Cybersecurity Report for 2021

Cybersecurity Report for 2021

Vienna, 2022

Federal Chancellery
Republic of Austria

Federal Ministry
Republic of Austria
Interior

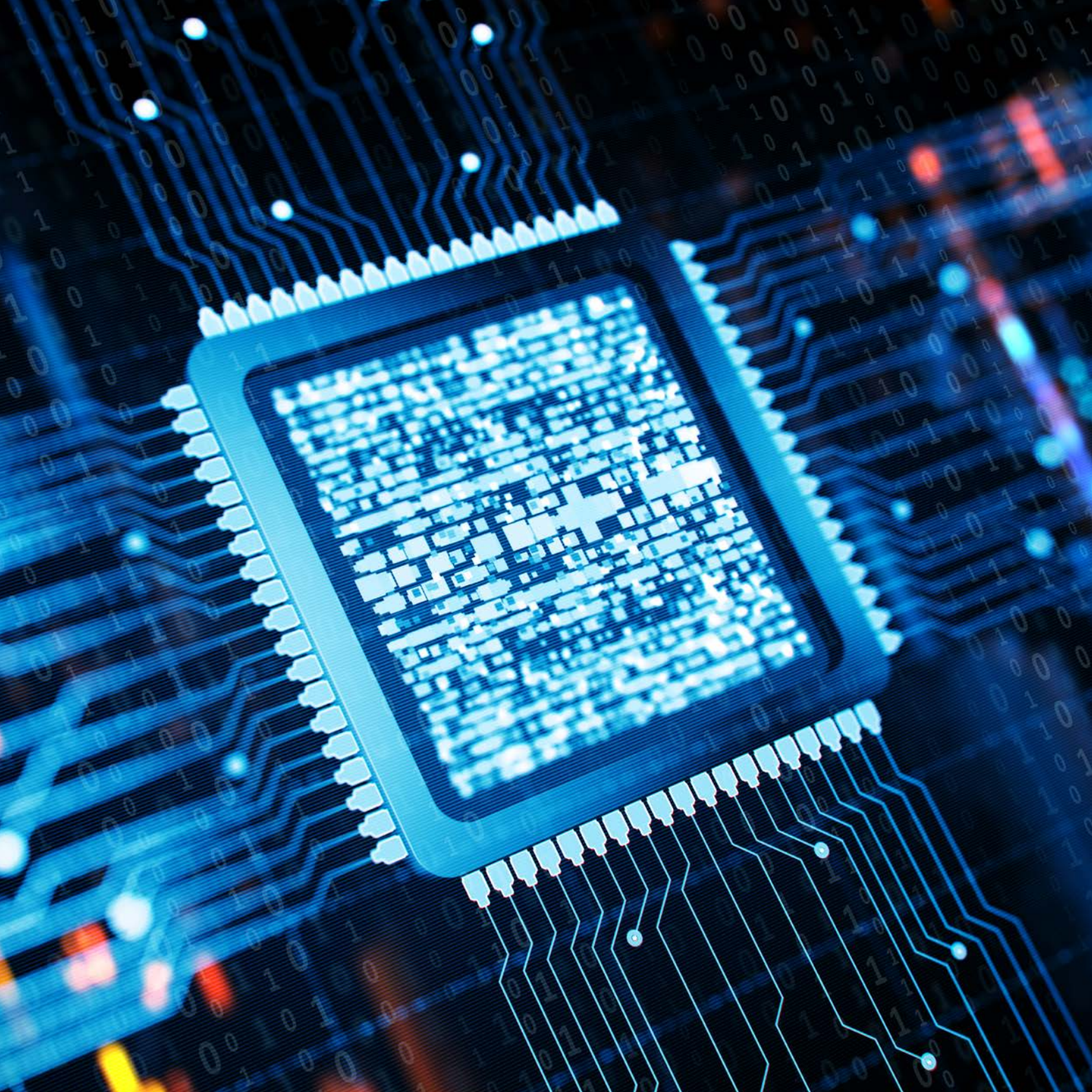
Federal Ministry
Republic of Austria
Defence

Federal Ministry
Republic of Austria
European and International
Affairs

Publication details

Media owner, publisher and editor:
Austrian Federal Chancellery
(Bundeskanzleramt)
Ballhausplatz 2, 1010 Vienna
Graphic design: BKA Design & Grafik
Printed by: Druckwerkstatt Handels GmbH
Vienna 2022

Inhalt



Editor's note

Cries of "habemus novum cybersecurity chartam!" rang through the halls of the Federal Chancellery the evening before Christmas Eve when the new Austrian Strategy for Cybersecurity 2021 entered into force through a circular resolution. Maybe not quite those words, but it was done!

After a few brief interludes such as a government of experts, a National Council election, a cyber incident in the Federal Ministry for European and International Affairs and a pandemic, the work was able to be completed successfully and presented to the Federal Government for a vote. The date 22 December 2021 will forever remain etched in the minds of those who were involved.

Using the approach of designing the strategy as a document AND a dynamic platform, a new, innovative path was taken – such a thing does exist in public administration (and in reality much more often than generally assumed). This enables the stakeholders to be more involved in the identification and definition of actions to achieve the goals of the Austrian Strategy for Cybersecurity 2021. The platform itself is also being developed continuously and cooperatively between the authorities and target groups, which will lead to interesting and valuable insights and functionalities in the future.

In the meantime, Brussels has been negotiating the exact design of the NIS2 Directive (as a successor to the EU Directive concerning measures for a high common level of security of network and information systems across the Union), with the active involvement of the Austrian representatives. While NIS1 still aimed to support the critical infrastructures and the operators of essential services to increase their security in the cyber space, the scope of NIS2 will be much broader. This is an opportunity for Austria and for Europe as a whole to become more cyber resilient together.

But of course, last year was not only characterised by the strategic level: There were also at least two incidents in the operational area in 2021, which showed Austria and the entire world their dependencies in the cyber supply chain as well as their dramatic vulnerability. Suddenly it was no longer just about companies securing and hardening their own systems. Software providers and in some cases even their subcontractors proved themselves to be highly problematic gateways for vulnerabilities and malicious functionality.

With the turn of the years 2020/2021, it became known that global software vendors and even security software vendors themselves had been infiltrated and would thus deliver malware to customers. The number of people affected and the extent of the damage were initially impossible to estimate, and only during the first six months of 2021 did it transpire that it was primarily government organisations or those close to them that were affected. State control of the attack seems likely.

But it's not always just targeted attacks which can lead to massive damage due to the complex dependencies on and between software.

Software development is time-consuming and cost-intensive. To avoid having to "reinvent the wheel" with every new product, developers use function libraries so non-domain-specific problems can be solved quickly and in a broadly standardised way. One of these libraries, Log4J, is used to implement the logging functionality necessary in any sufficiently competently developed software – i.e. the traceability of internal processes at program runtime. Unfortunately, a vulnerability in this software was overlooked. This meant that hundreds of thousands of applications were suddenly potentially at risk. The Director of the US Cybersecurity & Infrastructure Security Agency called this vulnerability probably the most serious of her career. It ultimately transpired that the development and maintenance of this central software was run by two developers as an open-source project, free of charge and in their spare time. These two people cannot be blamed at all,

but it clearly shows that mechanisms are needed to test even open-source software in a structured manner and to clarify responsibilities. Initiatives such as the unfortunately expired EU-FOSSA 2 Bug Bounty program,[1] could generate appropriate attention here.

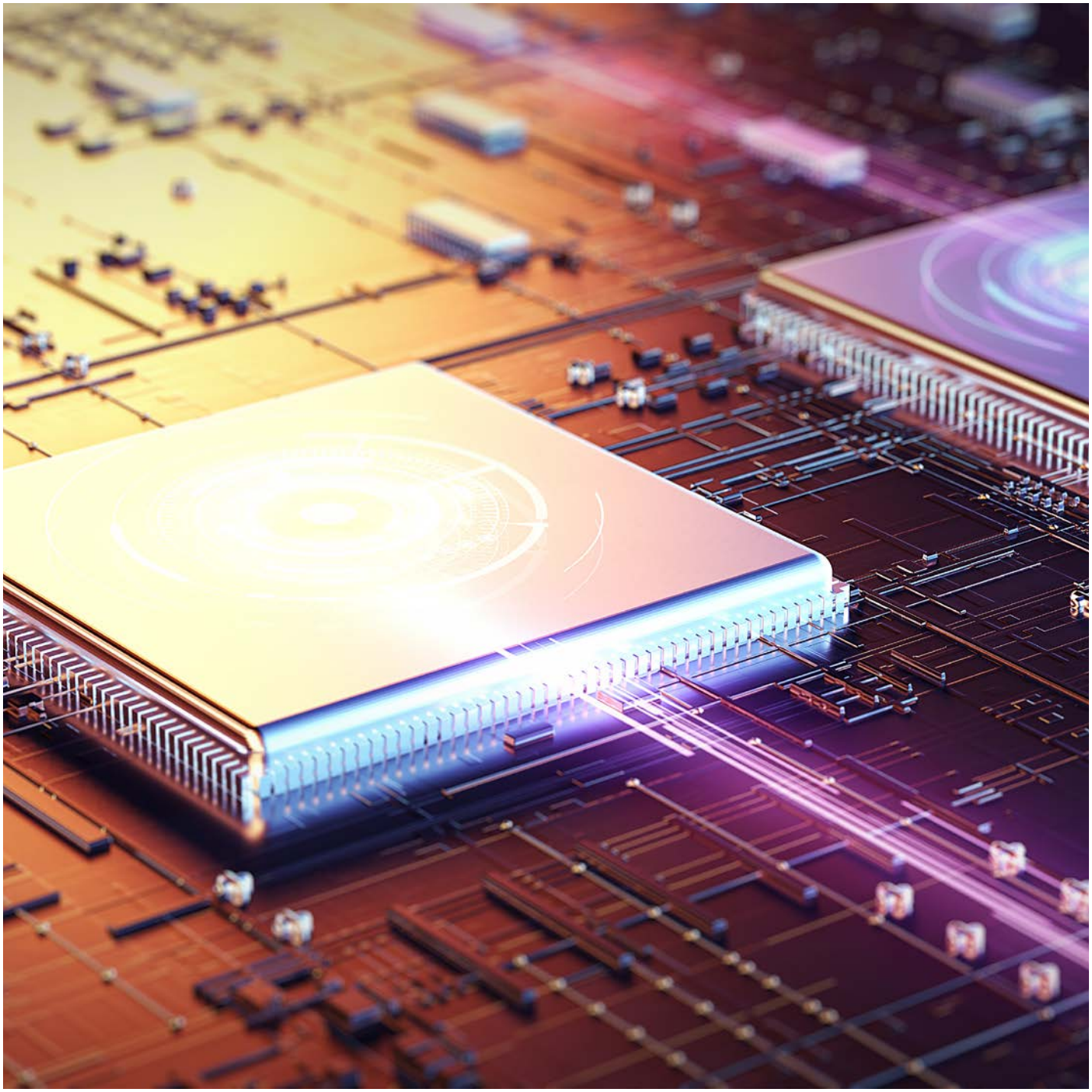
A company that tried particularly hard not to generate any attention got more than enough of it in 2021. There has been much discussion of the NSO Group and their spyware "Pegasus", which is used by state clients. Surprisingly, it was found not just on the mobile phones of alleged or identified terrorists. Politicians, dissidents, human rights activists and journalists were also being monitored by the software. Officially there are no known infections in Austria. Ultimately, the NSO Group was even put on the US blacklist, as the spyware manufacturer had acted "against the foreign policy and national security interests of the United States". However, it is doubtful that this will mean the end of the spyware industry.

There is still a lot to tell and readers who are so inclined can learn some of what happened last year from this report. Happy reading!

After all of the excitements of 2021 with the pandemic and the high numbers of cyber attacks, one thing is clear: 2022 can only be calmer...

…d'oh!

1 See https://ec.europa.eu/info/departments/informatics/eu-fossa-2_en



Introduction

In accordance with the Austrian Strategy for Cybersecurity 2021 (ÖSCS 2021), the Cyber Security Steering Group (CSS) has to prepare an annual report on cybersecurity in Austria. The last report was presented in July 2021.

The current Cybersecurity Report for 2021 is based on the content of last year's report with the addition of current developments focusing in particular on the areas of international and operational developments. The observation period is 2021 with the inclusion of a few current developments from 2022.

The aim of the report is to provide a summary review of the cyber threats and major national and international developments. The basis for this is department-specific reports on the topic.

1
Cyber situation / threat

Increasing Austria's digital resilience and ensuring cybersecurity in the digital world as a whole is of great importance for both our prosperity and our security.

Cybersecurity is a top priority for Austria, and a major challenge for all sectors, government, businesses, scientific institutions and society alike.

1.1 Cybersecurity situation – operational level

In the last few years, ransomware has been a constant problem for the economy and society. Cyber criminals responded to the improvement in security and back-up mechanisms with ever new ways to generate illicit profit. After ultimatums and threats to delete data, the threat to publish data files has been added. In itself data theft is not new, but in combination with ransomware and the threat of targeted publication of internal information, many companies and organisations feel compelled to meet the perpetrators' demands.

Ransomware is still a major problem for the economy and the society

In addition to the actual damage caused by the attacks, which can have business continuity and restoration costs as a consequence, many victims fear the reputational damage that would be expected as a result of the threatened publication of the data. This is confirmed by the changes in share price and sales figures directly linked to the incident in terms of timing. In turn, cyber criminals are highly financially motivated and very quickly adapt to new circumstances or published vulnerabilities. Since the criminals often collaborate, we also refer to these groups as "criminal enterprises".

From this perspective, the spectrum of the attacks can also be understood differently. The assumption can be made that it is groups of perpetrators with high financial motivation and at least some extensive technical understanding. It is these financial opportunities on the part of the attackers that enable them to buy as yet unknown vulnerabilities (zero days) on "grey markets" or "black markets". Due to the mentioned circumstances, the ability of the perpetrators to adapt, the increasing technical complexity and the inherently worse initial situation for defenders (the defenders dilemma), detecting and handling incidents is becoming an ever more complex and challenging field. Cybersecurity analysts in particular are faced with the task of having a wide range of knowledge and skills available accessible at all times.

The following subsections address some of the “highlights” from the topic of cybersecurity in greater detail.

1.1.1 Data leaks and thefts

Data leaks due to insufficiently secured systems or due to security gaps identified too late already seem to be a common occurrence. Last year a large number of online service providers, particularly social media providers, which naturally have large databases, had to face this problem. The diversity of the exfiltrated data in terms of type or quality varies significantly. In 2021 the trend of attacks with the theft of customer and company data continued. Sometimes it is not the individual stolen data set that is problematic, but rather the sum of previously published data sets, which in turn enable new attack vectors such as social engineering or password spraying.

Maintaining data- and cybersecurity is essential for companies and organisations

In addition to this there are the “data thefts” mentioned at the start as part of ransomware campaigns. In many cases, these are databases that are considered to be particularly worthy of protection from a data protection perspective (General Data Protection Regulation [GDPR]). One factor that has attracted relatively little interest so far is the deliberate manipulation of published data. One approach is to intentionally mix in manipulated, compromising material with the real data as part of the published data sets. Providing evidence of manipulation is difficult, and at the same time broad media coverage can be expected. A company’s reputation is closely linked to its economic viability. Data and cybersecurity is therefore a survival factor for companies and organisations.

Ransomware groups have also moved to analysing the victim’s financial capacity as part of the initial compromise of systems and adjusting ransom demand to their target’s economic performance. This led to some horrendous demands in the observation period.

1.1.2 Pegasus spyware

In 2021, it became known that the Pegasus software, which was sold by the Israeli company NSO Group to investigating authorities, was also being used against opposition figures and journalists in various countries. This was brought to light by the NGO Citizen Lab and Amnesty International.

According to the company's description, the purpose of the software is to provide investigating authorities with direct access to smartphones and to therefore circumvent various encryption and protection mechanisms. Infection is possible without active interaction by the user – receiving a manipulated message is sufficient. The software has various mechanisms of concealment and can also interrupt the switching off process to remain active.

The monitoring tool, which has been in circulation since 2016, makes use of previously unknown vulnerabilities (zero days, 0 days), which made detection almost impossible. Thanks to Amnesty International, open-source software was developed that enabled the detection of an infection with the monitoring software based on the verification of a back-up that was created (MVT – Mobile Verification Tool) prior to the infection.

Over the course of the publication of the details on the use and the countries where the tool was used, a broad civil society and media front developed, which had both political and economic consequences for the NSO Group.

1.1.3 Log4j/Log4Shell

At the end of 2021, the vulnerability known as Log4j/Log4Shell in a popular and widespread Java library led to one of the most extensive security gaps of the past few years.

