Austrian Strategy for Cybersecurity 2021

ÖSCS 2021

Austrian Strategy for Cybersecurity 2021

ÖSCS 2021

Vienna, 2021

Contents

Foreword **5**

Initial situation **7**

European, international and Austrian frameworks 15

Drafting the ÖSCS 2021 18

Structures and processes within sovereign administration 18

Challenges **23**

Strategic guiding principles **31**

Our commitment to national cybersecurity provision;
Austria’s contribution to cybersecurity in the EU 35

Vision and objectives 36

Structures and target audiences **39**

Structures 43

Target audiences 45

Measures, implementation and monitoring **55**

Measures 59

Implementation plan 60

Monitoring 60

Opportunities and outlook **63**

Cybersecurity opportunities 67

Outlook 69

List of abbreviations **73**

Annex to the ÖSCS 2021 .... **75**

Implementation guidelines 78

Foreword

Dear readers,

Digital technology has now established itself in every area of our lives. We shop online, we communicate using smartphones, and we carry out our banking transactions over the Internet. Systems for distributing goods are run via the cloud, our water and electricity networks are controlled electronically, and our hospitals have been reliant on computers for a long time now.

All these developments come with enormous potential, but they entail risks, and we need to take these risks seriously. With this in mind, cybersecurity is becoming increasingly important in our efforts to keep cyberspace safe and secure.

Cyberattacks are neither limited to individual sectors of the economy nor do they stop at national borders. To ensure society is as resilient as possible in the face of cyber threats, we need to work together even more closely at both the domestic and the international levels, intensifying existing dialogues and exchanging even more data. It is only by working together that we will be able to react to the constant change of the digital realm and adapt to the challenges it poses, to exploit digital technology's potential to boost our research institutions and economic development, and to deploy the limited numbers of cybersecurity staff available as effectively as possible in the long run.

The Austrian Strategy for Cybersecurity 2021 – referred to as "the Strategy" or by its German acronym "ÖSCS 2021", is designed to guide our efforts to meet cybersecurity challenges as effectively as possible. It serves to implement a major pillar of the current government's policy in this area also laying the groundwork for a systemic approach to cooperation between government agencies, research institutions and businesses.

What is more, the ÖSCS 2021 also forms part of the EU's "European Cybersecurity Strategy for the Digital Decade". In this way, Austria does not only make a significant contribution to its's cybersecurity, but it also works towards a global, open and safe cyberspace. The Austrian Strategy for Cybersecurity 2021 will create the conditions needed to exploit the opportunities of the digital world as effectively as possible over the coming years and decades and, above all, ensure that digital services are secure and safe for us all to use.

Karl Nehammer
Federal Chancellor

1

Initial situation

> ” The vision behind ÖSCS 2021 is to create a secure cyberspace over the long-term, and to make Austria and the European Union more resilient against cyber threats by adopting a national approach to cybersecurity.

We live in the age of digitalisation, and our society is more connected than it has ever been before. The advances of digital technology have transformed our private and working lives, as well as the way we do business. Citizens are every bit as reliant on digital services as companies and government bodies, which depend on digital networks and infrastructure to perform their core tasks. However, the more connected we are and the more dependent we are on digital services, the more vulnerable our society becomes. Cyberattacks and security incidents can have huge repercussions for our society and economy, for example by impairing services and disrupting the work of businesses and government agencies.

Therefore, it is extremely important to make Austria more resilient against cyber threats and to ensure that the digital world in its entirety is as safe as possible, both from an economic and a security point of view. With this in mind, cybersecurity is a top priority for Austria, and a major challenge for all sectors, government, businesses, scientific institutions and society alike.

Cybersecurity is not merely a national task, and Austria is a part of the European Union. By combating current and future cyber threats, the EU is making an effort to actively protect society and to secure our prosperity and values as well as the fundamental rights and freedoms in Europe. In so doing, the EU is also working hard to improve our defensive capabilities, to increase our strategic autonomy, technological capacity and specialist skills, and to promote a robust internal market. From the cybersecurity perspective, protecting the digital single market, and the single market more generally, is crucial for the economic performance of both Austria and the EU, which is why cybersecurity is a top priority both in Austria and the EU.

A global, open, stable and secure cyberspace in which the principles of international law – particularly those relating to human rights and humanitarian law – are upheld will be a key pillar of future economic development for both Austria and the EU. When it comes to the cyberspace, Austria is taking an active stance in bilateral and multilateral discussions, advocating respect for international law, strengthening voluntary standards, rules and principles that define responsible behaviour by state actors in cyberspace, and encouraging confidence-building measures on cyber issues.

The Austrian Strategy for Cybersecurity 2021 is made up of two parts. The first part sets out a long-term, overarching structure in which strategic considerations are stated. It includes a description of the situation, a summary of challenges and opportunities, the framework for implementing the Strategy, and how the Strategy will be monitored. The second part sets out the specific measures to be implemented under the Strategy in order to achieve the objectives. The implementation of the Strategy will be monitored using an online platform.

This structure makes it possible to react flexibly to the ever-changing threat pictures, and to respond quickly to challenges as they arise. Changes in the cybersecurity landscape may be triggered by political, technological, societal and economic developments within Austria as well as at the EU and the international levels.

European, international and Austrian frameworks

The ÖSCS 2021 draws on the principles set out in the Austrian Security Strategy, and represents a further development of the 2013 edition of the Austrian Strategy for Cybersecurity, which set out the underlying structures and processes required in order to formulate a comprehensive and coherent cybersecurity policy. The Austrian Strategy for Cybersecurity 2021 builds on its predecessor by incorporating the Austrian government's policy programme for 2020 to 2024 and the framework to be adopted at both the European and the international levels, which will be discussed below.

With the entry into force of the Directive on Security of Network and Information Systems[1] (NIS Directive), comprehensive cybersecurity legislation was adopted at the EU level for the first time. The Directive's definitions of harmonised security standards and reporting procedures for all enterprises considered essential for the continued operation of the EU's single market (and, by extension, of member states' economies) make up the core of this legislation. Austria has incorporated the NIS Directive into national law by means of the *Netz- und Informationssystemsicherheitsgesetz*, or the Network and Information Systems Security Act (known by its German acronym, NISG). The Network and Information Systems Security Act not only sets out standardised security requirements for all enterprises pertaining to critical infrastructure, but also provides the first ever legal basis for drafting a cybersecurity strategy.

The Directive on Security of Network and Information Systems, however, was only the beginning of the EU's intensive efforts to improve cybersecurity.

