- The number of (first) applications for standard essential patents in Europe has increased.
- The proportion of standard essential patents from Germany in international standards has increased.
- The number of German and European network components in telecommunications networks has increased.
- Technology roadmaps for the future 6G standard were taken into account so that effective, transparent criteria and benchmarks could be defined at an early stage in a safety catalogue for 6G network components.

[43] See strategic objective 8.2.6 Creating a uniform European regulatory framework for businesses.

8.3 Action Area 3: Strong and sustainable cyber security architecture for every level of government

Germany has a strong cyber security architecture. Federal Government institutions work closely together to provide security in cyberspace. In recent years, the close dialogue between authorities at federal and state level that has taken place for many years already has been expanded in key areas. This cooperation has a single goal: to enable everyone in Germany to use the digital domain with complete freedom, while being able to rely on the highest possible level of safety.

However, the breakneck speed of development in the cyber domain means that state actors are constantly facing new challenges:

- The penetration of digital technology into every area of life means that the importance of cyber security for the functioning of society, government and the economy is increasing.
- New technological developments can provide new scope for attacks, but also new opportunities for defence; we must exploit these.
- The willingness of other states to carry out cyber attacks for purposes of espionage, sabotage and gaining political influence is rising.
- Attackers are growing increasingly professional, constantly refining the methods and techniques they use for cyber attacks.

These challenges can only be countered effectively if the cyber security architecture in Germany undergoes an ongoing process of review and refinement:

- The structures and processes involved in interaction between state institutions must be continuously assessed and, if necessary, adapted so that any barriers to effective cooperation can be removed. Along with this, cooperation between federal and state governments must be continually enhanced and interfaces to stakeholders outside the (federal) administration taken into account. All tasks and responsibilities within the cyber security architecture must be clearly defined.
- Continuous checks must be carried out of whether state institutions have sufficient expertise and authority to guarantee the security of citizens, private industry and the state in the cyber domain too. If regulatory or skills gaps are identified, these must be closed. Authority that is no longer necessary should be revoked.
- In addition, new ways and means must be found of recognising new challenges in cyberspace quickly and overcoming them effectively.

We, the Federal Government, have set the following strategic objectives so that we can fulfil these tasks.

8.3.1 Improving the options available to the Federal Government for threat prevention in case of cyber attacks

Why is the objective relevant?

In general, Germany's federal states are responsible for threat prevention. However, cyber attacks tend to affect more than one federal state; often, they have an international dimension. Protecting against cyber attacks requires an extremely high level of technical know-how. To be most effective, this requires a consolidation of expertise in a small number of authorities. If cyber attacks originate abroad, foreign and security policy aspects must be taken into account in defending against such attacks; responsibility for these aspects lies with the Federal Government.

What is our current position?

According to current constitutional law, the Federation only has special jurisdiction over threat prevention in certain areas, such as national self-protection, international terrorism, border protection, and security in the territory belonging to the federal railways. In all other cases, the federal states have jurisdiction over threat prevention, which means that the Federation itself cannot take threat prevention action even in case of major, complex and/or international cyber threat situations that call for a solution at national level and often also require international coordination. This assignment of responsibilities is not appropriate for the current threat situation in the cyber domain, which is likely to deteriorate over time. It is not possible to effectively counter cyber threats in Germany in this way in the long term.

What do we want to achieve?

Our aim is to enshrine in the Basic Law extended legislative and administrative competence for the Federation in terms of countering risks from particularly severe and significant cyber attacks on IT systems and networks. On that basis, we will clarify whether the federal (security) authorities require new or extended tasks and authority to exercise this power.

What impact are we expecting?

Creating extended legislative and administrative competence for the Federation in matters related to preventing threats from particularly severe and significant cyber attacks will expand the possibilities for effective cyber threat prevention. Active steps can be taken against the causes behind serious cyber attacks so that, in the best case scenario, damages can be completely prevented. This will increase cyber security at every level of government.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- By amending the Basic Law, the options available to the Federation to counter threats from particularly severe and significant cyber attacks have been extended.
- The federal (security) authorities have been assigned additional tasks and powers in the field of cyber threat prevention.

8.3.2 Equipping the technical and operational divisions of the BSI for the future and creating a network for them

Why is the objective relevant?

The BSI must continually adapt its capabilities for the technical and operational detection of and reaction to cyber security incidents to keep pace with the very dynamic threat situation. To do so, it needs operational units that have sufficient technical, human and financial resources and that work closely in an effective network with their counterparts in other national bodies and bodies at EU, state, private industry and research community level.

What is our current position?

The BSI's technical and operational divisions consist of the National IT Situation Centre, the Computer Emergency Response Team for federal agencies (CERT-Bund), the Mobile Incident Response Teams (MIRTs) and the BSOC.

The National IT Situation Centre pools together and evaluates current observations and activities in cyberspace with the aim of detecting threat situations early and reacting quickly. The centre works closely with the CERT-Bund as the central office at the BSI for preventive and reactive measures in case of security incidents. The CERT-Bund belongs to the network of federal and state CERTs (VCV) along with the state CERTs, and is also part of the national network of CERTs with teams from major organisations and corporations.

The MIRTs provide on-site support for reacting to serious cyber security incidents. There is a growing need for support of this kind. The BSOC is mainly tasked with detecting and evaluating security incidents affecting the government network and federal IT systems.

What do we want to achieve?

Our aim is for the National IT Situation Centre and the state, private sector and research community monitoring units to expand their information channels and increasingly synchronise any relevant information they obtain, so that they can create as comprehensive a picture of the current situation as possible.[44] This will enable federal, state, industry and research community CERTs to evaluate incidents all the more effectively, to share their findings and to react. To reinforce this, the BSI will increase its capacity for analysis, share more information and findings with its partners, and compile its information in standardised, targeted formats. Networking structures will be regularly evaluated and improved.

The MIRTs will be provided with additional technical, human and financial resources, allowing them to continue responding to the growing need for professional on-site support for critical infrastructures and institutions of special public interest.

[44]For more information on the exchange of information in the National Cyber Response Centre, see strategic objective 8.3.4 Developing the National Cyber Response Centre

The BSOC will work closely with the state bodies responsible for detection tasks. A network of SOCs will be considered to supplement the VCV, with each network carrying out separate, distinct functions. At the same time, the BSOC will be established as the national coordination office for the Cyber Shield planned by the EU Commission.

What impact are we expecting?

The improvement in technical, human and financial resources and networking of the technical and operational divisions of the BSI means that they will be equipped to act quickly and effectively. Cyber security incidents in the government networks and in the federal administration will be detected quickly and reliably. Potential damages caused by cyber attacks will be minimised. Those within and outside of the federal administration will be given the best possible support in dealing with cyber security incidents. It will be possible to detect and counter new methods of attack and a higher number of cyber attacks. The exchange of information between federal and state levels and through the EU Cyber Shield will increase the detection rate of security incidents and will tangibly reduce the likelihood of successful attacks.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The BSOC has been established as the national liaison office for the EU Cyber Shield initiative.
- The BSOC cooperates with the state agencies responsible for detection.
- The MIRTs can respond rapidly and effectively to calls for support for critical infrastructures and institutions of special public interest.

8.3.3 Strengthening institutionalised cooperation between the BSI and the states

Why is the objective relevant?

Cyberspace is intricately networked across international borders. Close cooperation between federal and state governments, also involving local governments, is crucial for providing a uniform level of cyber security where possible, and for reacting effectively to cyber threats. Cooperation must be institutionalised to ensure the success of the intensive ongoing information, coordination and support processes this requires.

What is our current position?

There are tried and tested structures for federal and state cooperation in the areas of cyber crime and cyber espionage. In addition, the BKA and the BfV, with their respective hub roles, are also key pillars of the integrated federal cyber security architecture.

The BSI also has platforms in its remit that serve federal and state cooperation, particularly in the field of preventive self-protection for public administrations. Similarly, the cyber security working group of the Standing Conference of the Interior Ministers of the Länder in the Federal Republic of Germany has proved its success as a platform for federal and state exchange. The BSI has additionally been assigned the legal duty of supporting the states. The division of powers between the Federation and the states provided for in the Basic Law limits this support to supplementary administrative assistance in individual cases.

What do we want to achieve?

Our aim is to rapidly strengthen the effective cooperation between the BSI and the states through the signing of binding bilateral cooperation agreements which set forth the priorities for joint involvement. These cooperation agreements will bring together the areas in which the BSI already cooperates or will cooperate in future with the state in question in a single agreement and will provide a structured framework for this cooperation which will enable planning.

Institutionalised cooperation between the Federal Government and the federal states will be deepened. To that end, the BSI will also become a hub for federal and state cooperation in the prevention of cyber crime, creating a third pillar in the integrated federal cyber security architecture: it will take up position alongside the BKA, which already plays this role in the German police sector, and the BfV, which does so in the German domestic intelligence services. Federal authorities which serve as hubs will facilitate organisational connections between different federal and state authorities for ongoing information exchange, coordination and support.

What impact are we expecting?

Deeper federal and state cooperation based on bilateral cooperation agreements will lead to more effective deployment of government resources thanks to coordinated activities and pooling of skills and expertise. It will be possible to target groups in government, the private sector and society more broadly and more specifically. The transfer of knowledge and expertise between the Federation and the states will increase.

Developing the BSI into a hub will be a further step towards an effective cyber security architecture. The BSI's hub function will be based on the cooperative, complementary division of tasks between federal and state agencies. This will create a framework for a more complete exchange of information and ongoing, regular mutual support. This will lead to better prevention, detection and reaction capabilities in the face of cyber threats, improving cyber security at all levels of government.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The BSI has signed bilateral cooperation agreements with the states and joint projects are under way.
- Following changes to the Basic Law and subsequent amendments to ordinary national law, the BSI has been developed into a hub for federal and state cooperation.

8.3.4 Developing the National Cyber Response Centre

Why is the objective relevant?