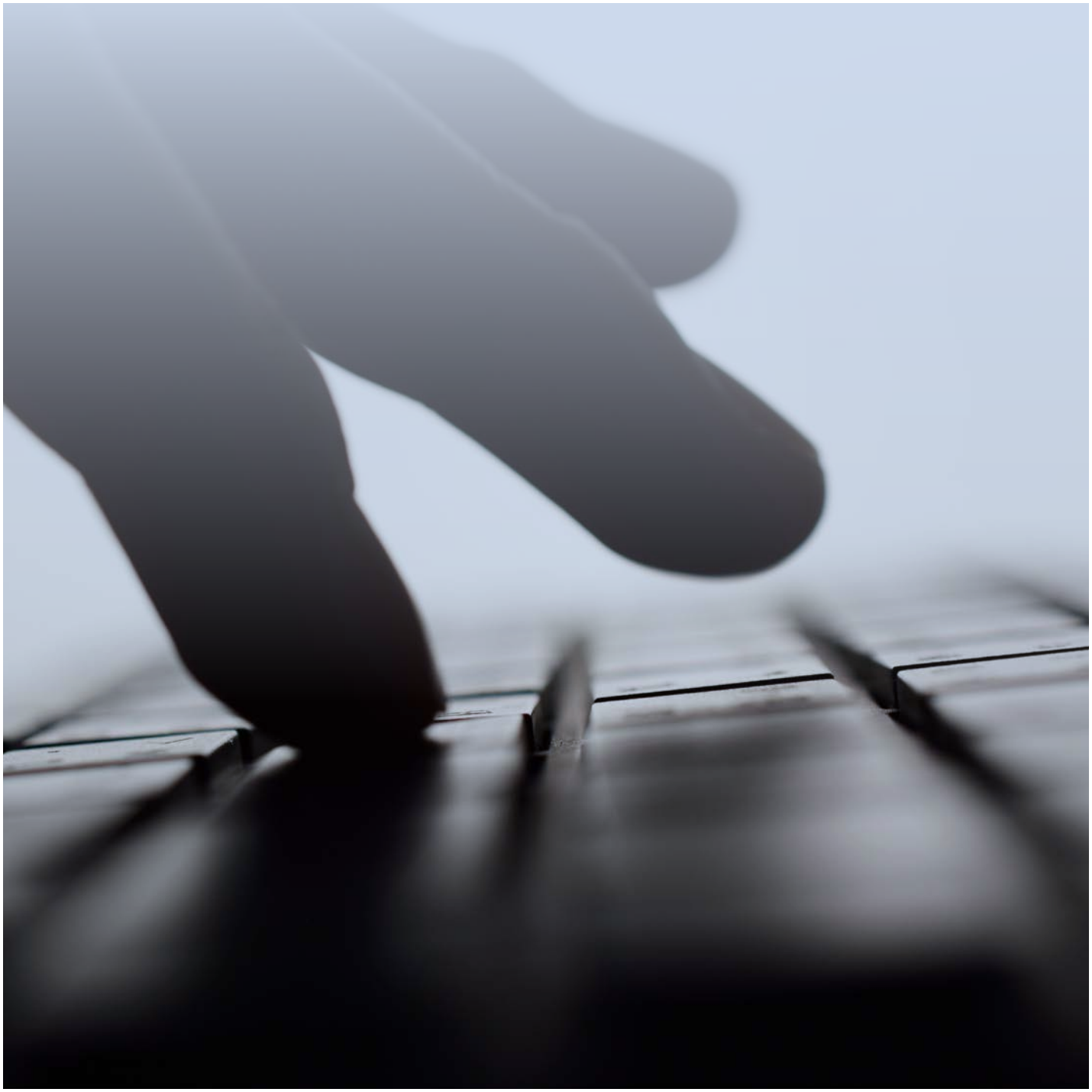
In software development, libraries are used to utilise functionalities that are frequently required over several development projects without having to implement them again every time. The library affected by the vulnerability provided logging and monitoring mechanisms, both of which are integral parts of any software project. This and the ability for developers to include it in their own software products, including commercial software products, as free and open-source mechanisms with no licence costs led to wide distribution. In an initial attempt it was not possible to determine which systems were actually affected, as the vulnerabilities had been integrated into numerous products through the library.

The high number of targets that were potentially at risk and therefore the possibility to take over systems more broadly led to a race between system administrators and attackers, with the speed at which this occured reaching unprecedented levels.

The state cybersecurity structures identified potentially affected systems in Austria and proactively contacted their operators. In this way lasting damage was to be prevented.

1.1.4 Advanced Persistent Threats (APT)

Advanced Persistent Threats (APT) are targeted cyber attacks that pose an increasing threat not only to the public sector, but to businesses and organisations. In addition to a high level of personal and financial background, APT are primarily characterised by technical skills above the normal extent. If a system is identified as worthwhile, it is often approached with persistence and a high level of resource commitment. If an attack of this type is successful, the APT often remain unnoticed in the victims' systems for a very long time. Sometimes security or intrusion detection systems are also manipulated specifically to undermine their security mechanisms.



APT are often used for spying. They therefore pose a particular risk in terms of spying on state secrets but also research and development results. In addition they can also be used for data manipulation or sabotage, for example in the area of critical infrastructure.

Both detection and defence against such attacks prove to be difficult. Once a system has been compromised, a comprehensive and challenging eradication and clean-up process is required.

Investments of critical infrastructure in the area cybersecurity are increasing again

The attribution of APT is only possible to a limited extent even if a significant effort is made. In many cases, technical indicators can be attributed to specific groups of perpetrators, although there are also documented false flag attacks at this level. Attributing an attack can therefore only be made in a strategic/political context.

1.2 Cybersecurity situation – companies and security service providers

For situation reports and assessment, state bodies work with the consumers using a collaborative model.

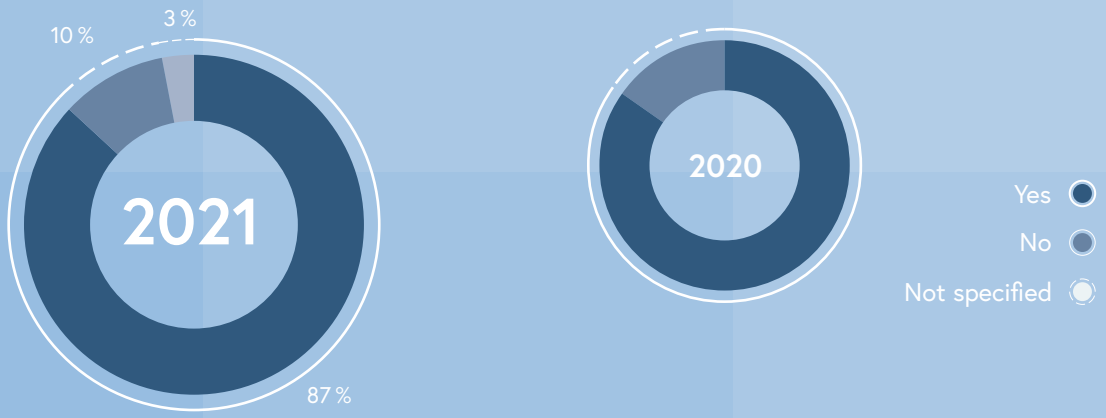
Therefore, in this reporting year again companies working in critical infrastructure, constitutional facilities and leading private companies in the cybersecurity industry, were invited to contribute. This helped creating a Common operational picture of Austria's cyber situation. The focus is not only on specific incidents, but also on trends and developments in the sense of an abstract overview presentation.

1.2.1 Companies working in critical infrastructure and government institutions

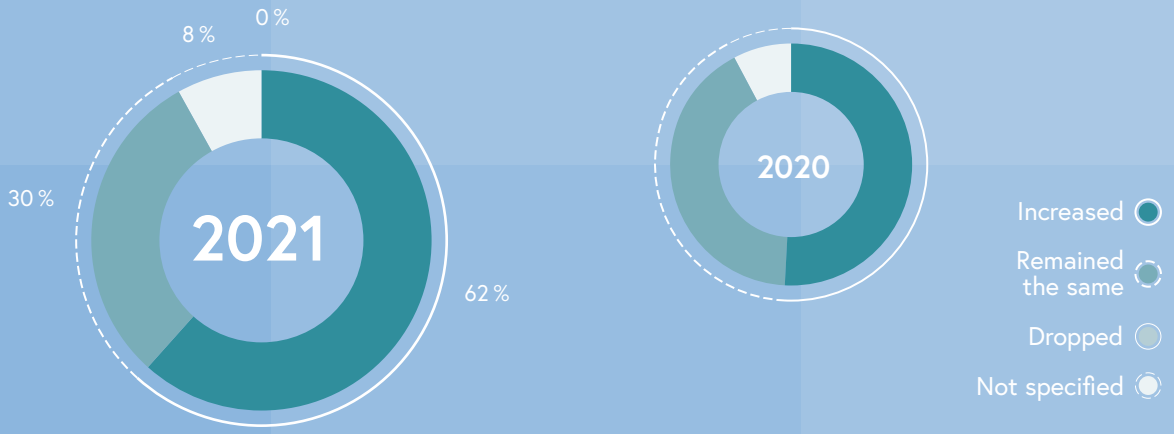
As in previous years, the majority of the 2021 surveyed Austrian critical infrastructure companies invested in cybersecurity. The ratio of companies that increased their cybersecurity budget to those that allocated the same amount of budget to cybersecurity as the previous year has been consistent over several years.

It is encouraging that no company reduced its cybersecurity budget. The targeted investments presumably prevented serious IT security incidents.

Has your company implemented any new IT security measures in 2021 that can increase the ability to detect IT security incidents?



How has the budget available for IT security in your company changed in 2021 compared to 2020?



The companies surveyed implemented a variety of different security measures during the reporting period. The following were named as examples:

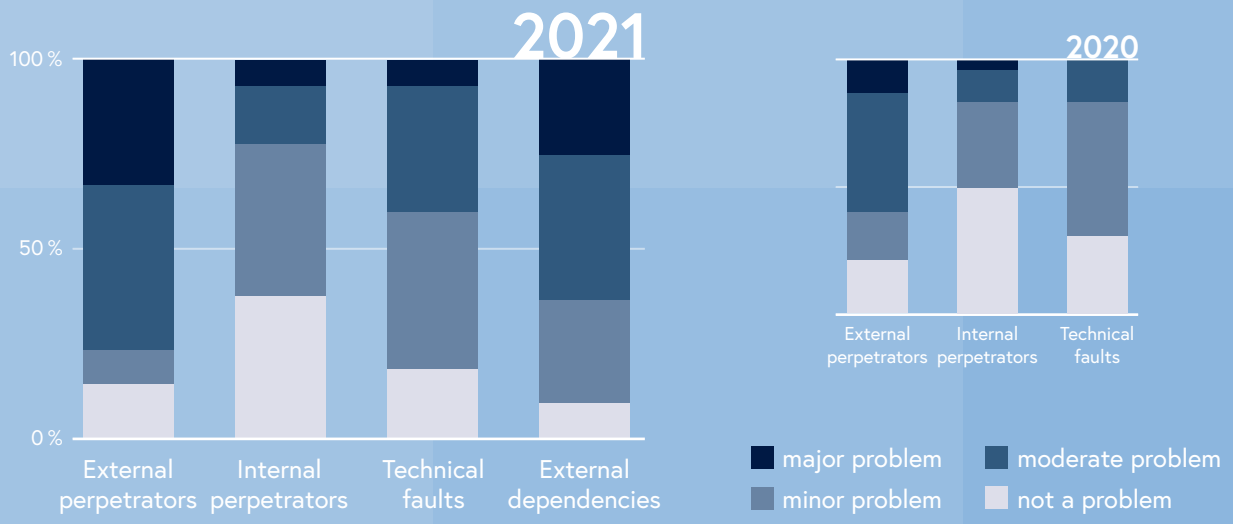
- Implementation of SIEM, SOC, EDR or ISMS solutions,
- Firewall optimisation and extension of IDS/IPS systems,
- Sandboxing, use of DNS filters,
- Enhanced logging and complementary monitoring tools, as well as further usage of multi-factor authentication (MFA).

Additional measures such as security awareness trainings for employees, penetration tests, security audits, phishing simulations, certifications (e.g. ISO 27001) and the implementation of various extended security concepts were identified as key drivers for increasing cybersecurity. This was often supplemented by targeted recruitment for the security sector.

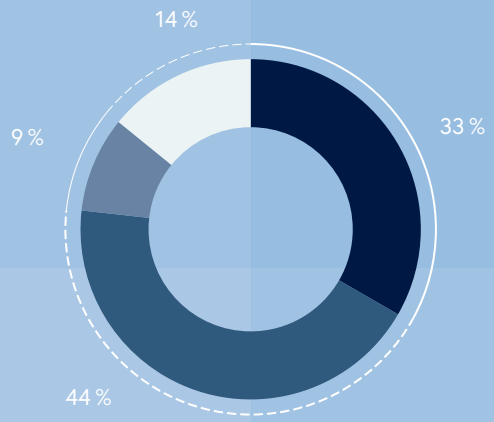
In 2021 primarily external perpetrators continued to be responsible for security incidents. External, sometimes non-controllable dependencies through the supply chain (e.g. the need to use certain software products), are increasingly being recognised as risks.

Among the respondents, technical faults mostly resulted in small to moderate problems, with actions taken to strengthen the resilience over the past few years. Accordingly, such incidents continued to decline compared to the previous year.

How would you rate the “causes of incidents”?

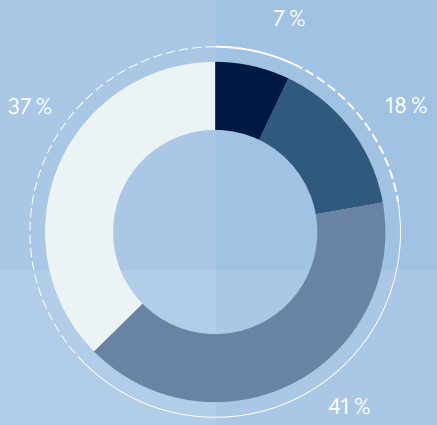


How would you rate the “causes of incidents” for external perpetrators for 2021?



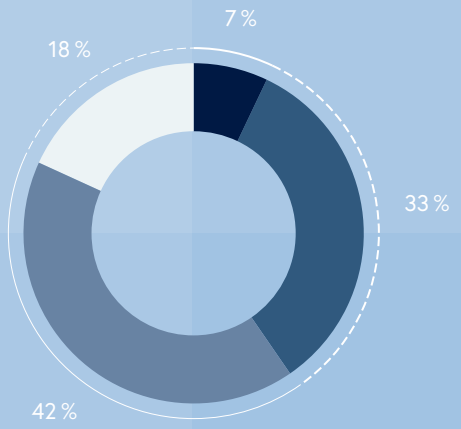
- major problem
- moderate problem
- minor problem
- not a problem

How would you rate the “causes of incidents” for internal perpetrators for 2021?



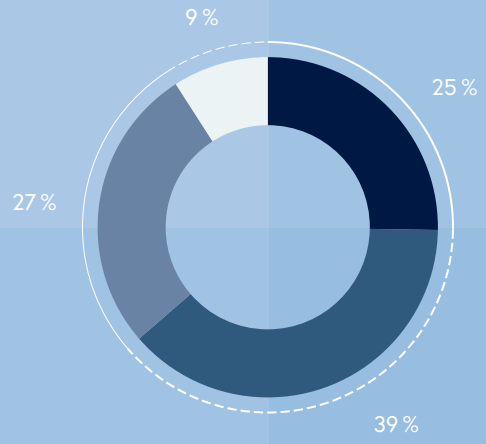
- major problem
- moderate problem
- minor problem
- not a problem

How would you rate the “causes of incidents” for technical faults for 2021?

