


Report Cyber Security 2019



Report Cyber Security 2019

Wien, 2019

 Federal Chancellery
Republic of Austria

 Federal Ministry
Republic of Austria
Interior

 Federal Ministry
Republic of Austria
Defence

 Federal Ministry
Republic of Austria
Europe, Integration
and Foreign Affairs

Imprint

Media owner, publisher and editor
Cyber Security Steering Group
Ballhausplatz 2, 1010 Vienna

Graphic Design: BKA Design & Grafik

Vienna, May 2019

Inhalt

Introduction	7
1 Cyber situation/threat	8
1.1 Cyber security situation – operative level.....	8
1.1.1 Spectre/Meltdown (01/2018).....	8
1.1.2 VPNFilter (05/2018).....	8
1.1.3 Advanced Persistent Threats (10/2018).....	9
1.2 Cyber security situation – enterprises and security service providers.....	9
1.2.1 Enterprises working in critical infrastructure.....	10
1.2.2 Leading private enterprises from the cyber security industry.....	12
1.3 Cybercrime situation.....	16
1.4 Cyber situation – national defence.....	17
2 International developments	19
2.1 European Union.....	19
2.1.1 Implementation of the NIS Directive.....	19
2.1.2 Regulatory proposals for cyber security.....	20
2.1.3 European Union Agency for Network and Information Security.....	20
2.1.4 Cyber security certification framework.....	20
2.1.5 Network of National Coordination Centres and European Competence Centre.....	21
2.1.6 Coordinated response to major cyber security incidents and crises (Blueprint).....	21
2.1.7 Cyber diplomacy.....	21
2.1.8 Cyber security in the European parliamentary elections	22
2.1.9 ECSO-cPPP.....	22
2.1.10 “Digital Europe” programme 2021-2027.....	23
2.1.11 Fight against terrorist content on the internet.....	24
2.1.12 Action plan against disinformation.....	24

2.2 Austrian Council Presidency cyber security.....	25
2.2.1 Cyber security conferences	25
2.2.2 Horizontal Working Party on Cyber Issues.....	26
2.2.3 NIS Cooperation Group.....	27
2.2.4 CSIRTs network.....	28
2.3 United Nations.....	29
2.4 NATO.....	32
2.5 OSCE.....	32
2.6 OECD.....	33
2.7 Council of Europe.....	33
2.8 Austria in other cyber relevant international forums.....	34
3 National actors and structures.....	36
3.1 Inner Circle of the Operative Coordination Structure (IKDOK).....	36
3.2 Cyber Security Center.....	37
3.3 ICT and Cyber Security Centre (ZIKT&CySih).....	37
3.3.1 Military Cyber Security Centre (MilCySihZ).....	38
3.3.2 Self-protection.....	38
3.3.3 milCERT (Military Computer Emergency Readiness Team).....	38
3.3.4 Cyber military training area	39
3.3.5 Information security.....	39
3.3.6 Electronic warfare.....	39
3.4 Cyber Defence Centre.....	39
3.5 Army Intelligence Office.....	40
3.6 GovCERT, CERT.at and Austrian Energy CERT.....	40
3.7 CERT Association.....	42
3.8 Cyber Crime Competence Center (C4).....	43
3.9 Cyber Security Platform (CSP).....	43
3.10 Austrian Trust Circle (ATC).....	44

3.11 ICT security portal.....	45
3.12 Office for Strategic Network and Information System Security.....	45
4 Cyber exercises.....	48
4.1 Austrian Strategic Decision Making Exercise (ASDEM) 18.....	48
4.2 CROSSED SWORDS 2018 (XS18).....	49
4.3 LOCKED SHIELDS 2018 (LS18).....	49
4.4 CYBER PHALANX 2018 (CP18).....	49
4.5 Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX18).....	50
4.6 COMMON ROOF 2018 (CR18).....	51
4.7 Cyber Europe and Cyber Europe Austria 2018.....	51
4.8 CyberSOPEX 2018.....	52
4.9 Cyber Incident Situational Awareness simulation game (CISA simulation game).....	52
4.10 EU HEX-ML 18 (PACE)	53
4.11 CYBER DIPLO ATTX18.....	53
5 Summary/outlook.....	54

Introduction

In accordance with Austria's Cyber Space Security Strategy (ÖSCS) the Cyber Security Steering Group (CSS) has to prepare an annual report on cyber security in Austria. The last report was presented in April 2018.

The current Cyber Security Report for 2019 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 2018 with the inclusion of a few current developments from 2019.

The aim of the report is to provide a summary review of the cyber threats and important national and international developments.

1 Cyber situation/threat

1.1 Cyber security situation – operative level

Austria's Cyber Space Security Strategy (ÖSCS) provides for periodical situation reports to be created along with situation reports in response to specific events at an operational level. In this reporting year, committees that have been well established for several years – OpKoord (Operative Coordination Structure) and IKDOK (Inner Circle of the Operative Coordination Structure) – carried out this task. The creation of a regular, comprehensive situation report on cyber security in Austria and the communication of this situation report to the stakeholders are key agenda items at the regular coordination meetings. A selection of the significant incidents from the IKDOK situation reports is summarised below. The compilation is set out in the order in which the incidents occurred.

1.1.1 Spectre/Meltdown (01/2018)

At the start of the year, information on a hardware vulnerability in Intel processors was published in a very effective way in the media. This vulnerability enabled computer programmers to access data that they should not normally have been able to access. Since the security vulnerability was in the hardware, not the software, security experts faced a number of obstacles that do not occur in normal vulnerabilities.

CERT.at and GovCERT worked together in close collaboration as an information hub and a continuous and reliable contact for enterprises and authorities to support them to minimise and repair the damage and overcome the obstacles that arose.

1.1.2 VPNFilter (05/2018)

In late May, security researchers published detailed information about a global botnet known to researchers as "VPNFilter". The perpetrators used a variety of vulnerabilities to take over network devices of various makes and models and infect them with malware that not only enabled the devices to be misused for further attacks but also the manipulation of network traffic. The precise extent is still not known even months later, but it is estimated that at least 500,000 devices around the world were affected.

The number of devices affected in Austria was very limited thanks to the care taken by network operators in terms of the security health of their networks. The small number of infections were quickly cleaned up after CERT.at provided information to the operators.

1.1.3 Advanced Persistent Threats (10/2018)

Advanced Persistent Threats (APT) are complex, targeted attacks on critical IT infrastructures of enterprises and authorities. In October 2018, Austria was the victim of just such an attack, with the aim of jeopardising the security of the IT systems of authorities and institutions and to steal data on a large scale. The attackers used various channels to try to infect the victims with malware to compromise user data with the ultimate goal of infiltrating the computer networks and stealing confidential data.

Through precautions taken by the institutions that were attacked and good collaboration between GovCERT and the Cyber Security Center (CSC), all of those affected were able to defend themselves against the attacks and prevent the outflow of data. The fact that the effects were minimal despite effort on the part of the attackers is a further indication of the effectiveness and importance of continued collaboration between all relevant bodies at a state level.

1.2 Cyber security situation – enterprises and security service providers

The implementation of Austria's Cyber Security Strategy (ÖSCS) is a permanent process coordinated by the Cyber Security Steering Group (CSS). One of the tasks of the CSS is to prepare an annual report on cyber security in Austria that aims to provide an overview of the cyber situation in the observation period, national and international developments and cyber exercises that were carried out.

State bodies, however, only get to see part of the situation in Austria within the scope of their activities. In order to obtain a picture of the cyber situation in Austria that is as valid and complete as possible when preparing this report,

- enterprises working in critical infrastructure and constitutional facilities and
- leading private enterprises from the cyber security industry

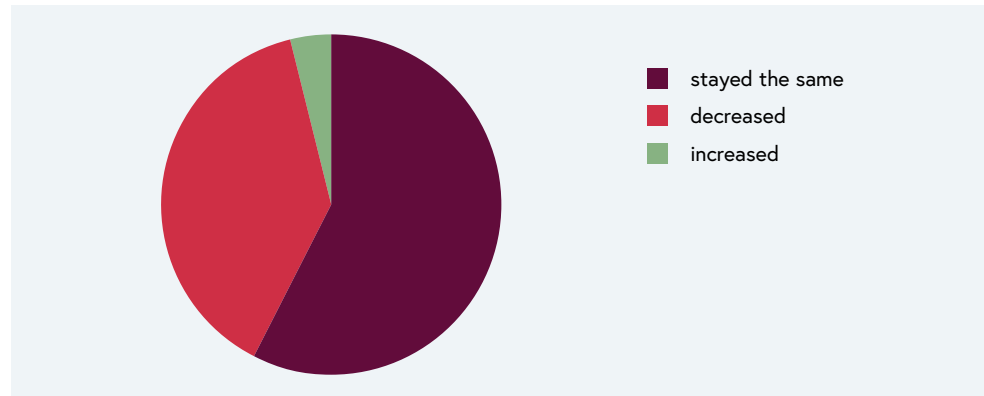
were invited to add to this knowledge on the basis of their activities and support the CSS with their expertise. The main focus was not on specific individual cases but rather on an abstract overview. We wish to thank all of the enterprises and organisations that provided us with their assessment¹.

1 The enterprises VACE Systemtechnik, FH Joanneum GmbH and Alpha Strike Labs GmbH agreed to be mentioned by name in the report. Thank you!

1.2.1 Enterprises working in critical infrastructure

A pleasing trend in terms of the budgets available for IT security was observed in enterprises working in critical infrastructure in 2017. The majority of the organisations surveyed had made investments in the field of cyber security. This trend continued unchanged in the subsequent year. While the vast majority of critical infrastructure and constitutional facilities continued to invest more money in IT security, the percentage of organisations having to get by with a reduced budget was pleasingly low and decreasing.

Figure 1: Change in the available budget



In line with the increased budget for IT security and well beyond this, new security measures of various kinds were taken in the organisations: this was the case in more than 80% of the feedback we received. Significant factors were probably the new legal requirements for IT security such as the General Data Protection Regulation that entered into force in May 2018 or the Network and Information System Security Law that is relevant to operators of essential services and providers of digital services.

Figure 2: Measures taken in 2018

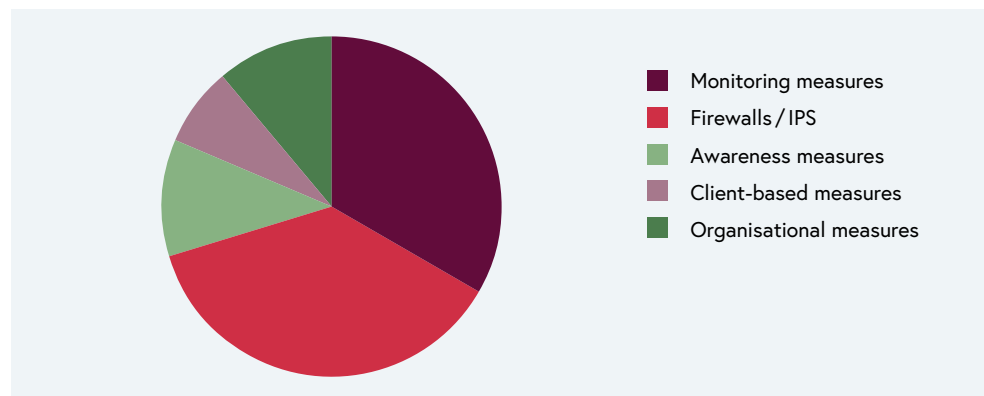


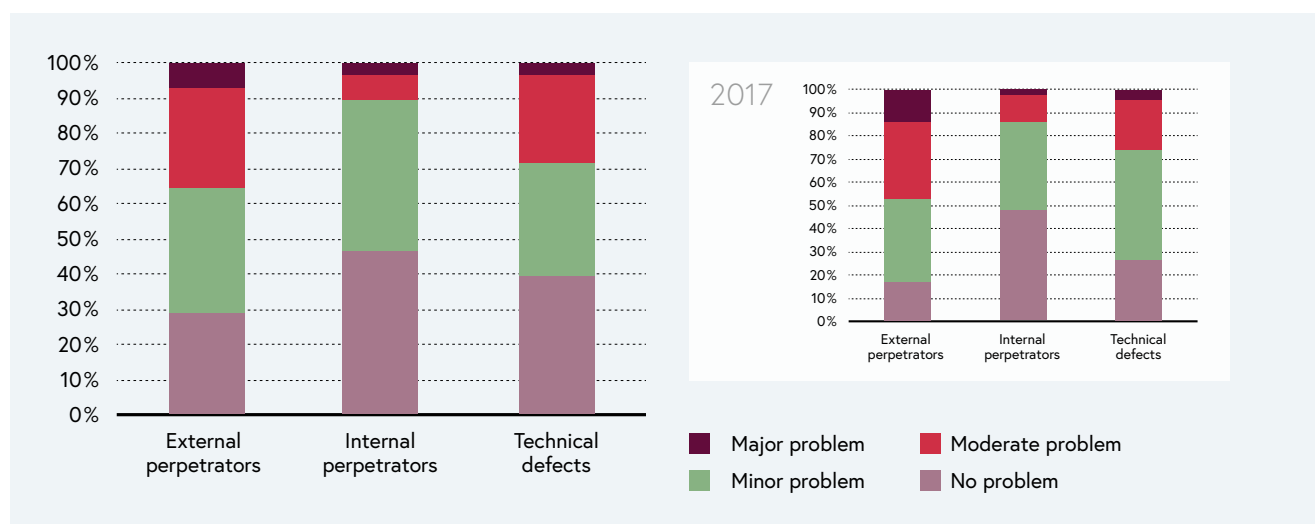
Figure 2 provides an overview of the security measures that were introduced. While technical advancement in the fields of firewalls/IPS and endpoint protection (albeit to a lesser extent) undoubtedly led to upgrades in the defence measures, in parallel to this the trend from the past few years also continued here: instead of relying purely on partitioning, increasing numbers of organisations are taking monitoring measures

to identify attackers in their network. This also includes actively searching for current threats to the respective organisation and in a second step the targeted checking of systems after infections. Alongside this, in many places preparatory measures were also taken to analyse security incidents using forensic methods.