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

The EU regularly adjusts its strategic framework with a view to building a digital Europe, in which security, trust, competitiveness, awareness of Europe's strengths, respect for the EU's shared values, and an open attitude towards the rest of the world can all be bolstered up alongside the development of an open, secure Internet. The EU Cybersecurity Act of 2019 upgraded ENISA to an EU cybersecurity agency in its own right, created the legal framework for IT security certification programmes in the EU, and since then has been an integral part of the European cybersecurity framework.[2] The last major update to the policy framework around cybersecurity was in 2020, when the EU presented a new package of cybersecurity measures. This package includes an updated "EU Cybersecurity Strategy for the Digital Decade", a revised Directive concerning measures for a high common level of security across the Union ("NIS 2.0"), and a new Directive on the resilience of critical infrastructure.[3] The EU is also setting up a European Cybersecurity Industrial, Technology and Research Competence Centre, as well as a network of national coordination centres intended to pool cybersecurity investments in research, technology and industrial development, as well as to direct that investment in a targeted manner and ensure more effective coordination. In addition, there are also plans to set up an EU "cybersecurity competence community", which will bring together key cybersecurity interest groups with a view to improving and deepening specialist cybersecurity expertise across the EU.

[2] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on the certification of cybersecurity of information and communications technology, and on repealing Regulation (EU) No. 526/2013 (Cybersecurity Act)

[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 (Retrieved on 13 December 2021)

If necessary, the EU can draw upon the full range of applicable measures under the Common Foreign and Security Policy in order to prevent and combat malicious cyber activity. This range of measures, known as the “Cyber Diplomacy Toolbox”, is designed to prevent conflict, contain cyber threats, and promote stable international relations. The Toolbox includes exchanges with third countries on cyber issues, as well as coordinated EU diplomatic response options to malicious cyberattacks, up to, and including, sanctions against the perpetrators.

Cooperation between EU member states is critical to the success of these measures. A number of working groups and networks have been set up at the EU level in order to draw up relevant concepts and define major topic areas related to cybersecurity. Austria plays an active role in these groupings.

Negotiations on cybersecurity will continue at the United Nations (UN) over the next few years on a broad basis. As part of these negotiations, Austria is working hard to ensure closer cooperation with third countries. By ensuring that international law is adhered and voluntary standards for good governance are implemented and strengthened, conflicts in cyberspace can be prevented. As Vienna is home to one of the UN’s headquarters, Austria will host important negotiations on a UN Convention on Cybercrime over the next years. The upcoming convention is intended to strengthen international cooperation with a view to combating cybercrime more effectively. The Vienna-based Organization for Security and Co-operation in Europe (OSCE) also plays an important role in preventing cyber conflicts.

Drafting the ÖSCS 2021

Cybersecurity is a highly-specialised and extremely dynamic field. To reflect this, experts from the areas of business, education and training, and research and development worked together with the Austrian Federal Government's specialists to draw up the ÖSCS 2021 as a part of a multi-stage process. This nuanced approach presents cybersecurity as a challenge and task that must be faced at every level of society.

Structures and processes within sovereign administration

Cybersecurity is a national task that touches upon numerous disciplines, and this is why effective coordination mechanisms and cooperation between state agencies is called for. Combining forces from all ministries involved in cybersecurity will make the state's efforts to combat cyber threats and incidents significantly more effective.

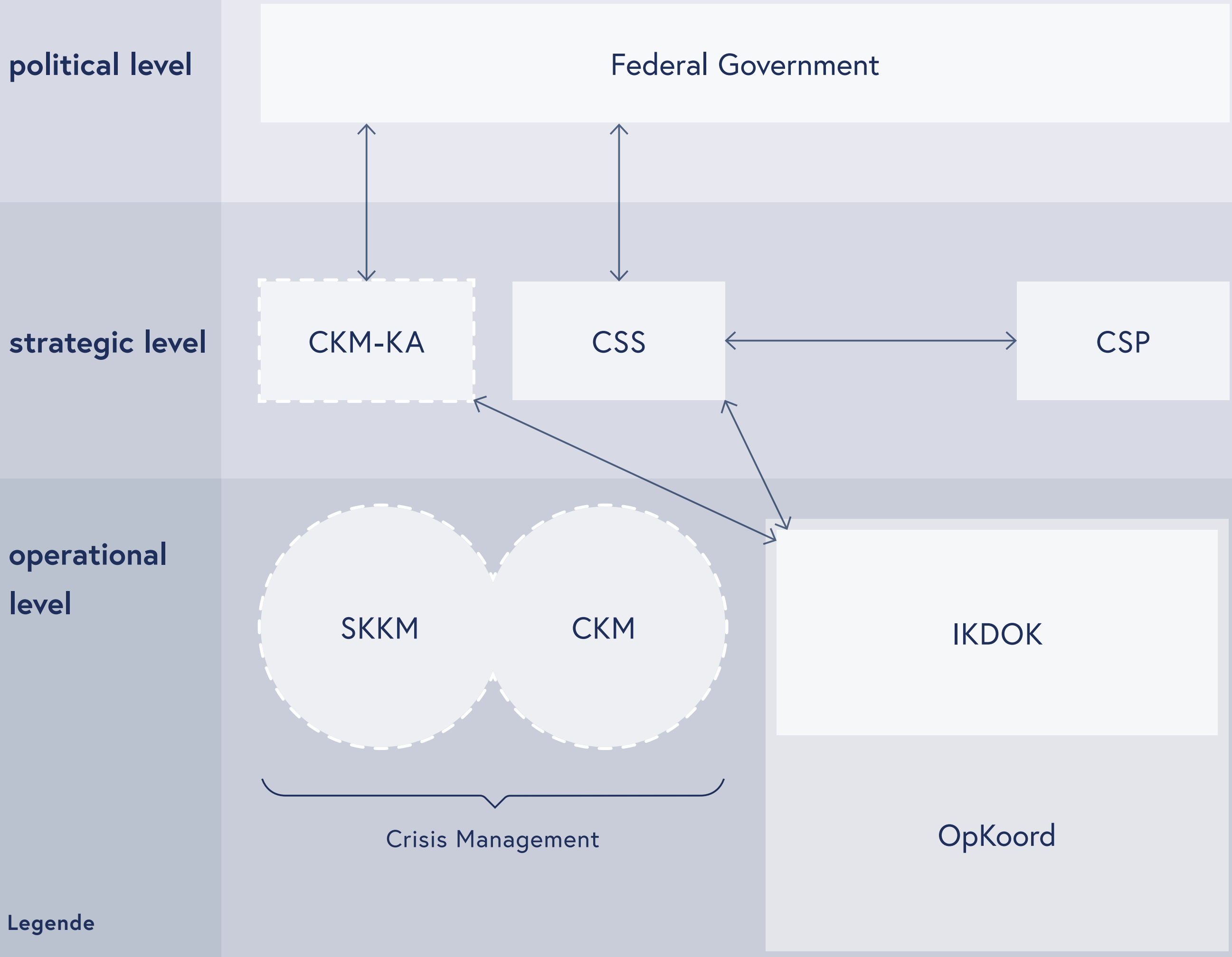
The ÖSCS 2021 builds on the national structures established as a part of the ÖSCS 2013, which are derived from the legal framework and responsibilities, as well as established committees, platforms and coordination mechanisms spanning across sectors and ministries.