Cyber threats and the motives and goals of cyber attacks are often not immediately clear. This means that depending on the situation, it regularly happens that only some of the responsible authorities, and sometimes only the individual institutions which are affected, are aware of cyber attacks and cyber threats. In addition, issues that are relevant for all levels of government are not always immediately recognised as such. This makes it more difficult to react appropriately to cyber incidents.

What is our current position?

The National Cyber Response Centre was set up in 2011 as a cooperation and information platform. Current participating organisations are the Federal Office of Civil Protection and Disaster Assistance (BBK), the Federal Office of Military Counterintelligence (BAMAD), the BSI, the BfV, the BKA, the BND, the Federal Police Headquarters (BPOLP) and the KdoCIR.

The Centre is a key component of Germany's cyber security architecture and must constantly adapt its way of working to encompass the latest developments. In 2019, cooperation within the National Cyber Response Centre was completely overhauled. Further measures were taken to improve the capacity for a coordinated, cooperative response to situations affecting all levels of government and to enhance the exchange of information.

What do we want to achieve?

Our aim is for the role of the National Cyber Response Centre as a central cooperation, communication and coordination platform for the relevant (security) authorities to be reinforced in line with the evolution of the threat situation. The basis for information-sharing between authorities will be adjusted, primarily to strengthen the interministerial exchange of information on cyber attacks and cyber threats; with the same goal in mind, communication will be intensified and further partners (particularly the states) will be integrated into the work of the National Cyber Response Centre, whenever useful.

Reporting by the National Cyber Response Centre will be expanded and improved through more in-depth information-sharing, the use of technical systems for the processing, evaluation and display of situation information, and better needs-based analyses. Digital sharing, including of information at higher classification levels, will be possible among all participating institutions. Evaluation by the Centre will be accelerated, and it will be possible to obtain an up-to-date, coordinated overall picture of the cyber security situation. New reporting formats used by the Centre will provide a comprehensive, up-to-the-minute overview of cyber attacks in, and cyber threats to, Germany. This will include an efficient exchange of information with the private sector. The transition from prevention to defence in complex cyber situations will be identified.

What impact are we expecting?

Information on cyber security incidents will be communicated more quickly to all relevant authorities, which will allow complex cyber situations to be coordinated better among the different authorities and ministries involved.

Expanding the National Cyber Response Centre by involving selected additional institutions, agencies or organisations will help open up additional sources of information or options for action.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The basis for the exchange of information among authorities in the National Cyber Response Centre has been updated.
- Cyber security incidents and cyber situations are processed quickly and effectively.
- A comprehensive, up-to-date cyber situation report is available at all times.

8.3.5 Strengthening cyber and information security in the federal administration

Why is the objective relevant?

The federal administration is undergoing a process of digital transformation. A digital administration is essential for a functional, efficient and modern government. At the same time, the state is increasing the proportion of services it offers in digital format to the private sector and the public. In this area, too, cyber and information security is indispensable for the provision of functional, trustworthy digital government services.

What is our current position?

The federal administration's information security management is based on the Cabinet guideline for information security in the public administration (UP Bund). This guideline sets out the binding requirements for the protection of information processed by the public administration and the IT systems and services and communications network infrastructure used to do so. Among other things, it makes it obligatory for federal authorities to comply with baseline IT security and the minimum standards drawn up by the BSI. According to UP Bund, interministerial projects must ensure that information security is adequately taken into account at an early stage, which means during project initiation and planning. The BSI is to be involved in an appropriate advisory role.

What do we want to achieve?

Our aim is to strengthen the federal cyber security architecture at the strategic level. At operational level, a centre of excellence for federal operational security advisory services will be set up at the BSI to support the ministries in implementing security projects. We will also strengthen the position of information security officers in the federal administration by creating a legal basis for the role.

What impact are we expecting?

We will improve and strengthen existing information security management in the federal administration and on-site support from the BSI for the information security officers in the different federal authorities. We will also ensure that the BSI is involved in federal digital transformation projects at an early stage. In this way, information security will become a natural component of the digital transformation of the federal administration.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The legal basis has been created for the role of information security officer in the federal administration.
- Existing roles and interfaces in information security management have been examined to find potential for improvement. A concept has been drawn up for the needs-based expansion of these roles and interfaces, or the development of new roles, with a view to

increasing cyber and information security and improving cooperation among the (ministerial) information security officers at Federal Government level.

- Cooperation among IT security officers in federal ministries has been intensified considerably. To this end, measures have been taken at institutional level and in terms of the substance of cooperation.
- The BSI's centre of excellence for federal operational security advisory services has been established and has started work.
- A targeted programme to strengthen the cyber and information security of the Federal Government has been agreed on among the ministries and adopted.

8.3.6 Stepping up cyber security associated with elections

Why is the objective relevant?

Universal, direct, free, equal and secret elections are the basis of our democracy. The digital transformation knows no bounds, however. The internet is a source of information for forming political opinions, social media are used as an election campaign tool, and the preliminary election results are even transmitted digitally. This means that protecting elections is also a cyber security challenge.

Moreover, specifically in the run-up to elections there is an increased risk of operations by foreign intelligence services aimed at influencing election results. Events in other countries highlight the ability and the basic willingness of malicious actors to try and influence election results by publishing compromising information obtained through spying, or even information that has been manipulated.

What is our current position?

The federal authorities raise awareness among the relevant stakeholders of cyber risks associated with elections, and provide advice on information security. The BSI draws up security requirements on behalf of the Federal Returning Officer aimed at protecting the transmission of results of federal elections. The intelligence services are responsible for investigating cyber attacks intending to influence elections. They serve as an early-warning system.

What do we want to achieve?

The use of digital technology in election processes and the surrounding infrastructure has increased steadily, making them increasingly vulnerable. Our aim is therefore to step up cyber security associated with elections.

The federal authorities will support the relevant stakeholders with cyber security concerns related to elections. In each area of responsibility, they will analyse risks, identify security requirements and serve as points of contact in the political domain for cyber security concerns in regard to elections.

What impact are we expecting?

Elections will be protected thanks to an appropriate level of security achieved through general prevention measures, preventive intelligence gathering, detection and reaction. The political sphere will be aware of the cyber threat situation in regard to elections and will be able take appropriate preventive measures.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Recommendations for action are available which are continually adjusted to keep up with current developments. Advisory services are available for election officers at federal and state level.

- Measures have been taken to raise awareness among target groups in the political sphere of cyber security issues associated with elections.
- A well-founded cyber threat situation report exists specific to the issue of elections. The report lists malicious actors, their motives and their modus operandi.

8.3.7 Ramping up law enforcement in cyberspace

Why is the objective relevant?

The number of computer systems and terminal devices affected by cyber crime is not the only thing that is increasing. The professionalism of perpetrators is too. On the one hand, offenders continue to try to infect as many computers as possible with malware with as little effort as possible to steal account data and passwords, for example. On the other, we see more and more extremely well-prepared, highly organised cyber attacks on selected targets (for example private companies or critical infrastructures) where the damage caused to those affected is potentially much greater. At the same time, current technical developments such as automotive IT and IoT create new trends in crime and opportunities for criminals.

Faced with this evolving threat situation in cyberspace, federal and state security authorities must be able to carry out their law enforcement duties just as well in the digital world as in the real world. Officers need to have sufficient powers to be able to protect the people and prosecute offences equally in either sphere.[45]

What is our current position?

Computer crime is regulated under sections 202a et seqq., 263a, 269 et seq. and 303a et seq. of the German Criminal Code (*Strafgesetzbuch*, StGB). In recent years, a number of proposals to amend and revise computer crime legislation have been submitted and discussed, including several legislative proposals from the Bundesrat.

What do we want to achieve?

Our aim is for federal and state security authorities to have sufficient powers to carry out their law enforcement duties just as well in the digital world as in the real world. Their powers will therefore be continually reviewed and will be adjusted as necessary in response to new technical developments. As part of this, there will be a review of whether investigative measures such as telecommunications surveillance and online searches should be used when investigating computer crime.

In addition, current computer crime legislation will be examined to assess whether reform is necessary.

What impact are we expecting?

The security authorities will remain able to do their job successfully in the digital age. They will be able to react appropriately to new trends in crime and the increased potential threat in cyberspace.

[45]For more information on the topics of international law enforcement and the fight against cyber crime, see also the strategic objective Strengthening international law enforcement cooperation and combating international cyber crime.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Powers under the Code of Criminal Procedure (*Strafprozessordnung*, StPO) satisfy requirements in practice.
- Legislative proposals have been submitted for amendments to the Criminal Code, if a review considered this to be necessary.

8.3.8 Expanding central skills and services of the BKA for combating cyber crime

Why is the objective relevant?

One of the current tasks of the BKA is to support the federal and state police forces by providing operational data and by making the latest technology in criminal policing available as a package. Cyber crime is still increasingly characterised by attacks that take place in waves over a fixed time period, with the number increasing and then decreasing again, affecting victims in several federal states or all over the country. Extensive coordination of all the investigating authorities involved is necessary to detect the relationship between the attacks.

What is our current position?

The BKA rolled out its CyberToolBox in 2019. This has since become an established operational information portal, providing information, data and tools. The tools and data sets provided in the CyberToolBox have been expanded in stages since its launch. More than 5,000 law enforcement agents currently use the tools provided. Within a 12-month period, it was possible to connect more than 8,000 isolated cases that had been detected in the federal states where the crime or perpetrator structures matched.

The BKA supports federal and state police offices in coordinating and/or carrying out central investigations related to crime waves.

What do we want to achieve?

Our aim is to improve both the quality and the quantity of information, skills and tools exchanged between the BKA and federal and state police offices in line with existing legislation. The CyberToolBox will be enhanced and will to a great extent meet the states' needs for data-based operational information and support. It will provide the states with access to all of the information, data and tools related to this area of crime that they need. A nationwide community of cyber crime investigation agencies will foster the direct, efficient exchange of operational and investigation-related findings and methods.

If one or more federal or state police offices or the BKA detect a crime wave, the authorities listed above will coordinate central investigations. This type of investigation will become more widespread in the future.

What impact are we expecting?

