Cyber Security Strategy for Germany 2016

Introduction

In just a few short years, the digital revolution has fundamentally altered government, society and the private sector in Germany. New ways of communicating and of accessing knowledge and innovative design lead to greater social interaction, new business models and new fields for research and development. Interconnected electronic devices have a growing influence on our daily lives and work. The growth of machine-generated data and the proliferation of smart meters and sensors are creating enormous amounts of data. Machines are learning on their own how to take on increasingly complex tasks. Routines and production processes are becoming increasingly interconnected and innovation cycles are speeding up. Borderless cyberspace demands new approaches. Government has the responsibility to work with the private sector and other actors in order to assess these processes of change in the public interest, actively influence them and create the conditions for their further development.

The ongoing digital revolution brings both opportunities and risks and therefore requires trust. There is no such thing as 100% security; there will always be potential for misuse. The task of government and the private sector is to lay the groundwork for such trust. Security is an important part of this effort. Individuals must be able to use the new technologies safely and autonomously, even when these technologies and the risks of using them are too complicated for ordinary people to understand fully. In this digital age, companies must be able to protect their intellectual property against unauthorized access and control their production processes even when using self-learning machines or cloud services that store their data on servers all over the world.

The Federal Government's Cyber Security Strategy for Germany that was adopted in February 2011 provided an important outline for forward-looking cyber security policy. Many of the measures proposed in that strategy have since been carried out. For example, the National Cyber Security Council is a high-level body for strategic initiatives at the interface between government and industry, while the National Cyber Response Centre serves as a platform for government agencies to share strategic and operational information. Since 2011, cyber security has become a key element of many strategic plans and interministerial projects of the Federal Government. It is

now clear that government institutions too must work together to ensure cyber security. In cyberspace, it is no longer possible to distinguish clearly between internal and external security. Maintaining cyber security and defending against cyber attacks have thus become a task for government as a whole.

The strategic approaches and objectives of the 2011 Cyber Security Strategy remain largely valid today. However, constantly changing conditions have made it necessary to expand the strategy and incorporate it into a larger interministerial effort which pays appropriate attention to the relevance and horizontal nature of cyber security and addresses this issue in a comprehensive way.

The 2016 Cyber Security Strategy provides the interministerial strategic framework for the Federal Government's activities related to cyber security and updates the 2011 Cyber Security Strategy. The federal states (*Länder*) and private industry were included in the process of developing the new strategy.

Cyber threat situation

The cyber threat situation in Germany is characterized by the increasing complexity and interdependence of the technology used and by constantly changing threats. The digitalization of modern societies has made them more vulnerable and increased the possibility of misuse in cyberspace. It also makes it much easier to attack the private sphere of individuals.

The impact of cyber attacks is not limited to cyberspace. Successful attacks may cause economic, political and even personal harm. Attacks on government institutions for the purpose of spying or sabotage can interfere with the functioning of public administration, the armed forces and the security authorities, thereby having an impact on public security and order in Germany. Cyber attacks on the energy supply network can shut down large segments of public and private life. Targeted cyber attacks on banking infrastructure or market manipulation can threaten the financial markets, with far-reaching consequences for the economy of Germany and the rest of the world. The manipulation of IT health-care applications, of IT-supported traffic routing systems or of self-driving cars and digital networks with which cars can communicate with each other and with traffic infrastructure can lead to very real threats to life and health. Intentionally spreading false information with the help of hacked IT systems can be used to manipulate public opinion, creating long-term threats to our open society and democracy.

Attackers often have a criminal, extremist/terrorist, military or intelligence background. The quantitative and qualitative diversity of potential actors at home and abroad and the technical possibilities for disguise make it difficult to detect, prevent and prosecute cyber attacks and identify attackers. Political and military conflicts are often accompanied by cyber campaigns or are waged in cyberspace below the threshold of armed conflict. This makes it more difficult to assess the political significance of cyber attacks and to decide what counter-measures to take.

The number and sophistication of cyber attacks is constantly growing, while IT systems are often inadequately protected. Some attacks show a high level of professionalism. Today, the tools to carry out attacks are available to state actors, criminal groups and individuals alike. Classic defences are often inadequate to protect

against sophisticated malware. Attackers have the technical skills to keep their attacks from being detected and to cover their own tracks. This is why it is becoming harder and harder to detect cyber attacks and who is responsible for them without a great deal of time and effort. We can assume that many attacks have so far gone undiscovered. This threat situation will have a significant impact on government, industry and society in Germany in the coming years.

Guiding principles of the Cyber Security Strategy

Germany must maintain its sovereignty and ability to function even in the digital age. Cyber security policy that is ready for the future will enable our country to take full advantage of the enormous opportunities and potential of the digital revolution to the benefit of all, by keeping the related risks under control.

Ensuring freedom and security is a core task of the state, also in cyberspace. So it is also a task of the state to protect individuals and businesses in Germany against threats from cyberspace and to prevent and prosecute crime in cyberspace. In the digital age, the state can perform these tasks effectively for the long term only by offering businesses and individuals protection and freedom to develop also in cyberspace. To do so, the state must make sure its own systems are secure. In view of the potential for digital innovation, the state must recognize possible developments and their relevance for cyber security issues at an early stage based on the necessary risk analysis; it must also investigate possible new solutions and incorporate them into public policy.