Strategic coordination in the area of cybersecurity is carried out centrally by the Federal Chancellery and includes all national as well as the European and the international coordination in the cyber field. The Federal Ministry for European and International Affairs handles European and international cybersecurity issues as a part of its overall responsibility for foreign and security policy. Within Austria, the Federal Ministry of the Interior is responsible for maintaining public order and security, including the security of cyberspace and combating cybercrime. Under the Austrian Network and Information Systems Security Act, the Federal Ministry of the Interior is also responsible for the practical implementation of cybersecurity measures at the operational level. Austria's

military national defence in cyberspace falls under the Federal Ministry of Defence. The various ministries in charge of cybersecurity issues cooperate closely at the strategic and the operational levels. The responsibilities of other ministries with regard to cybersecurity issues are set out in the *Bundesministeriengesetz* or Federal Ministries Act. Cooperation with Austria's provinces and municipalities takes place according to the principle of self-government. Local authorities act within their own individual remits, while remaining in close and active dialogue with federal agencies.

As far as the security of network and information systems is concerned, two organisations have been set up within Austria to facilitate coordination at the operational level by providing an updated picture of the situation at all times and helping to coordinate the response of cybersecurity specialists to cyber incidents. These two organisations operate under the auspices of the Federal Ministry of the Interior, and are known as the Operative Coordination Structure, and the Inner Circle of the Operative Coordination Structure. In the event of a crisis, the Inner Circle of the Operative Coordination Structure serves as the direct hub for communications with the Cyber Crisis Management, which works at the national level, supported by the Operative Coordination Structure. The Cyber Crisis Management provides a platform for coordinating the response to a cyber incident across ministries and agencies. The Federal Ministry of the Interior is in charge of operational control and coordination of the Cyber Crisis Management. Should in the event of a cyber crisis a military involvement in cyberspace (e.g. in defence against a cyberattack with the potential to compromise Austria's sovereignty) be called for, operational command is transferred from the Federal Ministry of the Interior to the Federal Ministry of Defence.

The Cyber Security Steering Group and the Cyber Security Platform operate additionally at the strategic level. The Cyber Security Steering Group is responsible for implementing the Austrian Strategy for Cybersecurity. It provides the main platform for cooperation and exchange of information between businesses, the scientific community, and public administration.



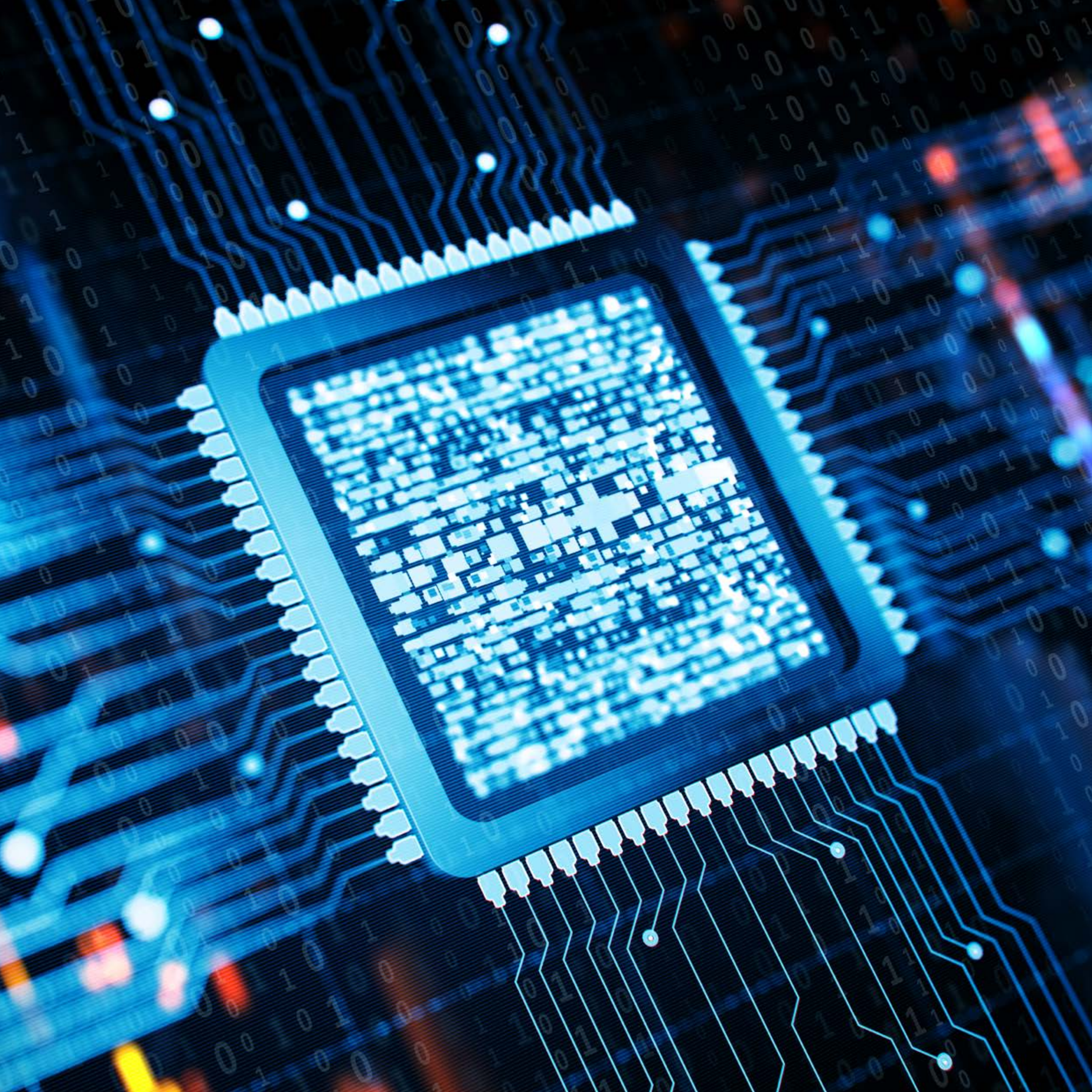
Legende

– – – –	event-related
CKM	Cyber Crisis Management
CKM-KA	Cyber Crisis Management Coordination Committee
CSP	Cyber Security Platform
CSS	Cyber Security Steering Group
IKDOK	Inner Circle of the Operative Coordination Structure
OpKoord	Operative Coordination Structure
SKKM	State Crisis and Catastrophe Protection Management

2

Challenges

> A future-oriented cybersecurity policy will allow us to make the most of the enormous opportunities and potentials digitalisation can offer, and to do so safely.