Awareness measures were also introduced or improved in several organisations. These were often identified as effective and indispensable in the prevention of a large number of cyber attacks under the question about “lessons learned”. These measures included specialist lectures and simulated phishing or ransomware attacks. In parallel to this, enterprises also stated that the measures taken in the past were successful in 2018 and that as a result attacks were better able to be identified by users in advance.

Organisational measures such as the introduction of SIEMs and stricter policies for passwords or changes to corporate processes were also on the agenda. A link to the answers given under “lessons learned” may also be able to be identified. According to these answers, the organisations surveyed are increasingly handling new regulatory measures such as the General Data Protection Regulation or the transposition of the EU Directive on Network and Information Security.

In this context, the requirements on software manufacturers in terms of manufacturer support, maintenance, logging and adaptability are also increasing. The regulatory measures with specific requirements and the quality of software updates that is perceived by some customers as declining increase the conflicts.



In terms of the assessment of the causes of incidents, in 2018 the picture was broadly similar to the previous year. In general, a slight shift towards “no problem” can be identified.

Figure 3: Causes of incidents in 2018 compared with data from 2017

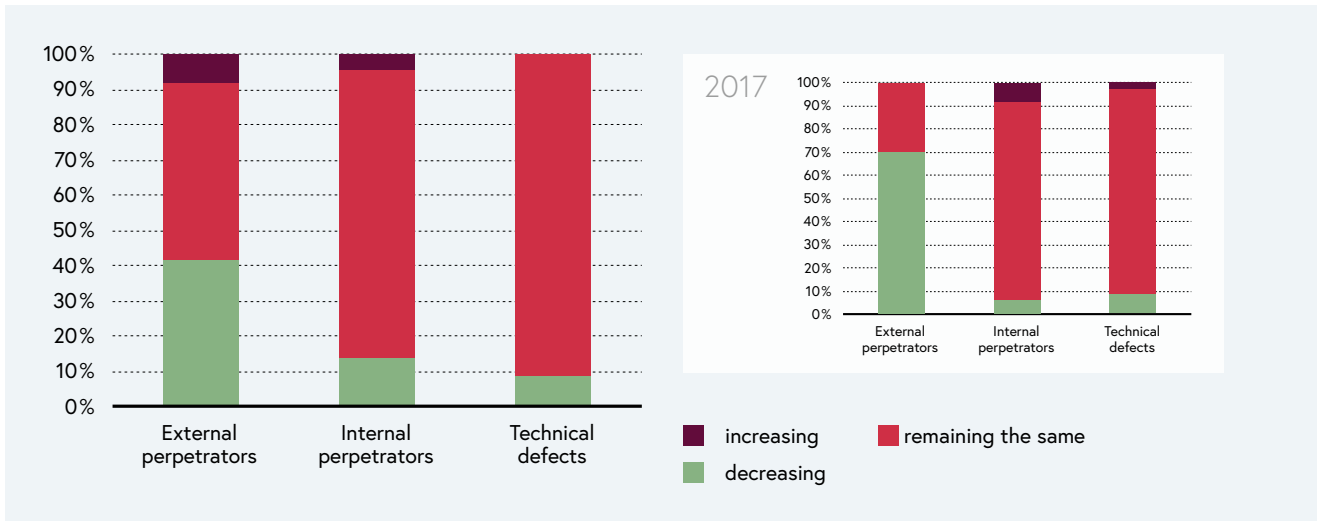
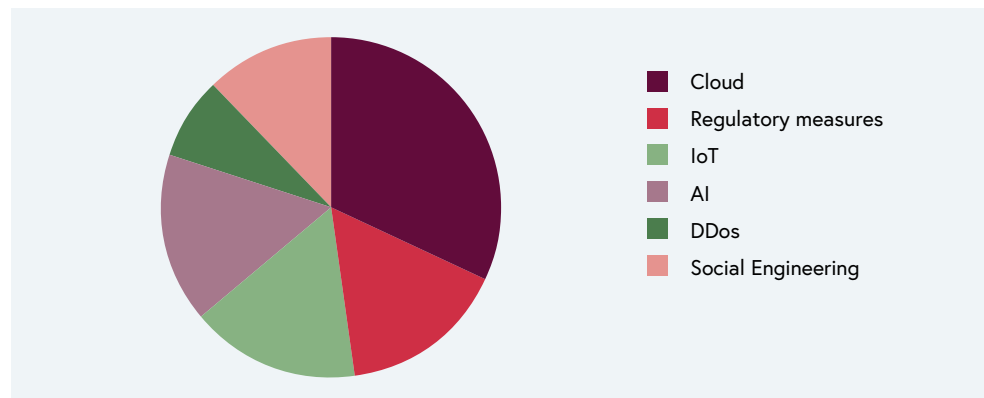


Figure 4: Trends in causes of incidents in 2018 compared with data from 2017

The trend, however, is increasing regardless of the cause, albeit somewhat slower than the previous year. In the case of external attacks, this interaction could be due to the fact that the increased defence measures, particularly in the field of ransomware and phishing, has resulted in a rise in the volume of attacks but these attacks are more frequently being identified and therefore defended against in advance.

Figure 5 shows general developments in the IT security industry. In addition to those already mentioned, cloud computing was mentioned as a very strong trend. However, this was consistently viewed critically by the enterprises surveyed, whether because of the “loss of sovereignty” over their data that they felt or the constant dependence on an external provider. It was also determined, however, that cloud solutions are being sold increasingly more aggressively to the detriment of local applications and that in the long term there will be no way to avoid the cloud.

Figure 5: General trends



1.2.2 Leading private enterprises from the cyber security industry

The survey of leading private security service providers showed a comparatively low response rate; we wish to thank VACE Systemtechnik, FH Joanneum GmbH and Alpha

Strike Labs GmbH in particular for their answers. The following trends and knowledge were able to be derived from the responses we received.

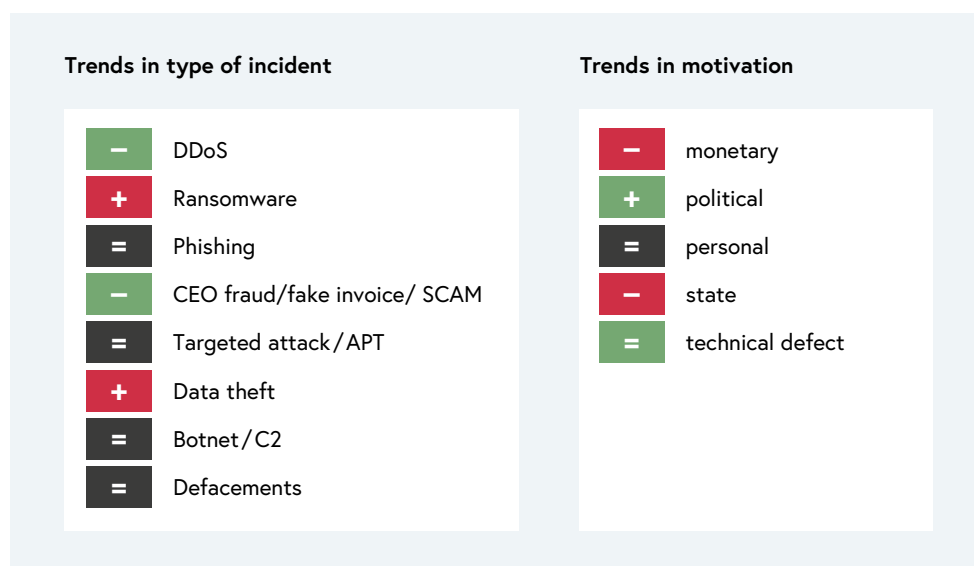


Figure 6: Trends in the types of incidents processed and the motivation for these

While 2017 already brought with it a decrease in incidents of DDoS, the number the following year had actually decreased. CEO fraud and related fraud attempts also showed a decrease, probably because people are now generally sensitised to the issue. Unlike in 2017, the security service providers were less commonly asked for help with technical defects, but on the other hand there was an increase in cyber attacks that were motivated by money or attacked a state directly. This can be linked to a further increase in ransomware attacks and data thefts.

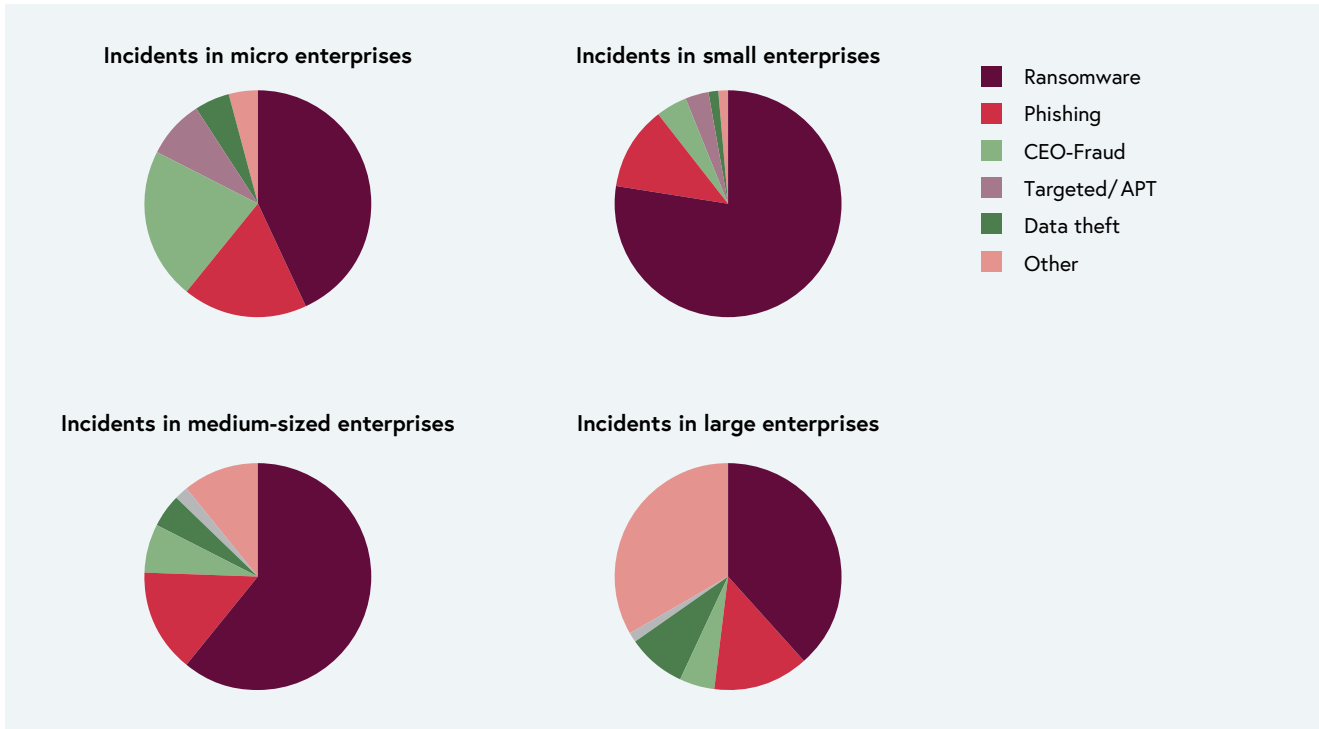


Figure 7: Types of incident by company size

When the incidents are broken down by company size, as expected we can see that widely spread attacks such as ransomware or phishing make up the majority, particularly in the case of small and medium-sized enterprises.

In terms of the types of incident that are obviously increasing the most, the corresponding “lessons learned” and knowledge from the leading private enterprises in the cyber security industry are particularly relevant.

The increase in attempted ransomware attacks detected may be explained by the numerous preventative measures of both a technical and non-technical nature that are now being taken. User training in awareness and simulated phishing attacks or new methods of detecting malware have been able to prevent many attacks in advance, and large enterprises are the pioneers on this.

Overall, the security service providers had more positive results than negative with phishing attacks. Although the volume of attacks remained constant, only a very small number of attacks were actually successful. It was shown that users are becoming increasingly sensitised to these methods and employ enterprises or have contacts for likely attacks.