Expanding the scope of functions and services of the CyberToolBox will increase user numbers and will mean a greater amount of operational data transmitted to the BKA. As a result, the BKA will be able to carry out the tasks required for its hub function.

Where crime waves emerge, central investigations will facilitate a needs-based distribution of workload among the police offices involved and contribute to effective investigations. In particular, it will prevent work being duplicated.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Central investigations are used more often.
- CyberToolBox user numbers have increased.
- The number of specialist enquiries to the CyberToolBox has increased.
- The rate of hits found and information provided by the CyberToolBox has increased.
- The amount of data provided via the CyberToolBox has increased.

8.3.9 Providing security through encryption, and security despite encryption

Why is the objective relevant?

Growing numbers of communication channels and data storage services are protected by end-to-end encryption. Secure encryption is an essential tool for protecting the basic rights and the digital security of government, the private sector and society. However, criminals also use encryption to prepare and commit offences. Encryption makes accessing and analysing the content of communication as part of lawfully ordered interception of telecommunication extremely difficult or even impossible. This type of access and analysis is a key source of information for authorities investigating extremely severe offences and organised crime.

Based on the principle of security through encryption, and security despite encryption, therefore, privacy and communication security must be protected with the help of encryption. At the same time, however, the responsible authorities must be provided with options for lawful access to data for legitimate and clearly defined purposes in their efforts to combat serious and/or organised crime, child sexual abuse material, and terrorism, including in the digital domain, while acting within the rule of law.

What is our current position?

To date, the operational and technical challenges associated with the compensatory measures established for information technology surveillance (interception of telecommunication at the source) and online searches have meant that these have in practice been limited to individual cases.

To ensure that the security authorities remain in a position to carry out their legal duties in full, new strategies will be necessary for unencrypted access to the content of communication that was originally encrypted.

In December 2020, the Council of the European Union adopted a resolution on encryption, highlighting the need for the principle of "security through encryption and security despite encryption". A dialogue with technology companies is required to find a technology-neutral approach to compensatory measures for telecommunications surveillance which are in line with the constitutional right to protection.

What do we want to achieve?

Our aim is to put in place the necessary conditions to enable the responsible authorities to gain lawful access to data for legitimate and clearly defined purposes in their efforts to combat serious and/or organised crime, child sexual abuse material, and terrorism, while at the same time protecting privacy, basic rights and security of communication.

To achieve this, technical and operational solutions will be developed to provide lawful access to content from encrypted communication. The process will involve close initial coordination with service providers, other stakeholders affected, and all responsible authorities. To prevent abuse of this solution both in Europe and worldwide, technical, organisational and legal measures will be incorporated.

What impact are we expecting?

The German security authorities will be able to make effective use of the technical possibilities for telecommunications surveillance provided for by law, including for encrypted content. Telecommunications surveillance will remain a key component of investigation and intelligence gathering. Effective law enforcement and rapid threat prevention in serious and extremely severe offences, along with intelligence gathering in specific cases, will therefore remain possible. It will also remain possible to fight organised crime and terrorism effectually, among other areas of crime.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The objective of a European approach with reference to the Council Resolution on Encryption, with a focus on a technology-neutral approach and ongoing dialogue with service providers, has been established.
- Technical and operational solutions for lawful access to content from encrypted communication have been developed at European level in close coordination with all affected companies, stakeholders and responsible authorities.
- Proposals have been drawn up for the legal basis offering lawful and proportionate access to content from encrypted communication.

8.3.10 Fostering responsible handling of zero-day vulnerabilities and exploits

Why is the objective relevant?

There is a certain tension between the objectives of providing the highest possible level of IT security while at the same time allowing law enforcement and security authorities to carry out their duties as required by law.

This tension must be resolved within the legal framework and safeguarding all legally protected (basic) rights as far as possible. In the interests of the security, confidentiality and integrity of IT systems, it is fundamental that any vulnerabilities detected be removed or reported to the manufacturer so that they can remove them. The law enforcement and security authorities must also be able to continue investigating and solving offences effectively while taking these provisions into account, with certain limited exceptions if necessary.

A **vulnerability** is defined as a weakness in software or hardware that can be exploited individually or in combination in order to obtain (usually surreptitious) access to a hardware or software system. Vulnerabilities are classified as zero-day (or 0-day), which are unknown to the manufacturer, and n-day vulnerabilities, which have been known to the manufacturer for n days.

An **exploit** is a tool or systematic opportunity (or description) for exploiting vulnerabilities and errors in hardware and software to obtain access to data or resources.

What is our current position?

The use of zero-day vulnerabilities for purposes of intelligence gathering, threat prevention and law enforcement currently takes place according to the internal regulations laid out by the authorities themselves. The general rules apply to these one-off uses.

Work is in progress to draw up a balanced strategy across all authorities to guide the way law enforcement and security authorities approach vulnerabilities (a vulnerability management, or Vulnerability Equities, process). This will improve the process overall.

What do we want to achieve?

Our aim is to put in place a balanced strategy across all authorities to guide the approach to zero-day vulnerabilities in accordance with current legal regulations for law enforcement and security authorities that goes beyond current internal rules at the authorities. This will help create a middle ground between the interests of cyber and information security and those of the law enforcement and security authorities. The basis for this will be standardised processes at the security authorities ensuring the safe, appropriate handling of vulnerabilities and exploits.

The key aspect of these processes will be the risk assessment, weighing up the threat potential of (zero-day) vulnerabilities where they are temporarily exploited by the security and law enforcement authorities against the anticipated usefulness for intelligence gathering, threat prevention and law enforcement (for more information on initiating the coordinated vulnerability disclosure process, see strategic objective 8.1.8 Responding responsibly to vulnerabilities – promoting coordinated vulnerability disclosure).

This framework will result in responsible vulnerability management, providing clear guidelines for handling vulnerabilities. This will resolve the tension between IT security and intelligence gathering, threat prevention and law enforcement. The highest possible level of protection for the public will be the priority. Careful consideration will therefore be given to threats associated with vulnerabilities in IT systems that could be used for the successful detection and prevention of serious threats and for effective law enforcement.

What impact are we expecting?

The increase in general IT security will bring with it improved public security. Handling of zero-day vulnerabilities and exploits will be harmonised and there will be a reliable national framework for a responsible approach to these instruments.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criterion:

- A binding process has been established regulating a responsible approach to zero-day vulnerabilities and exploits.

8.3.11 Increasing the digital sovereignty of the security authorities by expanding the Central Office for Information Technology in the Security Sector

Why is the objective relevant?

The security authorities need suppliers on which they can rely even in crisis situations, particularly in critical fields of work related to cyber security. They depend on tools of which the workings must be transparent, not least in terms of their serviceability for duties as required by law, for example in the case of telecommunications surveillance. The key capabilities required for this must be established and maintained, particularly when supply chains change or are not reliable in crisis situations. This is crucial to allow the security authorities to carry out their tasks autonomously and is an essential part of Germany's digital sovereignty in the context of government ability to act at all levels.

What is our current position?

The priority task of the Central Office for Information Technology in the Security Sector is to serve security authorities within the remit of the Federal Ministry of the Interior, Building and Community by developing, monitoring, assessing, and acting as central provider for tools and methods that it is expedient to package together on the basis of the similar challenges in cyberspace facing police and intelligence services.

However, rapid technical development in the field of security applications due to huge investments made by countries outside the EU in emerging technologies means a change in strategy is needed to ensure that government remains able to act on the basis of its own technology. Priorities in research and development should be under continual review and adjusted to incorporate new technological progress as required. These priorities form the basis of the mission of the Central Office for Information Technology in the Security Sector as service provider for the security authorities. The technical solutions that are deployed and necessary are often highly dependent on technology from non-European countries in particular. The absence of relevant industries therefore means that a considerable proportion of technical devices, tools and methods used for carrying out information technology surveillance, data analysis and pattern recognition duties as required by law is not available at national or EU level. This means that despite having the relevant capabilities, the security authorities often cannot act autonomously and independently in this field to the desired extent.

What do we want to achieve?

Our aim is for the Central Office for Information Technology in the Security Sector to be able to develop, assess and act as a central provider for tools and methods that will enable the security authorities to act autonomously and provide resilient security of supply, reinforcing their cyber capabilities significantly.

The key research and development process to create own tools and methods for these authorities will be further expanded at the Central Office for Information Technology in the Security Sector in compliance with applicable law. At the same time, the authorities in the remit of other ministries will also step up their research and development projects under the applicable law.

Wherever the police, the intelligence services and the executive authorities in the remit of the Federal Ministry of Defence use commercial products to help them carry out their duties as required by law, these products will be checked as thoroughly as possible to ensure that they are safe.

What impact are we expecting?

This process will further consolidate the Central Office for Information Technology in the Security Sector as a key component of cyber security at all levels of government. The Office will be able to tackle challenges rapidly and flexibly and, as central service provider for the security authorities, particularly in the remit of the Federal Ministry of the Interior, Building and Community, it will be able to develop emerging technologies.

The Central Office for Information Technology in the Security Sector will be able to provide a tailored range of solutions, tools and advisory services for the security authorities. This will strengthen the sovereign capabilities of German security authorities in the digital domain and will reinforce their independence from companies from outside of the EU.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The federal security authorities use the services provided and developments made by the Central Office for Information Technology in the Security Sector.
- The level of dependence of the security authorities on products and services from outside of Europe has reduced.
- The number of highly specialised experts in the key areas has increased.
- Sufficient internal capacity has been built up at the security authorities for the in-house development of critical or risk-affected systems and methods.
- The Central Office for Information Technology in the Security Sector has central competence for evaluating products and systems obtained from global supply chains. The security authorities make use of this competence.

8.3.12 Raising the level of cyber security through increased preventive intelligence gathering

Why is the objective relevant?