Digitalisation plays an important role in global networks, which makes it an enabler for both economic and social development, but this is not without its risks. These risks have the potential to develop into genuine threats, capable of jeopardising and destabilising Austria and its society. They can be divided into the following categories:

1. **Threats resulting from the abuse of information technology (IT)**
   Both state and non-state actors are using cyberspace as an arena in which to carry out ideological, political and criminal attacks. These attacks range from cybercrime and cyber espionage (either independently or as a part of a hybrid threat scenario) through to cyber warfare.

   Also the deliberate use of an IT-based information platform in order to manipulate, influence and destabilise democratic processes or public opinion also falls into this category.

2. **Threats resulting from the incorrect use of IT**
   While deliberate and malicious misuse of IT is a significant danger, inadvertently using the system the wrong way can pose challenges, too. Inadvertent misuse of IT is usually the result of lack of expertise on the part of the user. If the user fails to exercise due care and attention when using information technology, a variety of risks may be triggered. These risks, however, can be met with security technology only to a limited extent. Insufficient preparation for attacks and negligent use of IT systems can make companies and organisations particularly easy targets. This applies to all value creation and production processes, including any and all involved suppliers; particularly the latter should be taken into account in risk management procedures.

3. **Threats resulting from dependence on IT systems**
   Insecure IT products and services can pose risks, but the same is also true for our increasing dependence on IT systems and their availability. Therefore, the disruption of previously secure technology can lead to significant financial losses and a wide range of other dangers. The use of cloud technologies is particularly risky in this regard. Given our increasing reliance on these systems, the shortage of qualified cybersecurity staff is another challenge with which companies and organisations are faced.

   As the digitalisation process unfolds, our dependence on IT systems will continue to increase, which in view of the states' digital geopolitics, the complexity of internet governance regulations, the shortage of resources and our increased reliance on infrastructure in aerospace will cause new challenges to arise.

4. **Threats resulting from new technologies**
   As digitalisation spreads into areas and procedures where IT was not used in the past, new security challenges come up. What is more, the replacement of older IT applications with new technologies may also cause such challenges. Indeed, the development of artificial intelligence (AI), the Internet of Things (IoT), and other emerging and disruptive technologies, such as quantum technology, is expected to usher in a range of new security risks. Changes in the functionality of new IT systems can also trigger new risks, particularly where IT applications that were previously used in a supporting role become major or controlling elements of digital systems. In addition to these security-related issues, also technical and ethical concerns arise.

The ÖSCS 2021 marks a major contribution to confronting these new challenges.

3

Strategic guiding principles

> ” Guaranteeing freedom and security is among a state’s core duties, which must be fulfilled in cyberspace as they would be elsewhere.

Our commitment to national cybersecurity provision; Austria’s contribution to cybersecurity in the EU

Austria is committed to a national approach to cybersecurity provision, and to creating a secure cyberspace as a part of its comprehensive national defence and comprehensive security provision. The national approach to cybersecurity is designed to guarantee Austria’s sovereignty and ability to act on the international stage.

This approach is implemented by means of a comprehensive cybersecurity policy, which forms an integral part of Austria’s national defence and goes well beyond foreign, defence and security policy-related issues. Specifically, Austria’s national approach to cybersecurity also encompasses economic, infrastructure and financial policy considerations, as well as the policies on education, training, science and research.

Ensuring Austria is adequately prepared to meet any cybersecurity threat requires a national approach in which the state, businesses, the scientific community and society as a whole contribute. Hence, it can be said that the present Strategy is relevant to all of Austria.

Moreover, Austria both contributes to, and benefits from, the EU’s cybersecurity architecture. Due to the transnational character of cyberspace and mutual dependencies, security and resilience in cyberspace can only be guaranteed in the long term with a Europe-wide approach. Any measures that bolster the EU’s security in cyberspace simultaneously strengthens Austria’s cybersecurity as well. This is why Austria is committed to supporting and implementing the European Union’s Cyber Security Strategy.

Vision and objectives

Our commitment to national cybersecurity provision underpins the vision set out in this section:

> The vision behind ÖSCS 2021 is to create a secure cyberspace over the long-term, and to make Austria and the European Union more resilient against cyber threats by adopting a national approach to cybersecurity.

In order to turn this vision into reality, ÖSCS 2021 aims to achieve the following objectives:

1. Ensure that Austria has access to sufficient financial and human resources in order to prevent, recognise and defend itself against cyber threats and cyber incidents, and to prosecute the perpetrators of cyberattacks.

2. Ensure that Austria is capable of protecting and defending its critical information systems and infrastructure in the event of a crisis.

3. Ensure that cybersecurity is perceived as the joint responsibility of the state, businesses, and society as a whole in Austria, that clearly defined responsibilities and remits are set out, and that all stakeholders play an active role within their respective areas of responsibility.

4. Ensure that there is a national picture of the cybersecurity situation, and that cybersecurity skills are strengthened and promoted in all strata of society, the economy and in daily life, and that the awareness of cybersecurity is raised.

5. Ensure that all Austrians have a secure platform to take part in social and political life in cyberspace.

6. Ensure that Austria has the statutory and operational mechanisms in order to make it a secure and attractive destination for companies in cyberspace, and to prosecute cyber criminals in an appropriate manner.

7. Ensure that Austria is actively engaged in cybersecurity issues and working closely together with all stakeholders at the national, the European and the international levels.

8. Ensure cooperation with the EU so that Austria can defend its digital sovereignty and contribute to the strategic autonomy of the EU as a whole.

9. Ensure that Austria's cybersecurity field works in a coordinated and networked manner.

10. Ensure that Austria trains sufficient cybersecurity experts with a view to making the country more resilient, meeting the demands of the labour market, and combating cybercrime in the long term.