Cyber security results first of all from risk-appropriate behaviour and the use of secure systems in the operators' and users' area of responsibility. Many cyber attacks can be prevented with reasonable effort simply by taking tried and tested basic measures, such as consistently using risk-appropriate, effective and up-to-date security products and standards.

Close cooperation and coordination is necessary to prevent, detect, identify, defend against and prosecute cyber attacks. Government, private industry, society and the research community all share responsibility for ensuring the security of cyberspace. They must therefore also coordinate their response to current challenges. Due to interdependencies and threats that often extend across national borders, close European and international coordination is essential from the perspective of foreign and security policy.

As a result, the Federal Government's cyber security policy in the coming years will set priorities in the following four areas of action:

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

The measures in each of these four areas affect all areas of society to differing degrees.

Action area 1: Remaining safe and autonomous in a digital environment

A cornerstone of cyber security is the ability to be safe and in control in a digital environment. Individual users, businesses, government and others in Germany must be able to understand and assess the opportunities and risks involved in using information technology and to adjust their behaviour accordingly (ability to assess). For them to do so, trustworthy technologies and conditions must be available.

The possibility to be safe and in control in cyberspace lies within the context of technological or digital autonomy. It is based on targeted digital education for all ages and types of users. To counteract digital carelessness, awareness of cyber security must become firmly anchored in society.

In order to take advantage of what digitalization offers, all user groups must be able to access trustworthy and secure IT systems, thereby reducing their digital vulnerability. An important part of this is user-friendly and practical solutions – also those made in Germany – based on globally applicable technical architecture. So are targeted IT security research and development, needs- and user-based certification policy, support for secure electronic identities and encryption of both electronic communications and of services offered via the Internet. National regulations should be revised as necessary in line with current security needs. At the same time, the Federal Government will continue to work in the European Union and in international organizations on behalf of appropriate and uniform IT security standards and effective legislation.

Strategic objectives and measures:

Promoting digital literacy among all users

Responsible behaviour in cyberspace and awareness of the opportunities and specific risks when using IT systems are an integral part of digital literacy. Digital education must therefore become firmly integrated in the educational system, from school and the dual system of vocational education and training, to university, continuing professional training and general adult education. The federal states have primary responsibility for schools and universities. By the time young people finish school, they should all have the basic technical understanding and fundamental skills to use information and communications technology safely. The federal and state governments must work more closely together in this area. The Federal Government will align the dual system of vocational education and training more closely with the needs of digital society and will amend the training regulations accordingly. Vocational training centres for multiple employers are being equipped for the digital age. They must be able to offer high-quality continuing training in this area. The necessary investment in equipment has high funding priority. The Federal Government will also work with trade and labour unions as well as employers to create more flexible and individual digital continuing training.

The Federal Government will also push to expand course offerings in this area by establishing additional university chairs and by supporting leading institutions in the field of STEM education, in particular in computer science, for example with regard to Big Data analyses, industrial software and IT security. In the process, the Federal Government will also support greater cooperation with private industry, for example in the form of foundations and externally funded teaching and research posts.

Countering digital carelessness

In addition to education, responsible and risk-averse behaviour requires regular awareness-raising to counteract users' digital carelessness at home and at work. To this end, the Federal Government will work with initiatives such as Deutschland sicher im Netz e.V. (Germany secure on the Internet) to promote efforts to

increase awareness tailored to specific groups. The Federal Government also provides funding for specific projects to increase media literacy. The Federal Government initiatives related to cyber security and society are being expanded and updated. This also includes the public discourse on horizontal cyber policy issues using targeted formats. It is also necessary to counteract digital carelessness in businesses. Appointing IT security officers to drive the drafting and implementation of IT security measures is an effective, tried and tested way to accomplish this. To make cyber threats more visible, it is also necessary to provide the public with the latest information on the security aspects of IT products and services. For this reason, the Federal Office for Information Security (BSI) will expand its units dealing with public warnings and information on how to deal with IT security gaps.

Creating the conditions for secure electronic communication and safe web offerings

Secure and trustworthy electronic communication that cannot be manipulated is fundamental for individuals to be able to enjoy the rights related to communication, the right to privacy and the right to control one's own image. For businesses, it constitutes important protection against cyber spying and is thus the foundation for their financial success. Easy and secure encryption ensures confidential electronic communication for all and should become standard. The Federal Government explicitly welcomes research projects and industry initiatives aimed at this goal. The consistent use of strong encryption for web offerings will further increase security on the Internet. The Federal Government will analyse the specific barriers to the use of encryption and will promote initiatives to reduce these barriers.

Along with this approach, which could be called "security through encryption", Germany is also pursuing the approach of "security despite encryption". Users must have access to the highest level of protection for their data, values and rights. At the same time, Germany's law enforcement and security authorities are allowed, under strict legal conditions, to decrypt or bypass encrypted communications if necessary in the individual case to carry out their duties as required by law. To keep these powers from being undermined, the technical decryption ca-

pabilities of the law enforcement and security authorities must keep up with technical developments in encryption.