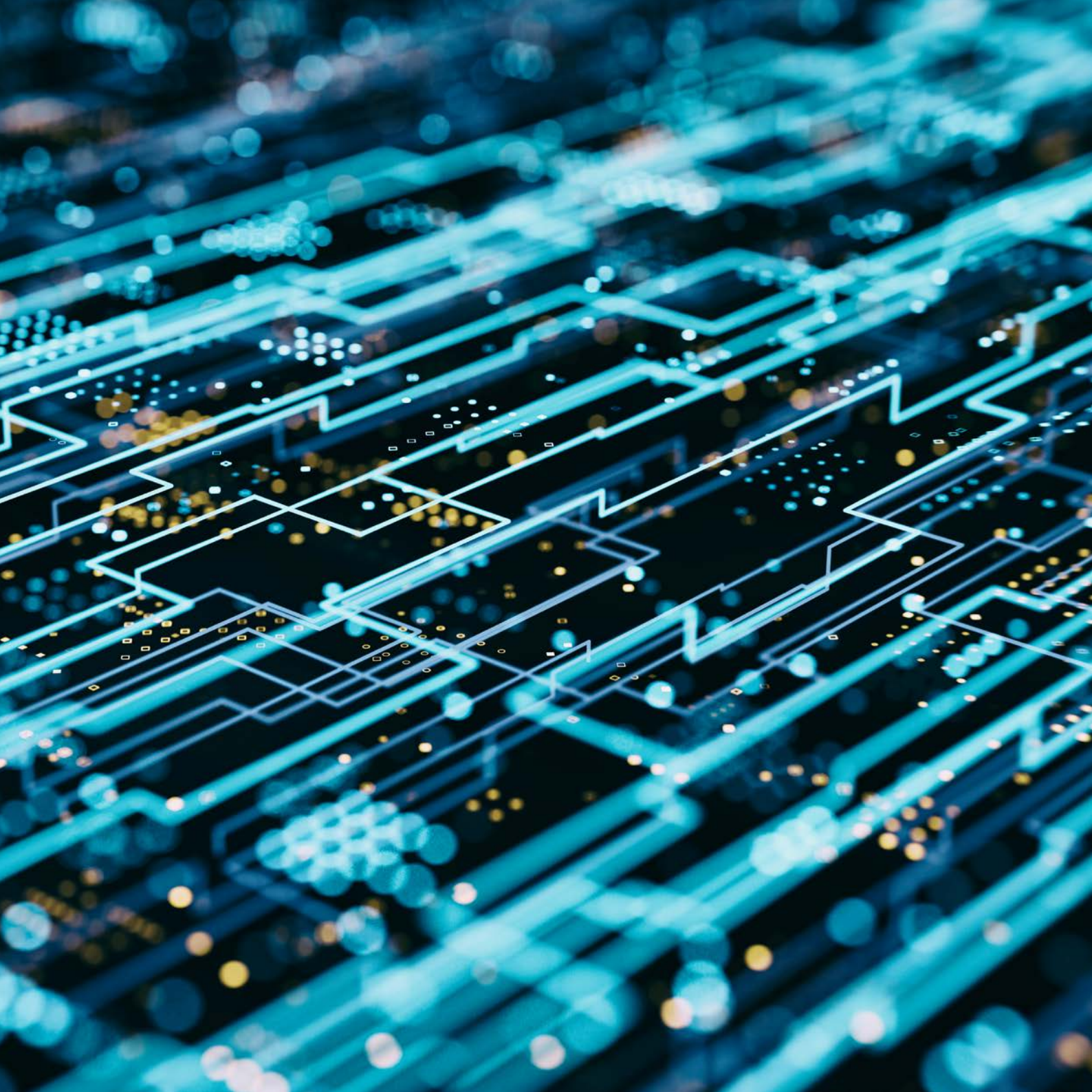


- major problem
- moderate problem
- minor problem
- not a problem

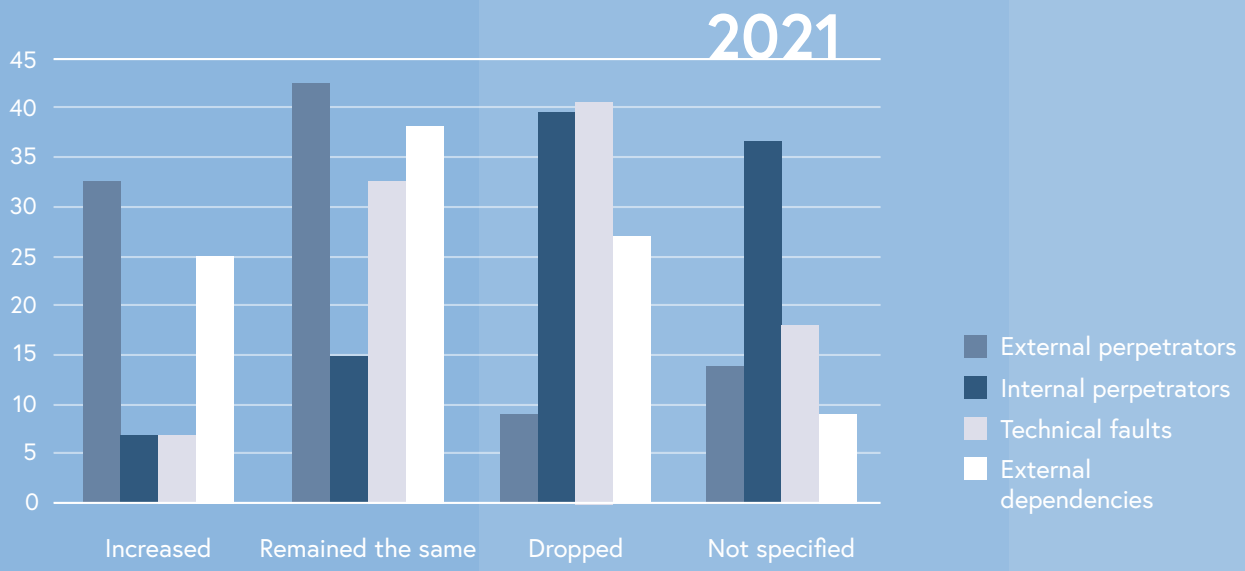
How would you rate the “causes of incidents” of external dependencies (suppliers, service providers etc.) – “supply chain” for 2021?



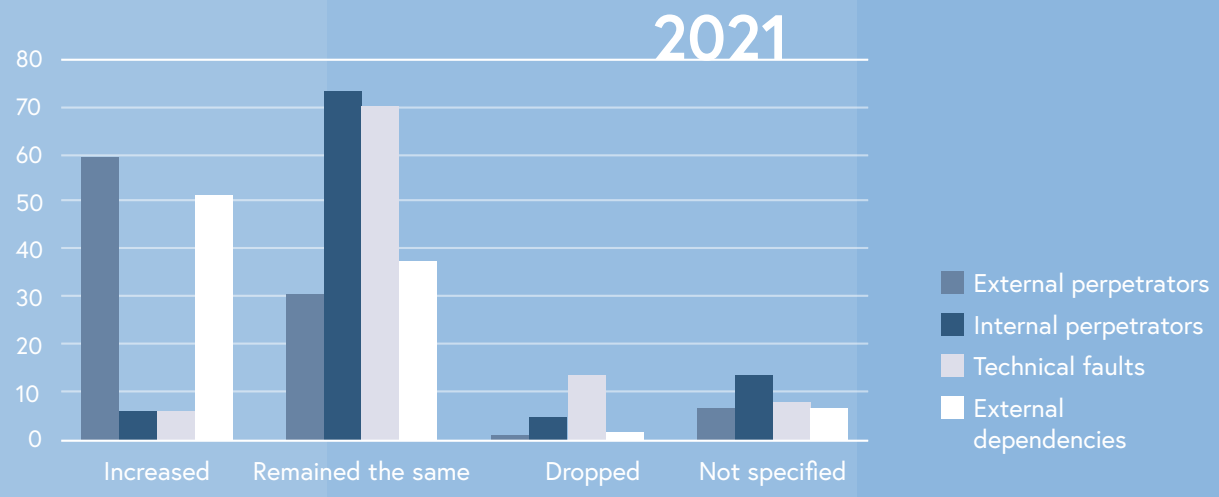
- major problem
- moderate problem
- minor problem
- not a problem



“Causes of incidents” compared to 2021?



What trends could you observe in this regard in 2021 compared to 2020?



The survey also asked which were the “lessons learned” for the critical infrastructure and constitutional facilities facing last year’s challenges.

In addition to awareness and raising it, the necessity for analysing dependencies in the supply chain and identifying vulnerabilities are essential.

The companies also indicated that penetration tests were becoming increasingly important for analysing vulnerabilities and therefore reducing one’s own attack surface.

Securing working from home environments is a key challenge

Detecting and handling incidents is becoming increasingly complex and time-consuming. Usable information from logging, EDR and SIEM systems should therefore be introduced and operated.

The timespan between publication and exploitation of vulnerabilities has reduced dramatically recently. It often only takes hours after the disclosure of a vulnerability for automated attacks to launch. Near-time Vulnerability and patch management is therefore becoming increasingly important.

Lastly, the emerging threats and challenges posed by the home office working environments and the resulting attack surface of widespread remote access was also cited. Appropriate security measures are becoming increasingly important here as well.

1.2.2 Leading private companies from the cybersecurity industry

The following trends and lessons identified can be derived from the survey responses received from leading private companies in the security services provider sector for the year 2021:

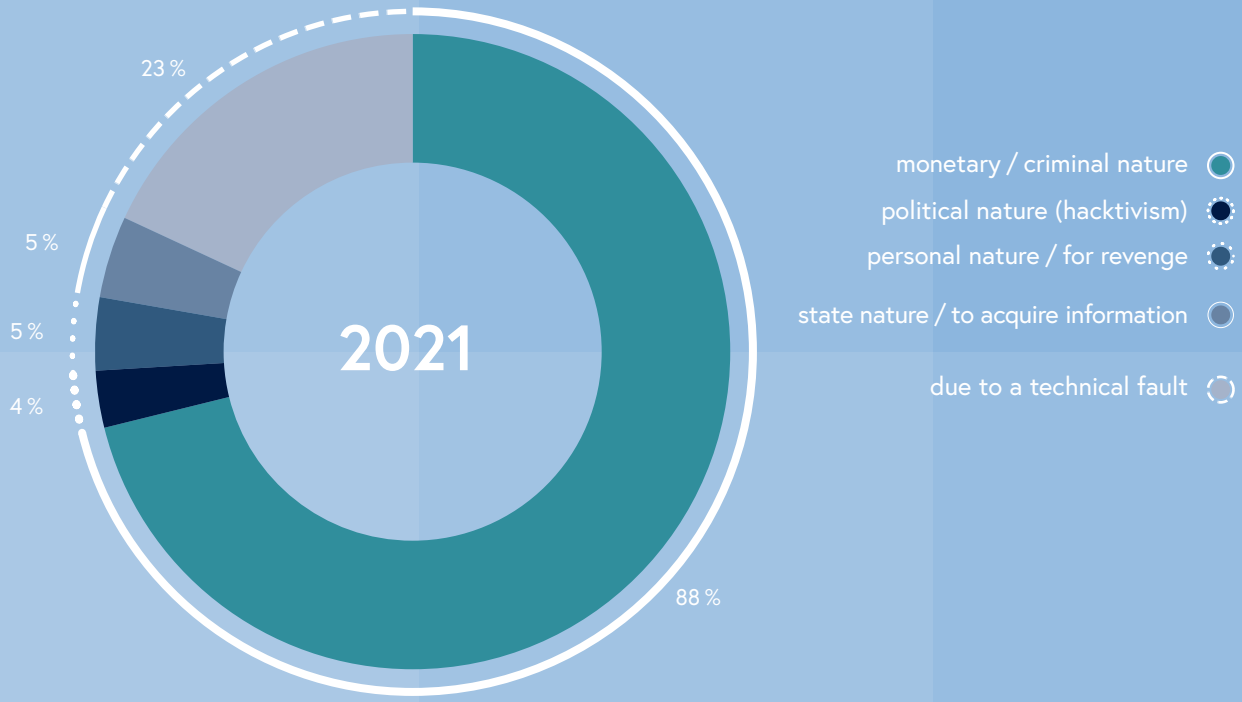
2021

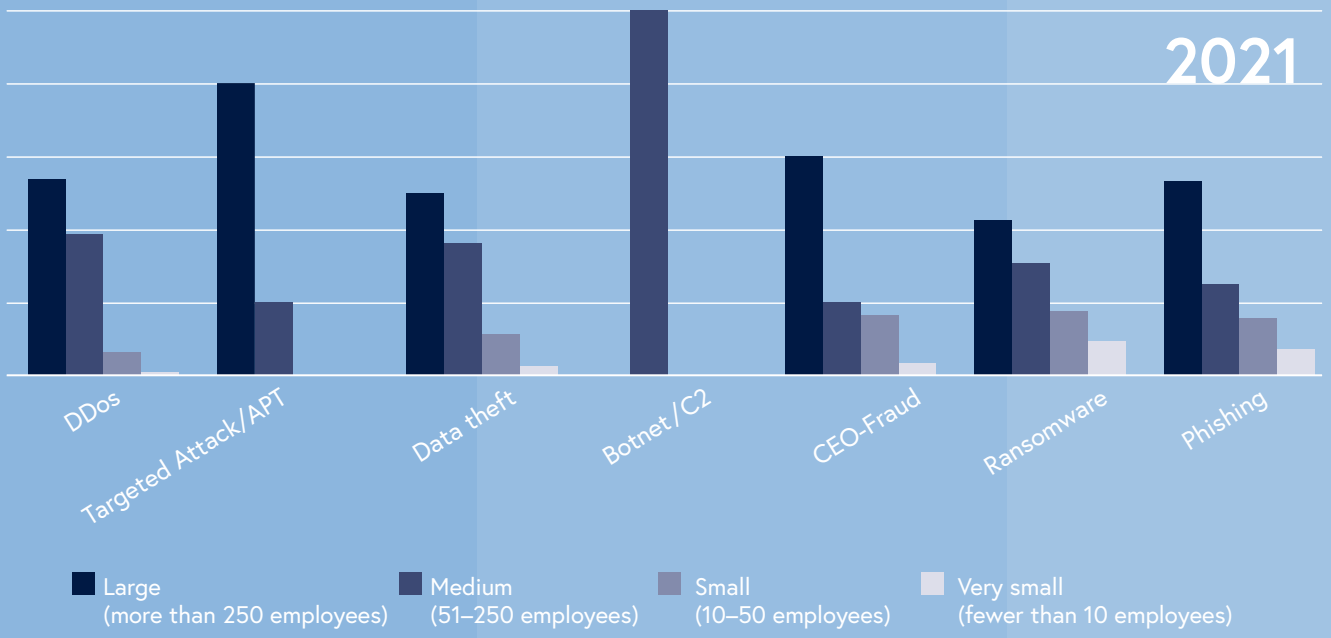
	SEC 01	SEC 02	SEC 03	SEC 04	SEC 05	SEC 06	SEC 07
Phishing	+	+	+	+	+	+	+
Ransomware	+	+	+	+	+	+	+
CEO-Fraud / fake Invoice / SCAM	=	+	=	=	=	–	=
Botnet / C2	=	=	=	=		=	=
Data theft	+	+	+	+	+	+	+
Targeted Attack / APT	+	=	+	=	–		=
DDoS	+	+	+	–	+	–	+
Defacements	=	–	–			–	=

2021

	SEC 01	SEC 02	SEC 03	SEC 04	SEC 05	SEC 06	SEC 07
monetary / criminal	+	+	+	+	+	+	+
political / hacktivism	+	+	+			=	+
personal / revenge	=	–	+		+	=	=
state / acquisition of information		=	+	=			=
technical faults		+	+	=		=	=

The following incident types were evident among the reporting private companies from the security service provider sector:




2021
DDos
Targeted Attack/APT
Data theft
Botnet/C2
CEO-Fraud
Ransomware
Phishing
Large
(more than 250 employees)
Medium
(51–250 employees)
Small
(10–50 employees)
Very small
(fewer than 10 employees)

Phishing: Companies' resilience to phishing is still considered to be insufficient. Targeted emails tailored to the company and its specific characteristics still have a high breakthrough rate. Although awareness training cannot completely eliminate this attack vector, it is an effective tool for reducing this potential risk.

"Detection and visibility are key" – in other words the timely detection and visibility of cybersecurity incidents in a company's own network – is seen as a core competency. Not only to detect phishing attacks, but also to be able to provide information for impact analysis.

Phishing Attacks are still troubling

Ransomware: In many companies, the lack of network segmentation is still a major problem, increasing the threat of malware spreading (lateral movement). The remote access solutions that are increasingly provided as more people work from home have proven to be a popular target for attacks. Security is still only considered up to the perimeter – once an attacker is inside the network, there is often little to stop them apart from virus scanners. Most companies lack a coherent and comprehensive security strategy that identifies and classifies risks and defines actions. In principle though, it can be stated that awareness is generally increasing, but it cannot yet be called sufficient, particularly regarding the criticality of the cyber sector in the fulfilment of core tasks. This is also reflected in the fact that, to this day, not every company has a dedicated back-up strategy – even company-wide implementation of the "least privilege principle" (only the authorisation and access rights required to perform a specific task) is rather the exception.

CEO-Fraud/Business Email Compromise (BEC)/Fake Invoice/SCAM: Due to the high sums that can be obtained, these attack vectors are becoming very popular and more sophisticated in their approaches, as well as harder to detect. BEC is often used for other, more extensive attacks. In general, it can be stated that awareness of this type of threat is continuing to rise. The dangers of social engineering are considered to be serious and are therefore extensively discussed in training sessions.

Botnet/C2: Without ongoing security monitoring, active bots often remain undetected for months. Outdated operating systems (legacy systems) are still exposed and in use without further security measures, thus providing a welcome gateway for bots.

Data theft: Despite increasing willingness to file reports on data theft, the number of unreported cases can still be assumed to be high. During the reporting period, data theft frequently occurred in combination with ransomware attacks, therefore posing a permanent threat.

Investments in cybersecurity reduce the amount of severe IT security incidents

Targeted Attack/APT: The number of registered targeted attacks reported by the companies surveyed is increasing, but is still considered low in terms of overall volume. However, APT- attacks are always associated with disproportionately high damage .

DDoS: Defence against DDoS attacks is most efficient at telecom provider level, so protection mechanisms should be implemented there. Where possible in terms of the content of a web service, Content Delivery Networks (CDNs) can protect against DDoS attacks or at least contain them regionally.

1.3 Cybercrime situation

The police crime statistics reveal an increase of approximately 28% compared to 2020, with over 46,000 reported cases in 2021. The exact numbers are published annually in spring with the police crime statistics. A more in-depth analysis and description of the criminal phenomena can be found in the annual cybercrime report published by the Criminal Intelligence Service Austria.

The term "cybercrime" includes:

- cybercrime in a narrow sense,
- internet fraud and
- other online criminal activity.