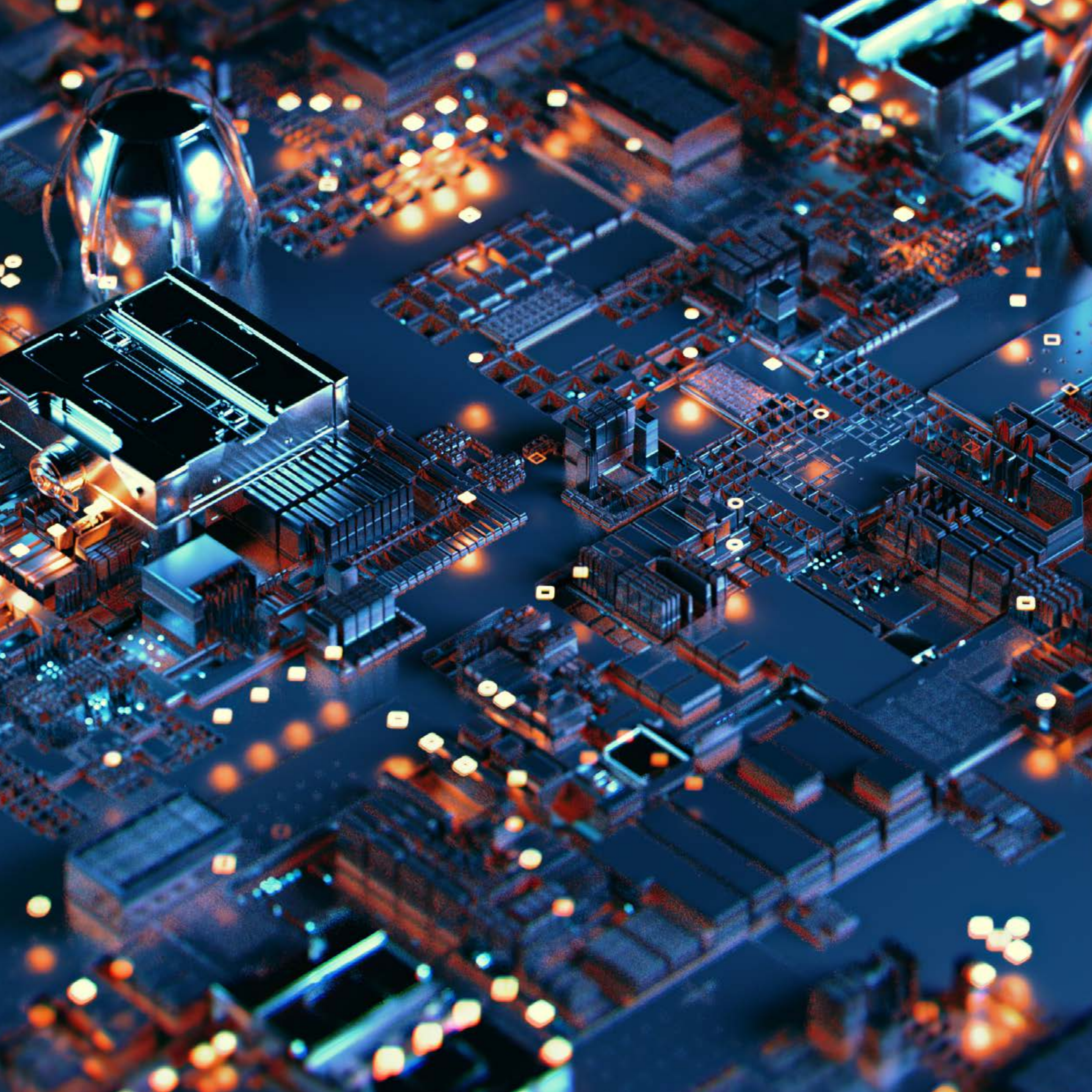
11. Ensure that Austria plays an active role in applying and strengthening international standards for cyberspace.

12. Ensure that Austria continues its national approach to developing the legal framework for cybersecurity to make cyberspace more secure and fight cybercrime.

Implementing the measures set out in the above list will help to achieve these objectives.

4

Structures and target audiences



Structures

The structures required to implement the ÖSCS 2021 are currently being developed, built on the structural requirements set out in the ÖSCS 2013.

Strategic level

Cyber Security Steering Group

The Cyber Security Steering Group is the central strategic planning body for cybersecurity in Austria. It is responsible for developing and coordinating all the measures laid down in the ÖSCS. It also monitors the implementation of the ÖSCS, updates the List of Measures, and elaborates an annual report on cybersecurity.

The Cyber Security Steering Group is made up of high-ranking cybersecurity experts from the ministries represented on Austria's National Security Council. The National Security Council also includes the ministries responsible for telecommunications and digitalisation. Depending on the subject(s) under discussion, the members of the Cyber Security Steering Group may invite other state bodies ("entities of public administration") to take part in so-called "Extended Cyber Security Steering Group" meetings. This includes especially those ministries that are either directly affected by the measures of the ÖSCS 2021 or whose area of responsibility touches upon enterprises and/or organisations affected by it.

Cyber Crisis Management Coordination Committee

The Austrian Network and Information Systems Security Act provides for the creation of a coordination committee, called Cyber Crisis Management Coordination Committee, which is tasked with identifying cyber crises and deciding on the operational measures to be taken to combat such crises. The Committee is headed by the Director General for Public Security, and made up of the Chief of Defence Staff, the Secretary General of the Austrian Federal Chancellery, and the Secretary General of the Federal Ministry of European and International Affairs. In the event of a crisis, the Committee is joined by additional representatives from federal and/or province authorities, providers of critical services, computer emergency response teams and emergency services as required.[4]

Operational level

Inner Circle of the Operative Coordination Structure

The Inner Circle of the Operative Coordination Structure was created under the auspices of the Network and Information Systems Security Act as an inter-ministerial body charged with coordinating cybersecurity activity at the operational level. It discusses and updates the national cybersecurity picture and supports the Coordination Committee in the Cyber Crisis Management.

The Inner Circle of the Operative Coordination Structure is currently being expanded. In the future it will be equipped with all the required resources to provide recommendations and assessments on cybersecurity issues for the federal administration on behalf of the Cyber Security Steering Group.

Operative Coordination Structure

The Operative Coordination Structure is designed to coordinate operational activity in the field of cybersecurity. It is composed of the members of the Inner Circle of the Operative Coordination Structure and the computer emergency response teams established under the Network and Information Systems Security Act. Representatives of the operators of critical services, providers of digital services and Entities of Public Administration, including their respective computer emergency response teams, may also be integrated into the Operative Coordination Structure as required.

[4] See Network and Information Systems Security Act Section 25. (1)f

Target audiences

The central target audiences for the ÖSCS 2021 are society as a whole, businesses, the education sector, and the research and development community. The individual measures required to meet the respective objectives are assigned to different target audiences according to their focus.

Society

Topic area “trust and privacy”
Trust in IT products and services is particularly important to citizens. This trust is to be built through transparency, data protection, data security and the protection of the users’ privacy. Secure communications are a basic prerequisite for citizens’ participation in society via digital channels, as well as for exercising fundamental human rights in cyberspace.

Digital proof of identity and secure communication channels are of central significance in the private environment, the business world and to services provided by the state and public administration. Access to personal and confidential data must be logged in a traceable manner, and minimised as far as required. High quality electronic identification is essential so as to ensure that data and privacy are adequately protected, and included in new concepts from the design stage. After all, data protection and data security as well as trust in their comprehensive incorporation in electronic identification (e-ID) are a fundament for their actual use. Electronic identification and the digital passport have the potential to improve the level of cybersecurity available to citizens, businesses and public administration across the EU, provided they are developed according to the latest technological advances.

Topic area "awareness"

Efforts to raise awareness of cybersecurity across society at large are aimed at capturing public perception, personal interest, and further raising awareness of the importance of this issue. This is a fundamental requirement for a self-determined and responsible behaviour in cyberspace, and will help to make Austrian society more resilient to cyber-attacks.