The purposes of cyber attacks include espionage, gaining political influence, and sabotage. Germany is among the targets of foreign intelligence units, which use very advanced attack techniques (Advanced Persistent Threats). In addition, extremist and terrorist actors are also among the users of cyber technologies, some of which can be obtained online as a service, to achieve their aims. Given these threats, it is important to raise widespread awareness of these threats (prevention), to identify the actors, their motives and their skills (intelligence gathering), to uncover specific attacks or preparation for attacks (detection), to provide information allowing defensive measures to be taken (warning) and to discover the authors of the attacks (attribution).

Early-warning functions for cyber attacks are primarily carried out in the cyber security architecture by intelligence services.

What is our current position?

The increasing importance of gathering intelligence on attackers is reflected in organisational measures in the federal intelligence services. For example, the increase in human resources for cyber threat prevention capabilities at the BfV and cyber analysis capabilities at the BND is a measure that will enable the intelligence services to watch relevant cyber actors more closely. By creating a sub-division for cyber counterintelligence, the Federal Office of Military Counterintelligence (BAMAD) has also improved its ability to counter the challenge posed by threats from cyberspace for authorities in the remit of the Federal Ministry of Defence.

What do we want to achieve?

To enable the federal intelligence services to continue making a major contribution to prevention, intelligence gathering, detection, warning and attribution, our aim is to reinforce their technical and specialised skills. In addition, we will ensure that in the future the federal intelligence services have sufficient legal powers to carry out their duties as required by law in accordance with the threat situation at any time. Their technical analysis capabilities will be kept at the required level through regular assessment and adjustment of analysis tools, environments and data filing systems and they will have sufficient human resources to exercise these capabilities.

The necessary exchange of information with other intelligence services, security authorities and other agencies, including private industry, will be further improved with the objective of using the resources dedicated to this more effectively and improving cyber threat prevention so that it is in line with the current threat situation.

What impact are we expecting?

The federal intelligence services will be able to carry out their mission efficiently and in a manner adapted to the threat situation. This will allow risks to be identified earlier and their impact to be minimised, and will increase the likelihood of identifying perpetrators. This will ensure that the greater scope for attacks created by the digital transformation can be further reduced with the help of measures taken far in advance of a cyber attack, which will contribute to raising the overall level of national cyber security.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The federal intelligence services have sufficient legal powers appropriate to the threat situation to carry out their legal duties.
- The necessary technical and staffing requirements for adequate, efficient intelligence gathering and prevention of cyber attacks have been established.
- The improved early detection and clearing up of cyber attacks has contributed to an increase in suitable warnings for threat prevention, to long-term support for prevention work, and to the political attribution of cyber actors of foreign origin.

8.3.13 Strengthening defence aspects of cyber security

Why is the objective relevant?

As a military part of overall defence, cyber defence is a constitutionally mandated task of the Bundeswehr and is subject to national and international law governing Bundeswehr operations. According to the 2016 White Paper, defensive aspects of national cyber security are the originary responsibility of the Federal Ministry of Defence and the Bundeswehr. The defence capabilities of the Bundeswehr in cyberspace are also an integral part of cyber security architecture. In defensive cases and cases of tension, cyber threat prevention, foreign and international cyber security policy and cyber defence are established complementary means of reducing the risks posed to Germany from cyberspace to an acceptable level. The nature of cyberspace and its highly dynamic nature mean that cyber defence must constantly be adjusted and refined to reflect new developments. This calls for an interministerial approach to defence in cyberspace.

As an army deployed around the world and using highly technical equipment, the Bundeswehr is constantly exposed to threats from cyberspace. At the same time, the use of cyberspace is crucial to the operational and enforcement capabilities of Germany's armed forces.

What is our current position?

Responsibility for cyber matters and IT has been centralised with the Directorate-General for Cyber / Information Technology at the Federal Ministry of Defence and the Bundeswehr's Cyber and Information Domain military organisational unit. The Directorate-General for Strategy and Operations is responsible for cyber operations. As well as pooling capabilities that were previously scattered, new capabilities have also been established.

Outside of defensive cases and cases of tension or during deployment, the MAD protects the Bundeswehr from espionage and sabotage and from extremism and terrorism in cyberspace. As an intelligence service within the remit of the Federal Ministry of Defence, the MAD has the relevant legal powers to support the mission of the armed forces.

Cyber defence design is being continually refined and adjusted in response to changing circumstances and challenges.

What do we want to achieve?

Our aim is to review the effectiveness of structures and capabilities in view of the constant, rapid evolution of cyberspace and if necessary to adapt them so that we can reduce risks in cyberspace to an acceptable level. Key capabilities in the cyber and information domain have been retained and expanded. Systems for securing core command capabilities and increasing the resilience of weapon and operating systems will be identified as critical IT components. They will be specifically designed as or replaced by trustworthy systems.

The IT services required to attain this objective will be established as a priority or will be retained.

Within the Federal Government, a strategy will be agreed for the performance of tasks associated with defence in cyberspace in defensive cases and cases of tension as well as in conventional areas, and will be practised regularly.

The defence aspects of cyber security as part of national and Alliance defence and other reaction options in the cyber and information domain will continue to be examined with the aim of fleshing out a more concrete approach, taking legal aspects into account.

What impact are we expecting?

Cyber defence will be effective and will continually be adjusted to the dynamic evolution of the cyber and information domain.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- A strategy has been agreed and put in place for defence in cyberspace in defensive cases and cases of tension and is practised regularly.
- The networks and systems of the Federal Government are sufficiently protected to ensure that cyber attacks cannot substantially impact their availability.
- The Bundeswehr is geared up to provide available resources for incident response in particular, in accordance with the legal provisions for administrative assistance. Regular exercises to practise this are carried out by the Incident Response Teams.

8.3.14 Adapting telecommunications and telemedia law and other specialist legislation to technological progress

Why is the objective relevant?

The legal powers for the security authorities to carry out their duties according to specialist legislation and telecommunications law must be continually adapted to keep pace with technological development. Rapid development in the networking and communication of the future is bringing about major changes, particularly in the fields of mobile communication, IoT and automotive IT. The transition to the fifth generation of mobile communication (5G) implies technological evolution that will be disruptive in nature. The number of connected mobile objects will increase greatly, with devices such as drones, robots, communication terminals, smart glasses, holographic displays, and a wide range of sensors making all kinds of everyday objects digital.

This development is borne by five megatrends which will have a particularly strong effect on the demands on the sixth-generation mobile communications network (6G):

- connected machines
- human-to-machine communication
- artificial intelligence
- the opening up of mobile communication with the introduction of open, standardised interfaces between the relevant network components (Open RAN) and
- the use of mobile communications networks in dealing with social, political and societal challenges.

The wide range of services available and the resultant new business models will continue to increase substantially. Existing and in particular new communication services will, however, also bring with them a huge variety of opportunities to abuse these technologies, for example in the areas of cyber crime, extremism, international terrorism and online hate speech and incitement.

What is our current position?

The security authorities face massive technological and methodological challenges in adapting to the breakneck speed of change in the digital world. Communication among potential criminals is facilitated by messenger services that were specifically developed for preparing crimes, as well as encrypted mobile communications devices and chat functions within online games; these are all becoming more widespread. The 2021 comprehensive recast of the Telecommunications Act (*Telekommunikationsgesetz,* TKG) makes legislative changes in response to these developments. However, it is important to keep pace with technological developments. Therefore, even after the reworked Telecommunications Act comes into force, the need for regulation in telecommunications and telemedia law and other specialist legislation will be examined so that the security authorities can also carry out their duties in the digital world while protecting fundamental rights as effectively as possible. In doing so, a balance must always be sought between the need for effective work by the security authorities that is up to date with the latest technological developments, and the protection of civil rights and liberties that might be affected by this.

What do we want to achieve?

Our aim is to regularly adjust the legal powers of the security authorities under telecommunications and telemedia law and other specialist legislation to keep pace with constant change in communication and the connected nature of the future, particularly in regard to mobile communication, IoT and automotive IT. This will prevent gaps emerging in threat prevention and law enforcement capabilities. As the central instrument in intelligence-gathering, investigation and searches by the federal and state security authorities, telecommunications surveillance is of paramount importance in all areas of crime, particularly organised crime and terrorism.

It is therefore extremely important for the security authorities that this instrument keep up with the latest technical developments. The capabilities of the security authorities in regard to combating crime and protecting the population from serious crimes, including terrorism, must not be undermined by the introduction of new services and business models.

What impact are we expecting?

The powers of the security authorities in the applicable specialist legislation, which must correspond with the relevant authorisation in telecommunications and telemedia law, will enable the security authorities to carry out their duties unrestricted and in line with technical progress. This will also be taken into account when 6G is introduced. This essentially affects the relevant regulations in the Telecommunications Act, the Telemedia Act (*Telemediengesetz,* TMG), the Telecommunications and Telemedia Data Protection Act (*Telekommunikation-Telemedien-Datenschutzgesetz,* TTDSG), the ordinance on telecommunications surveillance (*Telekommunikationsüberwachungsverordnung,* TKÜV), and the corresponding acts regulating the preventive and punitive powers of intrusion of the security authorities, such as the Code of Criminal Procedure, the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz*, BKAG) the Customs Investigation Service Act (*Zollfahndungsdienstgesetz*, ZFdG) the Federal Act on the Protection of the Constitution (*Bundesverfassungsschutzgesetz*, BVerSchG), the Federal Intelligence Service Act (*Gesetz über den Bundesnachrichtendienst*, BNDG) and the Act on the Federal Police (*Bundespolizeigesetz*, BPolG).

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- A system has been put in place which checks whether the security authorities have sufficient capabilities to carry out their duties as required by law in the digital world.
- The need for amendments to legislation is continually examined.

8.4 Action Area 4: Germany's active role in European and international cyber security policy

Growing levels of transnational networking are making the digital world smaller. Cooperation with our international partners in the EU and NATO and other partners who share our values, and the incorporation of national measures into European and international processes, are therefore essential to ensuring a high level of cyber security for Germany. While this must be taken into consideration in all action areas, Action Area 4 specifically addresses those objectives that Germany is actively striving for in European and international cyber security policy.