Cybercrime in 2021 again on the rise

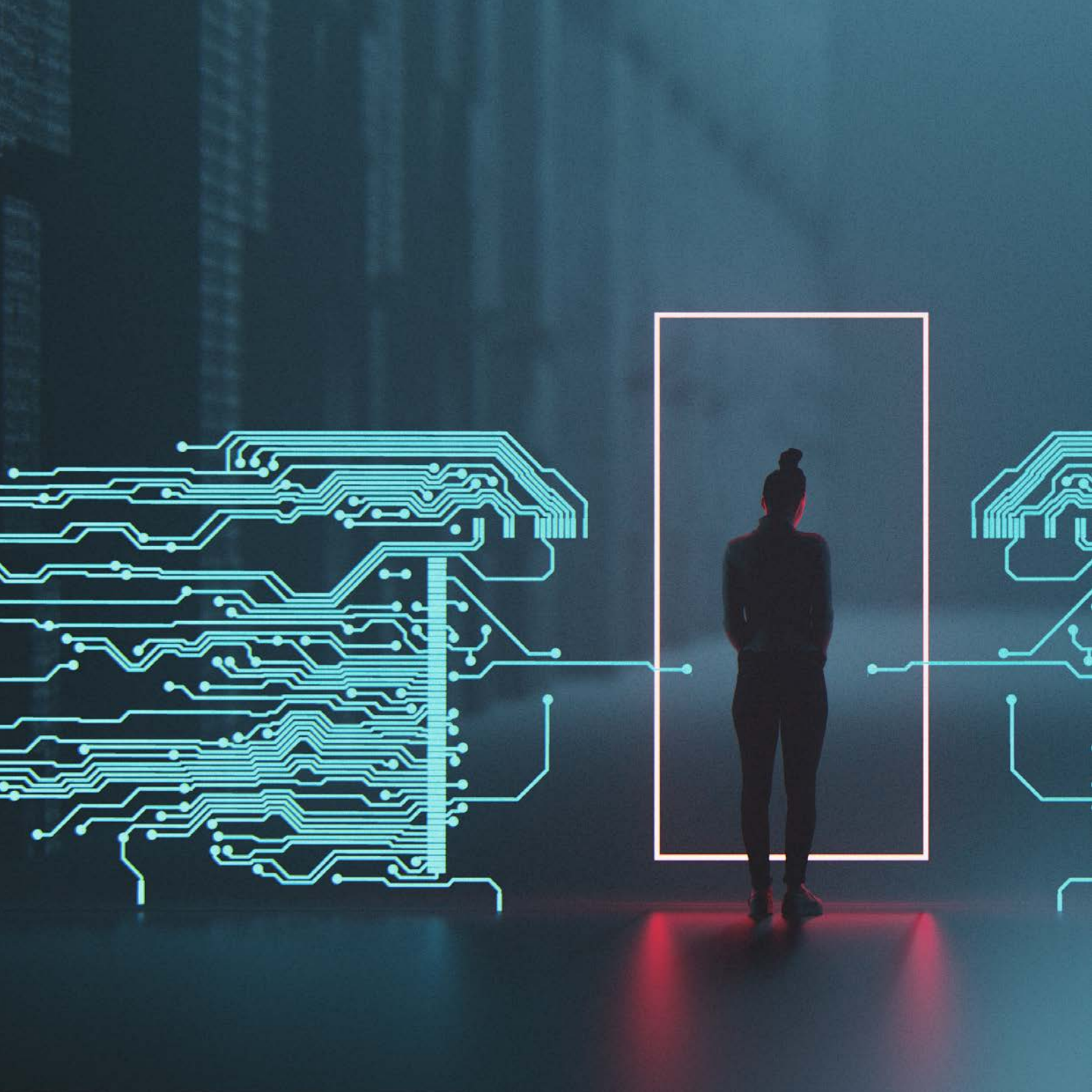
1.3.1 Cybercrime in a narrow sense

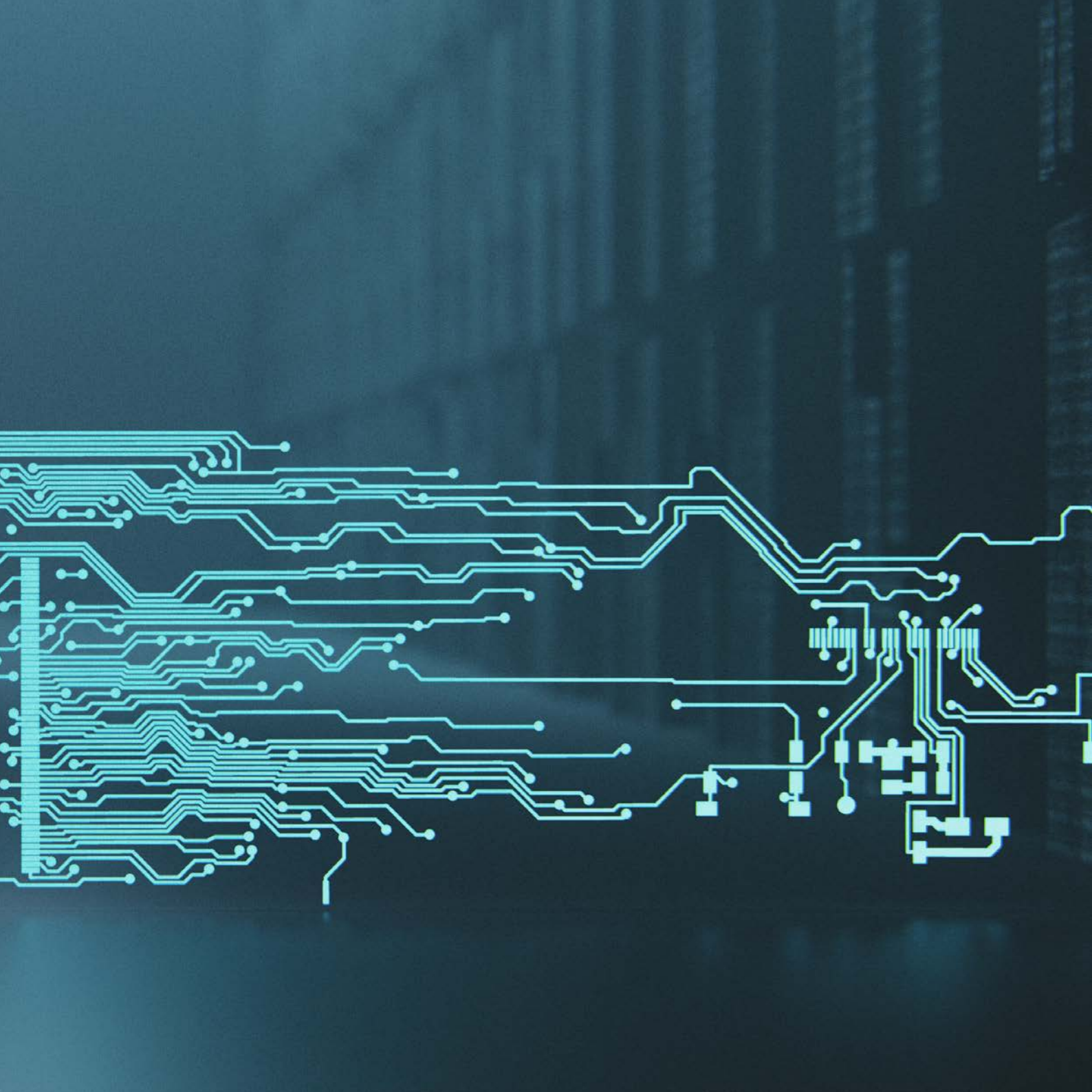
Reports of cybercrime in a narrow sense increased by around 20% in 2021 compared to 2020. This includes criminal offenses in which attacks on data or computer systems are committed by exploiting information and communication technology. Examples include unauthorised access to a computer system or data corruption. Reported cases of malware infections, DDoS attacks and unauthorised access to computer networks and systems have increased significantly in early 2021.

Reports of ransomware initially dropped, but the quality of the attacks (increasingly by exploitation of current security vulnerabilities) and the respective levels of damage in individual cases are rising significantly. The crime statistics figures published in spring 2021 also showed that cyber bullying incidents are being reported more often.

Rising ransomware related activity by various criminal groups is generally noticeable towards the middle of the year. Larger companies face an increased risk of company data being published in addition to their systems being encrypted.

After an incident, larger companies in particular can expect to have production downtime for at least three to seven days, despite having backups in place. Towards the end of the year, the number of reports concerning the spread of malware in Austria rose sharply.





1.3.2 Internet fraud

Internet fraud represents the largest factor in terms of numbers, being largely responsible for last year's increase in cybercrime cases. Almost half of the cybercrimes are fraud-related: in 2021 a total of 22,440 cases of internet fraud were reported, which was a significant increase of 19.5%. As digitalisation progresses, fraud is shifting more and more to the internet. For perpetrators it is easy to carry out fraud undetected and therefore "safely" due to technical anonymisation and the concealment of financial flows. As a consequence global access to the internet causes increasing numbers of potential victims. Order fraud – both on the buyer and seller side – is by far the leading category, followed by unauthorised debits from victims' bank accounts. The "FluBot" attacks peaked in mid-2021, were one of the key drivers. Furthermore digital investment fraud also made an impact in 2021.

1.3.3 Other internet crime

Other internet crime includes all crimes committed on the internet, with the exception of those that come under cybercrime in a narrow sense and internet fraud, as well as all crimes according to Section 207a of the Penal Code (pornographic images of minors) and Section 208a of the Penal Code (initiation of sexual contact with underage persons), regardless of the location of the crime. An increase in "other internet crime" was also recorded in 2021. The reason for this being the increasing shift of classic criminal activity done online. At the same time, what is known as "crime-as-a-service" is offered on the darknet and meets high demand. An increased trade in counterfeit money, child pornography, credit card data and forged documents was also identified. Due to the services offered on the darknet, extortion with ransomware and mass extortion emails in particular, usually accompanied by demands for money in Bitcoin, are seeing high numbers.

1.4 Cyber and national defence

Looking at the situation in cyber space in 2021 showed that the COVID-19 pandemic continues to have a massive impact on global events. Attacks on critical infrastructure in the healthcare sector were particularly concerning, especially in light of the ongoing pandemic. The Austrian Armed Forces (AAF) are in permanent contact with the national security bodies to maintain the security and sovereignty of Austria even in crisis situations.

critical infrastructure is seriously threatened by cyber attacks

The ever-increasing risk in cyber space in 2021 was shaped in particular by cyber attacks on critical infrastructures with some of them having serious impact on the real world. In late 2020 an attack started that lasted well into 2021. It was what is known today as the "SolarWinds" hack. The vulnerability caused enormous international stir – in the USA, where the respective software is mainly used – media reported that around 250 authorities and ministries were affected. The attackers managed to place a back door in the software through a system update which enabled them to penetrate the target networks using malware. The initial goal of the presumably government-related actors was not to gain financial value, as is the case with ransomware, but to obtain confidential information about the targets. The attack demonstrated particularly well how complex the field of information security and cybersecurity has already become. It showed that it is no longer sufficient simply to secure one's own systems, but to assess the entire supply.

Besides SolarWinds, the USA also experienced two other massive attacks against its critical infrastructure. The companies "JBS" (one of the biggest meat producers in the world) and "Colonial Pipeline" became victims of ransomware.

In addition to considerable financial damage to those affected, the attacks also had an impact on the population. For example, panic buying at gas stations caused fuel shortages in part of the USA. Both SolarWinds and the ransomware attacks on the two companies were attributed to Russian actors. This clearly illustrates to which extent geopolitical conflicts are now played out even in times of peace, some of which happens under the public radar. It is therefore imperative for the Federal Ministry of Defence (BMLV) and the Federal Austrian Armed Forces (AAF) to deepen and expand the competencies required to avert these dangers to the departmental and national systems. Around the world, almost all countries have further expanded their state, military and civil cybersecurity skills in the past few years.

Another trend that continued to be a focus for the BMLV in 2021 was the targeted influencing of the general public through disinformation campaigns. Both national and international campaigns against governments, authorities, institutions and individuals were observed, particularly as a result of the COVID-19 pandemic. The BMLV/AAF conducts intensive national and international media monitoring to identify tensions in society as early as possible and also to be able to react accordingly.

Like every year, national defence of cyber space is becoming increasingly important. Modern conflicts begin well before military troops are deployed, with hybrid influence and preferential use of cyberspace. Military actions are now normally conducted with support of modern technology, including Computer Network Operations and PsyOps in cyberspace, support for troops through drone reconnaissance or battle management assisted by Artificial Intelligence. At EU level, the “EU Military Vision and Strategy on Cyberspace as a Domain of Operations” was passed in 2021, which provides for the increased use of cyber skills during common security and defence missions and operations.

As a result of all of these developments, the AAF is actively engaged in expanding its cyber defence capabilities and researching modern technology through national and international cooperation.

2 International developments

The European Union and its member states strongly promote an open, free, stable and secure cyberspace where human rights, fundamental freedoms and the rule of law are fully respected for the social stability, economic growth, prosperity and integrity of free and democratic societies.

2.1 European Union (EU)

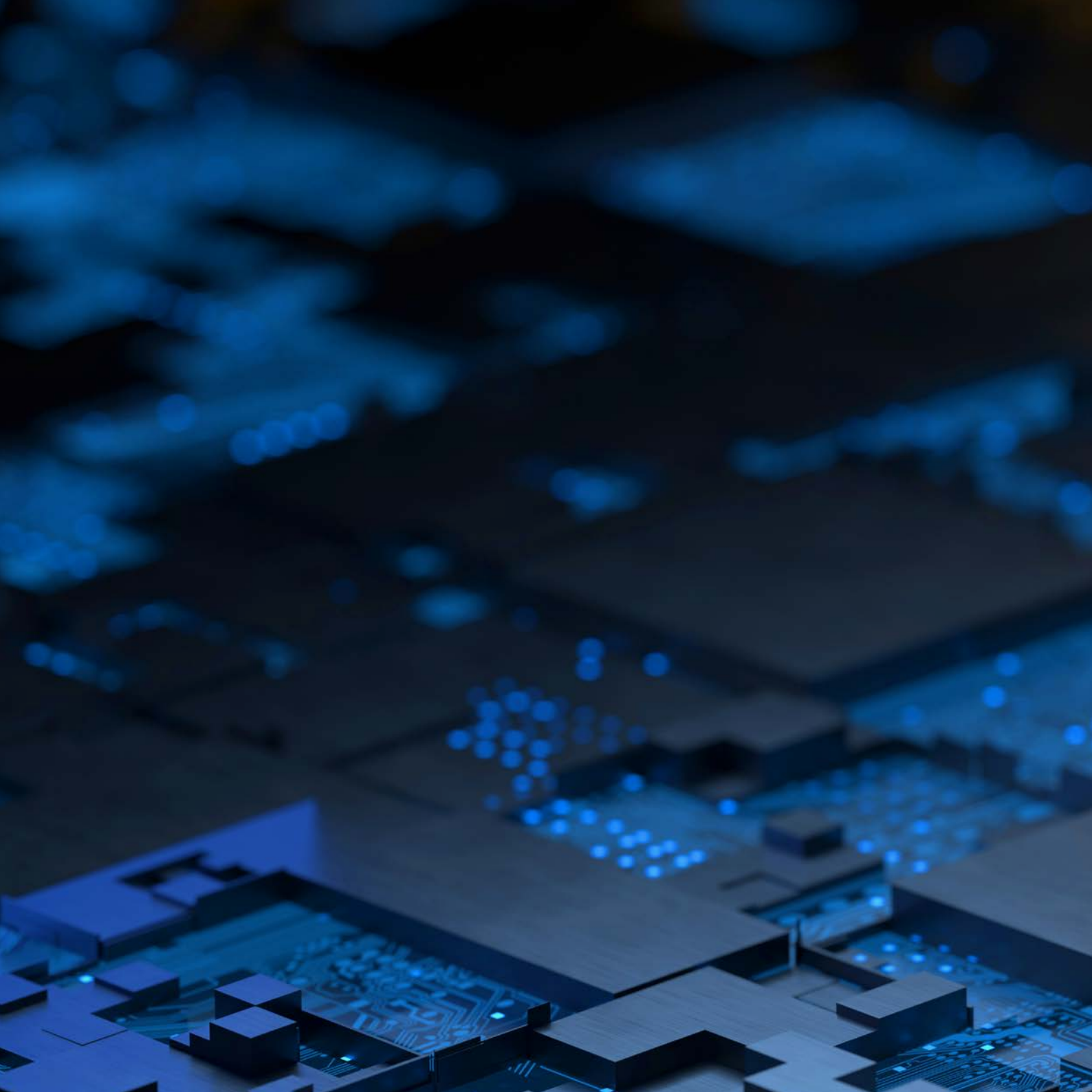
Cybersecurity is becoming increasingly important. In 2021, it was again topic in numerous international organisations and multilateral forums. There were some highly controversial discussions, and the different interpretations and perspectives relating to rights and obligations, regulations and limits on freedom of expression and opinion were a challenge for the negotiators.

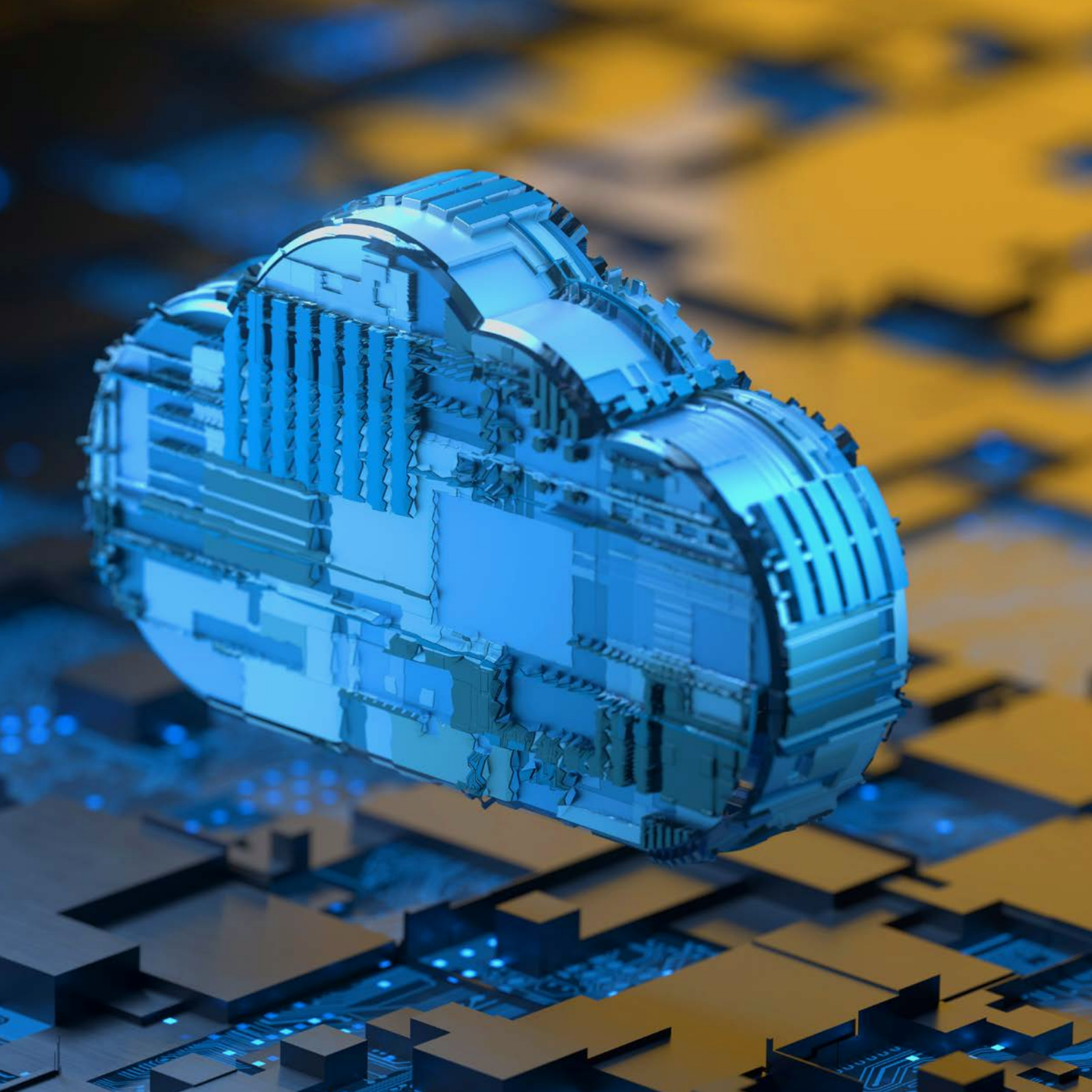
Foreign and security policy measures are coordinated by the Federal Ministry for European and International Affairs (BMEIA), while the Federal Chancellery is obliged to coordinate with the European Union (EU) on cybersecurity. In general, Austria actively campaigns for a free, open and secure internet at an international level, whereby the application of human rights must also be guaranteed in virtual space. An appropriate balance must be struck between the interests of criminal prosecution and ensuring that fundamental human rights are respected, such as the right to freedom of expression and freedom of information and the right to a private life and privacy. Austria is also already committed to ensuring compliance with human rights standards in the development of new digital technology.