Topic area "free opinion-building process"

Individuals cannot form their opinions freely unless the information they receive is genuine and reliable. As we consume ever more information digitally, the need to secure our information systems becomes ever more acute. A variety of actors have the capability to disseminate false or deliberately misleading information via digital communication channels. These interventions in, and from, the information space are a threat, often intended to manipulate public debate and the democratic opinion-building process, and can even extend to attempts to manipulate elections. With this in mind, it is essential that citizens are able to form their own opinions freely without outside interference.

Topic area "ethics"

In order to be able to assess the effects that the latest technological developments and the introduction of future technologies have on the fundamental rights and freedoms, appropriate mechanisms and forums need to be installed. These bodies are to examine technical and ethical questions associated with such technologies.

Business

Topic area “Austria as a business location”

The state and the economy have the shared objective to make Austria an attractive and safe business location. Improving cybersecurity in enterprises will greatly contribute to their continued growth and economic success. Reducing our dependence on IT products and services provided by enterprises from outside Austria and/or the EU will help to bolster Austria’s and the EU’s sovereignty in the digital realm.

Solutions or products designed to identify and defend against cyberattacks must be used more widely in order to ensure effective compliance with both Austrian and EU law.

Topic area “small and medium-sized enterprises (SMEs)”

Cybersecurity is a particularly important element when it comes to strengthening Austrian SMEs and improving their framework conditions. Cybersecurity is a major factor in Austria’s digitalisation drive, which is designed to encourage a range of digitalisation measures among domestic SMEs. In addition, the framework conditions are to be designed in such a manner that also measures will be taken that strengthen cybersecurity within small and medium-sized enterprises, for example by enhancing the digital skills of the employees, by ensuring compliance with basic technical and organisational basic security requirements, by helping enterprises to select, and cooperate with, reliable partner enterprises, and by helping them to use trustworthy cloud services.

Topic area “critical national infrastructure”

Critical national infrastructure is worthy of special protection against cyberattacks. Enhancing the overall level of cybersecurity and improved cooperation will contribute to making Austria more resilient against cyberattacks. Austria’s cybersecurity programme is harmonised closely with the national programme for protecting critical infrastructure.

Education, training, research and development

Topic area “education and training”

Expanding Austria’s cybersecurity capabilities and widening the range of respective training will play an important role in our efforts to defend Austria against cyberattacks. This will also help to address the current shortage of cybersecurity specialists. A large number of individual measures and initiatives are already underway across Austria; these initiatives should be brought together as part of a cohesive overall strategy. Since digitalisation and technological developments never stop, keeping up with progress requires life-long learning. This means educating all strata of society in cybersecurity matters, from children and young people to working age adults and pensioners.

Topic area “research and development”

Research and development are making a major contribution to improving our overall level of cybersecurity, and thus are also playing an important role in helping to identify the latest trends and technologies, and develop IT security solutions. Under the ÖSCS 2021, a framework will be established to close the gap between application-focused research projects and the public procurement process. This framework will cover everything from fundamental research to the introduction of specific products to the market. The Austrian state is both a client and a launch customer of cybersecurity systems developed in Austria, and in this dual role helps to enhance an application-focused approach to research and makes it easier for Austrian enterprises to market their cybersecurity solutions.

Public sector

Topic area “resilience”

In order to guarantee Austria’s resilience, it is necessary to establish effective and binding cooperation between federal, provincial and municipal authorities. Efforts to implement Austria’s Network and Information Systems Security Act and protect Austria’s critical national infrastructure are particularly important in this respect. The existing mechanisms for dealing effectively with cyber incidents and crises and the mechanisms for keeping channels of communication open in the event of an incident are subject to constant review, and are continuously being improved. Manufacturers and service providers in Austria and the EU play a particular role in boosting resilience. A major effort is underway to develop the legal basis for our national approach to improving cybersecurity.

Topic area “cybercrime and prosecuting offenders”

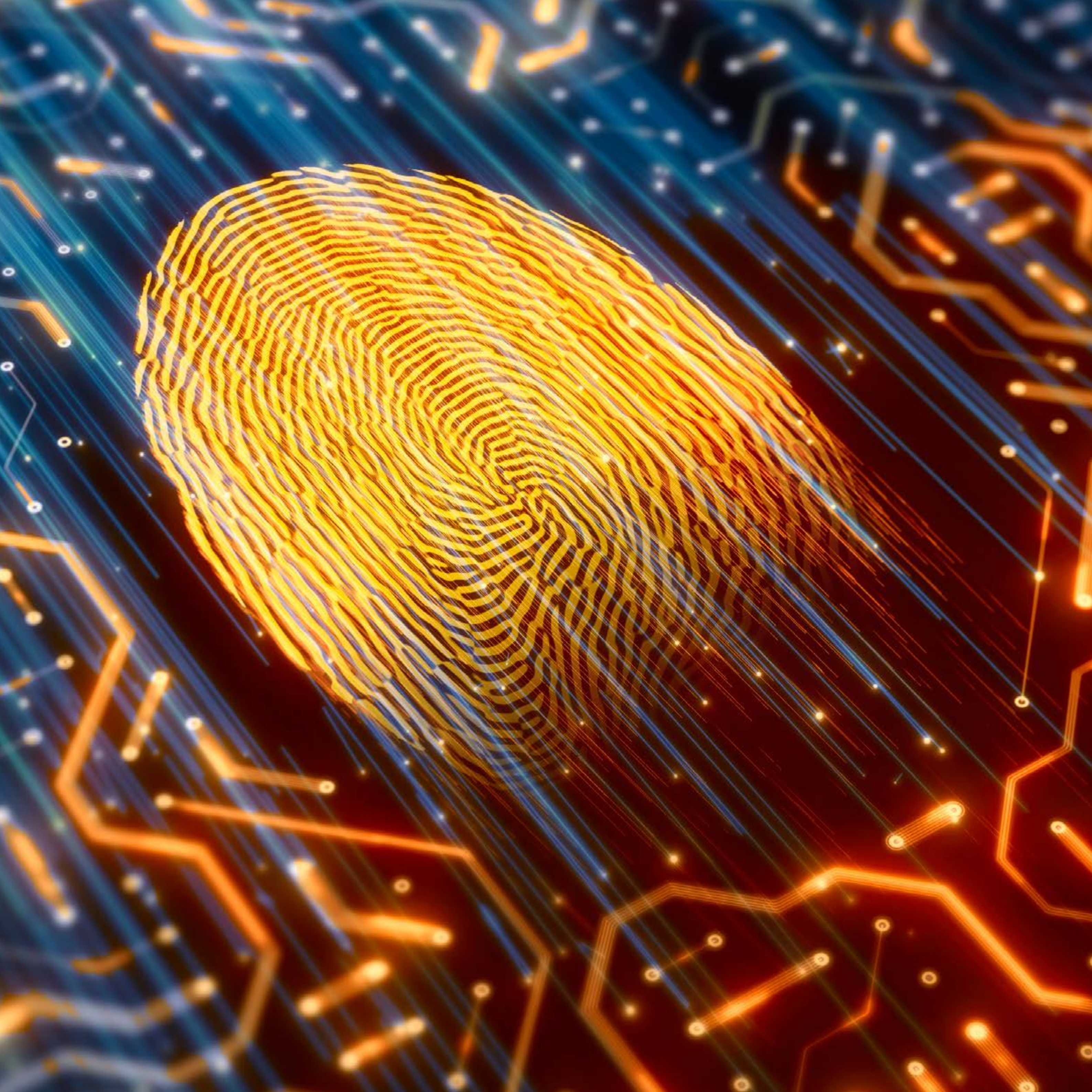
More and more people using more and more devices and rapidly developing technologies lead to an ever increasing degree of networking, augmenting the already considerable potential for cyber criminals to harm our society. This is why it is important to review and update our detection methods and preventive techniques for attacks as a part of an overall strategy that is open to the latest developments. By continually updating the legal basis, including by increasing the range of sentences associated with such offences, effective prosecution of cybercrime is facilitated, both in Austria and abroad. Moreover, technical investigation measures are expanded, support of detection and investigation is enhanced by way of social media and open source intelligence units, and specialist cyber expertise and structures are developed within prosecution authorities. Effective strategies for fighting cybercrime and an efficient criminal justice system are fundamental prerequisites for tackling cyber criminals. What is more, specialist cybercrime offices are expanded and further developed within the justice system. Since cyber criminals do not respect international borders, international cooperation on this issue needs to be continued and enhanced further. Cooperation in the context of Europol’s European Cybercrime Centre (EC3) and Interpol are absolutely essential. Particular attention is to be placed on the ongoing negotiations on the upcoming UN Convention on Cybercrime, which will be held in Vienna and New York in the coming years. Given the complex nature of the issues at play, structures need to be set up especially at the local level to support citizens and enterprises quickly and effectively when they fall prey to cybercrime.