Germany's involvement in the EU is of particular importance, with the following high-level objectives: a high standard of cyber security throughout the EU; working together with Germany's EU partners on the international stage; and enhanced dialogue as part of cooperation between police forces and judiciary, while taking EU competences into consideration. In this respect, the 2021 Cyber Security Strategy dovetails with the EU's 2020 Cybersecurity Strategy, working at national level to increase collective resilience to cyber threats in Europe.

Within the North Atlantic Treaty Organization, Germany is involved in developing NATO's cyber defence policy. Key factors for this are the protection of NATO's networks and systems, and the resilience of IT infrastructure and critical infrastructures of the NATO member states in an evolving security environment.

Similarly, Germany strives to strengthen the international regulations for states in cyberspace. The Federal Government is involved in resolutions and declarations, and plays an active part in international discussions, particularly within the United Nations (UN), to further this process. With the help of international platforms for discussion and measures aimed at creating trust, particularly within the Organization for Security and Cooperation in Europe (OSCE), Germany works to foster mutual understanding with other countries in regard to cyber threats. By extending support for the establishment of cyber capabilities in other countries, Germany also plays a part in improving global cyber security.

Working with international partners that share our values, Germany is committed to a free, open, secure global internet. To achieve this, efforts are under way to ensure a process of regular dialogue with representatives from civil society, private industry and the research community.

We, the Federal Government, have set the following strategic objectives so that we can fulfil these tasks.

8.4.1 Actively shaping effective European cyber security policy

Why is the objective relevant?

The rapidly advancing digital transformation and increasing connectivity within the EU underscore the need to find European solutions in cyber security. Germany sees cyber security as a central organisational task for the EU (within the limits of its competences) and works together with its partners in the EU to achieve a strong cyber security architecture and a better exchange of information among EU member states. A shared vision and strategy for cyber security must be developed and updated as needed. By enforcing minimum standards for prevention, detection and reaction, European cyber security policy can improve cyber security throughout the EU.

What is our current position?

We see cyber security as an advantage for European industry. Europe should be a leading supplier of secure IT solutions, improving the quality of life for its citizens. Germany is additionally a driving force in EU bodies, working towards reaction capabilities across the member states and a collective EU position in dealings with other countries. It also supports a joint EU presence in international bodies.

Together with its member states, the EU can use the Cyber Diplomacy Toolbox to react in a coordinated manner to malicious cyber activities originating in other countries. In 2020, the Council of the European Union imposed sanctions for the first time against foreign persons and institutions that were responsible for or involved in a number of cyber attacks on EU member states.

In addition, the Cybersecurity Act was passed at EU level in 2019. The Act defined a new mandate for ENISA and introduced a harmonised European ICT certification framework in the EU.

A revision of the Network and Information Security Directive, the NIS 2 Directive, has been in negotiation in the European Parliament and in the Council since early 2021. Germany is playing an active part in the process, helping to shape the directive.

What is the Cyber Diplomacy Toolbox?

In June 2017, the Council of the European Union adopted the Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.
Serving as a toolbox, the document provides the EU and its member states with tools to react appropriately and decisively in case of malicious cyber activities with a wide range of diplomatic, political and economic measures. The toolbox contains preventive, cooperative, stabilising and restrictive measures (sanctions), along with possible support from the EU for legitimate reactions by member states.

The Cyber Diplomacy Toolbox is available at https://www.consilium.europa.eu/de/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

What do we want to achieve?

Germany's aim is for the EU, with its member states, to take up an active position in international cyber security policy. It also aims for the EU to continually develop its international cyber policy arsenal, with the goal of further improving the EU's ability to act against threats from cyberspace.

Germany will be actively involved in the EU's shared vision and strategy for cyber security and European digital sovereignty, and will work continually to help develop these further. This includes in particular the three areas of EU action identified in the EU Cybersecurity Strategy: resilience, technological sovereignty and leadership; building operational capacity to prevent, deter and respond; and advancing a global and open cyberspace.

Germany will support greater cooperation among EU member states as far as allowed by law, and is committed to working together in greater depth at EU level. This should allow EU member states to learn even more from each other and to coordinate closely in crisis situations.

European and international operational cooperation (for example within the EU CSIRTs network and the CyCLO network) will be deepened as a key building block for effective cyber threat prevention. The individual forums for information exchange will be allocated clear responsibilities, and the correct channels for information and coordination will be strictly observed.

National cyber security standards and best practice approaches will be actively included in European projects and EU regulations.

What impact are we expecting?

A shared vision in the EU will create a necessary framework, providing direction and orientation on matters of cyber security policy. This shared vision should also help all EU member states to introduce and implement agreed minimum standards. This will ensure that standard, recognised and coordinated processes are used.

Close cooperation with the EU and the individual member states will improve the exchange of information at EU level. The EU member states will have a position on all important aspects of cyber security policy and will actively champion this position. The ongoing exchange of information will allow the EU member states to learn more from each other. This will enable them to coordinate closely if crisis situations do occur.

A shared position among EU member states will strengthen that position and make it more effective in all areas of the EU, and also when communicating the European position in international negotiations. This shared position will strengthen messages communicated by the EU, increasing its influence on the world stage.

A shared vision, agreed standards, better exchange of information, knowledge transfer, international networking, clear legal frameworks and greater resilience can be expected. This will increase and standardise the level of cyber security for Europe and Germany and will allow resources to be deployed more effectively.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The fundamentals of European cyber security policy are developed continually and as needed.
- The NIS Directive has been revised and the new NIS 2 Directive is being implemented in national law.
- The strategic initiatives of the EU's 2020 Cybersecurity Strategy are being examined, fleshed out and implemented jointly with our European partners.
- In consultation with its European partners, the Federal Government reacts appropriately to cyber incidents.[46]
- The Cyber Diplomacy Toolbox is used, taking established reaction mechanisms into account, and is continually reviewed and, if necessary, refined as required.

[46]The attribution of cyber attacks remains a member state competence. Supplementary to this, there is the possibility of coordinated or joint attribution.

8.4.2 Shaping cyber security and defence in NATO

Why is the objective relevant?

NATO is fundamental to German and Euro-Atlantic security. NATO brings its member states together in an organisation that is both political and military. For more than 70 years, it has worked to protect their sovereignty, security, stability and territorial integrity. NATO also relies on sufficient protection against attacks in and through cyberspace to carry out its core tasks. NATO's cyber priorities are therefore protecting NATO's own network, strengthening the resilience of member states in terms of protection against cyber threats, and ensuring the Alliance's ability to deter, defend against and otherwise react to cyber threats.

What is our current position?

At the NATO summit in 2016, the NATO member states signed the Cyber Defence Pledge.[47] This is a political commitment to increase the resilience of their networks and infrastructures and to react quickly and effectively to cyber attacks. At the same time, cyberspace was recognised as a dimension of operational command in which NATO must be able to defend itself as effectively as in the air, on land and at sea. At the NATO summit in 2021 a new cyber defence policy was adopted which creates an updated framework for cyber defence and increased resilience in NATO.

Cyber Defence Pledge

In June 2016, the Allied Heads of State and Government made a commitment in the Cyber Defence Pledge to enhance the cyber defences of national infrastructures and networks.

As well as strengthening national cyber security, the pledge also supports enhanced EU-NATO cooperation on cyber security, further cooperation on cyber defence, and an annual assessment mechanism.

What do we want to achieve?

Our aim is to further develop NATO's cyber defence policy as a cornerstone of national and Euro-Atlantic security, and to adapt it to the ever-changing security environment.

NATO's networks and systems will be protected against cyber attacks through high levels of cyber security and resilience.

NATO will make an important contribution to increasing the resilience of its member states by implementing the Cyber Defence Pledge.

NATO will serve as a forum for consultation and exchange of information on cyber security and on reacting to malicious activity in cyberspace.

By further developing cyberspace as a dimension of operational command (in line with NATO's defence mandate and in accordance with international law), NATO will be able to defend itself and

[47] Available at: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

carry out operations in cyberspace as well as it can in other domains. To this end, Germany has demonstrated its willingness to support NATO with cyber operations in mandated operations and missions to achieve military objectives.

The EU-NATO cooperation on cyber defence and resilience will be reinforced and will strive for improved coordination in the reaction to cyber threats to improve the effectiveness of the cooperation.

Germany will continue to support NATO with its expertise in drawing up future-proof cyber defence policy within the mandate of the Alliance. The balance will be preserved between action by the Alliance as a whole and the sovereign duties of the member states, and between the civilian and military aspects of cyber security.

What impact are we expecting?

NATO and its member states will experience improved cyber security. The Alliance's ability to act in crisis management operations will improve, as will its defence capabilities.

NATO and its members will be able to carry out the duties of national defence and defence within the Alliance, as well as of international crisis management and stabilisation.

Implementing NATO's Cyber Defence Pledge will strengthen cyber threat prevention and cyber defence. Germany will retain its ability to act in this alliance with its partners.

Close cooperation between the EU and NATO will improve the exchange of information and the coordination of reactions to malicious conduct from abroad.

This means that overall, Germany and NATO will provide less scope for cyber attacks.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The fundamentals of NATO's cyber defence policy are reviewed continually and refined as needed.
- Processes are in place through which NATO can be supported to an adequate extent when necessary with national cyber capabilities.
- The implementation of the objectives of the NATO Cyber Defence Pledge is under way and is moving forward at national level.
- The EU and NATO have deepened their cooperation on matters of cyber security and cyber defence policy.

8.4.3 Strengthening international law and the legislative framework for cyberspace and working towards responsible state behaviour

Why is the objective relevant?

Cyber security cannot be attained at national level by states working alone; measures at this level must be supplemented by the relevant activities at international level. Any attempt to regulate cyberspace alone, that is, solely at national level, is doomed to failure due to the far-reaching, cross-border interdependence of national cyber systems. Cyber security can only be provided and strengthened on the basis of close cooperation among states and international organisations, civil society, the private sector and the research community. International law plays a key role in this. The rules-based international order is therefore also generally a cornerstone of German foreign policy. Alongside this, voluntary commitments by states to behave responsibly can complement the framework of international law, helping to flesh it out. Germany is therefore working around the world to strengthen and further develop international law, its institutions, and voluntary commitments in the field of cyber security. Formulating international standards is crucial to creating trust and security in cyberspace.