2.1.1 Horizontal Working Party on Cyber Issues (HWP Cyber)

The Horizontal Working Party on Cyber Issues (HWP Cyber) was set up in 2016 and is responsible for coordinating the work of the EU Council on cyber space issues, in particular cyber policy and legislative activities. It sets out cyber priorities and strategic objectives of the EU as part of a comprehensive political framework and creates a working platform that enables harmonisation and a unified approach to cyber policy issues.

The Council Working Group works closely with other related working groups and the European Commission (EC), the European External Action Service (EEAS), Europol, Eurojust, the European Union Agency for Fundamental Rights (FRA), the European Defence Agency (EDA) and the European Union Agency for Cybersecurity (ENISA).





There was an impressive total of 60 meetings of HWP Cyber in 2021, more than ever before, which is a testament to the high intensity of the work to further develop European cybersecurity policy. In terms of negotiating legal acts, the focus was on the NIS2 Directive presented by the European Commission on 16 December 2020.

While the Portuguese Presidency was able to complete a first reading and present a progress report at the 4 June 2021 EU TTE Council meeting, the Slovenian Presidency succeeded in reaching a general approach on the NIS2 Directive at the 3 December 2021 EU TTE Council meeting.

The Council adopts conclusions on the EU's cybersecurity strategy for the digital decade

HWP Cyber prepared "Conclusions of the Council on the EU's Cybersecurity Strategy for the Digital Decade", which were adopted by the Council on 22 March 2021.

The Cybersecurity Strategy was presented by the European Commission and the High Representative for Foreign Affairs and Security Policy on 16 December 2020. It replaces the Cybersecurity Strategy 2013 as the new strategic reference framework for cybersecurity at EU level, and sets out the framework for EU measures to protect EU citizens and businesses from cyber threats, promote secure information systems and aim to ensure a more global, open, free and secure cyberspace. Council conclusions set out the member states' priorities and reaffirm that cybersecurity is essential to building a resilient, green and digital Europe. Achieving strategic autonomy while maintaining an open economy is identified as a key objective. This includes strengthening the capacity for autonomous cybersecurity decision-making to strengthen the EU's digital leadership and strategic capabilities.

With regard to the Joint Cyber Unit, on 19 October 2019 the Council accepted the conclusions "reviewing the potential of the initiative for a common cyber unit as a supplement to the coordinated EU response to large-scale cybersecurity incidents and crises", which was prepared by HWP Cyber.

For more information about the extensive work carried out by HWP Cyber in the field of cyber diplomacy, see Chapter 2.1.6.

2.1.2 NIS Cooperation Group

The NIS Cooperation Group was established by the NIS Directive and supports and facilitates strategic collaboration and the exchange of information between the member states. It is composed of representatives from the member states, the European Commission and ENISA. The respective Council President also chairs this Group.

The Cooperation Group performs its duties on the basis of biennial work programs. The work program for the period 2020 to 2022 commissions an inventory of the services provided to date, an assessment, their impact and the identification of potential improvement. The aim of the NIS Cooperation Group is to continue to facilitate the implementation of the NIS Directive, to further operationalise the exchange of information and to enable a strategic discussion about important political documents for cybersecurity in the EU, such as in reference to 5G, Artificial Intelligence or the Internet of Things.

The NIS Cooperation Group met for four plenary sessions and more than 23 meetings within its work stream meetings in 2021. For more information about the extensive work in the field of the cybersecurity of 5G networks, see Chapter 2.1.5.

2.1.3 Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT)

The Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats (HWP ERCHT) was set up in 2019. The focus of its work is on improving the resilience of the EU and its member states, ensuring a joint approach to defending against hybrid threats, improving strategic communication and fighting disinformation. The working group coordinates within the Council and ensures collaboration with other EU bodies, services and agencies. Malicious cyber activities are often the key element of hybrid threats and in this context are covered by the work of the HWP ERCHT.

The HWP ERCHT started working on a "hybrid toolbox" in the second half of 2021. This aims to enable a rapid, comprehensive and tailored response from the EU and its member states to hybrid threats. The strengthening of the EU's ability to manage hybrid threats is also an important element of the "Strategic Compass for Security and Defence". Current proposals by the European Commission (EC) contain measures that are relevant to the EU's resilience in the context of hybrid threats, such as the Digital Services Act, the Directive on measures for a high common level of cybersecurity across the Union (NIS2), the Directive on the resilience of critical entities (CER) and the Cyber Resilience Act (CRA).

2.1.4 EU certification framework (Cybersecurity Act)

The Cybersecurity Act, which entered into force in 2019, creates, among other things, a European certification framework for cybersecurity. It sets out a mechanism for creating the European cybersecurity certification scheme. Subsequently the European cybersecurity certification framework shall certify that ICT products, services and processes assessed according to a scheme of this type meet the specified security requirements. In the future, suppliers and manufacturers will be able to voluntarily choose to undergo cybersecurity certification of ICT products, services and processes. A cybersecurity certificate will be accepted throughout the EU. By providing evidence that a product fulfils the specified security functions or complies with certain security

requirements, cybersecurity certification can contribute significantly to increasing trust in ICT products, services and processes, thereby ensuring the proper functioning of the digital single market.

The European Cybersecurity Certification Group (ECCG) was established by the Cybersecurity Act, and began its work in 2019. The ECCG is composed of representatives of national cybersecurity certification authorities and representatives of other relevant national authorities. Austria is represented in the ECCG by the Federal Ministry for Digital and Economic Affairs (BMDW) and the strategic NIS Office of the Federal Chancellery. The ECCG met for five plenary sessions in 2021.

The Stakeholders Cybersecurity Certification Group (SCCG), which was established in 2020, continued its work under the joint chairmanship of the European Commission and ENISA. The SCCG is composed of representatives from academic facilities, consumer protection organisations, conformity assessment bodies, standards developing organisations, businesses, trade associations and others to advise on strategic cybersecurity certification issues.

In addition to the two possible cybersecurity certification schemes commissioned from ENISA by the European Commission in 2019, a third scheme for cybersecurity certification was commissioned in January 2021 titled EU5G. This targets the cybersecurity of 5G networks. For more information about the extensive work in the field of the cybersecurity certification of 5G networks, see Chapter 2.1.5.

All three schemes are currently being developed, with ENISA having already submitted its draft for the EUCC on to the European Commission.

2.1.5 Cybersicherheit von 5G-Netzen

The security of the technology referred to as the “fifth generation of the mobile network” (5G) remained the focus of the attention of cybersecurity authorities, as in the previous years. In 2021, the focus shifted away from the creation of general security measures or rules to the development of possible certification schemes for 5G products and processes in the ECCG (see Chapter 2.1.4).

In 2021 it was also possible to fully implement the “Cybersecurity of 5G networks EU toolbox of risk mitigating measures”, hereinafter referred to as “toolbox”, which was originally presented on 29 January 2020. The toolbox distinguished between “technical measures” and “strategic measures”.

The first part of the “technical measures” proposed in the toolbox was implemented with the RTR Regulation, which entered into force on 4 July 2020 (Telecommunications Network Security Regulation 2020 – TK-NSiV 2020).

The Telecommunications Act 2021 (TKG 2021), which entered into force on 1 November 2021, implemented the second part of the measures originating from the toolbox, the so-called "strategic measures." These include a separate provision in Section 45 on how to deal with any "high-risk" vendor. Accordingly, a high-risk vendor is someone "who is reasonably likely to be unable to comply, or to comply on a continuous basis, with the relevant standards applicable in the EU, particularly in the areas of information security and data protection". This creates the possibility to exclude a manufacturer from supplying components or network components in full or in part that are relevant to security. This can be limited to certain business areas, groups of goods or services or individual hardware or software components over a specific period of time or in a specific geographical area. The Federal Ministry of Agriculture, Regions and Tourism (BMLRT) decides on this for reasons of national security after consulting a specially established panel of experts.

TKG 2021 will also implement the European Electronic Communications Code (EECC, Directive (EU) 2018/1972) at national level.

In the past year, the work stream of the NIS Cooperation Group on the cybersecurity of 5G networks (NIS CG 5G Work Stream) has primarily dealt with the applicability of Open RAN for European telecommunication networks. Open-RAN (RAN stands for "Radio Access Network") is an initiative that aims to improve and promote interoperability in the radio access network (RAN) of mobile networks.

By defining additional standards and interfaces, the intention is to achieve a diversification of RAN manufacturers and better independence from existing manufacturers (keyword vendor lock-in) and thus implement the "diversity of suppliers" required in the 5G Toolbox.

The sub-work stream "SubGroup on 5G standardisation and certification", founded in 2020, plays a major role in the definition and publication of relevant standards and organisations. In 2021, the existing standards were collected and categorised. The insights of the working group were handed over to the ENISA "EU 5G Ad-hoc Working Group" within the ECCG. As a result, the ECCG set up three specific (sub-) work streams, to address the "as-is" translation of existing elements of the certification schemes NESAS, SAS-SM, SAS-UP and eUICC developed by the GSMA into their EU equivalents and develop a risk-based definition of security and certification requirements for participant-based applications in the 5G ecosystem. The resulting EU 5G certification scheme must be developed in line with the Cybersecurity Act (CSA, Regulation (EU) 2019/881), among other things. The NIS CG 5G Work Stream is still an interface for information exchange between the individual groups.

The third "Prague 5G Security Conference" also took place virtually on 30 September 2021 and 1 December 2021. This time, two new "Prague Proposals" were presented, one about "Telecommunications Supplier Diversity" and another about "Cyber Security

of EDTs" ("Emerging Disruptive Technologies"). The first looked at the problem already mentioned in the 5G toolbox of the dependence on a few manufacturers; the second provides information about possible future cybersecurity problems with EDTs, such as Artificial Intelligence (AI), Quantum Communication Infrastructure (QCI), Big Data Advanced Analytics (BDAA) and Autonomous Systems and Massive Internet of Things (IOT).

2.1.6 Cyber diplomacy

The EU's Cyber Diplomacy Toolbox provides diplomatic and political measures on how to respond in a coordinated manner to international law violations in cyberspace within the framework of the EU Common Foreign and Security Policy (CFSP). It was also used in 2021, when state actors were publicly criticised for serious cyber attacks. In the past year, EU declarations have been made on the SolarWinds cyber supply chain attack with 18,000 potential victims around the world, on the exploitation of a security vulnerability in the Microsoft Exchange server used for industrial espionage and the Ghostwriter campaign prior to the parliamentary elections in Germany. The toolbox includes preventative, cooperative and stabilising, as well as restrictive measures. The latter were first imposed on individuals and entities as part of the cyber sanction regime in 2020 and provide for entry bans and asset freezes. Not all the measures included in the Cyber Diplomacy Toolbox demand for an official attribution.

An important part of cyber diplomacy at EU level is the development of common positions and strategies on cyber topics at international level, first and foremost in cooperation with the United Nations (see Chapter 2.2). This is because standard and norm-setting for new technologies and cyberspace have long been geopolitical conflict zones, with the increase in cyber attacks by state-sponsored actors further fuelling the geopolitical polarisation. The conclusions of the Council adopted in March 2021 on the EU's Cybersecurity Strategy underline the importance of cybersecurity in the development of a resilient, green and digital Europe. With the demand for the EU taking the leadership role at an international and regional level, the EU vision for a global and open internet

should be promoted, thereby ensuring that new technologies focus on people and the protection of their privacy and are used lawfully and ethically.

In order to strengthen Austria's international cooperation in matters of cyber diplomacy, the BMEIA has appointed a Special Envoy on Cyber Foreign Policy and Cyber Security, who started work in May 2021. Responsibilities include leading delegations for multilateral negotiations, conducting bilateral cyber dialogues, as well as participating in the EU Network of Cyber Ambassadors.

2.1.7 European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centre

On 28 June 2021, Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the network of National Coordination Centres (NCC) entered into force. The Regulation establishes the ECCC, which will be based in Bucharest, and the network of NCCs. The ECCC is to take a leading role in the implementation of the Digital Europe Programme (Regulation (EU) 2021/694) and contribute to the implementation of Horizon Europe. It also creates a framework for increasing and coordinating investments in cybersecurity between the EU, member states and, indirectly, industry. In this context, it is the task of the ECCC and the Network to support the EU:

- strengthening its cybersecurity leadership to enhance trust and security, including data confidentiality, integrity and accessibility;
- promoting the defensibility and reliability of network and information systems, including critical infrastructure and common hardware and software;
- increasing the global competitiveness and high standards of the EU cybersecurity industry and transforming cybersecurity into a competitive advantage for other EU industries.

The Governing Board of the ECCC met three times informally in 2021 and one time formally and to constitute the Centre in October 2021. The primary focus was the adoption of administrative decisions necessary to make the ECCC operational.

In the network, each member state is to designate an NCC to work on the development of new cybersecurity capacities and further competence building. In Austria, the National Coordination Centre is operated by the Federal Chancellery in cooperation with the Austrian Research Promotion Agency (FFG). The aims of the NCC are in particular:

- the improvement of cyber defence capabilities,
- the development and market introduction of new European cybersecurity technologies,
- the support of start-ups and small and medium-sized enterprises (SMEs) in the field of cybersecurity,
- the promotion of cybersecurity research and innovation,
- strengthening of cybersecurity skills and cooperation,
- reinforcing Europe's digital sovereignty.

2.1.8 NIS2 Directive

In addition to a new EU Cybersecurity Strategy, on 16 December 2020, the European Commission also presented, among other things, a proposal for a new Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive [NIS2]). NIS2 aims to replace the previous Directive from 2016 and substantially improve on it. The objectives pursued are fundamentally the same and will be continued. Specifically, it aims to improve cybersecurity capacities in the EU, enhance cooperation among member states, and strengthen the cyber resilience of public and private facilities. The overall goal is to further increase the level of cybersecurity in the EU. This high common level of cybersecurity within the EU will be promoted through the following measures:

NIS2 is going to replace and enhance the current regulatory framework

- The member states are required to adopt national cybersecurity strategies and designate competent authorities, central focal points and CSIRTs (Computer Security Incident Response Teams in Europe).

- The cyber resilience of companies is to be strengthened and encompass all relevant sectors. All public and private facilities throughout the internal market that perform important functions for the economy and society as a whole are to be obliged, as so-called essential and important facilities, to adopt appropriate cybersecurity measures (in particular by establishing a cybersecurity risk management system as well as mandatory reporting of IT security incidents and cyber threats).

- Measures to increase resilience are to be promoted for sectors in the internal market that are already covered by the directive. This is achieved through the continuous alignment of the de facto scope of application, security requirements and IT security incident reporting obligations, provisions for national supervision and enforcement, and the capacities of the competent authorities in the member states.

- Common situational assessment as well as collective preparedness and response capabilities should be improved by taking steps to build trust among the compe-

tent authorities and enhancing the exchange of information. In addition rules and procedures are defined for the event of large-scale security incidents or crises (cybersecurity crisis management): For the first time, NIS2 includes an obligation to set a national framework for cybersecurity crisis management and provides for the establishment of a (European Cyber Crises Liaison Organisation Network [EU-CyCLONe]). This should support the coordinated management of large-scale cybersecurity incidents and crises and ensure the regular exchange of information between member states and EU bodies.

NIS2 is being discussed in the European Parliament in the Industry, Research and Energy (ITRE) Committee, where the draft of the negotiating mandate prepared under the rapporteur (MEP Bart Groothuis [NL; ALDE]) was adopted by ITRE on 28 October 2021 ITRE and consent to start negotiations with the Council was granted. This negotiating mandate was announced at the plenary session on 10 November 2021.

In the Council of the EU, NIS2 was discussed in the Horizontal Working Party on Cyber Issues (see Chapter 2.1.1). In the "general alignment" achieved under the Slovenian Presidency on 3 December 2021, an increased emphasis was placed on a risk-based and proportionate approach in terms of scope, obligations and penalties. Harmonisation with sector-specific provisions (DORA and CER) has also been achieved. Furthermore, provisions on administrative assistance, jurisdiction as well as territoriality have been improved.