Topic area "cyber defence"

Austria's military national defence in cyberspace is an element of Comprehensive National Defence, which means that it forms part of the Austrian Armed Forces' responsibility to ensure national security provision. Expertise and capabilities in the cyber field across the entire spectrum are to prevent, and defend Austria's sovereignty against, cyberattacks. This is a direct contribution to enhancing national resilience and allows the Austrian Armed Forces to provide assistance in dealing with cyber crises as a part of the national cybersecurity architecture.

The Austrian Armed Forces and the Federal Ministry of Defence both make strategic contributions to the national picture of the situation in Austria, help to identify the sources of cyberattacks, enhance the cyber defence capabilities in cooperation with national and international partners, and thus bolster the EU's overall cyber defence.

Cyber defence is a national process under the auspices of the Federal Ministry of Defence. It encompass all measures intended to prepare Austria for potential cyberattacks as well as to maintain and restore Austria's ability to act in the context of an attack that might endanger its sovereignty.



Topic area “international cooperation”
Cybersecurity needs to be planned beyond our national borders.

With this in mind, the ÖSCS 2021 takes a European and an international approach to the issue. Given that most networks in cyberspace are transnational, Austria can only ensure the security of its digital infrastructure by embedding and strengthening its own domestic measures as a part of European, regional and international processes. Austria is continuing to play a proactive role within the EU, the United Nations, the Organization for Security and Co-operation in Europe (OSCE), the Council of Europe, the Organization for Economic Co-operation and Development (OECD) and the NATO-Partnership for Peace, as well as cultivating and deepening bilateral cybersecurity relationships. As a part of the present Strategy, Austria will establish itself as a hub for an open, global exchange on cybersecurity issues.

At the same time, the Strategy will correct asymmetries that currently put the EU and/or Austria at a disadvantage, particularly those with the potential to affect Austria’s strategic autonomy and digital sovereignty in areas like data protection, hardware, software or cloud systems.

Austria is working on the international stage to secure a safe, open cyberspace where the rule of law is respected, international law applies, and where ensuring that all users are able to exercise their human rights is a top priority.

5

Measures, implementation and monitoring

” By using their expertise to implement these measures, stakeholders will make a major contribution to the success of this Strategy, and by extension to improving the overall level of cybersecurity in Austria.

Measures

The specific measures in the List of Measures are essential for the implementation of the present Strategy. The List of Measures will be updated and published at regular intervals as far as possible. Each individual measure is associated with at least one of the objectives set out in Section 3, and assigned to one or more of the target audiences discussed in Section 4.

The Cyber Security Steering Group will update the List of Measures to take account of the constantly evolving threat picture and to reflect new challenges as they arise. The Cyber Security Steering Group will suggest which actions should be assigned to which ministries in line with the respective ministries' individual areas of responsibility or be officially assigned to individual ministries for action by the Secretaries General of the ministries in question. When the Cyber Security Steering Group suggests that given measures are relevant to all ministries, individual actions will be agreed following a plenary meeting of the Secretaries General, before being referred to the relevant heads of the ministries responsible for cybersecurity for implementation. In the course of the assignment process of Secretaries General, care must be taken to ensure that all the organisational, financial and technical requirements are in place.

Guidelines designed to support implementation are provided in the annex.

Measures to be implemented by society as a whole, businesses, the education sector, or the research and development community can also be proposed by private sector stakeholders as a part of ongoing cooperation between the state and the private sector via the Cyber Security Steering Group, the Cyber Security Platform or the Cybersecurity Competence Community. The Cyber Security Steering Group will then examine whether the proposed measures should be included in the List of Measures.

Measures proposed should be flexible to respond to changes in the current threat situation and new cybersecurity challenges. Adjustments may also be required as a result of political, technological, societal and economic developments at the domestic, the EU or the international levels.

Implementation plan

Individual ministries draw up a detailed implementation plan for each individual measure that falls within their respective remits. These plans are then submitted to the Cyber Security Steering Group's Secretariat once every six months or as required. Implementation plans must set out specific tasks, activities and responsibilities in relation to the task at hand, as well as quality assurance procedures. Descriptions of these procedures must specify, as a bare minimum, a timescale for the relevant task and milestones by which progress can be measured.

To assist ministries in drawing up and implementing these plans, implementation guidelines have been included in the annex.

Monitoring

Responsibility for monitoring the implementation of the Strategy lies with the Cyber Security Steering Group. The Cyber Security Steering Group's Secretariat retains all the implementation plans centrally, and uses them as the basis for a progress report, which it submits to the plenary meeting of the Secretaries General biannually. Current measures are subject to interim review by the Cyber Security Steering Group once every six months.