What is our current position?

Much of the international community recognises international law in cyberspace. Discussions are under way at UN level and in expert circles to further specify exactly what this means in detail and how individual norms and principles of international law, for example those in the UN Charter, can be applied in cyberspace. There are also discussions on which voluntary commitments to responsible behaviour by states can be used to expand the legislative framework governing cyberspace. At the same time, there are individual states which challenge the validity of international law, wholly or in part, with their statements and actions.

In March 2021, the Federal Government published a position paper[48] which contributes to the ongoing discussions regarding the specific methods of applying international law in cyberspace. In the paper, Germany emphasises the legitimacy and relevance of international law as the central multilateral regulatory framework, including for cyber operations, and underscores its belief in international cyber policy based on international law.

What do we want to achieve?

Our aim is to strengthen the international law framework for cyberspace and the acquis of non legally binding norms for responsible state behaviour. Germany will work towards a shared international understanding of the application of international law in cyberspace and of responsible state behaviour, based on the general principle of a free, open, global, safe internet. Germany will work actively to achieve this while at the same time coordinating closely with its EU partners. In addition, Germany will promote measures aimed at maintaining international

[48] Available at: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

stability in cyberspace and measures aimed at protecting human rights at national, European and international level.

What impact are we expecting?

The consensus shared by most states, that current international law also applies in cyberspace, will be further consolidated and expanded. The case will be made for states which have to date been reticent to acknowledge the legitimacy of current international law or individual areas of international law in cyberspace to acknowledge the comprehensive validity of international law in cyberspace.

Continued discussions will raise awareness internationally of the international law framework and non legally binding norms for responsible state behaviour in the cyber domain. Open questions will be identified and efforts will be made to resolve them. The subsequent improvement in legal certainty regarding the application of international law in cyberspace will enable state, in particular German, authorities to react more effectively to cyber threats, taking the applicable legal framework into account.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- On the basis of the position paper from March 2021, the Federal Government is involved in discussions at bilateral and multilateral level and in communication with civil society about the applicability of international law in cyberspace and about the implementation of voluntary commitments on responsible state behaviour.
- Germany is involved in the relevant discussions at UN level regarding cyber security, where it actively puts forward its position.
- Regular dialogue has been established at international and national level with society, the research community and the private sector on aspects of the legislative framework for cyberspace.
- Germany participates in resolutions and declarations on the topic of human rights online and in support of a free, open, global, safe internet.

8.4.4 Promoting confidence-building measures

Why is the objective relevant?

It is often just as difficult to recognise the motivation and aims of malicious behaviour in the cyber domain as it is to ascertain who is responsible for a cyber attack. At the same time, cyberspace is highly interconnected internationally. This creates considerable potential for misinterpretations and misjudgements which can lead to tension between states. In this context, measures to increase transparency and build confidence are important in preventing the risk of conflict and escalation.

What is our current position?

The important role of confidence-building measures for security and stability in cyberspace was acknowledged and affirmed in 2021 in the UN by all states. For Germany, the OSCE is the most relevant regional security organisation. In 2013 and 2016, the 57 OSCE participating states adopted a total of 16 confidence-building measures which promote communication among states, establish the necessary channels for this, and facilitate cooperation on cyber security matters.

What do we want to achieve?

Our aim is to strengthen measures for international confidence-building. Bilateral, regional and international communication formats will be used to achieve this.

As well as advancing confidence-building measures, Germany will also strive to implement the agreed measures, particularly in the OSCE.

What impact are we expecting?

Confidence-building measures will play a role in both prevention and de-escalation: it is expected that regular communication and international cooperation on confidence-building measures will increase mutual understanding in regard to perception of threats and unacceptable behaviour in cyberspace. In case of conflict, contact persons will be available, and already established, reliable channels of communication can be used.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Germany reports on national assessments and developments in the field of cyber security in bilateral, regional and international forums.
- Germany is involved in the relevant discussions on confidence-building measures in the cyber security field at international and regional level, where it actively puts forward its position, in particular regarding the applicability of international law in cyberspace and responsible state behaviour.
- Germany ensures that the contact persons it has named and the communication channels it has agreed during confidence-building measures are available and reliable.

8.4.5 Strengthening bilateral and regional support and cooperation for cyber capacity building

Why is the objective relevant?

Given the advanced digital transformation and the global interconnection of the world, cyber capacity building is extremely important. Cyber threats and attacks can greatly hinder or reverse the economic, social and political development of certain countries and population groups. Special needs arise where resources, infrastructure and capacities for cyber security are lacking. Cyber capacity building in partner countries and regions can help protect human rights, strengthen the rule of law and foster sustainable economic growth. It is therefore an important instrument in Germany's development cooperation work. Cyber capacity building allows the opportunities offered by the digital transformation to be used in full and the associated risks to be mitigated. The necessary conditions and awareness to ensure the secure and dependable use of cyberspace require support, especially where development policy has provided access to cyberspace for the first time. This will also have a positive impact on Germany's cyber security.

What is our current position?

In June 2020, the Secretary-General of the UN set out a roadmap for digital cooperation. The importance of cyber capacity building is also underlined in the EU's Cybersecurity Strategy. Germany is involved in bilateral projects, and also in individual projects in multilateral settings.

The Federal Government already funds a range of digital projects in Africa within its development cooperation work. Strengthening and protecting digital security is an important future task for Germany's development cooperation work; without it, the digital transformation will not be able to reach its full potential. Cyber security is therefore included as a component of all digital projects within development cooperation.

What do we want to achieve?

Our aim is to advance bilateral and regional cooperation on capacity building, involving international partners from the political sphere, the private sector and civil society, so that the full potential of digital technology can be exploited and vulnerabilities can be reduced. Cyber security will be a more integral part of programmes supporting the digital economy and of stability measures. The topic will become even more of an international priority. Assistance for and coordination of national and international capacity building measures will be guaranteed.

What impact are we expecting?

Bilateral and multilateral cooperation will lead to a lasting increase in cyber security in partner states. It will be possible to enshrine democratic and normative values and ideals worldwide. Cyber capacity building will increase overall global cyber security.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- Cyber capacity building is established as a topic in international bodies and has been enshrined in policy documents.
- Germany participates in implementing and/or supporting capacity-building measures in the national, EU, NATO or international context.

8.4.6 Strengthening international law enforcement cooperation and combating international cyber crime

Why is the objective relevant?

Cyber crime is a global phenomenon that does not stop at international borders. Effective law enforcement is therefore often only possible as part of coordinated international investigations. Strengthening international cooperation in law enforcement regarding cyber crime can increase the success of the responsible agencies and their investigations. The increased likelihood of detection can lead to a tangible drop in cyber crime.

What is our current position?

The number of cyber crimes continues to rise in parallel to the increasing transfer of economic and social activity to the digital domain. This is shown by police case numbers and numerous studies and trend analyses. In addition, the number of unreported attacks can be assumed to be above average. Germany is already an important player in combating cross-border cyber crime. It is important to consolidate and build on this role. One example of a successful coordinated international measure is the takedown of the Emotet malware infrastructure in January 2021, initiated by Germany.

Europol's European Cybercrime Centre – EC3 plays a multilateral support role in international cooperation. EC3 supports the EU member states in analysing and evaluating cyber crime and coordinates cross-border law enforcement.

Germany is a signatory to the European Council treaty on cyber crime, the Budapest Convention,[49] which now has 65 signatories in total. This treaty is the first international convention on the topic of cyber crime.

In April 2018, the European Commission initiated a legislative package[50] governing what is termed "e-evidence". This aims to enable EU member states to collect electronic evidence across borders without recourse to the traditional route of legal assistance. The proposal is currently being negotiated at European level.

In parallel to discussions at EU level, the EU is also negotiating the signing of an administrative agreement with the US Department of Justice so that the instruments planned in the e-evidence dossier can be used in relation to the USA as well.

What do we want to achieve?

Our aim is for Germany to support foreign law enforcement authorities by providing police capacity building to enable rapid reactions to cross-border cyber crime, particularly where

---

[49] Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?module=treaty-detail&treatynum=185

[50] Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52018PC0225

Germany and Europe are affected. This will reinforce the fight against international cyber crime and will improve the options for cross-border law enforcement.

Germany will take part in coordinated international investigations in which Europol and EC3 play a multilateral support role. Germany will also take part in and organise international exchanges of experience and processes for developing solutions.

Germany will encourage non-signatory states to sign the Budapest Convention and will advocate for its implementation in national law. Germany will also play an active part in advancing the convention.

What impact are we expecting?

By working with and exchanging strategic and operational information with its international partners, Germany will improve its capabilities for effectively combating cyber crime.

This preventive approach will make Germany a less attractive target for cyber attacks. The use of internationally coordinated investigations and law enforcement activities will ensure that critical infrastructures and general state institutions, private businesses and citizens in Germany are better protected.

The opportunities offered by international law enforcement will be strengthened by the growing number of signatories to the Budapest Convention in combination with the adoption of the e-evidence dossier.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The number and value of internationally coordinated evaluation and investigation processes has increased.
- The number of police capacity-building measures carried out from Germany for foreign security authorities has increased.
- The number of conferences and workshops that Germany has participated in and organised on the topic of internationally coordinated law enforcement and cyber crime has increased.
- The Budapest Convention is being ratified by more states.

8.4.7 Working jointly in the EU on innovative solutions for combating crime more effectively

Why is the objective relevant?

For effective law enforcement, investigators need technical solutions that are available for operational use as quickly as possible. These solutions are often based on new and hybrid technologies, and developing them requires a great deal of specialist expertise and technical equipment. European law enforcement authorities do not all have these resources in equal measure, but every EU state is equally affected by crime and the need for technical support for investigation and law enforcement.

Developing innovative solutions for more effective international cooperation among law enforcement authorities is in the shared interest of all EU member states. As well as actually developing methods and tools, coordinating needs and communicating among experts are central components of this area of activity.