Secure electronic identities

In parallel with promoting secure electronic communications, the strategies for securely identifying persons and things should be expanded. Users must have access to secure, user-friendly and modern means of authentication on the Internet. The current standard of user name/password is widespread but not secure; it should be added to or if possible replaced. Identification documents with an online ID function are central; the Federal Government already provides such documents as a highly secure way to identify oneself on the Internet without shedding lots of data. The aim is to establish the online ID function, and secure identities based on it, as a standard means of identification for sensitive services, then to further develop this function and promote equally secure solutions in the private sector.

The Federal Government also advocates standardized identity management in all German public administration and is calling on makers of information and communications technology to work with Germany's IT security industry to develop and bring to market trustworthy products and services.

Strengthening certification and approval: Introducing a quality label for IT security

Effective, needs-based certificates and quality labels are an important tool for disseminating cyber security standards. Certifying or approving IT security products is already an established and recognized procedure. But it only covers a small segment of the information technology in use today. For this reason, the Federal Government encourages makers of standard technology in particular to certify more of their products. It will also introduce a basic certification procedure for secure IT consumer products, with criteria to be defined by the BSI. At the same time, the BSI's existing resources for drafting technical guidelines, certifying and supporting the national accreditation agency for IT security will be increased and the relevant processes streamlined in the interest of all involved. In the process, it will be necessary to use modern processes to overcome the challenge of rigorous but time-consuming certification and approval processes at a

time of shorter technology cycles. For example, this challenge can be met efficiently through greater involvement and accreditation of businesses and integrating them more thoroughly in the certification process. Scalable and delegated processes in accordance with BSI standards will be considered for this purpose. The Federal Government will advocate expanding the European and international agreements for IT security certification based on common criteria for evaluating security (Common Criteria, ISO/IEC 15408 and ISO/IEC 27000) in order to enable greater international recognition of these criteria.

In certain areas, labelling IT security features of products and services is still a special challenge. To make the security of IT products and services more transparent for individuals and small and medium-sized businesses, the Federal Government will increase its activities related to IT security quality labels and certificates and will make suitable proposals, especially concerning shared systems for certification and a standardized system of labelling. In future, a single quality label should help prospective buyers tell easily and quickly which IT products and services are designed to be secure and thus help protect data. Such a label is intended to make cyber security easier to understand and achieve.

Making digitalization secure

Individual consumers and businesses expect government to evaluate and actively influence the changes brought by digitalization. Examples include the E-Health Act (*E-Health-Gesetz*) and the IT Security Act (*IT-Sicherheitsgesetz*). We must continue to pursue this approach, paying attention to new technologies, new business models and changing user behaviour as well as new threats and new European and international regulations, such as the EU's Directive 2016/1148 on security of network and information systems. Requirements for the appropriate distribution of responsibilities and security risks on the Internet, for example by means of security requirements for makers of hard- and software and product liability rules for inadequate IT security, are being considered. The impacts of the use of digital technologies, especially on cyber security, should be taken into account already when drafting federal legislation and regulations.

And requiring the early implementation of security requirements should be allowed by law in order to ensure security by design. For this purpose, the BSI serves the federal ministries as a central source of advice.

As mobility becomes increasingly digitalized and more data are generated as a result, new cross-border requirements are needed to ensure the safety of vehicles and infrastructure and to protect privacy. Germany will play an active role in creating international standards especially at the level of UNECE to ensure sufficient protection against manipulation and misuse of technical structures, data and processes.

Advancing IT security research

New, all-encompassing IT security solutions are needed to be able to take full advantage of the opportunities offered by digitalization, such as Industry 4.0, medical technology and Mobility 4.0. This is why innovative IT security solutions for tomorrow must be researched and implemented today. The Federal Government is expanding its research framework programme on IT security, *Selbstbestimmt und sicher in der digitalen Welt 2015–2020* (Independent and safe in the digital world 2015–2020), and closely linking it to other measures of the Cyber Security Strategy.

The existing centres of excellence for IT security research will also be further strengthened: CRISP in Darmstadt, CISPA in Saarbrücken and KASTEL in Karlsruhe. These centres address current research topics, provide estimates and assessments for policy-makers and develop concrete solutions. The results of government-funded projects should be applied and marketed in products and processes as quickly as possible. In the area of military applications of IT and cyber security, this is the task of the cyber cluster at the Bundeswehr University in Munich, with its Cyber Defence and Smart Data (CODE) research centre. The commercial application and further development by businesses and start-ups of innovative ideas in the field of IT security should be an explicit goal of government investment in order to bring about the greatest possible economic benefit. Active technology scouting can help discover, introduce and further refine the latest

technologies. Private venture capital investors can also play an important role in this regard.

Action area 2: Government and private industry working together

Trusting cooperation and close interaction between government and the private sector are essential to maintain a high level of cyber security in Germany over the long term. New avenues should be taken as part of a cooperative approach in order to combine strengths.