6

Opportunities and outlook

> ” A fully implemented cybersecurity policy opens up an array of possibilities and opportunities. Such a policy is decisive to the prosperity of the citizens as well as to their ability to take part in society and public life, and to ensuring their security.

Cybersecurity opportunities

Alongside the challenges and threats mentioned in Section 2, cybersecurity also provides a wide range of opportunities and potential benefits, which should be exploited as far as possible.

Specifically as far as Austria is concerned, increasing digitalisation would appear to provide the following opportunities:

1. **Opportunities for society**
   A cyber-secure environment will make it easier for individuals to partake fully in society and public life, and encourage the use of cyberspace as a platform to participate in society. However, this environment cannot be created without secure means of communication and interaction in both the private and public sectors.

2. **Opportunities for the economy**
   Cybersecurity is a growth market. As digitalisation continues apace, it is opening up a wide variety of potential attack vectors and other risks, which have to be addressed by innovative products and services. In turn, the need for these products and services means there is scope to open up new sectors and markets within the economy. In this regard, Austria should place a particular emphasis on developing sustainable, environmentally-friendly products. Providing businesses with a secure, innovative environment and resilient digital infrastructure will lay the foundations for all economic activity in the future. A resilient economy that is well prepared for cyberattacks will help to strengthen Austria’s position as an attractive location in which to do business, and will provide long-term competitive advantages in what is an increasingly complex and digitalised environment.

3. **Opportunities for education, research and development**
   Demand for qualified specialists is increasing rapidly, and there is an acute need to expand the range of training available, to improve the overall posture of Austria's universities, and to promote innovative projects in this field. Cybersecurity offers great potential to expand the primary, secondary and tertiary education systems in an effective and targeted way, and Austria must make use of this.

4. **Opportunities for the public sector**
   The development and use of secure IT systems will help the public sector to interact securely and directly with individual citizens and with businesses. A cyber-secure environment and reliable crisis management systems will serve to bolster trust in state institutions, and ensure the state is able to act when necessary. International engagement on cybersecurity issues also serves to strengthen Vienna's position as a diplomatic hub.

Outlook

Cybersecurity issues are increasingly affecting Austrian citizens in every aspect of their daily lives. Cyberspace is not static; indeed, it is constantly evolving. Nevertheless, existing legal frameworks, and in particular the principles of international law, human rights law and humanitarian international law, still apply in the digital realm. Threats and challenges in cyberspace can rarely be contained within national borders. This means that security can only be ensured through a comprehensive cybersecurity policy and close cooperation with all relevant stakeholders. This is what the ÖSCS is designed to achieve. With its list of specific measures to be implemented, it provides a flexible, effective and inclusive tool for detecting, preventing and dealing with threats and challenges in cyberspace, with the dual aims of achieving the highest possible level of cybersecurity and making the most of the opportunities digitalisation brings in every area of our lives.

” Cybersecurity affects us all. Making cyberspace safe over the long-term, and making Austria more resilient against cyberattacks, will require all stakeholders to work together. This is the only way to make the most out of the many and varied opportunities cybersecurity can deliver.

152.68
200.84
123.05
971.91
451.91
229.56
279.82
977.65
292.76
555.74
73.79

List of abbreviations

AI	Artificial intelligence
BKA	Federal Chancellery
CKM	Cyber Crisis Management
CKM-KA	Cyber Crisis Management Coordination Committee
CSP	Cyber Security Platform
CSS	Cyber Security Steering Group
E-ID	Electronic proof of identity
EC3	European Cybercrime Centre
ENISA	European Union Agency for Cybersecurity
EU	European Union
IKDOK	Inner Circle of the Operative Coordination Structure
IT	Information technology
IoT	Internet of Things
NATO	North Atlantic Treaty Organisation
NISG	Network and Information System Security Act
OECD	Organisation for Economic Co-operation and Development
OpKoord	Operative Coordination Structure
OSCE	Organisation for Security and Co-operation in Europe
ÖSCS	Austrian Strategy for Cybersecurity
SKKM	State Crisis and Disaster Protection Management
SMEs	Small and medium-sized enterprises
UN	United Nations

7

Annex to the ÖSCS 2021

Implementation guidelines

The guidelines below are designed to help and guide ministries to implement individual measures as straightforwardly and efficiently as possible. All or several of the guidelines may apply depending on the specific task concerned.

1. **Security:** The operation and further development of IT systems has be based on an overarching security philosophy incorporating strategic, organisational and technical elements (such as security by design). A common approach must be drawn up across all ministries.

2. **Risk-based approach:** The ÖSCS 2021 is based on a holistic and risk-based approach that aims to identify and prioritise the most likely and most serious risks, and to develop suitable countermeasures to deal with them.

3. **Transparency:** The principle of transparency is followed when it comes to implementing measures. This is reflected in the fact that the List of Measures and the progress report are published whenever possible.

4. **Cooperation:** Relevant stakeholders work together to implement specific measures.

5. **Multi-stakeholder approach:** As a part of the cooperative approach, all relevant interest groups are to be involved in discussions and be given the opportunity to influence processes and activity wherever possible. It is particularly important to ensure that measures taken in the public and private sectors are complementary.

6. **Self-responsibility:** As long as the ministries' IT systems are not run on a joint basis, each ministry is responsible for its own IT systems.

7. **Cost-effectiveness:** Measures have to be implemented using existing economic and financial resources and synergies.

8. **Legal drafting:** In order to ensure that legislation on cybersecurity is clear, comprehensible, and applied as a part of a cohesive system, legal provisions in this area should be drafted as clearly and comprehensively as possible and, where this is permitted under constitutional law, incorporated into a set of regulations.

9. **Conformity with the EU:** Priorities and developments at the European level have to be taken into account when implementing measures.

10. **Ethics:** Ethical issues associated with new technologies should be considered on the basis of existing European and Austrian fundamental values.

Legal notice

Media owner, publisher and editor:
Federal Chancellery, Ballhausplatz 2, 1010 Vienna
Authors: Federal Chancellery, Department I/8 – Cybersecurity, GovCERT, NIS-Office and ZAS
Produced by: Federal Chancellery
Photo credits: iStock, BKA/Andy Wenzel (Federal Chancellor Karl Nehammer)
Layout: BKA Design & Grafik
Printed by: Druckwerkstatt Handels GmbH
Vienna, 2021. Last updated: 22 December 2021

Please note that no warranty is extended in relation to any of the details contained in the present publication. Although every care has been taken to ensure the information is accurate, neither the Federal Chancellery, nor and the author(s) of the present document accept any liability in relation to its content. Any statements regarding legal matters represent the personal opinions of the author(s). Such statements are not legally binding, and do not prejudice the applicability of existing jurisprudence or case law under any circumstances.
Feedback: Please send any comments you may have about this publication to cybersecurity@bka.gv.at.

Federal Chancellery
Republic of Austria