What is our current position?

A clearing board, the EuCB, was successfully set up at European level during Germany's Presidency of the Council of the EU. The aim of the clearing board is to establish and channel communication and ad hoc coordination between the working level of the security authorities in the member states, at EU level, and with Europol on pressing requirements for tools and methods.

Relevant partners and networks with neighbouring countries such as the Central Office for Information Technology in the Security Sector, the European Network of Forensic Science Institutes (ENFSI) and the European Network of Law Enforcement Technology Services (ENLETS) are integrated into the process.

What do we want to achieve?

Our aim is for the EuCB to offer actual added value for investigators and for it to be operational in nature. In particular, it will:

- work directly with users (law enforcement agencies) to identify and pool together operational needs and requirements for technical solutions using emerging technologies;
- initiate project-related cooperation among experts in the Europol Innovation Lab on specific, clearly defined operational matters of a technical nature;
- disseminate the results of work by the Europol Innovation Lab and its core groups among the law enforcement authorities and serve as a forum for experts and investigators from the EU member states to exchange knowledge.

What impact are we expecting?

Germany's ability to effectively combat crime will improve due to cooperation on the development of innovative solutions and communication with European partners. The European partners will also benefit from German expertise, enabling them to improve their ability to combat crime.

How will we measure this?

The Federal Government will examine attainment of the objective based on the following criteria:

- The EuCB has been established.
- The EuCB has pooled together, initiated and, as the case may be, coordinated valuable European projects for combating crime more effectively.
- A regular exchange of experience takes place among the members of the EuCB, the Europol Innovation Lab and the EU Innovation Hub.

9 Cyber Security Strategy: implementation, reporting, strategic controlling and evaluation

The next section outlines basic provisions for the Guiding principle: Setting measurable, transparent objectives". They provide a framework for implementing the strategy, its reporting requirements (which are still to be put in place), its new strategic controlling provisions and the systematic preparation of future evaluations.

The 2021 Cyber Security Strategy sets out two levels:

- Strategic level: this encompasses the strategic objectives and the strategy itself. It includes coordination and involvement of other ministries by the Federal Ministry of the Interior, Building and Community.
- Operational level: this encompasses the measures below the strategic objectives and implementation in the ministries. The individual ministries are responsible for this level.

9.1 Implementation

The relevant ministries are responsible for implementing the strategy at operational level. This means that, based on the principle of ministerial autonomy, they are responsible for putting the strategy into operation. To do this, the ministries draw up measures at a level below the strategic objectives of the strategy. They independently monitor the implementation of these measures and are responsible for costs, burdens and effectiveness.

The strategy is put into operation by the ministries or their executive agencies. The ministries serve as the points of contact for the Federal Ministry of the Interior, Building and Community.

The strategy does not set out any binding provisions for its implementation. The ministries are to submit the information necessary for strategic controlling (see section 9.3 Controlling). The Federal Ministry of the Interior, Building and Community provides best practices to ensure consistency.

Measures are compiled and implemented downstream of the strategy. When they have been compiled, they are to be included as a rolling catalogue of measures as an annex to the strategy. The measures are assigned to the competent ministries.

The planning of measures can be adjusted by the ministries during the term of the strategy, for example to respond to changing conditions.

Implementation of the Cyber Security Strategy is subject to the availability of allocated budgetary resources.

9.2 Reporting

The responsible ministries submit a summary and evaluation to the Federal Ministry of the Interior, Building and Community by 31 March each year outlining the current status of target

achievement based on the indicators that have been determined. In addition, they inform the Federal Ministry of the Interior, Building and Community of budgetary and staffing needs, as well as expenditure and staffing costs, for the 2021 Cyber Security Strategy. The Federal Ministry of the Interior, Building and Community provides templates to ensure a uniform process.

The Federal Ministry of the Interior, Building and Community collates the reports from each ministry into a single joint report on the implementation of the 2021 Cyber Security Strategy. Eight weeks after receiving the individual reports, the Federal Ministry of the Interior, Building and Community submits a draft overall report for agreement by the ministries.

Based on the joint report, the Federal Ministry of the Interior, Building and Community works with the ministries concerned to assess the implementation of the 2021 Cyber Security Strategy and to examine whether changes in the threat situation or to risk assessments call for adjustments to the Cyber Security Strategy. Implementation of the strategy should be examined with regard to effectiveness and attainment of objectives. The initial response to the need for adjustments is to be through changes in implementation. Individual indicators can be added with the consent of the ministries. If a change is needed to the strategy itself, an evaluation is initiated.

9.3 Controlling

As coordinator, the Federal Ministry of the Interior, Building and Community establishes controlling at strategic level. This is termed strategic controlling.

Strategic controlling takes place at ministerial level. The Federal Ministry of the Interior, Building and Community acts as coordinating authority and involves the other relevant ministries. Strategic controlling encompasses ongoing monitoring of the attainment of objectives and a risk assessment. To make strategic controlling as efficient as possible, suitable and already existing surveys, reviews and KPIs on the status of cyber security at federal and state level are to be included in the indicators of the 2021 Cyber Security Strategy and are to be expanded and harmonised where necessary.

The Federal Ministry of the Interior, Building and Community draws up a controlling plan and coordinates this with the ministries. The plan sets out the framework for systematic long-term coordination.

9.4 Evaluation of the 2021 Cyber Security Strategy

The 2021 Cyber Security Strategy outlines and establishes basic processes that will accompany this and future cyber security strategies in the long term. The objective is to systematically prepare the implementation, future evaluations and future updates of the strategy.

Evaluations should take place after four years at the latest. They should be prepared so that objectives are based on transparent indicators that enable unbiased monitoring of their attainment. The strategic objectives are to be defined based on SMART (specific, measurable, actionable, realistic and time-bound) criteria. Indicators can be based on suitable instruments (output) or on the desired impact (outcome) on government, the private sector and society.

Measuring effectiveness is generally the higher-value method of evaluation. At the same time, the effort required for evaluation must be proportionate to the effort of the measure itself and its potential for optimisation through a higher-value method of evaluation.

Current recommendations such as ENISA's National Capabilities Assessment Framework are taken into account during evaluations.

In addition, depending on the current legislative period, evaluations or assessments may be carried out as needed, for example during audits by the Bundesrechnungshof (the German SAI).

In particular, it must be possible to measure target achievement based on defined indicators. It can be helpful for evaluations to involve non-government stakeholders such as manufacturers, service providers and higher education establishments. Communication processes for this should therefore be coordinated among the ministries and implemented.

The strategy is to be updated after four to six years, taking the current legislative period into account. If, as a result of evaluations, it becomes clear that there is significant need for changes to be made, an update can be brought forward.

Following assessment of the results of an evaluation, an update to the strategy may be sought. If only minor adjustments are needed, the Federal Ministry of the Interior, Building and Community can postpone the update to the next evaluation.

10 Glossary

Preliminary remark: The following definitions apply to this Cyber Security Strategy and are intended to enhance its clarity and consistency. The validity of definitions found in other contexts in the area of cyber security remains unaffected.

Term	Explanation
user-friendliness	As part of the user experience, user-friendliness describes the experiences and impressions of a user in their interaction with a product or service. The objective of product design based on user-friendliness is to meet or exceed user expectations from the interaction.
attribution	Attribution is the process of naming the author of a cyber attack.
Budapest Convention	The Budapest Convention is an international treaty of the European Council on the issue of cyber crime. It encompasses (i) the criminalisation of conduct ranging from illegal access to and interference with data and systems, to computer-related fraud and conduct related to child sexual abuse material; (ii) procedural law instruments for the investigation of cyber crime and the preservation of evidence in electronic form in connection with any criminal offence; and (iii) efficient international cooperation. The Budapest Convention is supplemented by a Protocol which criminalises xenophobia and racism committed through computer systems. A second supplementary protocol is at the negotiation stage. The aim of this second supplementary protocol is to reinforce international cooperation in the preservation of and access to evidence in electronic format in criminal proceedings by authorities in other countries.
cloud	Cloud computing refers to the dynamic provision, use and billing of IT services on demand via a network. Cloud provision encompasses the whole spectrum of IT services and includes infrastructure (processing power, memory space), platforms and software.
Common Criteria	The Common Criteria for Information Security Evaluation (or Common Criteria for short) provide an international standard (ISO 15408) for the evaluation and certification of computer system security. This means that components or systems do not need to be certified repeatedly in different countries.
cyber threat prevention	Cyber threat prevention encompasses all measures aiming to prevent or mitigate the success of actual or planned cyber attacks.
cyber attack	A cyber attack is an action against one or more other information technology systems in or through cyberspace with the aim of using information technology to interfere with its IT security.