2.2 United Nations (UN)

Since the 1st Committee (Disarmament and International Security) of the United Nations General Assembly (UNGA) first addressed the issue of cybersecurity in 1998, the UNGA has been dealing with this issue with increasing intensity. Within this framework, the states aim to minimise the risks to international security and stability arising from the use of cyberspace. In the course of the negotiations, it was possible to identify four priority areas that are particularly important for the establishment and enforcement of an international set of standards for cyber space:

- international law,
- non-binding standards for responsible state behaviour,
- confidence-building measures and
- building capacities.

After a number of pandemic-related postponements in 2020, 2021 was a particularly eventful year for conflict prevention in cyber space. The two working groups initiated in 2018 by the UNGA and operating in parallel but nominally independently were able to complete their work in the first half of the year, each submitting substantial final reports that were adopted by consensus. Austria actively participated in the work of the Open-Ended Working Group (OEWG) on cybersecurity, which was open to all member states. Austria was not represented in the Group of Governmental Experts (GGE) which consisted of only 25 members, but nevertheless followed the debate.

In terms of content, it is significant that in the final report of the OEWG all member states clarified for the first time the validity of existing international law, in particular the UN charter, in cyber space, albeit there remain some significant differences in interpretation of the precise applicability of international law (particularly human rights and international humanitarian law). There was further agreement in terms of the need to expand capacity and the importance of confidence-building measures.

For Austria, the EU and like-minded countries, the recommendations of the OEWG and the GGE adopted by consensus form the basis for the work on the new OEWG on Cybersecurity 2021–2015 launched at the request of Russia and China. The first session of the new OEWG in December 2021 ended without an agreement on the rules of procedure due to a lack of consensus on the participation of representatives of civil society, the private sector and research. It also remains to be seen how the new OEWG will negotiate an action-oriented Programme of Action on Cybersecurity publicised by over 50 member states, including Austria.

The field of international cybersecurity is also included in the disarmament agenda of the General Secretary of the UN (UNSG) launched in 2018. Two areas of action are dedicated to cybersecurity in the associated implementation plan. One relates to peaceful conflict resolution and the other to the strengthening of evolving norms in cyberspace. In 2021, the implementation measures were continued by the states.

The implementation of the disarmament agenda is supported by the United Nations Office for Disarmament Affairs (UNODA). The United Nations Institute for Disarmament Research (UNIDIR) contributes to international discussions on cybersecurity by publishing academic papers.

In the UN Security Council, Estonia put the issue of cybersecurity back on the agenda in June 2021 and arranged a virtual open debate with high-ranking participants, to which Austria also contributed with a national written statement.

The High-level Panel on Digital Cooperation (HLPDC) convened by UNSG Guterres in 2018 set out specific recommendations on strengthening the collaboration between governments, the private sector, civil society, international organisations, science, the technical community and other relevant stakeholders in the digital space in 2019. Building on this, in 2020 UNSG Guterres drew up a report (“Road Map for Digital Cooperation”)

entitled “Connect, respect, protect”, which provides for the use of a “Tech Envoy”, among other things. The position is to be filled in spring 2022.

In the context of the UN in Geneva, the International Telecommunication Unit (ITU) is working on guidelines for the use of its “Global Cybersecurity Agenda” (GCA), which aims to strengthen trust and security in the information society, but is sometimes viewed very critically by western states due to the potential increase in state control in the digital realm. One of the recommendations in the draft guidelines, developing legal regulations to address global cybersecurity issues within the ITU, will be the focus of the discussions in the ITU Council in 2022 and the ITU Plenipotentiary Conference in Bucharest (from 26 September to 14 October 2022).

The secretariat of the Internet Governance Forum (IGF) has its headquarters in Geneva. With the establishment of the “Leadership Panel” and ongoing debates on reforming the forum, as proposed in the “Common Agenda” of the UNSG-GS, the significance of the IGF as an incubator for new cybersecurity initiatives is expected to increase.

At the 11th WTO Ministerial Conference (MC11) in 2017 in Buenos Aires, a joint initiative on e-commerce was created. The work made progress, but there is still no prospect of agreement on a number of essential topics, as the positions of the EU and other participants are still very disparate. This applies in particular to the topics of data flows, but also cybersecurity and source codes.

Cybercrime has quickly become a global and extremely profitable crime sector. The United Nations Office on Drugs and Crime (UNODC) in Vienna continues to be an indispensable component in the effective global fight against cybercrime. Through the “Global Programme on Cybercrime”, the UNODC assists member states developing capacities, prevention and awareness-raising in the fight against cybercrime. Austria has been involved in the implementation of initiatives in this area since 2020 with voluntary contributions.

The Intergovernmental Expert Group (IEG) established in the field of cybercrime in 2010 met in April 2021 for the seventh and final time. There was a failure to extend the mandate although many states wished to do so due to the minority position that the working group had become invalid in light of the establishment of the ad-hoc committee (AHC) to develop a new UN Convention (see below). The work of the IEG was completed with the adoption by consensus of 61 recommendations and conclusions.[2]

The increase in cybercrime as a result of the COVID pandemic was discussed in all committees, including the Commission on Crime Prevention and Criminal Justice (CCPCJ) and the Commission on Narcotic Drugs (CND). The topic was also a priority in the 2022-2025 work plan of the CCPCJ and will be the focus of the first thematic discussion during the 31st meeting of the CCPCJ in May 2021.

In addition to the discussions of cybersecurity in the First Committee of the UNGA, the issue of the negotiation of a UN Convention on Fighting Cybercrime was also discussed in the Third Committee of the UNGA (social, humanitarian and cultural issues). As a result of the creation of the ad hoc committee (AHC) to develop a comprehensive international agreement on Countering the Use of Information and Communications Technologies for Criminal Purposes (UN Cybercrime Convention) in 2019, the process of agreeing on the working modalities for the new AHC dragged on until May 2021. The final result provides for a negotiating process that will last until 2024, half of which will take place at the UN site in Vienna and the other half in New York. Thanks to a special clause in the arrangements, NGOs and the private sector can participate in the process, alongside UN member states. UNODC acts as a secretariat for the negotiation process.

2 V2102595.pdf (unodc.org)

As part of the 47th session of the UN Human Rights Council (UN-HRC) in June 2021, Austria successfully introduced the second and this time content-related resolution on the topic of "new and upcoming technologies and human rights" as one of the main sponsors (alongside South Korea, Brazil, Denmark, Morocco and Singapore). It tasks the UN-OHCHR (UN Human Rights Office) with two strands of work, namely the holding of expert seminars on the implementation of the UN Guiding Principles on Business and Human Rights in Tech Companies as well as liaising with the ITU and exploring ways at expert level to ensure that technical standards always meet human rights standards.

The resolution on the "right to privacy in the digital age" introduced by Austria in September 2021 as one of the main sponsors addresses the impact of the progressing use of private data by algorithms on the right to privacy. The resolution now requires that states and companies include the protection of human rights over the course of the entire life cycle ("design, development, deployment and use" of Artificial Intelligence (AI) to minimise risks. In connection with the Pegasus revelation, the resolution also discusses the use of technologies developed by private companies, the effects on which on the work of human rights defenders or journalists are in some cases significant. The protection of privacy should also not be depicted as an obstacle to innovation by developers.

The resolution introduced by Austria at the 45th session of the UN-HRC in September 2020 on the safety of journalists condemned the intentional and total disconnection of the internet as a violation of human rights for the first time.

2.3 NATO

As a military and political alliance with a significant focus on security and common defence, the North Atlantic Treaty Organization (NATO) has been dealing increasingly with the defence aspects of cybersecurity since the adoption of its new strategic concept (2010) and the recognition of cyberspace as an operative domain. As part of the current discussion of the opportunities and threats posed by emerging and disruptive technologies, NATO has become increasingly aware of the importance of secure data (in particular in the context of Big Data, AI, autonomy, quantum technology and space) and thus the need for protective measures. In response to the changing threat landscape and the intervening resilience measures, NATO reviewed its cyber defence policy from 2014, which was adopted at the June 2021 NATO Heads of State and Government Summit.

Austria continues to cooperate closely with NATO as a partner country, and participates at the technical level in meetings of the NATO-C3 (Consultation, Command and Control) Board as well as those related to relevant smart defence projects.

Since 2013, the Federal Ministry of Defence (BMLV) has provided an officer at the "NATO Cooperative Cyber Defence Centre of Excellence" (CCDCoE) in Tallinn. The goal of the collaboration is to increase cyber defence capabilities. Austrian departments make extensive use of the courses made available in this way, and use the exercises offered to review the national capabilities within the scope of an international comparison. In addition to this, Austria also sends a BMLV employee to the "European Centre of Excellence for Countering Hybrid Threats" in Helsinki, in which the NATO member states are also involved.

2.4 Organization for Security and Co-operation in Europe (OSCE)

As the largest intergovernmental security organization in the world, the Organization for Security and Co-operation in Europe (OSCE) plays a dual role in international cybersecurity policy. On the one hand, it supports the implementation of resolutions passed at the UN level (in particular the increase in capacity through its executive structures, primarily the secretariat in Vienna and the broad network of field missions). On the other hand, the OSCE took a leading role in the development of confidence-building measures (CBM) in cyberspace. From a global perspective, the adoption of the 16 CBM is the most ambitious attempt ever to increase international collaboration in the field of cybersecurity outside of the UN.

The goal is to minimise the intergovernmental tensions arising from the use of cyberspace among participating OSCE states by exchanging information, establishing communication channels, and building capacities. The work of the OSCE also concentrates on the protection and strengthening of human rights in cyber space and on fighting disinformation and hate speech.

The informal working group on cybersecurity (Cyber-IWG) is primarily responsible for the development and implementation of the CBMs. The understanding of security used as a basis within the OSCE also guides the work of the Cyber-IWG. In 2021, the Cyber-IWG continued its activities as part of the "adopt a CBM (Confidence Building Measure)" initiative, as part of which states or groups of states are supposed to drive forward the implementation of CBMs. Important steps in this regard include establishing a network of point of contacts, regularly reviewing communication channels and preparing for effective collaboration in the event of a cyber crisis. Austria together with Belgium, Estonia, Finland, Italy and Sweden is driving the implementation of CBM 14 on public-private partnerships and presented the Austrian cybersecurity platform as a role model in November 2021.

In addition to the institutionalised discussion of the topic by the Cyber-IGW, the respective OSCE chairmanships have been placing cybersecurity on their agendas holding cybersecurity conferences now for several years. In 2021, this conference focused on "new technologies and conflict prevention and the impact on the humanitarian situation and human rights". It was held in Stockholm as part of the 2021 Stockholm Forum on Peace and Development.

2.5 Organisation for Economic Co-operation and Development (OECD)

The "Working Party on Security in the Digital Economy" (WPSDE) is one of four working groups under the "Committee on Digital Economy" of the OECD. The objective is to develop evidence-based digital security policies and practical guidelines to build trust in digital transformation and support resilience, continuity and security of critical activities. The focus is on the management of digital security risks for economic and social activities and on the improvement in security in digital products and services. It draws on expertise from OECD and partner countries, businesses, civil society and the technical internet community. The WPSDE normally meets twice a year in Paris and organises workshops and conferences. Due to the pandemic, only virtual meetings were possible in 2021 – an additional meeting was held in addition to the two regular sessions.

In Austria, the Federal Chancellery coordinates the content of this working group.

As mentioned in last year's report, the review of the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity from 2015 was continued. The original report was divided into separate sub-chapters, which will appear separately: a recommendation on digital security risk management, a recommendation on national digital security strategies, a recommendation on the digital security of products and

a recommendation on vulnerability treatment. These documents are edited separately and hopefully can be finalised and published in 2022.

Three additional reports with very interesting topics were also presented and will also be finalised in Q1/2 of 2022: “Enhancing the Securing communication networks: Infrastructure”, “Security of the DNS: An introduction for policy makers” and “Security of Routing”.

The working group also discussed using the term “cyber” in publications or reports increasingly (instead of or in addition to “digital”) in order to ensure greater visibility in public perception. The Swiss delegate from the Cybersecurity Association, Florian Schütz, was appointed as the new Chair of the working group.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

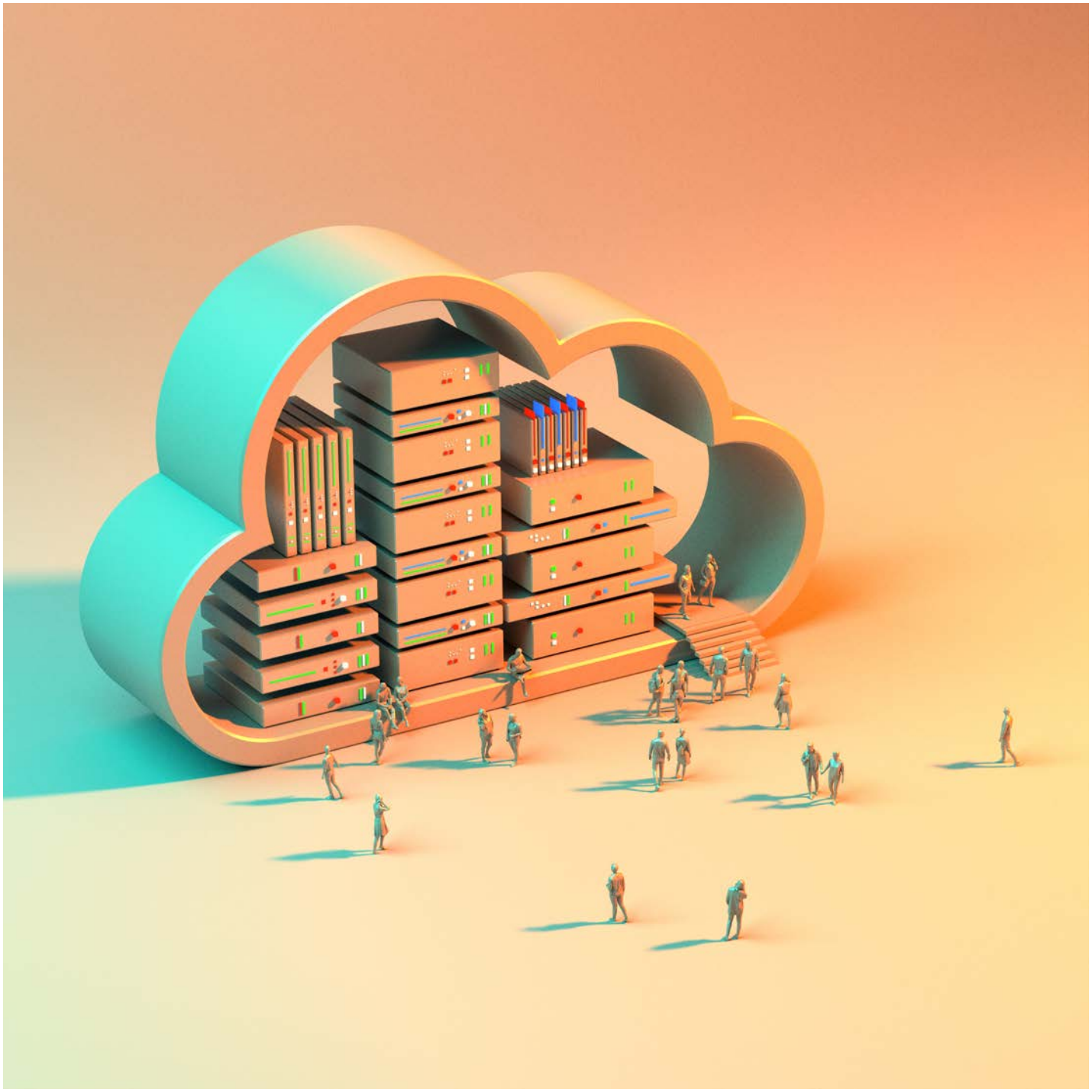
2.6 Council of Europe

The core activities of the Council of Europe relating to cybersecurity are set out in the Budapest Convention of 2001, which has achieved significance well beyond Europe with currently 66 ratifications (Sweden in 2021). The main purpose is to pursue a common criminal justice policy to protect society from cybercrime, in particular through appropriate legislation and the promotion of international cooperation.

The implementation of the Convention is supported through capacity-building projects, coordinated by a Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest. This includes advising on relevant legislative measures and assisting in the training of judges and prosecutors. The projects iProceeds-2 in South-Eastern Europe focusing on the revenue of cybercrime, Cyber South in North Africa, the global project conducted in cooperation with Interpol GLACY+ and Cyber East, which aims to improve the partnership structures with eastern states and is funded by the European Neighbourhood Instrument, are also supported.

The Octopus Project also promotes the implementation of the Budapest Convention and associated standards. The Octopus Conferences provide an important platform for experts and organizations in the field of cybercrime. The last conference held 16 to 18 November 2021 marked the 20th anniversary of the Budapest Convention and focused on collaboration within the scope of existing instruments and the challenges posed by the COVID-19 pandemic.

On 17 November the Committee of Ministers of the Council of Europe passed the second additional protocol to the Budapest Convention. This addresses international mutual legal assistance and the associated cross-border access to electronic evidence. It will be presented for signature in the course of 2022.



Since 2012, Guidance Notes on the Budapest Convention have also been developed and published. These are intended to facilitate the effective use and implementation for the contracting states. The last guidance note of this type discussed the topic of influencing elections.

Other instruments of the Council of Europe include the Data Protection Convention of the Council of Europe (ETS 108), which was modernised in 2018, and the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. The latter makes a significant contribution to the protection of children on the internet.