CEO fraud occurred again numerous times, in some cases in connection with actual hacking attacks carried out in advance. The information obtained in this way was then used to make the “real” fraud attempt. Since large enterprises are now very sensitised to this and corresponding processes have been set up, the volume has shifted towards small and particularly micro (fewer than 10 employees) enterprises compared to the previous period. In these enterprises, direct personal contact between the people in question proved to be effective protection. A trend for new spin-offs from enterprises to be attacked was also observed.

Targeted attacks/APTs aiming to obtain information focused on larger enterprises, and like DDoS attacks are on the decline. In addition to the actual defence, correct allocation was a major problem in this case.

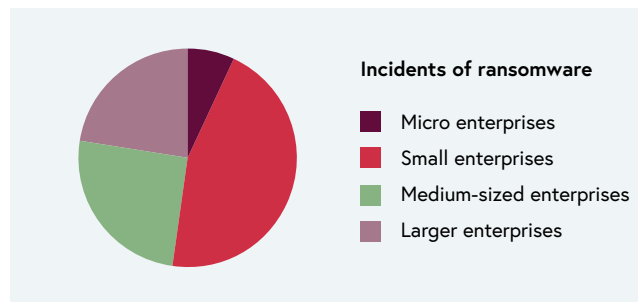


Figure 8: Incidents of ransomware

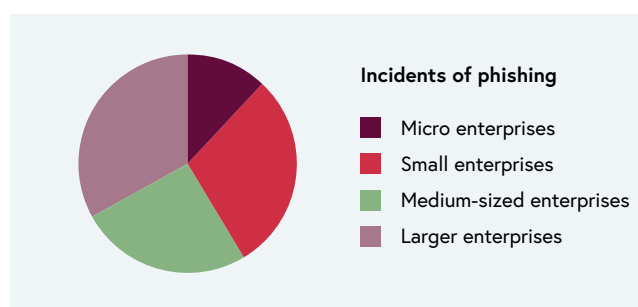


Figure 9: Incidents of phishing

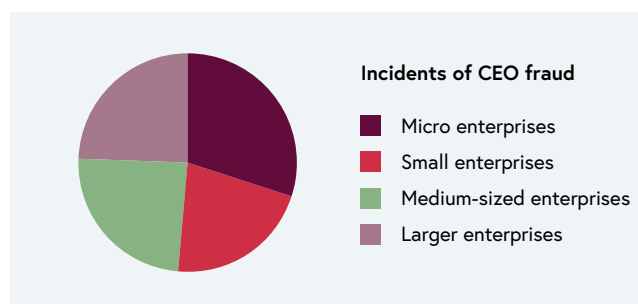


Figure 10: Incidents of CEO fraud

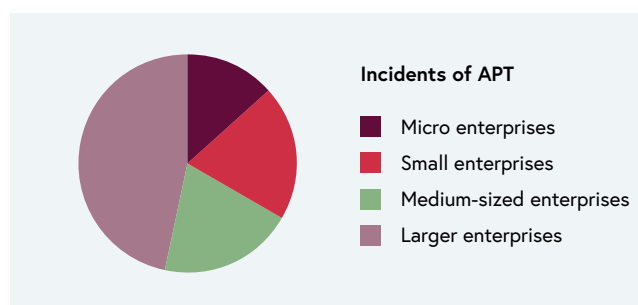


Figure 11: Incidents of APT

The following graphic provides a summary:

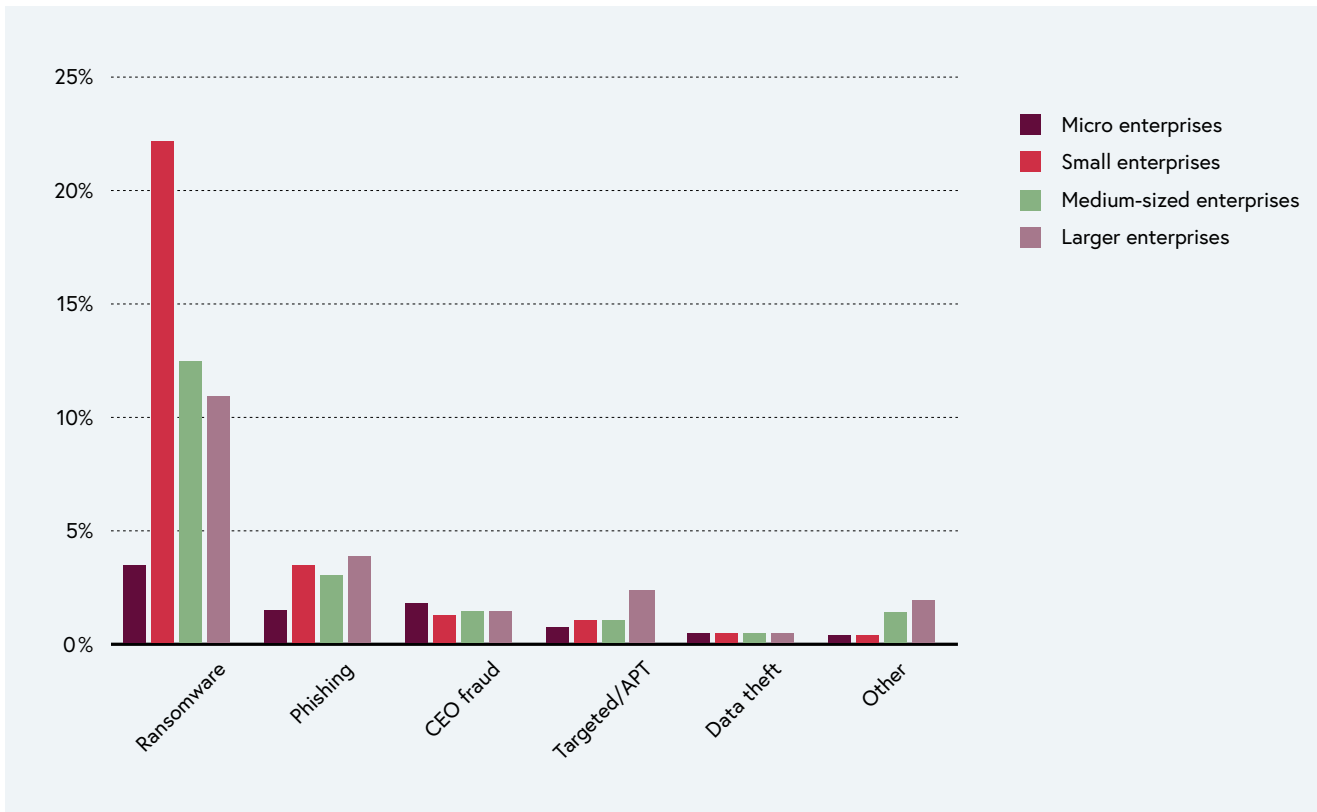


Figure 12: Summary graphic

1.3 Cybercrime situation

The number of reports of cybercrimes in the narrow sense (offences committed against IT systems or data, for example unlawful access to a computer system or damage to data) was declining in 2018 compared to the previous year. It is primarily preventative measures and intensive investigative work that are responsible for this positive development.

Among other things, the Federal Criminal Police Office was able to continue the work of the “SOKO Clavis” special commission on combating ransomware centrally in 2018. In the case of ransomware (also known as encryption trojans), the victim’s files are encrypted by malware. The perpetrators then demand the payment of a “ransom” (generally in the form of bitcoins) to decrypt the data. “SOKO Clavis” was able to investigate several suspects in this field in close collaboration with Europol (EC3).

Decryption tools, which were developed as part of a collaboration between Europol, international law enforcement authorities and private IT security enterprises, are available free of charge on <https://www.nomoreransom.org/>.

There was also a decrease in the number of reports of crimes according to § 107c of the Austrian Criminal Code “Continuous harassment using telecommunications or a computer system”, also known as cyber bullying. This positive trend may be due to increased prevention work and police projects such as “CyberKids” and “Click & Check”. In the case of internet blackmail, victims are asked to make monetary payments with general threats, threats of violence through to threats to publish private sex videos or similar. In some cases, the blackmail continues even after a payment is made and further payments are requested. In 2018, the number of reports of internet blackmail increased significantly. This rise can be explained by the fact that blackmail emails were sent in very large numbers (as is the case with spam emails).

The Federal Criminal Police Office advises all recipients of these emails not to answer them and under no circumstances to pay or follow any other demands. *Do not open any email attachments or links from unknown senders. If you have a screen with an integrated camera, use a webcam blocker. If you have already made contact with the senders, break it off immediately. If you have already made a payment, report it to a police department. Take all of the relevant documents with you.*

1.4 Cyber situation – national defence

In addition to the physical domains of land, air, sea and space, technological developments and global digital networking mean that cyberspace as an intangible domain has become massively more significant in the military sector.

In present and future military conflicts and the “grey area” between war and peace (“hybrid conflicts”), efforts will be made to achieve effects in cyberspace. It should be noted in particular that the attribution of defensive and offensive actions can be concealed in cyberspace. This can also favour the (hidden) implementation of strategic and strategic military objectives.

For the Federal Ministry of Defence, this means aligning itself with national military defence in cyberspace as well as possible in the sense of the core mission of the Austrian Army as set out in § 2 lit. a of the National Defence Law and to prepare for this. This includes both all measures in Information and Communication Technology (ICT) security and all measures to defend against cyber attacks on the military ICT system that jeopardise national sovereignty.

In general, the following trends can be inferred from the experiences of the past few years:

- An equivalently high number of automated attacks at a network level
- Less frequent use of advanced malware, but more professional social engineering via email and larger-scale attacks
- Increase in recognised vulnerabilities at a hardware level
- Fewer politically motivated activities

Border protection

Data from the Federal Ministry of Defence security systems indicate that trends that were identified previously will continue unchanged. An accelerating increase in incidents of access to network levels in security facilities that were able to be blocked by in-house security measures was able to be observed. These were mainly caused by automated attacks and scans. A further increase in this form of attacks can be assumed for the coming year as was the case in 2018.

Attacks via email

Fewer attacks with specially tailored malware were identified than in the previous time period. There were, however, more large-scale attacks in the form of email attachments, for example with the widespread malicious Emotet code².

Vulnerabilities

In the observations on vulnerabilities published this year, it was possible to determine that there has been an increase in newly detected vulnerabilities in hardware in particular. Problems here show the limited repair options, which can go as far as needed to replace the entire hardware.

Outlook

A further increase in automated attacks is expected in the future. The assumption of a trend towards automated personalisation, particularly when email is used as a vector, has been confirmed and should also be assumed for the next year. This means that the attackers not only pose as known services (bank, post office, invoices etc.) but are also and will also make (clearer) references to the company or person themselves.

2 Malicious Emotet code: a manipulated Word file is attached to the email which downloads the actual malware invisibly in the background when the macros are opened and activated (source: heise.de).

2 International developments

Cyber security issues have been addressed and discussed (in some cases very controversially) by numerous international organisations and multilateral forums in the last few years. The relevant foreign policy measures are coordinated by the Austrian Federal Ministry for Europe, Integration and Foreign Affairs (BMEIA). When it comes to the European Union, the topic of cyber security is coordinated by the Federal Chancellery.

The rapid developments in the cyber sector throw up a number of fundamental issues related to fundamental and human rights. At an international level, Austria generally advocates a free internet and the exercise of all human rights in the virtual space too. An appropriate balance must be struck between the interests of law enforcement and respecting fundamental human rights such as the right to freedom of expression and freedom of information and the right to a private life and privacy.

2.1 European Union

Last year, the European Commission and the high representative proposed a broad package of measures to increase cyber security in the EU. The aim of this was to provide Europe with the right tools to tackle the constantly changing threat arising from cybercrime. In 2018, the various parts of the package of measures was discussed intensively in the cyber security committees and some of them have already been passed. The most important activities are set out below.

2.1.1 Implementation of the NIS Directive

Probably the most important part of the package of measures is the transposition of the Directive on security of network and information systems (NIS), a legal instrument that was adopted in August 2016. The aim is to improve the deterrent and increase the EU's defences and reactions to cyber attacks by expanding the cyber security capacity, increasing collaboration at an EU level and introducing measures to prevent risk and handle cyber incidents.

The European NIS Directive entered into force through national legislatures from May 2018. From this point onwards, member states needed to transpose specific measures according to the specifications of the NIS Directive, such as setting up NIS authorities and central points of contact, specifying security measures, agreeing reporting obligations and selecting and communicating essential services to operators.

2.1.2 Regulatory proposals for cyber security

In addition to the NIS Directive, two further legal instruments are proposed by the Commission and aim to improve collaboration between the Commission and the member states.

The legal instrument on cyber security aims on the one hand to strengthen the European Union Agency for Network and Information Security and on the other hand to set up an EU-wide certification framework to ensure the cyber security of products and services within the EU. On 10 December 2018, while Austria held EU Council Presidency, the European Parliament, Council and Commission reached a political agreement about the legal instrument on cyber security.