Businesses in Germany must be able to protect themselves and their customers effectively against cyber attacks. Operators of critical infrastructure deserve special attention. But other businesses are also very important for government, society and the economy and require special protection. With the help of the cooperative approach established with the IT Security Act, the necessary conditions should be improved and extended to other economic sectors as needed. Government and private industry need to work together closely and on the basis of mutual trust in developing and implementing effective, needs-based IT security standards. For this to happen, Germany needs a strong IT industry promoted with the help of modern economic policy. The Federal Government will also draft measures to improve Germany's start-up culture in the field of IT and cyber security, which is weak in international comparison. In detecting and averting cyber attacks, it is essential to include providers and IT security services in Germany.

Strategic objectives and measures

Securing critical infrastructures

Protecting critical infrastructures is the central focus of joint activities by government and the private sector. The interconnectedness of these systems means that protecting the IT of critical infrastructures is especially important. This cyber prevention and defence task is shared by the federal, state and local governments, because internal and external security in the cyber area are closely interrelated. In implementing the IT Security Act, government and the private sector must work together closely at all levels and share information on the basis of trust, among others in the public–private partnership UP KRITIS. Minimum standards and reporting channels are drafted, implemented and further developed in cooperation with the private sector. Whether to extend such obligations

concerning prevention and response to other businesses with great relevance for society will also be considered.

Protecting businesses in Germany

The Federal Government will expand and increase links between its offerings to increase awareness and support German business and industry. Medium-sized businesses in particular must be able to protect themselves effectively against threats in and from cyberspace in order to take full advantage of the opportunities associated with digitalization. The relevant implementation strategies should be developed by government, the private sector and the research community working together. Government should provide concrete support for businesses to help them achieve the necessary level of IT security. Businesses and government agencies must be able to trust each other to handle sensitive topics professionally and with discretion.

The Federal Office for the Protection of the Constitution (BfV) and the central cyber crime contact point of the federal and state police play a key role in preventing cyber crime and espionage against businesses. The Federal Government will also work with the private sector and research community to expand existing initiatives, such as the Allianz für Cyber-Sicherheit (Alliance for cyber security), the German Competence Center against Cyber-Crime (G4C), and the initiatives IT-Sicherheit in der Wirtschaft (IT security in the private sector) and Initiative Wirtschaftsschutz (Economic security initiative), and to strengthen the connections between them, also to create synergies.

Strengthening Germany's IT industry

Cyber security in Germany requires a strong and innovative German IT industry based on secure network infrastructures and on identifying key technologies in the field of IT security and defence from trustworthy IT manufacturers. To make Germany's IT industry more competitive, the Federal Government will promote the quality label "IT Security Made in Germany" and expand the existing instruments for foreign trade. In national key technology fields, networks with the national IT security industry should be strengthened and own capacities should be built up, promoted and protected wherever possible and useful.

Further, a broader portfolio of qualified, trustworthy service providers is needed, for example for IT security solutions, forensics, and attack detection and response. Here too users should be able to rely on a broader range of service providers. The Federal Government provides support for IT companies through special research programmes. In joint projects with universities, research institutes and other private-sector partners, they develop innovative approaches for new products and services.

Working with providers

Working with providers plays a key role. In the framework of current law, this is especially true of provider activities to detect cyber threats, deal with known incidents/infections and reduce the impact of ongoing attacks. One effective option for improving data security on the Internet in general is to increase the use of sensors, in compliance with data protection regulations, to detect anomalies. The findings should be anonymized or pseudonymized to protect the rights of data subjects.

Getting providers of IT security services involved

At a time when skilled IT workers are in short supply, government and the private sector have an interest in encouraging the mutual exchange of IT expertise and the creation of expert networks. In the framework of applicable law, private providers of IT security services will be more involved in case of need than in other areas of government activity. The Federal Government will therefore take targeted advantage of possibilities to promote skilled and trustworthy IT security service providers. It will also work with representatives of Germany's IT security industry to develop and carry out staff exchange programmes in the field of cyber security. In doing so, protecting government confidentiality and official secrecy is just as important as protecting trade secrets.

Creating a platform for sharing information on the basis of mutual trust

The cooperative approach also includes intensive information-sharing. For this purpose, the Federal Government will institutionalize a cooperation platform for government and the private sector; within the predefined legal boundaries, this

platform will above all enable the sharing of information relevant for averting cyber attacks.

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

Government must ensure security, law and freedom in our country, also in cyberspace. This requires up-to-date cyber security architecture that effectively connects the various actors at federal level without losing sight of the state and local governments and the private sector.

The ongoing digital revolution means that many federal and state government agencies today deal with cyber security issues. The range of tasks is broad, extending (in compliance with the constitutionally imposed limits) from prevention, threat prevention and law enforcement to counter-espionage, intelligence-gathering and cyber defence. Both internal and external security in cyberspace are equally affected. Government institutions must be organized in such a way that they can fulfil their duty to protect society also in the digital age and can protect themselves against cyber attack.