2.7 Computer Security Incident Response Teams Network (CSIRTs Network)

In summer 2016, the European Parliament (EP) and the Council of the EU passed EU Directive 2016/1148 (NIS Directive), creating the CSIRTs Network (CNW) and defining its scope of activities. The CSIRTs Network is composed of representatives of the CSIRTs of the member states (according to Article 9 of the NIS Directive) and the CERT-EU. The European Commission (EC) participates in the CSIRTs Network as an observer, and the ENISA agency provides the secretariat and actively supports cooperation between the CSIRTs. Austria's participants in the CSIRTs Network are GovCERT Austria, CERT.at and the Austrian Energy CERT (AEC).

The Network primarily works online with communication via a web portal, mailing lists and an instant messaging system. The CNW meetings are used to exchange information regarding the services, activities, and cooperative capabilities of the CSIRTs, as well as to voluntarily share information on relevant security incidents and discuss lessons learned from network and information security system exercises. The central task of the CNW is to build and enhance trust between the member states and to promote rapid and effective operational cooperation to ensure a high common level of security of network and information systems in the EU.

The first two meetings in 2021 were purely held virtually, but the third took place in a hybrid format.

In March, in the policy section the draft of the second version of the NIS Directive was presented and discussed for the first time. The main topics on the technical level were the events surrounding the EMOTET takedown and the SolarWinds supply chain attack. At the second meeting in June 2021, there was a joint session with the NIS Cooperation Group and the EU Cyber Crisis Liaison Organisation Networks (CyCLONe) Chair. On a technical level, current incidents in the area of ransomware and disinformation were discussed. The meeting in November 2021 took place both in Ljubljana and online. There was once again a shared session, this time with CyCLONe.

On the technical side, 2021 was shaped by collaboration on vulnerability handling (MS Exchange and various firewalls/VPNs stood out), while on the policy side the draft NIS2 Directive dominated.


152.68
123.05
279.82
977.65
555.74
73.79

3
National actors

3.1 Cyber Security Centre (CSC)

By reforming the Federal Agency for State Protection and Counter-Terrorism (BVT) and creating the State Security and Intelligence Directorate (DSN), as of 1 December 2021 the previous agendas of the II/BVT/5 department were divided between the DSN and Section IV of the Ministry of the Interior. In the future, the DSN Cyber Security Centre (CSC) will act as the operational coordination site for reports and inquiries regarding attacks on the systems and infrastructure of constitutional facilities and those classified as critical infrastructure. The focus is increasingly on targeted attacks and technical incident handling. In order to do this, the CSC uses a wide range of skills and techniques such as Cyber Threat Intelligence, Incident Response, Malware Analysis and Reverse Engineering. The activities do of course also include taxonomy, handling new phenomena in the field of cybersecurity and responding to current trends. To enable and promote the exchange of experience and knowledge, the CSC relies on the swarm intelligence of the cybersecurity community, which includes stakeholders from the private sector and research. The goal here is to jointly promote resilience and communication in this area. Likewise, the exchange with partner services takes place in order to share individual knowledge and gain a global perspective of the matter.

3.2 Cybercrime Competence Centre (C4)

The Cybercrime Competence Centre (C4) is the national and international coordination and reporting centre to combat cybercrime. The centre is composed of highly specialised technical and professional experts in the fields of detection, forensics and technology.

The competent police authorities responsible for both cybercrime in the narrow sense and digital forensics and data security in Austria operate on three levels. At the federal level and as a higher-level organisation, C4 is located in the Criminal Intelligence Service Austria. Divisions providing specialised cybercrime and forensic assistance are part of the State Criminal Police Offices and have been established in each of the nine state police directorates. Specially trained, uniformed police officers (district IT investigators) work at the district level to provide the necessary support to first responding officers (first responders).

C4 is currently being restructured. Building on the existing structures, C4 resources are being expanded. Furthermore in future following structures will be established:

3.2.1 Core tasks

Central administration and organisation of projects and funding programs, international cooperation, development and organisation of national and international training programs, procurement of ICT hardware and software.

3.2.2 IT preservation of evidence

Specialist expertise in the securing and assessment of electronic evidence is one of the core elements of C4. In addition to IT forensics and mobile forensics, this also includes the specialist areas of multimedia forensics, electronics and IoT forensics and vehicle forensics.

3.2.3 IT investigation

In order to adequately combat high-tech crime, operational support teams will expand existing investigative areas and will also as mobile teams. Specialised investigative units for the darknet as well as cryptocurrencies/blockchain (sometimes responsible for cryptocurrency seizures and recovery) are needed to provide the necessary expertise in investigations. The area of "Complex Cybercrime", where cybercrime offenses and mass phenomena are addressed, will also be covered there in the future.

3.2.4 Development and Innovation

Support for digital forensics and digital investigations with scientific expertise as well as demand-oriented development of tools and scripts are provided internationally to other law enforcement agencies (international cooperation with research institutes and institutions).

3.2.5 Digital Evidence Management

Digital Evidence Management combines the competencies required for modern criminal police processing of complex cases with large quantities of data. This includes the technical preparation of seized digital evidence for systematic indexing and subsequent provision to the Criminal Intelligence Service and the State Criminal Police Offices. It furthermore acts as an interface between forensic experts, investigators, technicians and if the judicial system.

3.2.6 Reporting office and ZASP

The reporting office is the point of contact for citizens (against-cybercrime@bmi.gv.at) and law enforcement officers (national and international) in regard to IT offenses. It is responsible for conducting mutual assistance requests, advance data securing, detection of new cybercrime phenomena as well as identifying new modi operandi. The Central Enquiry Point for Social Media & Online Service Providers (ZASP) was established to streamline and facilitate queries and the underlying processing for consultants on social media platforms and online service providers.

3.3 ICT & Cyber Directorate

The cyber forces are the elements in the Austrian Armed Forces (AAF) that connect the other branches (such as land force and air force). They are also responsible to establish communication line across all echelons of command (from the ministry to the group commander) and thus providing for communication and command capabilities.

In the newly created ICT & Cyber Directorate, elements of ICT and cyber forces are brought together. The ICT & Cyber Directorate forms the AAF Competence Centre for information and communication technology, cyber defence, electronic warfare and mission related military geo-information both in peacetime as in military operations.

Hierarchy wise everything is now in one place: from military strategic planning in cyberspace to command and control down to the provision of ICT services. As a result, planning and implementation of ICT are closer together, allowing for optimised process times and better meeting military needs.

The core task of the ICT & Cyber Directorate is providing interoperable, secure and innovative services – both for the use within Austria and abroad, guaranteeing Command, Control & Communication superiority in cyber space.

The ICT & Cyber Directorate are permanently confronted with threats from within the cyber and information space as well as hybrid threats and therefore must be capable of immediate incident response.

3.3.1 Cyber Force

Cyber Force deals with adversaries in cyberspace. It therefore has to act within the full spectrum of Computer Network Operations (defence, exploitation, attack). Cyber Force is responsible for ensuring the protection of the ICT systems and the information stored and processed within. It must maintain or restore information protection at any given time, especially in the event of cyber attacks.

If required, it supports the protection of ICT systems in constitutional facilities and critical infrastructures. Cyber Force takes on this task independently in the event of an attack in cyber space that jeopardises sovereignty.

3.3.2 ICT Force

ICT Force plans, establishes and operates the Armed Forces' ICT systems. It provides the information and communication technology for the forces in day-to-day life and during exercises and missions both within Austria and abroad.

In addition to fixed ICT infrastructures, deployable and mobile infrastructures are used as required and connected to military-secured networks. Independent operation is an essential feature of ability. Transitions to other networks and/or access to the internet can be technically created and operated.

3.3.3 EW (Electronic Warfare)

Specifically for the electromagnetic spectrum, Electronic Warfare (EW) is tasked with collecting, identifying, assessing and preparing information for the respective level of management using technical means. Electromagnetic signals are to be technically analysed, stored and used to protect troops against hostile electromagnetic effects as well as to deny an aggressor/opponent unobstructed use of the electromagnetic spectrum by measures of interference.

3.4 Austrian Armed Forces Security Agency (AbwA)

The term cyber defence refers to all efforts of the AAF in cyberspace as a whole. The AbwA contributes to this with its competencies and by providing intelligence, creating a common operational picture with focus on cyberspace. Based on their assessments courses of actions for countering cyber attacks are being evaluated.

Through this and other measures, the goal is to provide a permanently high level of security for the military ICT infrastructure.

3.5 Austrian Strategic Intelligence Agency (HNaA)

The Austrian Strategic Intelligence Agency is Austria's strategic foreign intelligence service. As such, it obtains information about other countries, assesses it and provides the results to the highest levels of political and military leadership. This includes monitoring developments and processes relevant to intelligence in and about cyber space as an aspect of the general intelligence-related situation. By detecting cyber threats it makes a significant contribution to decision-making with regard to the general state countermeasures to be taken and possible attribution.

3.6 GovCERT, CERT.at and Austrian Energy CERT

GovCERT Austria

Under the provisions of Austria's Network and Information Systems Security Act (NIS Act), GovCERT Austria responds to computer emergencies within the public administration and is part of the Inner Circle of the Operative Coordination Structure (IKDOK). Its strategic operations are based within the BKA and its operational services are provided as part of a public-private partnership with CERT.at. GovCERT functions as Austria's point of contact for public administration networks and is in close dialogue with various international organisations and interlocutors, including the European GovCERT Group and the Central European Cybersecurity Platform (CECSP).

CERT.at has been acting as Austria's national computer emergency team since March 2019, in accordance with the NIS Act. CERT.at sees itself as a point of contact for all ICT incidents in Austria with a security dimension. It is renowned as a reliable and widely recognised information hub for Austrian organisations and companies in the cybersecurity sector.

CERT.at

The Austrian Energy CERT (AEC) is an industry-specific Computer Emergency Response Team (CERT) for the Austrian energy industry. In 2020 it was accredited as the sector-specific computer emergency team for the energy sector under the NIS Act. The main tasks of the AEC are geared towards strengthening IT security expertise within the energy sector and making it more resilient against cyber attacks. In addition to managing security incidents, the AEC is also responsible for handling day-to-day queries and security reports, providing training sessions, taking part in international cybersecurity exercises and helping to draft technical security plans for the electricity and gas sectors. The AEC also acts as the single point of contact in the event of security incidents affecting the energy sector at home and abroad, ensuring rapid communication and coordinating the work of IT security experts and authorities within the energy industry.

AUSTRIAN ENERGY CERT

The three CERTs work together to exercise their responsibilities under Section 14 of the NIS Act, thus meeting the requirements set out in the European Directive on the Security of Network and Information Systems (NIS) and the recommendations of the European Union Agency for Network and Information Security (ENISA) for increasing IT security in critical infrastructure. They also represent Austria within the EU's CSIRTs Network. All three CERTs work primarily on security threats and incidents, either under agreements with relevant bodies or on the basis of their own research. All three also carry out work to prevent cybersecurity incidents, including early detection of potential threats and raising public awareness, as well as providing advice and support as required and requested.

The remits of the CERTs were codified when the NIS Directive was transposed into Austrian law as the NIS Act. Among other provisions, the law places operators of essential services and digital service providers under an obligation to report serious security incidents. These mandatory reports are sent by affected parties to defined, sector-specific recipients (sector-specific computer emergency teams) and then forwarded to the BMI and/or the CSC, which is part of the DSN. The same procedure also applies to voluntary reporting, with the exception that voluntary reports can be anonymised by the sector-specific CERTs before they are forwarded to the CSC.

Unless the reporting organisation is a member of IKDOK in its own right, incident reports from organisations within the public administration are sent to GovCERT, which forwards them on as appropriate. GovCERT can issue early warnings, alerts, recommendations for action and notifications. It also provides general technical support as part of the initial response to security incidents, analyses risks, incidents and security vulnerabilities, and assesses the overall cybersecurity situation. To enable GovCERT to fulfil its role as a report's authority, the NIS Act provides for an industry or sector-specific CERT to be set up for each of the sectors covered by the Act. Where specific sectors do not yet have CERTs of their own, the duties normally assigned to the computer emergency team and the reporting authority are carried out by CERT.at.

3.7 Office for Strategic Network and Information System Security

The Office for Strategic Network and Information System Security ("Strategic NIS Office") located in the Federal Chancellery continued its work successfully in 2021. In particular, the determination of the operators of essential services based on the NIS Regulation could be completed in 2021.

In terms of Austria's representation in the NIS Cooperation Group and in other EU-wide and international committees for the security of network and information systems to which strategic tasks are allocated, extensive activities have been undertaken. For more information, please refer to Section 2.1. The focus is on the coordination and representation of the Austrian position in the negotiation of the NIS2 Directive.

3.8 Operative Network and Information System Security

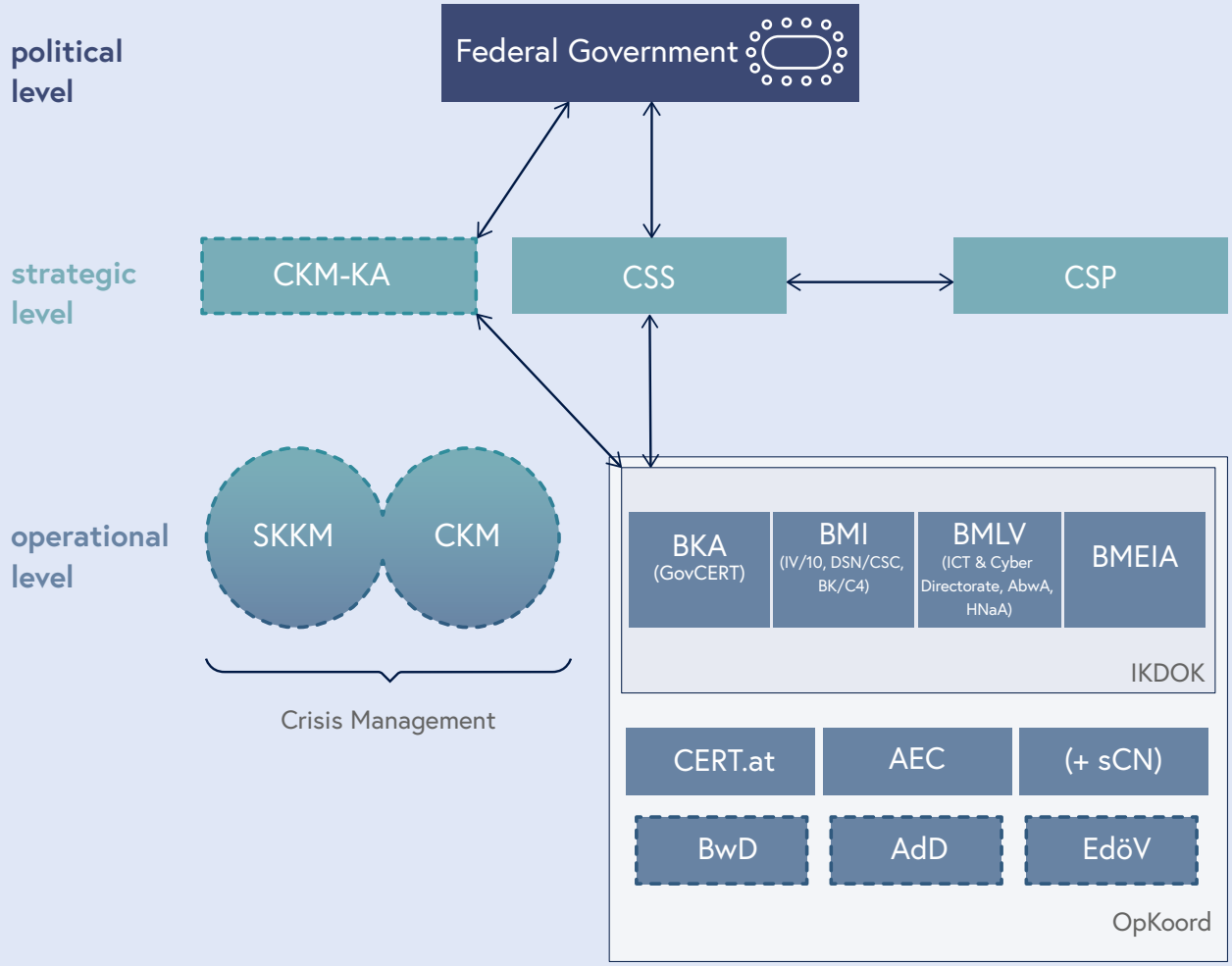
On 30 November 2021, the Federal Agency for State Protection and Counter Terrorism (BVT) was dissolved as part of an extensive reform, and recreated as the State Security and Intelligence Directorate (DSN). The tasks that had previously been carried out by the II/BVT/5 department to this point were subsequently divided between the DSN and Division IV of the Federal Ministry of the Interior (BMI). As part of this allocation of competence, department IV/10 "Network and Information System Security" in Division IV of the BMI was reformed.

The main task of this new department is to carry out all of the functions of the operational NIS authority in Austria. This essentially includes implementing the specifications of the Network and Information System Security Act (NIS Act) with respect to the operators of essential services, providers of digital services and public administration facilities. This includes, among other things, the regular verification of compliance with mandatory security measures at affected companies and organisations, the operation of a reporting collection point for security incident reports and a single point of contact for communication with the NIS authorities of other EU member states in the event of cross-border cyber incidents.

In the future and on the basis of the regulations set out in the NISG, department IV/10 will also take on a coordinating role within the general governmental Operative Coordination Structure (OpKoord) and the Inner Circle of the Operative Coordination Structure (IKDOK), which was previously filled by the CSC in the BVT. Furthermore, the department supports authorised companies and organisations in the area of cyber prevention within the framework of the tasks standardised in the NISG by offering a comprehensive range of consulting services, workshops, lectures and publications for their employees.