The second legal instrument is a Regulation on the pooling of resources and specialist knowledge in research and innovation with the aim of Europe taking on a leading role in next-generation cyber security and digital technologies. The proposal was handed to the Council Working Group HWP Cyber and to the ITRE Committee of the European Parliament for negotiations. The target date for political agreement is 2019.

2.1.3 European Union Agency for Network and Information Security

Through the new provisions, the European Union Agency for Network and Information Security (ENISA) was given a permanent mandate and an expansion to its range of activities. These include new tasks in terms of supporting member states, EU institutions and other interested parties on issues of cyber security. It will support EU policy on cyber security certification and play a key role in the development of the certification systems. It will promote the introduction of the new certification system and set up a website with information about the certificates. ENISA will also organise regular cyber security exercises at an EU level, including a large and comprehensive exercise every two years. A network of national liaison officers will help to facilitate the exchange of information between ENISA and the member states.

2.1.4 Cyber security certification framework

The EU-wide European cyber security certification framework for ICT products, processes and services aims to increase the security of networked products, of devices on the Internet of Things and of critical infrastructures using certificates.

Thanks to this framework, security features are taken into account in the early phase of technical design and development. The framework also enables users to confirm the security level and ensure that the security features have been independently checked.

2.1.5 Network of National Coordination Centres and European Competence Centre

The Network of National Coordination Centres and the European Cybersecurity Industrial, Technology and Research Competence Centre is already supporting existing EU initiatives and developing new European capacities in the cyber field.

The European Competence Centre aims to coordinate the use of funds set aside for cyber security for the years 2021-2027 for the programmes “Digital Europe” and “Horizon Europe”. The Centre will support the Network of National Coordination Centres and the competence community and drive forwards research and innovation in the field of cyber security. It will also organise joint investments by the EU, member states and industry.

Within the Network of National Coordination Centres, each member state must appoint a national coordination centre which will work to develop new cyber security capabilities and further develop competence. The network will contribute to the determination and support of the most relevant cyber security projects in the member states.

The competence community in turn will create a large, open and diverse group of interested parties in the field of cyber security from science and the private and public sectors, including civil and military authorities.

2.1.6 Coordinated response to major cyber security incidents and crises (Blueprint)

The aim of Blueprint is to ensure a rapid and coordinated response to large-scale cyber attacks by setting out suitable processes within the EU.

In 2018, several workshops and events were carried out to set out processes and operations. The CSIRTs Network and Europol adopted new crisis management processes in 2019, and the integrated measures for crisis response within the EU were revised. Blueprint was the main topic at the Cyber Security Conference in Sofia. The Bulgarian Council Presidency adopted Council Conclusions on Blueprint and the NIS Cooperation Group developed a joint taxonomy system for cyber attacks to bring together the various mechanisms of crisis process management in Blueprint.

The Blueprint processes are the subject of special exercises and will play an important role in all further Europe-wide crisis exercises in the future.

2.1.7 Cyber diplomacy

Significant expansions for practical implementation were made to the Cyber Diplomacy Toolbox (framework for a joint diplomatic response from the EU to malicious cyber

activities, see last Cyber Security Report) in 2018. The development of parameters for a cyber sanction regime started in October 2018. Since, unlike in other areas, it is not possible to build on international agreements or organisations in the field of cyber security, important foundation work needed to be done here, which is being continued in 2019. There were further discussions around the topic of the attribution of cyber attacks and a coordinated European approach to this in the event of serious incidents on the basis of the Cyber Diplomacy Toolbox. Attribution is fundamentally a sovereign, political decision made by each member state. Attribution is not a requirement for all of the measures included in the Cyber Diplomacy Toolbox.

An important part of cyber diplomacy at an EU level is the development of joint positions on and strategies for cyber issues at an international level, particularly in the United Nation, where important decisions were made on the setting of standards in 2018 (see UN Chapter).

2.1.8 Cyber security in the European parliamentary elections

The preparations for the European parliamentary elections in 2019 started in 2018 from a cyber security perspective. The risk of disruption or manipulation has never before been as great as it is now. Election regulations need to be adapted to the digital age to protect democracy in Europe.

The authorities in the EU member states need to take technical and organisational measures to guard against risks to the security of network and information systems that are used to organise elections to the European Parliament. A Compendium on Network and Information Security developed in the Cooperation Group provides guidelines of this type to protect against cyber threats in an election environment. The security precautions it includes need to be implemented at a national level to make the election systems more resilient. An exercise for all member states shortly before the elections aims to test the implementation again.

2.1.9 ECSO-cPPP

The European Commission and actors on the cyber security market represented by the European Cyber Security Organisation (ECSO) founded a contractual Public-Private Partnership (cPPP) for cyber security in 2016.

The contract between the European Union and ECSO was signed on 5 July 2016. ECSO is both an implementation measure of the European Union Cyber Security Strategy from 2013 and an implementation initiative of the EU Strategy for a Digital Single Market.

The ECSO is a non-profit organisation that is fully self-funded. The members include large European enterprises, SMEs, research centres, universities and local, regional and national administrations from the EU and the European Economic Area (EEA), the European Free Trade Association (EFTA) and countries associated with the Horizon 2020 programme.

Several Austrian organisations and research facilities are members and take part in the various committees and working parties of the ECSO. The Federal Chancellery joined the ECSO on 22 March 2017 and from that point onwards took part in the ECSO public authority meetings known as the ECSO-NAPAC Group (National Public Authority Representatives Committee). As part of the Council Presidency, it took on chairmanship of this group in the second half of 2018.

Here are a few topics and highlights from the very many activities carried out in 2018: Network of European Sector ISACs, participation and role of the ECSO in the future NCCC, cyber certification in Europe, priorities for EU standards in the field of cyber security, collaboration with standard organisations, market radar to set up targeted initiatives in the field of cyber security, synergies with third-world countries, reports on various sectors (Industry 4.0, health, smart cities, energy), access to markets and finances, development plans for regional markets, cyber ranges, analysis of gaps in further training and professional training, promotion of the role of women in the field of cyber security, priorities for future research programmes, technical papers on artificial intelligence, Internet of Things, blockchain, synergies between cyber security and cyber defence.

2.1.10 “Digital Europe” programme 2021-2027

In summer 2018, the European Commission proposed a Regulation for the “Digital Europe” programme to maximise the advantages of digital change for all European citizens, public administrations and enterprises.

The “Digital Europe” programme is a comprehensive investment programme for the strategy of the digital single market and is part of the multi-year financial framework of the EU for the period 2021-2027. It is tailored to the operative requirements of the development of capacity in the fields of supercomputing, artificial intelligence, cyber security and advanced digital skills and broad use in the entire economy and all of society.

Two billion euros are set aside for the field of cyber security alone. This aims to strengthen the EU's capacity for cyber security, protect citizens against cyber threats, promote the latest cyber security solutions and bring together skills to achieve sufficient capacity and excellence in the EU.

2.1.11 Fight against terrorist content on the internet

The persistent presence of terrorist content on the internet is the most serious risk to citizens and the entire society. The damage that can occur because of it is made worse by the fact that it can be rapidly spread beyond platforms.

In 2018, the Commission proposed a new concept with clear and transparent rules to ensure that the following procedures are followed when terrorist content is identified:

- the content is removed as quickly as possible;
- online platforms take measures to ensure that their services are not abused and removed content cannot be re-uploaded elsewhere;
- fundamental rights to freedom of opinion and freedom of information are comprehensively protected.

It is accompanied by various measures for the providers of hosting services, member states and Europol.

2.1.12 Action plan against disinformation

The right to freedom of expression is a key value of the EU. For open, democratic societies it is important for citizens to have access to a large amount of verifiable information and therefore to be able to form an opinion on various political topics. This enables citizens to participate in public debate with knowledge of the facts and express their will in free and fair political processes. The conscious, comprehensive and systematic dissemination of disinformation can lead to threats to democratic processes and to public goods such as human health, environment and security.

The assumption is that there will be an increase in persistent, targeted disinformation campaigns against the EU, its bodies and its policies before the elections to the European Parliament. The rapid change in the instruments and techniques used means a response to them needs to be developed just as quickly. State actors are increasingly using disinformation strategies to influence social debates, cause divisions and intervene in democratic decision-making.

The EC College therefore adopted an Action Plan against Disinformation in December 2018. The European Council requested that the Action Plan be implemented immediately.

The Action Plan provides for various measures in four areas. These include (1) the expansion of the abilities of bodies of the European Union to detect, investigate and uncover disinformation, (2) coordinated and joint measures against disinformation, (3) the mobilisation of the private sector to fight against disinformation and (4) the sensitisation of society and an increase in their resistance. Each of the areas is made up of several measures.

The Action Plan will be discussed in the competent Council working parties in 2019 and should help to make the elections to the European Parliament more secure.

2.2 Austrian Council Presidency cyber security

Austria has done a lot for the Council Presidency when it comes to cyber security. An ambitious joint work programme (Trio Presidency Cyber Security Work Programme) with the two other trio presidencies, Estonia and Bulgaria, was set up at the instigation of Austria. This programme served as a guideline over the one and a half years of the joint trio Council presidency and the Austrian responsibility for the second half of 2018. During this period, Austria took over chairmanship of the most important cyber security groups in the European Union. The Austrian result is extremely positive, as confirmed by numerous member states.

Austria managed to implement all of the priorities from the trio work programme and the activities from the work programme of the presidency committees/groups completely and in full.

Examples of the Austrian results during the Council Presidency are the cyber security conferences and selected European cyber security groups:

2.2.1 Cyber security conferences

Three conferences were organised in total by the Austrian Presidency of the Council of the European Union:

- As part of the Austrian Presidency of the Council of the European Union and as a conclusion to the trio Council Presidency between Estonia, Bulgaria and Austria, the Federal Chancellery organised and held a cyber security conference in Austria. This took place on 3 and 4 December 2018 in the Austria Center Vienna. The aim of the conference was to take stock of the developments in the past 18 months in the field of cyber security and therefore improve awareness of cyber resilience in Europe at both a technical and an operational level.
- The Austrian Representation in Brussels also organised two sector conferences on the topic of cyber security. “Finances 5.0 – a challenge for cyber security?” (together with the Austrian National Bank) on 16 July 2018 and “Cyber security in the energy sector” (together with the European Commission and the German Economic Institute) on 11 October 2018. Both of these conferences took place in Brussels.

2.2.2 Horizontal Working Party on Cyber Issues

In order to highlight the significance of cyber security in the digital and networked world of the 21st century, the group “Friends of Presidency on Cyber Issues” was introduced in 2012 and in 2016 became a standing Council working party (Horizontal Working Party on Cyber Issues – HWPCI or HWP Cyber). HWP Cyber is responsible for all cyber policy issues and coordinates the cross-border and multi-disciplinary “cyber security” material in a strategic and horizontal manner. Since having the status of a Council working party, it has also worked on legislative projects.

The Austrian Presidency was able to achieve the following, among other things, in the HWP Cyber Council Working Party during their Presidency:

- The Council under Austrian Presidency, the European Parliament and the European Commission achieved a political agreement on 10 December 2018 about the legal instrument on cyber security (Cyber Security Law), which strengthened the mandate of the EU Agency for Network and Information Security and created an EU framework for cyber security certification.
- The proposed Regulation, NCCC (setting up the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres) was discussed in the Council Working Party HWP Cyber after being presented on 12 September 2018. Significant progress has already been able to be made under the Austrian Presidency.
- The project to create an “EU Institutional Cyber Map”, a representation of all EU institutions and committees related to cyber security, was carried out with the support of ENISA. The official presentation of the cyber map was made at the Cyber Security Conference in Vienna.
- The “Cyber Resilience” project was also carried out with the support of ENISA. The preparatory work started in the NIS Cooperation Group in the form of a survey. The reference document created is used as the basis to prepare Council Conclusions.
- In the field of cyber diplomacy, the focus was on the further development of the EU’s joint diplomatic response to malicious cyber activities (“Cyber Diplomacy Toolbox”). A table-top exercise on this, called “CYBER-DIPLO-ATTX-18”, was carried out in late November. The achievement of a joint EU position on international developments in cyber security, for example in a UN context or in relation to a possible cyber sanction regime and discussions on attribution was a further focus. Austria was also able to organise and chair a technical workshop for delegates.

2.2.3 NIS Cooperation Group

A NIS Cooperation Group was established when EU Directive 2016/1148 (NIS Directive) was adopted. This supports and facilitates strategic collaboration and the exchange of information between the member states. The Cooperation Group is made up of representatives from the member states, the Commission and ENISA. The Cooperation Group performs its duties on the basis of two-year work programmes. The respective Council President also chairs this Group.