In this context, modern cyber security architecture regards cyber security as an ongoing national task. It is essential that, in case of need, information is shared and the performance of tasks is coordinated efficiently. Synergies among ministries and agencies at all levels of government and across national borders are especially important. At federal level, the National Cyber Response Centre already offers the necessary structure for individual actors to work together within their respective roles and responsibilities. This cooperation should be intensified and the federal states more closely involved. The Federal Government will review the legal responsibilities as well as the technical and staffing capabilities, bring them more closely into line and adjust them as needed. This is the only way to ensure that government remains able to prevent, detect, investigate, avert and prosecute cyber attacks even in the digital age.

Strategic objectives and measures

Further developing the National Cyber Response Centre

In carrying out the 2011 Cyber Security Strategy, the National Cyber Response Centre was established under the leadership of the Federal Ministry of the Interior to strengthen information-sharing among the relevant federal agencies. At the Centre, the federal agencies responsible for cyber security issues currently share information on cyber incidents as well as their assessments and analyses.

This activity will be further intensified. To improve the ability to avert cyber attacks, the Centre must be suitably organized within the framework of cyber security architecture for all levels of government. As an inter-ministerial institution, under the supervision of the Federal Ministry of the Interior the Centre will be further developed into a central platform for cooperation and coordination. In future, the Centre will have its own evaluation and analysis capabilities and a current cyber situation report reflecting the cyber security situation in Germany. In case of cyber attack, it is crucial for all national actors to inform each other and coordinate their response in compliance with applicable law. If a cyber attack originates abroad, foreign and security policy aspects must also be taken into account. In case of cyber security incidents affecting numerous institutions across Germany, the Centre becomes a crisis response centre. In this case, the affected IT systems can be secured and restored and cyber attacks investigated and averted only through coordinated measures taken by the national actors. This operational cooperation is to be coordinated more intensively. The planning and implementation of joint exercises and reciprocal training are also to be established.

The federal states are invited to share their capabilities in this coordination process in the context of tasks performed by every level of government.

Improving local analysis and response capability

Recent cyber attacks have shown that there are hardly any institutionalized government structures, other than the usual IT security measures, to help those affected assess an incident quickly and locally. Firstly, this involves managing security incidents in technical terms, for which the BSI has special expertise. Secondly, cyber attacks may require action by the local security authorities based on the relevant law. The National Cyber Response Centre oversees the necessary coordination for such operations involving multiple authorities while respecting

the legal limits. The interests of these authorities in restoring IT systems, investigating incidents and prosecuting the perpetrators are taken into account, as are the interests in protection of the party affected.

The BSI will set up Mobile Incident Response Teams (MIRTs) to analyse and clear up cyber incidents affecting institutions which are especially important to society. On request, these teams will travel to constitutional bodies, federal agencies, critical infrastructure operators and similarly important institutions to help them deal quickly and flexibly with the technical aspects of managing security incidents, when there is a special public interest in doing so. This assistance is intended to rapidly restore the safe technical operations of the institution concerned.

Cyber attacks may also require action by federal security authorities. For this reason, the Federal Criminal Police Office (BKA) is setting up a specialized investigative unit, the Quick Reaction Force (QRF). In consultation with the responsible public prosecutor's office or the Office of the Federal Prosecutor, the QRF will take the first action that cannot be delayed under the Code of Criminal Procedure on behalf of the law enforcement authorities. The Federal Office for the Protection of the Constitution (BfV) is creating Mobile Cyber Teams made up of IT specialists, intelligence specialists experienced in analysing cyber attacks and, if necessary, staff with foreign language skills. These teams will travel to the scene of cyber attacks with an intelligence or extremist/terrorist background, including possible sabotage cases. The Military Counterintelligence Service (MAD) handles this task for agencies within the defence remit. As far as allowed by law, the Federal Intelligence Service (BND) may monitor attacks as they are being prepared and carried out. Information flows resulting from attacks are also registered. The Bundeswehr may also contribute, as far as allowed by the Constitution, to security preparedness with its Incident Response Teams and other relevant units.

Classic preventive measures may not be enough to deal with serious cyber attacks in the necessary time. The Federal Government will therefore examine the

legal framework to determine whether government agencies could conduct network operations and if so, what technical options they could use in these cases.

Intensifying law enforcement in cyberspace

The Federal Government will further intensify its efforts to fight cyber crime in the coming years. To do so, intensive information-sharing and knowledge transfer at national and international level will be necessary.

Justice and law enforcement authorities will also need additional technical and specialized capabilities. The relevant basic and advanced training curriculum is being developed. The Federal Government will also work to improve the conditions for recruiting and developing skilled staff in the fields of investigation, cyber crime and digital forensics.

High-performance analysis and evaluation systems are to be built for the federal and state-level security authorities.

The Federal Government will work to make sure that the powers and capabilities of the security authorities keep up with the latest technological developments so that there are no gaps in threat prevention and law enforcement. Investigative measures in the field of information technology surveillance must not be dependent on a particular technology, to ensure that they remain efficient and state of the art.

Fighting cyber espionage and sabotage effectively

For foreign intelligence services, cyber attacks on government IT systems and those of businesses, research institutes and their employees represent a significant source of information. The Federal Government has responded by reorganizing its counterintelligence efforts and will continue its 360° monitoring of all activities by foreign intelligence services in Germany. The BfV's directorate-general for counterintelligence has added staff and undergone targeted restructuring, with a focus on cyber espionage: technical and expert analysis and evaluation of attacks on federal agencies and other targets which are thought to be the work of

intelligence services. The BfV will also increase its efforts to fight cyber attacks with an extremist or terrorist background.