	A cyber attack is considered particularly severe and significant if its potential effects may cause damages that span several regions or that have far-reaching consequences, or if it may interfere with government activity. Indicators for this may be that critical infrastructures or other essential institutions are affected, attacks are embedded in hybrid attempts to gain influence, or the need emerges for action by all levels of government.
cyber criminal	A cyber criminal is a perpetrator of criminal activity carried out using or with the help of information technology systems (for example blackmail).
cyberspace	Cyberspace is the virtual area of all information technology systems in the world which are or could be interconnected at data level. Cyberspace as a publicly accessible network is based on the internet, which can be expanded by means of any other data networks.
cyber security	Cyber security is the IT security of all information technology systems which are and could be interconnected at data level in cyberspace.
cyber terrorist	A cyber terrorist is an actor motivated by ideology who uses cyber attacks to damage or destroy targets, to disseminate their ideology, or to extend their influence.
cyber defence	Cyber defence covers the defensive and offensive capabilities in cyberspace which the Bundeswehr possesses to fulfil its constitutional tasks, and which are suitable and necessary for operational command or to avert (military) cyber attacks and thus to protect own information, IT, weapons and other systems. This also includes the use and co-design of cyber threat prevention structures, processes and reporting in defence-relevant aspects and situations.
data protection	Data protection is the protection of natural persons during the processing of personal data (not to be confused with data security).
Denial of Service	Denial of Service means a site or system is unable to operate. An attacker causes Denial of Service by creating large amounts of traffic to an IT system, resulting in system overload leading to partial or complete system outage.
Distributed Denial of Service	Distributed Denial of Service (DDoS) attacks are when attackers use several IT systems rather than single systems to carry out attacks. The high number of IT systems involved in the attack makes this type of attack hard to mitigate, which makes these attacks particularly effective.
disinformation	Disinformation is false or misleading information that is deliberately disseminated. It is distinct from false or misleading information that is spread without the intention to deceive.

detection	Detection is the recognition of events affecting cyber security, such as indicators of cyber attacks, in own IT systems and networks or during preventive intelligence gathering. Attacks can be detected, for example, during comparisons of processed data with information and technical patterns that suggest malicious conduct. To deal with the increased intensity of attacks, modern detection places more emphasis on technology systems to detect attacks, but organisational and staffing measures remain important.
digital sovereignty	Digital sovereignty is defined as the capabilities and options of individuals and institutions to exercise their role(s) in the digital world independently, autonomously and safely.
digital economy	The term digital economy represents the shift that is currently under way in the economy as a result of the increased use of technology. As well as providing greater efficiency and effectiveness of business process, the digital revolution also enables greater innovation in opening up and developing entirely new business areas and models.
e-government	The term e-government (electronic government) means the provision of public administration services online so that users can use these services without having to go to government offices in person.
end-to-end encryption	End-to-end encryption is the encryption of data from start to finish between sender and recipient.
exploit	An exploit is a tool or systematic opportunity (or description) for exploiting vulnerabilities and errors in hardware and software to obtain access to data or resources.
EU Cybersecurity Act	The European Cybersecurity Act (CSA) came into effect on 27 June 2019. Key components of the Act are a permanent mandate for ENISA and the introduction of a harmonised European certification framework for ICT products, services and processes.
European Cybercrime Centre	The European Cybercrime Centre (EC3) was set up in 2013 by Europol to strengthen the law enforcement response to cyber crime in the EU and thus to help protect European citizens, businesses and governments from online crime.
Europol	Europol is an EU agency that supports the law enforcement authorities of the EU member states in combating serious and organised international crime and terrorism.
hybrid threat	The Federal Government defines hybrid threats as a range of forms in which other states aim to exert influence, particularly against the security interests or the sovereign forming of political will of the Federal Republic of Germany.

information security	The aim of information security is to protect information. Information can be held on paper, on computers, or in individuals' heads.
information technology	Information technology (IT) includes all technical means of processing or transmitting information. Processing information includes the collecting, recording, using, storing, transmitting, software-driven processing, in-house presentation and disclosure of information.
baseline IT security	Baseline IT security is a method of establishing a security management system and for safeguarding information networks using standard security measures. The term also describes the situation in which the standard security measures recommended by the BSI have been implemented. This package of infrastructure, organisational, staffing and technical security measures provides sufficient security for organisations with normal protection requirements.
IT security	IT security is a situation in which the risks associated with the use of information technology due to threats and vulnerabilities are reduced to an acceptable level by taking appropriate measures. IT security is therefore the condition in which the confidentiality, integrity, authenticity and availability of information and information technology are protected by appropriate measures.
critical infrastructures	Critical infrastructures are those institutions and facilities, or parts thereof, which are crucial to the functioning of society and whose failure or disruption would cause serious supply shortages or threats to public security.
cryptography	Cryptography is the science of encrypting information in "secret codes". Its aim is to prevent third parties accessing information that is not intended for them.
National Pact on Cyber Security	The National Pact on Cyber Security is part of the coalition agreement for the current legislative period. The aim of the pact is to involve all relevant groups, manufacturers, providers and users in society, as well as the public administration, in a national pact that reflects the shared responsibility for digital security.
Open RAN	Open RAN is a standardisation project that is being developed and advanced by private-sector initiatives like the Telecom Infra Project and the O-RAN Alliance. A range of companies from the whole ICT value chain are involved, including network operators, component manufacturers and software companies. They are active in the different working groups of the two organisations. The aims of Open RAN include drawing up technical specifications that will allow or make it considerably easier for other equipment suppliers to incorporate their products, with the aim of increasing competitiveness and open interfaces between components. The focus areas include developing a reference design for "white box" hardware and developing software for the individual RAN components. In addition, lab and field studies are used to ensure that the hardware and software components from the different manufacturers are in fact interoperable in reality. In the next step, the Federal Government aims to upgrade the specifications

	drawn up for open interfaces by transferring them to a recognised standardisation organisation (ETSI, the European Telecommunications Standards Institute).
patch	A patch is a software program that resolves programming errors or vulnerabilities in user or system software or firmware, among other things.
post-quantum cryptography	Post-quantum cryptography describes cryptographic processes where it is assumed that the resulting encryption cannot be decoded in a realistic time frame, even by a quantum computer. In contrast to quantum cryptography, these processes can be deployed on standard hardware. As an alternative, security mechanisms based on the principles of quantum mechanics are proposed with the help of quantum cryptography. Quantum cryptography and post-quantum cryptography are processes based on a range of principles. These processes can be considered complementary, rather than competing.
provider	A provider can be a service provider with a range of focus areas, such as network providers which, as mobile communications providers, internet service providers or carriers, provide the infrastructure for data and speech communication, or service providers which offer additional services beyond simple network access.
quantum computing	Quantum computers are computers that make targeted use of the principles of quantum mechanics so that they can carry out certain calculations considerably more quickly than normal computers. The usefulness of this “quantum supremacy” has been demonstrated for solving specifically defined mathematical problems.
quantum communication	Quantum communication, in particular the distribution of cryptographic keys using components of quantum mechanics (Quantum Key Distribution, QKD), is a technology that promises secure data transmission on the basis of physical principles rather than mathematical hypotheses. QKD requires an additional traditional communication channel.
ransomware	Ransomware is the term for malicious programs that limit or prevent access to data and systems and only release these resources when a ransom is paid.
vulnerabilities	A vulnerability is a security-relevant error in an institution or IT system.
UP KRITIS	The UP KRITIS is a public-private cooperation between operators of critical infrastructures, their associations, and public bodies such as the BSI.
update	An update is a new version of or addition to an item of software or firmware that resolves programming or functional errors or creates improvements to programming or functions.

encryption	Encryption uses a piece of additional information, the “key”, to scramble readable text into a secret code (“cipher”) which cannot be deciphered by anyone who does not know the key.
international law	International law is the central element of the rules-based international order. International law is a legal system created through the cooperation of equal, sovereign states and in some cases other subjects of international law, on the basis of mutual agreement, and advanced in the same vein. In contrast to national law systems, there is no superior central legislative authority that creates generalised rights and obligations which all states must abide by. International law is more a question of voluntary obligation, as the acceptance and validity of international law as a whole can be traced back to a principle of consensus among states. As a result, international agreements (known as the international law of treaties) or state practice on the basis of a congruent opinion of law (known as international customary law), as well as the rules recognised in national law by most states, which also apply at intergovernmental level (known as the general principles of law) are binding sources of law in the international legal order.
hub	Federal authorities which serve as hubs facilitate organisational connections between different federal and state authorities for ongoing information exchange, coordination and support. This helps prevent duplication of structures by federal and state governments.
zero-day vulnerability	A zero-day vulnerability is a vulnerability in information technology systems that is unknown to the manufacturer.
5G/6G	5G and 6G are network standards of the fifth or sixth mobile communication generation. They are the direct successors of LTE (4G) and UMTS (3G). The new standards aim for higher data rates and reduced latency, improved capacity and an intelligent network. They open up new opportunities in digital transformation for businesses. For example, 5G and 6G networks can improve data exchange within and between companies or revolutionise system controls with the help of machine-to-machine communication. For consumers, this technology means a considerably faster mobile network in future, coupled with a growing number of connected objects in everyday environments.

11 List of abbreviations

Abbreviation	Explanation
APT	Advanced Persistent Threat
BAMAD	Federal Office of Military Counterintelligence
BDI	Federation of German Industries
BfV	Federal Office for the Protection of the Constitution
BKA	Federal Criminal Police Office
BMBF	Federal Ministry of Education and Research
BMI	Federal Ministry of the Interior, Building and Community
BMVg	Federal Ministry of Defence
BMWi	Federal Ministry for Economic Affairs and Energy
BND	Federal Intelligence Service
BPOL	Federal Police
BSI	Federal Office for Information Security
BSOC	Federal Security Operations Centre
CERT	Computer Emergency Response Team
CVD	Coordinated Vulnerability Disclosure
Cyberagentur	Agency for Innovation in Cybersecurity
Cyber-AZ	National Cyber Response Centre
DDoS	Distributed Denial of Service
DsiN	Deutschland sicher im Net (Germany secure on the internet)
EC3	European Cybercrime Centre

eID	Electronic identity
ENISA	European Union Agency for Cybersecurity
EU	European Union
EuCB	Clearing board at European level
IoT	Internet of Things
ICT	Information and communication technology
ISO	International Organization for Standardization
IT	information technology
KdoCIR	Cyber and Information Domain Service Headquarters of the Bundeswehr
AI	Artificial Intelligence
KRITIS	critical infrastructures
SME	Small and medium-sized enterprises
MAD	Military Counterintelligence Service
MIRT	Mobile Incident Response Team
NATO	North Atlantic Treaty Organization
NCSR	National Cyber Security Council
NIS Directive	European Network and Information Security Directive
OSCE	Organization for Security and Cooperation in Europe
OZG	Online Access Act (*Onlinezugangsgesetz*)
QKD	Quantum Key Distribution
PKI	Public Key Infrastructure
SOC	Security Operations Centre
TISiM	Transfer point for IT security for medium-sized businesses

TKÜ	Telecommunications surveillance
UP Bund	Guideline for information security in the public administration
VCV	Federal Administration CERT Group
UN	The United Nations
VPN	Virtual Private Network
ZITiS	Central Office for Information Technology in the Security Sector