The Austrian Presidency was able to achieve the following, among other things, in the “NIS Cooperation Group” (CG):

- One of the largest surveys on cyber security in the EU was carried out on the topic of cyber resilience and arose from the “Trio Presidency Cyber Security Work Programme”. The results prepared were used on the one hand as the basis for conclusions on the topic of cyber resilience in the EU, and on the other hand as best practice support for member states to optimise their own implementations.
- A number of reference documents from the NIS Cooperation Group were adopted and published. These include, among other things, the identification of operators of key services, cross-border consultation processes, security measures, the reporting obligation in the event of incidents, compulsory exchange of information between the member states, cross-border dependencies and how these can be managed and cyber security for election technology. The results can be accessed on the CG website.
- New working parties were launched under Austrian leadership: The working party “sector-specific aspects focusing on energy” aims to bring together national and European experience in the energy sector. The working party “cyber security capacities in the EU” aims to produce a reference document on cyber capacities in the EU. The working party “major cyber incidents and crises” was recently set up to address the future roles of national contact points in the event of a European crisis.
- The publication of a report by the NIS Cooperation Group was very important. It provided initial feedback on the quality of the work in the Cooperation Group. The handling of the findings from the report was one of the main topics of the Austrian Presidency and initial implementation activities have already been started.
- The Austrian Presidency invited the strategically-oriented Cooperation Group and the operative CSIRTs network to a back to back meeting in Vienna. The topics that were most important to these two group were discussed during a joint session. A regular functional exchange was engineered. The joint meetings will continue to take place in the future.
- The focus of the NIS Cooperation Group is on activities linked to the transposition of the European NIS Directive. This topic is the focal point of each meeting. The Austrian Presidency felt that it was important to address important topics quickly. Our activity helped to ensure that almost all EU member states have already

transposed the NIS Directive into national law. This means there has been a harmonised legal basis for cyber security across the EU for the first time from 2019.

- One of the objectives of the trio presidency was to bring all European groups working on cyber security closer together to make use of synergies. Under Austrian Presidency, a regular exchange of information was established in all of the groups and occasional reports on activities are prepared. In the future, all of these groups will work together as partners to avoid redundancy.

2.2.4 CSIRTs network

EU Directive 2016/1148 (NIS Directive) created the CSIRTs network (CNW) as a cooperation platform consisting of representatives from the CSIRTs in the member states and CERT-EU.

The initial preparatory steps for the network were taken by the Dutch Council Presidency. The official start of the CNW was then during the Maltese Council Presidency. Malta also passed the initial rules of procedure for the CNW, which passed the chairmanship of the CNW along together with the European Council Presidency.

The Austrian CSIRTs that take part in the network therefore had a particular role to play while Austria held the presidency. The following activities were carried out:

- Intensive collaboration in the various working parties of the CSIRTs network. The working parties addressed topics such as tools (e.g. software for CSIRTs) for the network or the processes involved when CSIRTs from the various member states collaborate.
- As part of the trio (Estonia, Bulgaria, Austria), Austria had already contributed to the agenda of the network before it officially took over chairmanship of the CNW.
- While Austria was Chair of the CNW:
 - the work plan for the CNW was updated,
 - the report from the CNW to the NIS Cooperation Group set out in the NIS Directive was prepared, the content was agreed and it was handed over,
 - after a long and intensive process, the initial rules of procedure for the CNW were fundamentally revised and adopted by the members of the CNW.
- In November 2018 a joint session of the CNW and the NIS Cooperation Group was successfully held during overlapping work sessions for the two groups for the first time. This format brought collaboration between the NIS Cooperation Group, which deals with the strategic side of NIS implementation, and the CNW, which works on the operational and technical side, to new levels.
- CSIRTs from Switzerland and Norway were also invited to the CNW meeting as guests for the first time.

Austria's participants in the CSIRTs network are CERT.at, GovCERT Austria and the Austrian Energy CERT of the Austrian energy sector (AEC).

2.3 United Nations

The issue of information security has been on the agenda of the United Nations since 1998 when a resolution was first adopted by the First Committee (on disarmament and international security) of the General Assembly (UN-GA). In this context, "Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (GGE) have been established since 2004. The fifth of these expert groups dedicated itself to the existing and potential threats to international security in the field of information security and measures to counteract this including standards, rules and principles beyond the responsible behaviour of states, confidence-building measures and the development of competence in 2016/17. This expert group was not able to agree on a consensus report due to considerable differences, particularly on issues of international law and its applicability in cyberspace. After the issue of continuing the work of the expert group was adjourned in 2017 too, there was a division in the First Committee in 2018 when the Russian Federation (RU) and the United States (US) submitted competing draft resolutions on the next steps. While the US draft broadly corresponded to the last GGE mandate (previously presented by RU) with 25 experts, RU suggested that an open-ended working group be set up with the participation of all UN member states but with difficult preliminary decisions on content. Ultimately, both resolutions were adopted by the UN General Assembly, so there will now be two parallel processes from the second half of 2019. The EU member states which spoke against the RU approach will still be actively involved in the work of the open-ended working group. Austria brought the US resolution together with EU partners. Austria also organised an event on the applicability of international law in cyberspace together with Estonia and the European External Action Service.

Other UN committees are also working on cyber related topics. From an Austrian perspective, the efforts of a group of like-minded states led by Brazil and Germany in the Third Committee and in the UN Human Rights Council (HRC) that have been ongoing since 2013 are particularly important. The resolution Austria brought as one of the main sponsors on the right to privacy in the digital age was able to be adopted by the HRC by consensus. The initiative was last driven forwards successfully in March 2017 (Res A/34/7) and contains further ambitious elements to ensure that interventions into the private sphere only occur in line with the principles of human rights law. Joseph Cannataci has been the UN Special Rapporteur in a mandate created by the HRC since July 2015. The Russian Federation brought a resolution on Information and Communication Technologies (ICT/cybercrime) that to the Third Committee of the UN-GA, which was adopted after a vote. The resolution tasked the Secretary-General of the United Nations (UN-SG) to

prepare a report for the 74th session of the United Nations General Assembly on the approach to be taken against the criminal misuse of information and communication technologies and resolved to create a new agenda item for the 74th session on “Countering the use of information and communications technologies for criminal purposes”. The resolution thereby created a starting point for these issues to be addressed in a formal and substantial manner by the United Nations General Assembly, which could present a significant challenge to existing legal instruments (particularly the Budapest Convention) and the processes underway in Vienna. The EU member states therefore voted resoundingly against the resolution.

Cybercrime has rapidly become a global and extremely profitable area of crime. The United Nations Office on Drugs and Crime (UNODC) in Vienna continues to represent an essential component of the effective global battle against cybercrime in the sense of the comprehensive study published in 2013³ and focuses on the following three points in its assistance to affected member states:

- Improving the identification, prosecution and assessment of cybercrime, particularly in the field of sexual exploitation and child abuse on the internet in compliance with and promotion of human rights;
- Promoting an integrated and government-wide approach including national coordination, data collection and effective legal framework conditions to sustainably combat and provide an effective deterrent against cybercrime;
- Strengthening national and international cooperation and information exchange mechanisms between governments, law enforcement authorities and the private sector and improving public awareness.

The Intergovernmental Expert Group (IEG) set up in 2010 in the field of cybercrime met for the fourth time from 3 to 5 April 2018 after meetings in 2011, 2013 and 2017.

The controversial issue of whether a new cyber convention should be negotiated or the Budapest Convention should be expanded/implemented was not able to be resolved, but the IEG did agree to continue the discussion. The decision was also made to continue with regular meetings of the IEG to discuss fundamental topics and developments regarding cybercrime and exchange information on national legislation, best practice examples, technical support and international collaboration in terms of strengthening the international measures against cybercrime. In the meantime, UNODC will continue to collect information on new developments, advancements and best practice examples.

3 http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

In this context, an international conference on cybercrime took place in Vienna in September 2018 at the initiative of interested states outside of the IEG framework. Due to the lack of broad support for a UN Cyber Convention within the scope of the IEG, RU floated the topic of cybercrime in the UN General Assembly (see above). Cybercrime was also the main topic of the 27th session of the Commission on Crime Prevention and Criminal Justice (CCPCJ) 3 in May 2018. Despite the thematic focus, the draft resolutions in this session primarily focused on human trafficking, with a reference to cybercrime in Res. 27/2 “Preventing and combating trafficking in persons facilitated by the criminal misuse of information and communications technologies” and in Res. 27/3 “Improving the protection of children against trafficking in persons, including by addressing the criminal misuse of information and communications technologies”.

The UNODC Cybercrime Division implements new initiatives in school and university education at an operative level within the scope of the new Education for Justice programme (E4J). In this context, UNODC is showing particular interest in the comic book “the online zoo” created by Internet Service Providers Austria (ISPA), which is used in school classes to teach children about the dangers of the internet and increase their online skills. As part of the 27th CCPCJ, Austria worked with the UNODC initiative “Education for Justice” (E4J) and El Salvador to organise the very well attended side event “Helping Children Stay Safe Online: Education, Initiatives and Tools”.

In terms of the sale of illegal substances on the dark web and the use of cryptocurrencies as a means of payment in drug deals, these phenomena currently only make up a relatively small percentage of total current transactions. Even the UNODC assumes that this “segment” of the illegal drug trade will continue to develop in a very dynamic manner in the future and that fighting these practices will therefore be very important.

The International Atomic Energy Agency (IAEA) addressed the topic of cyber security in nuclear facilities in 2018 with a publication entitled “Computer Security of Instrumentation and Control Systems at Nuclear Facilities”, which sets out recommendations for action at relevant points, such as how the constantly increasing threat can be handled and how weaknesses within systems can be fixed. For the coordinated research project between the IAEA and 10 member states entitled “Enhancing Computer Security Incident Analysis at Nuclear Facilities”, which will continue to be implemented until mid 2019, the Austrian Institute of Technology (AIT) created a special virtual IT training and simulation platform designed for highly sensitive industrial control systems. This platform can be used to simulate, test and provide training on new technologies, tools and processes to defend against cyber threats in nuclear plants. In October 2018, the IAEA also launched an “International Training Course on Protecting Nuclear Facilities from Cyber Attacks”, which offered 37 participants from 13 countries a two-week intensive training session on best practices in computer security.

2.4 NATO

As a political alliance with a significant focus on common defence, NATO has been dealing with the defence aspects of cyber security since the adoption of its new strategic concept in 2010 and the recognition of cyberspace as a domain in 2016. Austria is collaborating closely with NATO as a partner country. Austria is also involved in numerous meetings of the NATO-C3 board at a technical level and those linked to relevant smart defence projects.

Austria was the first non-NATO state to be invited to a meeting of the NATO Cyber Defence Committee (CDC) in the format 28+1 in February 2015. Austria took on the partnership objective “Cyber Defence” as part of the NATO Partnership for Peace (NATO/PfP). The agreements on this for 2015-2017 were all able to be met by Austria. The next Partnership for Peace Planning and Review Process (PARP) cycle is currently underway.

Collaboration with NATO since October 2013 (Technical Arrangement until 2022) in the field of national military defence in cyberspace has also been expanded to include the permanent presence and collaboration of an officer of the Federal Ministry of Defence in the “Cooperative Cyber Defence Center of Excellence” (CCD COE) in Tallinn, Estonia. The Austrian department will make use of the extensive range of courses available as a result and will use the exercises offered to check its national skills against those of other countries.

2.5 OSCE

To date, the OSCE is the only regional, international organisation whose member states have been able to agree on confidence-building measures in the field of cyber security: an informal working group developed an initial catalogue of eleven measures in 2013 to respond more efficiently to cyber threats through transparency and collaboration. In March 2016, a resolution was able to be passed on five further confidence-building measures.

In 2014, the 57 participant states also started keep one another informed about developments and problems in the field of information and communication technology security through a structured mutual exchange of information. They set up contact points for dialogue and exchange information on the national organisation of cyber security plans.

Cyber security was also one of the main topics of the Italian Presidency of the OSCE in 2018. On 27 and 28 September, Italy organised the OSCE Cyber Security Conference in Rome dedicated to both international developments, particularly cyber diplomacy, and collaboration between the state and the private sector. A scenario-based discussion

took place for the first time before the conference in which the delegations set out their approaches to a fictitious cyber attack schematically. The work of the informal working group on cyber security focused on the implementation of the confidence-building measures that were agreed. Against the background of the difficult international starting position and in particular the ongoing criticism from Russia of the work of the informal working group (IWG) (Russia claims that it does not have any discernible added value over the work being done by the UN), no significant advancement was able to be made.

2.6 OECD

The “Working Party On Security and Privacy in the Digital Economy” (SPDE) is a working party of the OECD that carries out analyses and makes high level recommendations to governments and national stakeholders on the topics of cyber security and privacy. The working party relies on expertise from OECD countries and partner governments, economics, civil society and the technical internet community to develop approaches for the future.

The SPDE treats cyber security and privacy as complementary topics that are essential in terms of ensuring the sustainability of the internet economy as a platform for wellbeing. Political decision-makers should be enabled to observe trends, exchange experiences and analyse the effects of technologies. The SPDE meets twice a year in Paris and organises workshops and conferences. In Austria, the Federal Chancellery coordinates the content of this working party.

The following topics were addressed in the two meetings in 2018, among others:

- Recommendations for critical information infrastructure systems,
- Comparability of infringements of data protection,
- Measurement of digital risk management practices in enterprises,
- Internet of Things and artificial intelligence,
- OECD data protection strategies.