An early-warning system for cyber attacks from abroad

As mandated by law, the BND monitors cyber spying and other cyber attacks from abroad targeting government and/or critical infrastructures in Germany and can send potential targets an early warning to take the necessary defensive action (Signals Intelligence Support to Cyber Defence (SSCD)). In this way, the BND is using IT specialists and experienced analysts to create an early-warning system for cyber attacks. Once detected, attacks are assessed in terms of their quantity and quality in order to get a picture of the current threat situation.

Centre for Information Technology of Security Authorities (ZITiS)

The national security authorities must be as effective in the digital environment as in other areas. To help them with their operational cyber capabilities and to take advantage of synergies, a centre for technical support for the federal security and expert authorities, including the intelligence services, is being set up within the remit of the Federal Ministry of the Interior. The centre's tasks will be supportive and based on those of the authorities they serve. Development, support and advising the security authorities will have priority. This Centre for Information Technology of Security Authorities (ZITiS) will work closely with these authorities to develop the necessary methods, products and strategies for the security authorities to use in their operations. ZITiS itself will have no operational powers.

Strengthening the defensive aspects of cyber security

As a military part of overall defence, cyber defence is a constitutionally mandated task of the Bundeswehr and is subject to national and international rules 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. Cyber prevention, foreign and international cyber security policy and cyber defence are three supplementary means to achieve cyber security. The defence capabilities of the Bundeswehr in cyberspace are also an integral part of cyber security architecture. This is demonstrated by the similar content in the technical implementation of protective measures

and by using and sharing cyber defence structures, processes and reporting with regard to defence-related aspects and situations. As high-tech army deployed around the world, the Bundeswehr constantly faces threats in cyberspace. But the armed forces depend on cyberspace in order to function.

Cyber defence and cyber prevention must be incorporated into all overall defence planning, structures and processes. Information security and the protection of the Bundeswehr's IT systems are assured around the clock as a standing operational task, both in Germany and in its areas of operations. For the Bundeswehr to perform its tasks in cyberspace, its own capabilities are being expanded, the security architecture of its IT systems is being consolidated, and previously fragmented structures are being brought together in a ministerial division and a new, separate military organizational unit.

In addition, the Bundeswehr has special expertise, capabilities and resources which can be made available to other government actors through administrative assistance, within the limits allowed by constitutional law. The Bundeswehr can also use the services of civilian businesses to help it carry out its tasks as mandated by the Constitution.

Strengthening CERT structures in Germany

Government and non-governmental computer emergency response teams (CERTs) are single points of contact for technical prevention and response in the field of IT security and are an important component of any sustainable cyber security architecture. They meet the need for information-sharing and coordination at the IT expert level everywhere in the world. In Germany, the BSI serves as national CERT, with its CERT-Bund for the public administration; its services for operators of critical infrastructures, the private sector and individual users; and as single point of contact for CERTs in other countries. Other federal agencies have independent CERTs, as do state-level public administrations, some businesses and research institutions. These structures should be further expanded and connected in a network in the interest of national cyber security. The BSI will further intensify cooperation within the network of federal and state CERTs and with the business and research CERTs and will bring all the key actors together to im-

prove and complete the existing CERT structures in Germany in an inclusive process which builds on what has already been achieved. This process should also take the development of the National Cyber Response Centre into account.

Keeping the federal administration secure

Rapid technological development, the growing complexity of information and communications technology and digitalization in public administration are creating new challenges for IT security management in the federal administration as well. The implementation plan for ensuring IT security in the federal administration (UP Bund) is the binding IT security guideline for all federal agencies and will be revised in line with current technical and organizational developments.

The comprehensive project to consolidate federal IT (IT-Konsolidierung Bund) seeks in principle to merge the IT operations of the direct federal administration. One major goal of the project is to increase IT security. The project Netze des Bundes (networks of the Federal Government) is creating a consistent and secure network infrastructure for the federal administration. In a first step, the existing networks which are the responsibility of the Federal Ministry of the Interior are being migrated to a joint network, thereby establishing a single, higher level of IT security. In order to gradually migrate the remaining federal administration networks, this joint network will then serve as an integration platform for all federal IT networks.

In addition, the Federal Government has launched a programme to promote secure mobile communications. The programme seeks to increase awareness of the need to use secure IT products and to pay attention to security-relevant features when procuring new products. The resilience of federal IT systems will also be increased in order to handle unavoidable incidents better.

Working more closely with federal and state governments

There are proven structures for federal and state cooperation in the areas of cyber crime, cyber espionage and self-protection. To further strengthen this cooperation, the BSI will be assigned the new task of assisting state-level agencies

which are responsible for dealing with cyber security incidents. Up to now, the BSI has only provided such assistance to law enforcement authorities.

In 2013, the IT Planning Council adopted a guideline for information security in the public administration, which set a general standard for the IT security of all agencies and institutions of the federal and state administration. The federal and state governments have agreed to jointly defend against attacks on information infrastructures of the public administration. To improve their joint situation report, information-sharing between the federal and state levels on cyber attacks, which has been voluntary up to now, will be subject to a binding agreement.