Legend

- - - - - - - - - - - - event-related
AbwA ..... Austrian Armed Forces Security Agency
AdD ..... Digital Service Providers
AEC..... Austrian Energy CERT
(= sector-specific CSIRT for sector energy)
BK..... Criminal Intelligence Service Austria
BKA..... Federal Chancellery
BMEIA ..... Federal Ministry for European and International Affairs
BMI ..... Federal Ministry of the Interior
BMI IV/10 ..... Department Network and Information Systems Security
BMLV..... Federal Ministry of Defence
BwD ..... Operator of Essential Services
C4 ..... Cybercrime Competence Center
CERT.at ..... the national CSIRT
CKM..... Cyber Crisis Management
CKM-KA..... Cyber Crisis Management Coordination Committee
CSC ..... Cyber Security Center
CSP..... Cyber Security Platform
CSS ..... Cyber Security Steering Group
DSN ..... State Security and Intelligence Directorate
EdöV..... Entities of Public Administration
GovCERT ..... Government Computer Emergency Response Team Austria
HNaA..... Austrian Strategic Intelligence Agency
IKDOK ..... Inner Circle of the Operative Coordination Structure
OpKoord ..... Operative Coordination Structure
sCN..... Sector-specific CSIRT
SKKM..... State Crisis and Catastrophe Protection Management


political level
Federal Government
strategic level
CKM-KA
CSS
CSP
operational level
SKKM
CKM
Crisis Management
BKA (GovCERT)
BMI (IV/10, DSN/CSC, BK/C4)
BMLV (ICT & Cyber Directorate, AbwA, HNaA)
BMEIA
IKDOK
CERT.at
AEC
(+ sCN)
BwD
AdD
EdöV
OpKoord

4
National Structures

4.1 Inner Circle of the Operative Coordination Structure (IKDOK)

The NIS Act came into force on 29 December 2018. In the field of cybersecurity, this forms the most important foundation for interministerial cooperation in Austria. One immediate result of the advent of the NIS Act was the creation of a permanent structure for cooperation at operative level (known as OpKoord). This body incorporates an interministerial structure for operative cooperation on network and information systems security, known as the Inner Circle of the Operative Cooperation Structure (IKDOK). While the OpKoord itself is primarily tasked with assessing the overall security situation, taking account of voluntary and mandatory incident reports, the IKDOK is responsible for recording and assessing the overall risk, incident and security incident picture and for providing support to the Cyber Crisis Management Coordination Committee (CKM).

In the event of a crisis, the IKDOK assumes the role of a direct interface with the government-wide CKM, supported by the OpKoord. In terms of the mechanisms and processes to be applied in such a crisis, the CKM will be guided by the tried and tested procedures used by Austria's State Crisis and Catastrophe Protection Management (SKKM).

In early 2020, IKDOK and the CKM were put to their first severe test when a cyber attack on a constitutional institution was repelled without permanent damage and a cleanup of the affected network was successfully coordinated and executed.

IKDOK is now composed of representatives of the BMI (IV/10, DSN/CSC, BK/C4), BKA (GovCERT), BMEIA and BMLV (AbwA, ICT & Cyber and HNaA). The BMI (IV/10) coordinates the work in the committee and leads the discussions. The IKDOK prepares a monthly IKDOK and OpKoord situation report, which is made available to the respective target group.

4.2 CERT-Verbund Austria

The CERT Verbund Austria was founded in 2011 to bring together all the Austrian CERTs operating at the time across government and the private sector. It is intended to pool the available resources in order to exploit shared expertise as effectively as possible. Participation in CERT Verbund Austria is voluntary. All members of the group, which is jointly led by its members and operates on the basis of cooperation between them, commit to taking part in regular exchanges of information and experience, helping to identify and provide core expertise, and supporting CERTs across all sectors of the economy.

One of the differences between a 'traditional' IT security team and a CERT is that readiness to communicate and work with third parties is an essential requirement for a CERT. Part of a CERT's role is to act as an interface with outside stakeholders, network, and work together with other teams. At international level, CERTs are organised within FIRST (Forum of Incident Response and Security Teams), while in Europe they fall under the TF-CSIRT and EU CSIRTs Networks.

The reason for this emphasis on cooperation is that a comprehensive network of CERTs is recognised as one of the most effective tools for securing networked information and communications systems, as confirmed by the steady growth in the number of CERTs, CSIRTs, Security Operations Centres (SOCs) and cyber defence teams within Austrian companies and the close partnerships that have been forged between them.

Since the Corona situation for the 10th anniversary in November 2021 was not foreseeable, a social event was already held in the summer. This was very well received after the long period of mainly online CERT network meetings and contributed significantly to strengthening the cooperation.

Since the CERT Association Austria was founded, the currently 17 participating teams have met in 50 sessions and are also in constant exchange with each other outside the regular meetings via secure communication channels. This allows for a near-time common operational picture and measures can be coordinated rather quickly across organisational and company boundaries.

Cyber Sicherheit Plattform

4.3 Cyber Security Platform (CSP)

As an integral part of the Austrian cyber ecosystem, the Cyber Security Platform (CSP) has been functioning as a central strategic exchange and cooperation platform between business, science and public administration for six years now. It is trusted by all relevant stakeholders and is used to exchange experience and information in the field of cybersecurity, with a particular focus on critical infrastructure. The CSP makes important contributions to the development of the Austrian Strategy for Cybersecurity and to the design of the legislative framework for cybersecurity in Austria (keyword NIS, NIS2).

As a cross-sectoral cooperation model, the CSP attracts attention well beyond Austria. For example it got presented to the Confidence-Building Measures Working Group of the OSCE during a meeting in 2021. It is also well involved in international working groups such as ENISA or the UNODC Cyber Crime Convention rounding off the overall picture. In 2022, the CSP will continue to make its contribution to shaping cybersecurity in Austria and will form an essential part of the Austrian Cybersecurity Competence Community (CCC) within the framework of the National Cyber Security Coordination Centre (NCC, see also chapter 2.1.7).

4.4 Austrian Trust Circle (ATC)

The Austrian Trust Circle (ATC) is a national initiative designed to facilitate exchange of information on cybersecurity and related incidents at a technical level. Its work is targeted at all sectors of Austria's strategic infrastructure, as well as the public administration. The ATC was founded in 2011 by CERT.at with the support of the Federal Chancellery. It consists of a series of sector-specific security information exchanges and is aimed at companies and organisation running Austria's critical infrastructure and relevant government authorities. CERT.at and the AEC, in cooperation with GovCERT Austria and the BKA respectively, provide a formal framework for exchanging practical information and joint working across the security sector.

The ATC's primary objectives are:

- to create a basis of trust allowing joint action in the event of a major incident;
- facilitating networking and exchange of information within and between sectors involved in critical infrastructure, as well as with the government;
- exchanging contacts between CERTs and participating companies, organisations and authorities;
- helping sectors involved in critical infrastructure to help themselves on IT security;
- establishing operational contacts with the CERTs, for example
  - regarding reporting and handling;
  - security incidents within organisations;
  - establishing contacts with BKA experts in the event of a crisis.

Regular meetings within the individual sectors were sporadic in 2021 as a result of the coronavirus pandemic, but dialogue between sectors and the government is encouraged through a two-day annual conference.

At least this meeting could be held in 2021 in compliance with the regulatory requirements, which enabled an important exchange on security-related topics.

4.5 ICT security portal

The ICT security portal at onlinesicherheit.gv.at is an interministerial initiative launched in cooperation with Austrian business. It is a central internet portal for issues related to security in the digital world. The portal is a strategic measure, set up as part of Austria's national ICT Security Strategy and the Austrian Strategy for Cybersecurity (ÖCSC). It aims to create and strengthen a culture of cybersecurity in Austria over the long term by raising awareness of related issues among its target audience and providing them with tailored recommendations for action.

The range of information and services available via the portal is continuously expanding, and regular editorial meetings are held with the 40 organisations involved in the project, including federal ministries, the governments of Austria's federal states, state authorities, universities, technical colleges, research institutes, companies, associations and representative bodies. It provides access to the latest reports and warnings, important information and advice for cybersecurity beginners and experts alike.

In 2021, activities on the ICT security portal included the making available 130 news articles, 24 publications and 68 events. Each month a focus topic on current trends was defined, for which a total of 107 specialist articles were published. This included, for example, IT security in the home office in March, in May the digital office and secure digital government procedures and in October a recurring focus on "European Cyber Security Month" (ECSM) and the Austrian activities organised in the course of it. Furthermore, the Cyber Monitor, a statistical presentation of the twelve most significant threats in ICT and cybersecurity, has been completely redesigned. The Cyber Monitor offers a graphical representation of the development of the threat situation for the respective categories and thus displays current trends.

5
Cyber Exercises

5.1 Blue OLEx 2021

On 12 October 2021, ENISA organised the third Blue OLEx cyber exercise together with the Romanian National Cyber Security Directorate (DNSC). The primary goal of the exercise was to test and practice the Standard Operating Procedures for large-scale, cross-border cyber incidents set out by CyCLONe. Due to the COVID-19 pandemic, the exercise took place in hybrid format in Bucharest and online.

The exercise was a so-called tabletop exercise. This means that the exercise scenario was only played out in theory and there were no actual restrictions on the facilities addressed. The exercise scenario focused on security incidents in the field of rail-bound transport infrastructure and the energy sector in several European countries. In the course of the exercise, injects on various impairments of regular operations such as disruptions in energy supply, manipulation of rail signalling systems, prolonged power outages and accompanying disinformation campaigns were processed and appropriate measures and responses were assessed.

High-ranking representatives of authorities from a total of 22 EU member states took part in the exercise. People from the EC and ENISA were involved from the EU. The Austrian delegation was involved in the exercise online, with participants from the central office of the BMI, the DSN and the Federal Chancellery.

5.2 KSÖ simulation game

On 20 and 21 September 2021 together with the Austrian Institute of Technology (AIT), the Competence Centre for a Safe and Secure Austria (KSÖ) organised an international cybersecurity simulation game in Germany, Austria and Switzerland in which the defence against cyber attacks was played out realistically in hybrid form. The focus of the simulation game was on cyber-physical and concurrent information measures. The exercise brought together a wide range of technical and strategic players, observers and multipliers at the Raiffeisen Forum in Vienna and – connected online – in Switzerland and Germany. The exercise was sponsored by the BMI and involved eight teams playing in Vienna practising together with the national coordination structure for cybersecurity (IKDOK/OpKoord) and with partners from the Swiss National Cyber Security Centre (NCSC) and the German Federal Office for Information Security (BSI) in a challenging scenario. This threat scenario was developed and implemented by AIT experts in the "AIT Cyber Range".

The scenario of the exercise was adapted to the current political and social situation in light of the COVID-19 pandemic. In this scenario, a group of militant anti-vaxxers attempted to bring a fictitious international pharmaceutical group, which plays a key role in fighting a pandemic, to its knees through various cyber attacks accompanied by massive disinformation campaigns. The individual teams acted as employees of the attacked group, and together tried to defend against the attacks and restore normal business operation. The participating representatives of the authorities supported the group in line with their real-life roles, thereby testing and optimising national and international reporting and communication channels.

5.3 milCERT Interoperability Exercise 2021 (MIC21)

The AAF milCERT (military Computer Emergency Readiness Team) successfully participated in the MIC21 exercise, organised by the European Defence Agency (EDA) for the first time, and took third place in the overall ranking. The special "Situation Reports" award was also won by the Austrian team.

Cooperation and information exchange are key factors in combating threats in cyber space. That is why the EDA focused on these very topics in the new series of exercises. The participating teams had to detect live attacks on typical military IT environments (e.g. office environment, command structure/"C2", communication systems, critical infrastructure and sensor/weapons systems), analyze them and identify relevant threats, all in a virtual environment. Regular reports called "situation reports" (SITREP) had to be produced and assessed.

The primary goal of the exercise was to bring milCERTs within the EU closer together to strengthen cooperation as well as information exchange. In addition, cybersecurity incidents were also to be jointly detected, identified and resolved. Typical characteristics of detecting an attack, known as Indicators of Compromise (IoC), needed to be provided to the other milCERTs. They could then search their own environments and retrospectively identify attacks that may have been overlooked and initiate appropriate countermeasures.

As the Estonian Defence Minister, Kalle Laanet, noted in his speech as virtual host, "Today we can see that at the EU level civilian CERTs have established good community and their cooperation is improved continuously. However, military CERTs, which play vital role in cyber defence, are not communicating with the same methods. This is understandable considering the more sensitive information they are dealing with. Yet, despite these limitations, it is still important to offer opportunities for extending information-sharing practices. And this live-fire exercise does exactly that".

The Austrian milCERT is committed to continue participating in this exercise series and to improve the exchange of information on cyber attacks with partners at EU level. After all, only by working together will it be possible to effectively meet the challenges in cyberspace in the future.

5.4 Locked Shields 2021 (Red Team)

Exercises are crucial for increasing state resilience

Austria has participated in the international cyber exercise "Locked Shields", organised by the NATO training facility Cooperative Cyber Defence Centre of Excellence for almost ten years. So far, Austria as the defending team ("Blue Team") has always been among the top five of the participating nations and organisations.

This year, though, the delegation from the ICT & Cyber Directorate was on the Red Team, changing back on being the defending Blue Team again in 2022, this time as a joint team with Germany.

This year's exercise involved more than 5,000 virtualised systems that had to be defended against more than 4,000 attacks. In addition each team had to maintain more than 150 complex IT systems. The Blue Teams had to report incidents, make strategic decisions, face forensic, legal and media challenges and prevail against cyber enemies.

This year, the exercise focused on improving communication between technical experts, civil and military participants and leadership levels. The NATO Centre created this technical and strategic "game" to rehearse the implementation of the command chain in the event of a serious cyber incident affecting civilians and the military.

5.5 Common Roof 2021

The multinational exercise “Common Roof 21” took place from 2 to 19 November 2021 in the Schwarzenberg barracks in Wals-Siezenheim. The exercise scenario was an earthquake in the Rhine Valley in Switzerland with impact on Germany and Austria. An interoperable, military control network was set up to support the civilian infrastructure, maintain state crisis management and protect against cyber threats.

The provision of an emergency communication network to maintain command and control capability was an essential part of the military operational command. The challenge was to create secure transitions to other military and civilian IT networks. In order to do this, interoperability standards and operational processes were specified for “Federated Mission Networking”.

The exercise focused on multinational and joint operations management, in which IT service management and ICT security processes were practiced and evaluated. For this purpose, the networks of Austria, Germany and Switzerland were interconnected, centrally monitored and controlled.

The exercise scenario also included a wide variety of operations that had to be coordinated jointly in the event of an emergency. Thus, the civil-military and tri-national cooperation for the support of emergency forces in a disaster situation could be supported in the best possible way.

A total of 150 people from Germany, Switzerland and Austria took part in the joint exercise. The approximately 55 exercise participants from Austria were predominantly IT experts from the Austrian Armed Forces’ ICT & Cyber Directorate. The exercise was led by the newly created ICT & Cyber Operations Department.

5.6 Multilateral Cyber Defence Exercise 2021

The Military University Institute in Lisbon carried out this year's "Cyber Phalanx". A total of 130 participants from the EU and NATO were trained as managers on operative planning processes. The cyber experts of the Austrian Armed Forces were also present. The Multi-Lateral Cyber Defence Exercise took place at the cyber range of the CODE research institute in Munich from 4 to 8 October 2021. The cyber teams were not formed based on nationality; rather the emphasis was on mixing the groups by individual skills. Each team member also proved to be a team leader.

Nationally and internationally gained knowledge from cooperation and collaboration is of uttermost importance in case of an emergency. Participants are trained in dealing with transnational threats, which leads to an increase in cybersecurity protection and strengthens the capability to defend against cyber attacks on critical infrastructure.

There is no alternative to running realistic exercises in cyber space for both military organisations and for authorities, companies and others. Only scenarios that are regularly practised will actually work when they are put to the test.

6
The new Austrian Strategy for Cybersecurity 2021

In 2021, the new Austrian Strategy for Cybersecurity 2021 (ÖSCS 2021 for short) was passed. It aims to achieve a secure cyber space in the long term and should be viewed as a contribution to increasing the resilience of both Austria and the European Union (EU) and is being implemented using a national approach.

The ÖSCS 2021 is a further development of the ÖSCS 2013 and builds on its national structures and principles. The publication was preceded by intensive collaboration and numerous discussions with stakeholders at national, European and international level. Experts from economy, education, research and development as well as federal government were involved in the development of the strategy.

With the new Austrian Cyber Security Strategy 2021 a new, comprehensive and whole of society concept for the protection of cyberspace and people in virtual space is introduced

Strategic documents tend to stay valid for a long time. This is a particular challenge for highly dynamic topics such as cybersecurity. The decision was therefore made to split the ÖSCS 2021 into a strategic framework and a dynamic, web-based catalogue of measures.

The ÖSCS 2021 document sets out the overarching long-term strategic structure and specifies the initial position, challenges and opportunities. It contains the vision of the ÖSCS 2021 and defines twelve objectives for its realisation. The target groups of the ÖSCS 2021 are society, business, education, research and development and the public sector.

Cybersecurity is not something that can be conceived of at a regional level, so the ÖSCS 2021 is embedded in the European Cyber Security Strategy for the Digital Decade. The strategic document additionally defines how to collect and manage measures as well as laying out the controlling and monitoring process.

The second part is a web-supported, database-based management tool. This allows for the collection, management, control and monitoring of measures for the implementation of the objectives of the ÖSCS 2021. This way an agile and prompt response to changing

framework conditions, challenges and threats can be provided. The USP in this is that the target groups can define measures affecting their own area of activity and add detailed implementation plans. With each measure being assigned to at least one objective and one target group the coverage of the strategic demands is trackable.

Ultimately, the CSS is responsible for monitoring the implementation of the ÖSCS. Based on the implementation plans, a progress report is prepared every six months and – as far as possible – published.