2.7 Council of Europe

The core of the Council of Europe’s activities in the field of cyber security is the Convention on Cybercrime (Budapest Convention) from 2001, which has achieved significance well beyond the borders of Europe with 62 ratifications to date (including Argentina, Costa Rica, Cape Verde, Morocco, Paraguay and the Philippines in 2018). The main purpose of the Convention is to pursue a common criminal policy to protect society from cybercrime, particularly through corresponding legal regulations and the promotion of international collaboration.

The implementation of the Convention is supported through capacity-building projects coordinated by a Cybercrime Programme Office of the Council of Europe in Bucharest (C-PROC). Of the projects funded by off-budget contributions, the following should be mentioned: advice on the relevant legislative measures, help training judges and public prosecutors along with “iProceeds” in south-eastern Europe focusing on the profits from cybercrime, “Cyber South” in North Africa and the global project being carried out in collaboration with Interpol, “GLACY+”. As part of the latter, the “First African Forum on Cyber Crime” took place in Addis Ababa from 16 to 18 October 2018. Fifty African states took part and the organisation of the conference was seen as a new level of quality in collaboration.

Negotiations are currently underway for a second additional protocol to the Budapest Convention looking at international legal assistance and the associated cross-border access to data. Close collaboration with the European Union on the relevant documents that are currently under development is planned.

Guidance notes on the topic of election interference are also being prepared and are expected in July 2019. Guidance notes of this type, nine of which have been published to date on various topics, aim to facilitate the effective application and implementation of the Convention.

The further developments within the Council of Europe in 2018 include the modernisation of the Data Protection Convention of the Council of Europe (ETS 108), which brings new relevance in terms of the current challenges in the online world to the original Convention from 1981. The Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse also makes a significant contribution to the protection of children online. The so-called “Octopus Conferences” address relevant topics every six months, and in 2018 looked at attacks on democratic processes, particularly interference in elections and election manipulation using the internet. As an organisation that focuses on human rights, the rule of law and democracy, the Council of Europe also actively participates in various international discussions on internet governance, particularly in the area of the United Nations.

2.8 Austria in other cyber relevant international forums

In addition to the forums mentioned above, Austria is also involved in a range of other international collaboration committees in the field of cyber security. These include:

- The “Freedom Online Coalition” – a coalition founded by the Netherlands in December 2011 that works around the world for the effective application of human rights online in various forums and currently has 30 member states.

- The “Central European Cyber Security Platform” – a cooperation platform of countries (and the CERTs /in some cases milCERTs) of the Visegrad Group (Hungary, Czechia, Slovakia and Poland) created in 2013 on the initiative of Czechia and Austria.
- The Global Forum on Cyber Expertise (GFCE) is a global platform that was founded in 2015. Austria has been a member since 2017.
- The Internet Governance Forum (IGF), which came out of the World Summit on the Information Society (WSIS) took place in Paris this time. There have to date been no specific final documents issued by this meeting, which focuses in particular on civil society and the private sector.
- As part of IGF Paris, the French President Macron launched the “Paris Call for Trust and Security in Cyberspace”. The call is designed as a political platform for collaboration between states, enterprises and civil society and aims to support all of those involved in their commitment to principles such as compliance with the international legal position in cyberspace and include their input into the upcoming standard setting processes in New York. All EU member states support this initiative.

3 National actors and structures

The repeated tackling of cyber attacks in various forms against critical infrastructure enterprises and constitutional facilities is a significant challenge for national actors and structures. The range of different kinds of attack is broad and spans from simple DDoS attacks to complex cases of attempted cyber espionage. What we see again and again in this context is that successfully tackling attacks of this type requires the comprehensive, trusting collaboration of all of the actors involved, both state and non-state. While cooperation between state bodies has been established for several years in the committees OpKoord (Operative Coordination Structure) and IKDOK (Inner Circle of the Operative Coordination Structure) and communication with the enterprises affected has a solid basis, in this reporting year the implementation of what are known as sector CERTs is a further important milestone in collaboration.

3.1 Inner Circle of the Operative Coordination Structure (IKDOK)

The Network and Information Systems Security Law (NIS Law), which entered into force on 29 December 2018, provides, among other things, for the creation of a structure for coordination at an operative level (“Operative Coordination Structure - OpKoord”) and an interministerial structure for coordination at an operative level in the field of the security of network and information systems (“Inner Circle of the Operative Coordination Structure - IKDOK”). While OpKoord was essentially set up to discuss an overall situation report that also includes voluntary reporting, the main tasks of the IKDOK include discussing and updating the situation report to include risks, incidences and security incidence and supporting the coordination committee with cyber crisis management.

Specifically, this means that IKDOK, supported by OpKoord, forms the direct interface with the general government cyber crisis management team (CKM) in the event of a crisis. In terms of the mechanisms and processes to be used, the CKM relies strongly on the tried and tested processes of state crisis and catastrophe protection management (SKKM). Regular cyber exercises aim to test cyber crisis management and crisis management and continuity plans.

The IKDOK comprises the Cyber Security Center (Federal Ministry for the Interior, BMI) and the Cyber Defence Center (Federal Ministry of Defence, BMLV), both of which

chair the IKDOK, and other state actors/facilities. Specifically, these include the Cyber Crime Competence Center (BMI), the Army Intelligence Office (HNaA, BMLV), the ICT and Cyber Security Centre (ZIKT&CySih, BMLV) along with others including the Military Cyber Security Centre and the milCERT, the GovCERT (BKA) and the BMEIA.

3.2 Cyber Security Center

The Cyber Security Center (CSC) in the Federal Office for the Protection of the Constitution and Counterterrorism was confronted with significant challenges, both organisational and content-based in this reporting year. The CSC received a significant organisational update with the conversion of a unit into an independent department, but as a result of this now has to carry out a wide range of new tasks.

As strategic tasks have come under the scope of the Federal Chancellery since the entry into force of the Network and Information System Security Law (NIS Law), the operative implementation of the corresponding regulations is the responsibility of the Federal Ministry for the Interior. The role of the operative NIS authorities will in the future be carried out by the cyber security department in the Federal Office for the Protection of the Constitution and Counterterrorism. As a result, the current reporting year was shaped by extensive organisational and technical measures to prepare for these new tasks.

At the same time, the area awareness raising and cyber prevention was massively expanded. In addition to the ongoing awareness talks and events at critical infrastructure enterprises and constitutional facilities, the Cyber Security Center regularly carries out various training measures on ICT security for its own and other Ministries. This area also involved intensive engagement in awareness about security as part of the 2018 EU Council Presidency and the 2019 European parliamentary elections.

3.3 ICT and Cyber Security Centre (ZIKT&CySih)

During the armed forces restructuring in 2019, the former command support and cyber defence, which was previously developed in virtual form, was dissolved. The core tasks are predominantly continuing and will be described in greater detail for the following areas of competence.

3.3.1 Military Cyber Security Centre (MilCySihZ)

The MilCySihZ as part of the ZIKT&CySih is the point in the Austrian Armed Forces that defends against threats or attacks from cyberspace against the military's own ICT systems and networks.

In order to maintain this protection, it is essential that all aspects of cyber security are covered both thoroughly and consistently. This is reflected in the tasks and area of competence of the MilCySihZ:

- Selection, introduction and operation of ICT security components (e.g. firewalls, end-point protection - virus protection etc.)
- Creation of a cyber security situation report (by monitoring and assessing current technologies, ICT systems and components used by the Austrian Armed Forces)
- Forensics
- Auditing internal ICT systems and networks
- Cyber security management
- Cyber military training area
- Electronic warfare (self-protection and assistance)

3.3.2 Self-protection

The Military Cyber Security Centre is obliged to carry out the planning and implementation of cyber security systems and components for self-protection and the defence of the Austrian Armed Forces against cyber attacks. These systems are constantly being developed and adapted to the current threats. A full situation report on cyber security can be prepared in combination with observations, assessments and measures to tackle weaknesses in current technologies, ICT systems and components used by the Austrian Armed Forces. In order to check all ICT systems for their suitability to be used in the Austrian Armed Forces on an ongoing basis, design and structural weaknesses in technologies, products, components and systems are identified early through system and component audits.

3.3.3 milCERT (Military Computer Emergency Readiness Team)

In the event of an imminent or ongoing cyber attack, sufficient technical and staffing capacities must be available for detection, containment and defence. An essential part of this is the ability to detect and demonstrate the current cyber situation. In order to obtain information on cyber security incidents and current knowledge that is as accurate and current as possible, the milCERT is constantly exchanging information with national and international partner organisations. It coordinates the measures that are

carried out in the event of IT security incidents and provides warnings about any gaps in security in good time.

3.3.4 Cyber military training area

Since highly specialised forces are only available to a limited extent, training on the concepts and processes for members of the army is needed. Exercises are coordinated in the cyber environment in the cyber military training area (Cyber Range) and research projects are developed together with scientific facilities. Current cyber security trends are analysed and integrated into the Austrian Armed Forces cyber defence processes.

3.3.5 Information security

Information security, cyber specific risks and collaboration with Austrian and international partners are managed so as to supplement the technical and tactical abilities. The Military Cyber Security Centre operates comprehensive ICT and cyber risk management embedded in an information security management system and represents the Austrian Armed Forces to national and international regulatory authorities. The Austrian Armed Forces carry out security authorisations and audits of systems based on national and international security regulations to ensure the secure exchange of information.

3.3.6 Electronic warfare

As part of cyber defence, the centre is also responsible for the provision of services in the field of electronic warfare. The technical basics needed for self-protection and the provision of assistance for the defence of foreign systems are provided. The aim is to obtain and maintain combat superiority, to carry out jobs as a national or multinational group and to increase the viability of the force.

3.4 Cyber Defence Centre

The Defence Office (AbwA) runs the Cyber Defence Centre (CyVZ) of the Austrian Armed Forces (ÖBH). It prepares the active funds and abilities needed for cyber defence. It therefore supplements the cyber defence of the Austrian Armed Forces and also the national cyber defence efforts. To this end, the CyVZ prepares a situation report analysing national and intelligence information from and about cyberspace and uses it to assess countermeasures.

The AbwA also organises the largest ICT security conference in the German-speaking world to further increase awareness of security.

3.5 Army Intelligence Office

As a strategic foreign intelligence service, the Army Intelligence Office (HNaA) primarily contributes to the national cyber situation report by representing the strategic context in large-scale cyber incidents. In addition to the prompt detection of cyber threats from abroad, information it has obtained about the intentions and abilities of international cyber actors makes an important contribution to attribution and therefore to decision-making by the highest level of political and military leadership, among other things with regard to any countermeasures.

3.6 GovCERT, CERT.at and Austrian Energy CERT

GovCERT is the public administration computer emergency team according to the NIS Law and part of the above-mentioned IKDOK. GovCERT is the CERT Point of Contact for Austria and is therefore closely linked to international organisations and contacts such as the European GovCERT Group and the Central European Cyber Security Platform. GovCERT (together with CERT.at) also represents Austria in the EU CSIRTs network.

CERT.at is the Austrian Computer Emergency Response Team (CERT) and was established in 2008 together with GovCERT in cooperation with nic.at. The team at CERT.at primarily works actively on acute security threats and events. This happens by communicating with areas that are affected or on the basis of its own research.

CERT.at also carries out preventative measures such as early detection, PR work, advice and support on request as the need arises. CERT.at is a contact point for security-related ICT events in Austria and is a trusted and recognised information hub within Austrian organisations and enterprises in the field of cyber security.

GovCERT, which comes under the Federal Chancellery, works closely with CERT.at in the form of a public-private partnership.

The transposition of the NIS Directive into national law in the form of the Network and Information Security Law (NIS Law) set out the remit of GovCERT. This transposition provides, among other things, for an obligation to report serious security incidents on the part of operators of essential services and providers of digital services. These compulsory reports are sent by those affected to certain, sector-specific reporting points (sector-specific computer emergency teams) and from there forwarded to the CSC. This also applies to voluntary reports, although these reports can be anonymised by the sector CERTs before they are forwarded to the CSC. GovCERT receives reports of this type for public administration facilities and forwards them on if the facility is not represented in IKDOK. In addition to this, GovCERT can also issue early warnings,

alarms, recommendations for action and notifications and provide initial general technical support when responding to security incidents to monitor and analyse risks, incidents and security incidents and to assess the situation.

The NIS Law provides for a sector CERT of this type in each sector to carry out this function of being a reporting point. In addition to the reporting point function, these CERTs carry out a large number of additional CERT tasks for the organisations in their sector.

If a sector still does not have its own sector CERT, the task of being a reporting point is carried out by the national computer emergency team, which is still yet to be appointed. If no national computer emergency team is set up, GovCERT will do this. This ensures that enterprises in the affected sector can meet their statutory reporting obligations.

The Austrian Energy CERT (AEC) is an industry-specific CERT (Computer Emergency Response Team) for the Austrian energy industry. The AEC is an important component of the increase in the resilience of the energy economy to cyber attacks. It is considered to be a sector CERT in the sense of the NIS Directive and the NIS Law and also meets the requirements of the European Directive on Security of Network and Information Systems (NIS) and the European Union Agency for Network and Information Security (ENISA) for increasing IT security in critical infrastructures.