In addition, more attention will be given to cyber security at local government level, for example in modernizing baseline IT security and its recommendations concerning organization, personnel, infrastructure and technical matters. The IT Planning Council is a suitable forum for this effort. The Federal Government supports central state-level structures to promote cyber security at local level, for example by local IT service providers. In future, federal agencies will be able to share more of their expertise with local governments via the federal states. The BSI will draw up a situation report for the local level with the help of the federal states and the national associations of local authorities.

Using resources, recruiting and developing staff

Cyber security costs money. In the coming years, major expenditures will therefore be necessary at federal, state and local level to keep Germany sufficiently and permanently up to date in the area of cyber security.

Staff recruitment and development plays a key role in ensuring effective public administration. The guideline of the IT Planning Council offers valuable information in this regard. It will be crucial to emphasize that the public service is an attractive employer and to make targeted use of the existing pay and employment conditions for civil servants and other government employees. Government must also work closely with training institutions. Cyber “clusters” where government, the private sector and the research community work together can be an important factor for success in the competition for highly skilled workers. Staff re-

cruitment within the Federal Government should be more closely coordinated, and staff exchanges should be made easier.

Access to the new cyber security course of study at the Bundeswehr University in Munich should also be as broad as possible. The expertise of existing staff and supervisors should be expanded and developed while creating new career and personal prospects. In-house basic and advanced training plays a special role in this context. The Federal Academy of Public Administration (BAköV) will offer relevant courses, and the training modules at the Federal University of Public Administration will be revised and added to. In addition, an innovative model is needed for staff exchanges with private industry and businesses.

The Bundeswehr is creating a new cyber reserve pool which can serve as a blueprint for similar civilian volunteer organizations wanting to gather and use the existing know-how of experts from industry, research, administration and civil society. Close cooperation with Germany's IT industry is very important in this context as well.

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

In view of transnational interconnections in a digitalized world, a high level of cyber security can be achieved only by embedding national measures in the relevant European, regional and international processes and thereby reinforcing them. With this in mind, Germany will continue to play an active role in European and international cyber security policy. A clear legal framework, increased trust and greater resilience in Europe and the rest of the world will also mean greater protection for Germany.

Especially in the digital age, security must be understood in global terms. With regard to measures to strengthen national and regional cyber security capabilities, Germany will also push for interoperable cyber security architectures and standards. At European level, the digital single market with an emphasis on sharing secure and interoperable data is crucial to ensure that European cyberspace is secure. Within the framework of existing Union competences, the same applies to police and judicial cooperation, to the Common Foreign and Security Policy and to the European IT security research network.

Germany also actively campaigns for greater cyber security in the relevant forums. The central aim of NATO's cyber defence policy is to make the Alliance resilient and to protect NATO's own networks. At the United Nations, Germany will continue to work hard to address numerous new issues concerning the application of international law in cyberspace and to maintain and improve openness, security and legal certainty in cyberspace. Bilateral cyber consultations and cooperation with selected partner countries with which Germany is pursuing development cooperation can reinforce this process and achieve a global minimum level of cyber security. Strengthening international law enforcement also plays a special role.

In the case of cyber attacks which use foreign systems, the use of diplomatic channels is always also to be considered, in addition to measures to protect and restore the systems affected and to prosecute the perpetrators.

Strategic objectives and measures

Actively shaping effective European cyber security policy

Security is a cornerstone of the digital single market. Germany will work to make sure that IT security is sufficiently taken into account in all digitalization processes, for example by means of a European data location policy based on data security and of European rules for international data exchange which pay attention to data protection.

Germany will participate in EU pilot projects addressing the legal and technical issues related to the cross-border processing and use of data. Key elements include the cross-border application of electronic identification, qualified electronic signatures, digital stamps for businesses and government agencies and other electronic trust services. Germany will also strive to make the Common Foreign and Security Policy pay greater attention to cyber security. Further, the Federal Government will help the German IT security research community form networks at European level and position itself in EU measures in order to take an active role in forming the European research landscape and research programmes.

Further developing NATO's cyber defence policy

As a cornerstone of German and Euro-Atlantic security, the North Atlantic Treaty Organization depends on sufficient protection against attacks from cyberspace in order to fulfil its core tasks, especially in the area of collective defence and in the framework of international stabilization missions. In adapting to the changing security environment, the Alliance must also continue to develop its cyber defence policy. Germany will actively participate in this process. The aim is to steadily improve the resilience of Allies and of the Alliance as a whole, and to increase their deterrence and defence capabilities, not least in the context of hybrid threats. NATO has recognized cyberspace as a domain of operations, reflecting the increased importance of cyber defence policy.