The main tasks of the Austrian Energy CERTs are to strengthen the IT security skills of the energy sector. These tasks include ongoing security incident management, in other words the handling of queries that come in each day and security reports, carrying out training sessions, participating in international cyber security exercises and collaborating on the development of technical security concepts for the electricity and natural gas industry. The AEC also takes on the role of single point of contact for national and international security incidents in the energy sector. In addition to rapid and efficient communication, coordination between IT security experts and authorities within the industry is also ensured.

The aim of operating an independent CERT and the corresponding exchange of information is to increase awareness and prevention in the energy sector. In 2018, it also became a member of the international network of global CERTs (FIRST) and achieved the status of an “accredited member” of the European Association of CERTs (trusted introducer). Information about best practice approaches can be exchanged with other CERTs in these trusting committees in order to increase the overall level of security.

3.7 CERT Association

The interaction between society, the economy and science needs to be further promoted and expanded to further increase the level of security of Austrian society in cyberspace. A key role in this increase is played by the Computer Emergency Teams (CERTs) in Austria.

It is the inherent job of the CERTs to protect ICT systems and digital networks. The aspects of prevention, reaction and awareness-raising are the highest priorities as the first point of contact for all areas of cyber security. An intensive exchange of information and networking at a national and international level are both required to develop the necessary expertise.

The focus of the remit of the National CERT Association (Austria) is improving collaboration between Austrian CERTs and promoting CERT activities in Austria. A comprehensive network of CERTs is the most effective way of protecting the networked information and communication systems. This is a point of view that has been confirmed by an increasing number of CERTs in Austria.

The CERT Association was founded in 2011 as a collaboration between all of the Austrian CERTs that existed at the time from the public and the private sector. The intention was to bring together all of the available forces to make the best possible use of joint expertise to ensure the best possible ICT security.

Participation in the CERT Association is voluntary. Each individual participant commits to exchange information and experience on a regular basis, to identify and provide core competencies and to contribute to the promotion of the CERTs in all sectors in the sense of a community-led and cooperation-based CERT Association.

Since the CERT Association was founded, the 15 current members have met 33 times and constantly exchange information with one another outside of the meetings via secure communication distributors.

The most important topic addressed in the meetings is the joint operative exchange of information and experience and the establishment of mutual trust. This means that support and additional expertise are available in the event of a cyber crisis. In 2018, the existing cyber security structures (OpKoord, IKDOK etc.) were given a legal basis by the Network and Information Systems Security Law (NIS Law). The NIS Law also paved the way for sector-specific computer emergency teams to be set up and anchored their participation in OpKoord in law. The CERT Association welcomed these developments.

3.8 Cyber Crime Competence Center (C4)

The Cyber Crime Competence Center (C4) is the national and international coordination and reporting point to combat cybercrime. The Center is made up of highly specialised technical and functional experts from the fields of detection, forensics and technology.

The cybercrime reporting point at C4 acts as an international point of contact on cybercrime issues and an interface to the CSC and contact point for the general public. This means new phenomena can be detected early. As the contact point for all police stations in connection with cybercrime, the cybercrime reporting office also carries out an important task.

“SOKO Clavis” also processes all ransomware crimes in the entire country centrally and operationally and coordinates international collaboration alongside other countries.

Mobile forensics, multimedia forensics and vehicle-based forensics supplement and further expand C4’s skill in the field of digital preservation of evidence.

As a technical and scientific service, the Development and Innovation department is dedicated, among other things, to the research of special cyber-related areas, the investigation and assessment of phenomena which occur in IT communication and the investigation and development of protection and detection options in hardware and software.

The original technical infrastructure which was tailored to C4 has been tried and tested and has as a result already been provided to other departments in the Federal Criminal Police Office (BKA) and the state criminal police offices.

3.9 Cyber Security Platform (CSP)

The Cyber Security Platform (CSP) is the central exchange and cooperation platform between the economy, science and public administration. It is used to exchange experience and information on cyber security, with a particular focus on critical infrastructures. The CSP also advises and supports the Cyber Security Steering Group (CSS) on strategic issues of cyber security.

Since it was set up in 2015, the platform has become an exemplary model and is an umbrella for numerous cyber security initiatives. The results of the work done by the platform are important when it comes to shaping national cyber security policy.

The sixth and seventh CSP workshops took place in 2018. The topics in the sessions were on the one hand the main focuses of the 2017-2022 government programme on cyber security and the competencies and responsibilities in this area as amended by the new Federal Ministries Act.

On the other hand, extensive guidance was provided on the current status of the transposition of the NIS Directive in the form of the NIS Law and the accompanying regulations. There were numerous inputs, particularly from those who may be affected and are represented in the CSP, and these were taken into account in the adaptations to the NIS Law.

Another thematic focus was progress reports on the working parties established under the CSP on the areas of “legal and regulatory issues”, “technologies, processes, training, research and development” and “operational crisis management”.

Specifications, basic assumptions and methods of operation were also presented and discussed to create an updated Austrian National Cyber Security Strategy (ÖSCS 2.0). At the election for the new chair of the CSP held during the seventh workshop in autumn 2018 (according to the rules of procedure the chairs are appointed for a three-year term of office), Dr Thomas Stubbings and Dr Wolfgang Schwabl were reappointed as chairs for a further term.

3.10 Austrian Trust Circle (ATC)

The Austrian Trust Circle is an initiative of CERT.at, Austrian Energy CERT and the Austrian Federal Chancellery and consists of security information exchanges in the individual areas of strategic information infrastructure.

The Austrian Trust Circle of public administration has existed since 2016.

CERT.at and Austrian Energy CERT in collaboration with GovCERT Austria and the Federal Chancellery offer a formal framework for a practical exchange of information and joint projects in the field of security.

Key objectives of the Austrian Trust Circle are:

- Supporting self-help in the sectors in the field of security,
- Being an operative contact for CERT.at/Austrian Energy CERT/GovCERT Austria for information about and handling of security incidents within the organisations,
- Providing operative experts for public administration in the event of a crisis,
- Creating a foundation of trust so that serious cases can be addressed together,

- Facilitating networking and information exchange within and between the strategic infrastructure sectors.

In addition to the regular meetings within the individual sectors, exchange between the sectors including public administration is promoted once a year at a two-day event.

In 2018, the topics discussed included transposition of the NIS Directive, secure software development, measures to prevent Distributed Denial of Service (DDoS) attacks and the exchange of experience of handling security incidents.

3.11 ICT security portal

The ICT security portal onlinesicherheit.gv.at is an interministerial initiative in cooperation with the Austrian economy and acts as a central internet portal for topics related to security in the digital world.

As a strategic measure of the national ICT security strategy and the Austrian National Cyber Security Strategy, the initiative aims to promote and sustainably strengthen the ICT security and cyber security culture in Austria by sensitising the affected target groups and raising awareness with them and by providing target group-specific recommendations for action.

The information and services on offer are constantly being expanded during regular editorial meetings with the 39 cooperation partners (federal ministries, regional governments, authorities, universities, technical colleges, research institutes, enterprises, associations and advocacy groups). It includes current reports and warnings, advice and further information for both beginners and experts.

In 2018, the ICT security portal wrote 150 news articles, 50 publication records and 70 event records. Each month a main topic on current trends was chosen, with a total of 34 specialist articles being published. The focus at the start of the year, for example, was the General Data Protection Regulation and before Christmas it was the security measures behind online shopping. In October, there was a report on activities carried out by Austria for the “European Cyber Security Month” (ECSM).

3.12 Office for Strategic Network and Information System Security

The Office for Strategic Network and Information System Security is housed within the Federal Chancellery as part of department I/8 and is responsible for issues linked to

the transposition of the legal obligation from Directive (EU) 2016/1148 in Austria and the Federal Law on the Security of Network and Information Systems (NIS Law).

It carries out the tasks of a strategic NIS authority in Austria and is responsible for the regulation of criteria and limits for operators of essential services, providers of digital services and CSIRT reporting points.

The addressees of the NIS Law are informed of their responsibilities and obligations by the NIS Office in the Federal Chancellery. The NIS Office runs a service centre for all issues related to strategic implementation.

The implementation responsibilities arising from the NIS Law also include participation in the European NIS Cooperation Group and other EU-wide and international cyber security committees with a strategic focus, strategies for cyber security and public-private cooperation.

The NIS Office had two areas of focus in 2018. The adoption of the NIS Law was driven forwards and preparations were carried out for the implementation of the Directive in Austria. The NIS Office was also involved as the leading authority on the topic of European cyber security during the Austrian Council Presidency.

On the Directive and its implementation:

- The Network and Information Systems Security Law was published after being adopted by the National Council on 11 December 2018 and by the Federal Council on 19 December 2019 in BGBl. I No. 111/2018 and as a result entered into force on 29 December 2018. The NIS Law therefore transposes Directive (EU) 2016/1148 in Austria.
- Before the entry into force, extensive national preparations were carried out to replicate the specifications of the European NIS Directive as well as possible in an Austrian environment, including taking into account existing national cyber security processes and structures. The involvement of the state, the economy, education, research and society was an important goal from the start.
- At a European level, the NIS Office was active in all sessions about the transposition of the NIS Directive. This included
 - the participation in plenary sessions of the European NIS Cooperation Group and
 - active involvement in all European working parties that were developing specific proposals for the transposition of the NIS Directive.
- At national level, the NIS Office started to prepare for the NIS Law coming into force in 2018. This occurred in several rounds of discussions with representatives of the relevant sectors. The content of these discussions included the identification of essential services in Austria, the selection of operators of essential services, the determination of criteria and parameters for cyber incidents, the

preparation of the reporting obligation processes and the development of security measures.

- All of the topics are agreed in close collaboration with the competent operative experts in the BMI. The addressees of the NIS Law are kept informed of the status quo through fact sheets.
- The NIS Office will support the implementation of the measures in the NIS Law as well as possible with a joint NIS website (accessible on nis.gv.at) together with the BMI and its own contact point (accessible on nis@bka.gv.at).

On the Austrian Council Presidency:

- During the Austrian Council Presidency, the NIS Office chaired the European cyber security groups “Horizontal Working Party on Cyber Issues” and “NIS Cooperation Group” and took a leading role in shaping the content and organising the conference in Vienna in December 2018.
- For more information on this, see the chapter “Austrian Council Presidency cyber security”

4 Cyber exercises

Cyber exercises were also an important part of testing established processes, checking measures taken and practising domestic collaboration on cyber issues in this reporting year.

The knowledge obtained from participating in the simulation games (“lessons learned”) was a key factor in increasing overall national resilience. By actively participating in a wide range of different exercises, the state stakeholders in the field of cyber security were able to cover a wide range of scenarios.

4.1 Austrian Strategic Decision Making Exercise (ASDEM) 18

The ASDEM is a national cyber security/hybrid exercise. It is a simulation game, which took place on 20 and 21 February 2018 at the National Defence Academy (LVAK) in Vienna with significant involvement of the KdoFüU&CD, particularly with its commanders in the role of (former) cyber coordinators for the BMLV.

A total of 118 participants from IKDOK (BKA, BMLV, BMI, BMEIA, CERT) and critical infrastructure took part in this event. Seventy international observers from 21 countries and many national observers from public institutions and enterprises also took part in the exercise.

The purpose of the exercise was to review national cyber crisis management (CKM) processes to protect critical infrastructure through to clarifying the transition from the civil CKM to a military cyber defence case, the applicability to hybrid incidents and the associated political, legal and international legal problems in a manner adapted to the situation.

The focus of the exercise was on the strategic (decision-making) level and communication within ministries and critical infrastructure. This exercise therefore did not look at technical problems. Austria supported the development of the exercise, with the planning carried out by the “Estonian Defence League” (EDL) commissioned by the European Defence Agency (EDA). The EDL was integrated into the ASDEM and supervised the game.

4.2 CROSSED SWORDS 2018 (XS18)

This technical cyber defence exercise took place from 30 January to 2 February 2018 in Riga, Latvia (LVA). It was run by the NATO CCD-COE in collaboration with CERT.LV, and around 80 soldiers and civilians from 20 countries took part. The BMLV sent two participants from KdoFüU&CD and ZIKT&CySih.

The purpose of the exercise was for penetration testers, forensic experts and special operations forces to work together as a team to achieve the mission objectives and overcome the technical challenges in a virtual cyber environment. The main focus was on developing tactical skills in a reactive cyber defence scenario and making the participants suitably aware of the situation. Another goal of participation was to improve existing skills in penetration testing, which is needed to check ICT systems. The exchange of experience with specialists from other countries was also relevant.

4.3 LOCKED SHIELDS 2018 (LS18)

The focus of this, the largest technical “life-fire” exercise in cyber defence, was on defence, but supportive processes (legal position on “cyber”, PR work, collaboration and forensics) were also used. The exercise took place from 23 to 27 April 2018 in Tallinn, Estonia (EST) and was run by NATO CCD-COE. More than 1000 soldiers and civilians from 30 countries and NATO and EU organisations took part. Austria sent six people to participate in Tallinn and had a further 38 exercise participants in Vienna as the Blue Team (BT) in the KdoFüU&CD offices.

This exercise primarily practised the skills of protecting a less familiar network, identifying attacks and reacting appropriately to these.

As teams, the participating IT specialists had to identify cyber attacks, limit the effects of these and handle the incidents in line with uniform specifications (e.g. legal aspects, exchange of information, forensic analyses). The aim was to use the actions taken by the exercise participants to derive solutions to real problems, to strengthen international collaboration by creating trust, to improve the ability to carry out similar exercise projects, to test tools, to expand cyber defence skills and to improve active cyber negotiation skills.

4.4 CYBER PHALANX 2018 (CP18)

CP18 was a Table-Top Exercise (TTX) carried out from 4 to 8 June 2018 in the Schwarzenberg barracks in Salzburg. The exercise was a pilot project of the European Defence

Agency (EDA) and 135 soldiers and civilians from 16 countries took part. The exercise was carried out with an EXCON, a JOPG, CJOPG and a CyCell all being formed, using a Real Life Support cell.

The purpose of the exercise was to sensitise managers and their employees to cyber topics and prepare to handle the full range of cyber incidents that may occur during a military operation. The focus of the exercise was on leadership, so the technical details were not addressed in detail.

On the first two days, the principles for handling the subsequent exercise were established at a cyber awareness seminar.

The exercise period was broken down into two areas: the first two days were set aside for a specialist seminar. The exercise portion of the event then followed over the next three days. The content of the seminar was staggered and tailored to the needs of the participants starting with the global contexts of the crisis management mechanisms (collaboration on EEAS-EUMS planning activities, cyber governance, cyber diplomacy, legal aspects) and on to the concentrated handling of topics which directly support the implementation of the exercise from STARTEX (e.g. cyber defence at EUMS level, taking into account cyber aspects when planning an EU CSDP operation, reference documents, cyber defence aspects that need to be taken into account in the collaborative planning cycle between BXL and a designated OHQ and FHQ). All of the talks were rounded off with specialist and factual information with a specific link to the situation to be simulated.

4.5 Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX18)

CWIX18 was a large-scale Command Post Exercise (CPX) with a particular focus on interoperability tests and V&V of mission-oriented ICT systems, services and applications that took place from 11 to 28 June 2018 in Bydgoszcz, Poland.

Just under 1300 soldiers and civilians from 29 countries and NATO organisations took part in the exercise. Austria sent 25 participants. The main topic of the CWIX is recurrent interoperability tests using agreed scenarios and the opportunity to carry out additional tests in parallel to this, for example on data exchange with test partners following prior arrangement.

4.6 COMMON ROOF 2018 (CR18)

CR18 was a three-week exercise that took place from 2 to 18 May 2018 across the three countries of Germany, Austria and Switzerland. The lead nation for the exercise this year was Germany. Around 100 soldiers and civilians from the three countries took part in CR18, with Austria represented by 41 participants.

Over the course of the exercise, a multinational mission network was developed and operated and used to protect against cyber threats. The focus was on standardised (or in some cases still to be standardised) ICT service management processes, ICT security processes and the ICT services used. The monitoring and control of the multinational network elements was carried out by a multinational Network Operation Cell (NOC).

4.7 Cyber Europe and Cyber Europe Austria 2018

Every two years, the European Union Agency for Network and Information Security (ENISA) organises the largest pan-European IT emergency and crisis exercise “Cyber Europe”. This exercise was carried out for the fifth time in 2018 and focused on a cyber threat scenario related to the European aviation sector. Under the direction of the Federal Chancellery, Austria has been involved in Cyber Europe since 2010. Since 2012, it has done so in the form of a national exercise, “Cyber Europe Austria”, which is held in parallel.

The primary objective of the international Cyber Europe is to improve cooperation at a European level. As a result, in 2018 there was an opportunity to practise process and cooperation mechanisms which arise from the European NIS Directive among the participating countries as part of a scenario in which an international, large-scale cyber attack was targeting the aviation infrastructure in Europe.

At a national level, too, relevant actors from the public and private sectors were able to test their coordinated response to a serious cyber event in the form of a large-scale attack on the Austrian aviation sector.

Cyber Europe Austria enabled national structures, cooperation and communication processes to be tested to determine their effectiveness and efficiency to highlight strengths and possible weaknesses. In this way, the actors involved were able to optimise their preparations for a serious cyber event, thereby improving Austria's resilience.

In addition to developing recommendations for action from the results of cyber exercises such as Cyber Europe Austria, continuity and regular checks on structures and processes

play an important role in keeping up with the developments in cyber threats and as a result achieve a sustainable level of resistance to these threats.

4.8 CyberSOPEx 2018

The CSIRTs network that was created by the NIS Directive and serves to ensure operative collaboration between the designated CSIRTs in the EU, has developed operating procedures (Standard Operating Procedures - SOPs) for precisely this cooperation in the event of a crisis. These are based on the set of rules compiled over the years during the Cyber Europe exercises. CyberSOPEx 2018 was carried out on 30 January 2018 and aimed to test these collaboration procedures for the first time in the CSIRT Network. It was therefore not a domestic escalation exercise but rather purely about the processes between the CSIRTs across the EU.

Attacks on container ports were used as the scenario. The aim of the simulation was to collect information from all of the countries affected and use it to develop a joint situation report and a tailored approach. Since Austria was only marginally affected itself, the representatives of the Austrian CERT took on the role of facilitator within the CSIRT Network.

The exercise achieved the objective of testing processes and working out their strengths and weaknesses. The results were used to further develop the SOPs, which were soon used again in the larger framework of Cyber Europe 2018.

4.9 Cyber Incident Situational Awareness simulation game (CISA simulation game)

The Cyber Incident Situational Awareness simulation game (CISA simulation game) had different objectives to the other simulation games. This exercise sought to use a cyber attack scenario to determine what representation and linking of data during an ongoing cyber attack would create optimal capacity for action for a central point (situation centre). Several situation centres of this type were formed by the participating organisations during the exercise, which were each given the same information on the cyber situation. The aim was for these situation centres to record, process and represent the information in a suitable manner individually so an assessment of the situation could be carried out.

4.10 EU HEX-ML 18 (PACE)

The crisis management exercise “Hybrid Exercise Multilayer 18” (HEX-ML 2018 PACE) took place from 5 to 23 November 2018. It was organised by the EU, and Austria was also involved.

The aim of the exercise was to practise handling hybrid threat situations in collaboration with NATO to improve the ability of the EU to respond to future hybrid crises.

The scenario is based on a fictitious intervention by the EU in a conflict in a neighbouring country, which is dealing with a domestic security problem and with opposition and terrorist forces. Since the country is an anchor of stability in the region and has cooperated with the EU on economic, military and political matters to an increasing extent in the past few years, the EU is helping this country.

The EU member states have the option to bring their preferred areas into the exercise, particularly hybrid threats with a military responsibility that requires training. A key part of the exercise is handling fake news, the dissemination of propaganda and movements working against western interests. Terrorist, health and consular crises all needed to be managed in the exercise, with a focus on defending against complex cyber attacks, disinformation and attacks both within and outside of the EU.

4.11 CYBER DIPLO ATTX18

In the context of the framework for a joint diplomatic response from the EU to malicious cyber activities (Cyber Diplomacy Toolbox), the Austrian Council Presidency (Cyber Security Department of the BKA together with BMEIA) held a table-top exercise for EU member states at a Council level in Brussels on 29 November 2018 to test possible diplomatic measures taken in response to a crisis. The content of the exercise was based on the previous EU-NATO exercise HEX-ML 18 and was organised with the significant support of the European External Action Service and the General Secretariat of the Council of the EU. Representatives of various relevant organisations (European Commission, Europol EC3, ENISA, CERT-EU, NIS Cooperation Group, EDA and EUISS) took part as observers.

5 Summary/outlook

In 2018, the preparation of extensive situation reports on cyber security and the communication of the situation to stakeholders was a well-functioning process. The operative coordination structures IKDOK and OpKoord created during the implementation of the Austrian National Cyber Security Strategy met regularly and processed the situation through a joint process.

The collaboration between state organisations worked very efficiently on the basis of the coordination structures, new and challenging threats were able to be counteracted well and quickly. This was demonstrated during the major incidents of 2018: in the cases of the hardware weaknesses Spectre and Meltdown, the botnet VPNFilter and a large, targeted attack on the critical infrastructures of enterprises and authorities, the threat was able to be analysed and assistance provided quickly.

The pleasing trend towards Austria's enterprises setting aside a sufficient budget to protect their network and information systems continued into 2018. New security measures were introduced in many enterprises to increase cyber security. These included technical updates, organisational precautions and sensitisation of the employees. Increased activities to identify attackers in enterprises own networks and the associated introduction of SIEMs and stricter corporate processes were observed. Alongside technical advancement, investments in cyber security were driven by the legislative instruments relevant to security that entered into force in 2018 – the NIS Law and the General Data Protection Regulation.

An increase in security-related incidents in the cyber sector was a trend in 2018 too. Cyber attacks motivated by money such as ransomware attacks and data thefts increased in particular in 2018. Broad attacks such as ransomware and phishing were the most commonly identified attempted attacks in all company sizes. In contrast to this, DDoS incidents were on the decline, following a trend that started the previous year. Targeted attacks aiming to obtain information were also on the decline.

Increased defence measures taken by the enterprises and good sensitisation of employees meant that attacks were often able to be identified and defended against in advance. This was particularly significant in the case of ransomware and phishing. A trend for new spin-offs from enterprises to be attacked was also observed in 2018.

Reports of cybercrimes and cyber bullying decreased in Austria in 2018, and here too prevention measures and intensive detection work were effective. The number of cases of internet blackmail increased significantly, however, bucking the trend.

In addition to the topics mentioned above, the Austrian Ministry of Defence saw less widespread use of advanced malware but more professional social engineering via email and larger-scale attacks in 2018. An interesting observation over the year was a decline in politically motivated activities.

Cyber threats in 2018 were generally classed as a threat to national security. National cyber security strategies and legal principles consistently need to be adapted to keep up with developments. The significance of the field of cyber security is reflected in the various activities carried out in international organisations. Questions of cyber security were discussed with the active involvement of Austria in the following forums that are important to Austria: EU, UN, OSCE, NATO, OECD, Council of Europe and multilateral forums.

The transposition of the Directive on Security of Network and Information Systems was the focus within the EU. The Directive entered into force across the Union and through national laws in 2018. All EU member states started to implement it in 2018. Further regulatory policy proposals – the legal act on cyber security that would result in a strong Cyber Security Agency and an EU-wide certification framework and the regulation on pooling resources and expertise in research and innovation – were discussed in committees in 2018.

Processes and procedures were established within the EU for a coordinated response to cyber security incidents in order to react quickly to large-scale cyber attacks. The framework for a joint diplomatic response by the EU to malicious activities was expanded to include a cyber sanction regime in 2018. Particular interest was placed on the topic of attribution of cyber attacks and coordinated European approaches to serious incidents.

Other large EU topics included an extensive investment programme for cyber security as part of the “Digital Europe” 2021-2027 programme, the preparation for the European parliamentary elections in terms of cyber security, the fight against terrorist content on the internet and an action plan against disinformation to protect democratic processes.

In the second half of 2018, Austria chaired the most important cyber security groups in the EU while it held the Presidency of the Council. A challenging joint trio work programme for cyber security was set up at the instigation of Austria. The objective of driving forward cyber security in the EU in selected areas was very ambitious and was able to be achieved completely and in full. The Austrian Council Presidency organised a cyber conference in Vienna in December 2018.

Cyber security topics and issues of international law in cyberspace were discussed in various UN committees. There was a division in the most important thematic groups known as Groups of Governmental Experts (GGE) in 2018 due to significant content

differences, and two parallel processes will be continued in the future. An Austrian Resolution on “attacks on privacy only in accordance with the principles of human rights” was discussed in the UN Human Rights Council (HRC). A conference on cybercrime took place in Vienna in September 2018 as part of the IEG – the Intergovernmental Expert Group set up to address cybercrime.

Austria took on the partnership objective “Cyber Defence” as part of the NATO Partnership for Peace. The agreements on this for 2015 to 2017 were all able to be met by Austria. The next PARP cycle is currently ongoing.

Cyber security was one of the main topics of the OSCE in 2018. International cyber diplomacy, collaboration between the public and private sector and solutions to fictitious cyber attacks were all areas of focus. The work of the informal working group on cyber security focused on the implementation of the confidence-building measures that were agreed in 2018.

The importance of cyber security in Austria is reflected in the number of national structures that focus on this topic. National cyber structures proved their functional capacities in regular operation in 2018. They were established, networked and adapted to current challenges.

Public-private partnerships and platforms brought the various national actors together at a strategic and operative level. Continued close collaboration between all stakeholders, private and public, military and civil, national and international is needed in the future to further improve Austria’s resistance to cyber threats.

Various regulatory tools such as the NIS Law, the General Data Protection Regulation, the Austrian National Cyber Security Strategy and the corresponding point in the government programme formed the framework for a national cyber ecosystem. The entry into force of the NIS Law in 2018 was the transposition of the European NIS Directive. This will lift cyber security in Austria to a level appropriate to tackle the threats to which the country is exposed.

The functional capacity of national structures was demonstrated in a number of national and international cyber exercises in 2018.