Shaping international cyber security

In the international community, access to and use of digital technologies varies greatly between countries and regions. The relevant forums pursue sometimes

diverging policy and economic goals. At the UN, Germany will continue to contribute to the debates on applying international law to the actions of states and non-state actors: To expand the system of international norms, Germany will particularly engage in efforts to develop norms, rules, principles and additional recommendations for responsible state behaviour in cyberspace. In view of international cyber threats, Germany will also advocate measures to maintain international stability and increase the UN's capacities in this area. Germany supports deliberations on how, on a global level, the problem of attributing cyber attacks can be addressed and the sharing of information can be promoted, the latter of which is essential in this regard. International laws that can be enforced across German and European borders must make economic espionage and cyber attacks more difficult to carry out. Germany will actively support international efforts to make the export control regime stricter with regard to surveillance technologies. In view of the threat of escalation caused by incidents in cyberspace, confidence-building measures must be implemented, improved and expanded. Existing forums and partnerships can be used for this purpose. Efforts within the OSCE, in which Germany has been involved since the beginning, thus play a pioneering role.

The Federal Government will furthermore establish a German institute for international cyber security, intended to bring together private industry, the research community and government organizations in the interest of international stability and crisis prevention, and to serve as a reliable and independent adviser to governments.

Bilateral and regional support and cooperation for cyber capacity building

Special needs arise where resources, infrastructure and capacities for cyber security are lacking. Cyber threats and attacks can greatly hinder or reverse the economic, social and political development of certain countries and demographic groups. Germany will help selected partner countries and regions build up their cyber security prevention and response capabilities (network robustness and resilience). This includes encouraging other regions to agree on confidence-building measures and to increase security. In its development policy, the Federal Government is working to realize the potential of digitalization worldwide and

to counteract the related risks. Security aspects play a key role in building and supporting digital infrastructures in partner countries with which Germany is pursuing development cooperation.

All over the world, the Federal Government is viewed as a trustworthy actor. It can also utilize existing skills to increase the help it provides to partner countries and regions through cyber capacity building. This includes developing its own cyber security strategies, legislation, institutions, certification, research, basic and advanced training and regional initiatives. 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.

Strengthening international law enforcement

Germany will work hard at international level to fight cyber crime. To do so, it will increase cross-border law enforcement and joint police investigative capabilities. The Federal Government will work to improve the international regulatory framework for threat prevention and law enforcement and will actively participate in existing initiatives at international level to further develop the legal framework for cross-border law enforcement investigations in cyberspace. In addition, it is examining ways to simplify and expedite requests for legal assistance with selected international partners to ensure effective law enforcement. The Federal Government will also continue to encourage as many countries as possible to join the Council of Europe Convention on Cybercrime and transpose it into national law.

Ongoing strategy development in the National Cyber Security Council

An open-ended cyber security strategy must not be limited to defining strategic measures. Instead, digital change should be accompanied by an ongoing strategy process on cyber security issues out of which additional strategic measures may evolve. New threats must be recognized early and innovative solutions investigated and worked out. The National Cyber Security Council, established with the 2011 Cyber Security Strategy to serve the Federal Government as a strategic adviser, is supposed to play a key role in this regard. The National Cyber Security Council brings together high-level representatives from the federal (Federal Chancellery, Federal Foreign Office and the federal ministries of the Interior, Defence, Economic Affairs and Energy, Justice and Consumer Protection, Finance, Education and Research, and Transport and Digital Infrastructure; additional ministries as needed) and state levels, as well as the private sector, thereby offering a suitable format to advance the strategic cyber security issues most important for Germany.

The National Cyber Security Council identifies long-term trends and needs for action, then develops ideas for strengthening cyber security in the areas of action mentioned. These ideas are then incorporated into the efforts of the Federal Government. In future, the National Cyber Security Council will increasingly draw on expertise from society, private industry and the research community. Invited experts speaking on individual strategic topics will provide background for discussion and for drawing up recommendations for action.

In Action Area 1, based on the latest technical developments, the National Cyber Security Council should propose further national rules to improve cyber security. In Action Area 2, the Council should indicate further fields of cooperation between government and the private sector to increase cyber security and should make relevant proposals for implementation. In Action Area 3, the Council should address the federal cyber security architecture and offer important ideas for the Federal Government and Standing Conference of Interior Ministers. In Action Area 4, the Council should seek contact with similar strategic bodies of other key international partners to generate new ideas for national cyber security policy.

The Council will regularly provide a written report to the Federal Cabinet informing the latter of the results it has achieved on the various strategic issues. The report will be presented to the Cabinet for its information.

Glossary

Definitions

Preliminary remarks: 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.

cyber threat prevention

Cyber threat prevention includes all measures intended to preserve or increase cyber security.

cyber attack

A cyber attack is an effect on one or more other information technology systems in or through cyberspace with the aim of using information technology to interfere with its IT security.

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 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 defence structures, processes and reporting in defence-relevant aspects and situations.

information technology

Information technology (IT) includes all technical means to process or transmit information. Processing information includes the collecting, recording, using, storing, transmitting, software-driven processing, in-house presentation and disclosure of information.

information-technology system

An information-technology system (IT system) is a technical system to process information which constitutes a complete functional unit. Typical IT systems are servers, clients, stand-alone computers, mobile telephones, routers, switches and security gateways.

IT security

IT security (also known as information security) means the fact that the authenticity, confidentiality, integrity and availability of an information-technology system and the data processed and stored in it are intact.