Council of the
European Union

Brussels, 28 July 2017
(OR. en)

8185/1/17
REV 1 DCL 1

GENVAL 41
CYBER 56

DECLASSIFICATION

of document:	8185/1/17 REV 1 RESTREINT UE/EU RESTRICTED
dated:	18 May 2017
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Austria

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.

Council of the
European Union

Brussels, 18 May 2017
(OR. en)

8185/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 41
CYBER 56

DECLASSIFIED

REPORT

Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Austria

ANNEX

Table of Contents

1. EXECUTIVE SUMMARY 5

2. INTRODUCTION 9

3. GENERAL MATTERS AND STRUCTURES 12

3.1. National cyber security strategy 12
3.2. National priorities with regard to cybercrime 13
3.3. Statistics on cybercrime 15
3.3.1. Main trends leading to cybercrime 15
3.3.2. Number of registered cases of cyber criminality 16
3.4. Domestic budget allocated to prevent and fight against cybercrime and support from EU funding 19
3.5. Conclusions 20

4. NATIONAL STRUCTURES 22

4.1. Judiciary (prosecutions and courts) 22
4.1.1. Internal structure 22
4.1.2. Capacity of and obstacles for successful prosecution 23
4.2. Law enforcement authorities 25
4.3. Other authorities/institutions/public-private partnership 27
4.4. Cooperation and coordination at national level 29
4.4.1. Legal or policy obligations 29
4.4.2. Resources allocated to improve cooperation 30
4.5. Conclusions 30

5. LEGAL ASPECTS 34

5.1. Substantive criminal law pertaining to cybercrime 34
5.1.1. Council of Europe Convention on Cybercrime 34
5.1.2. Description of national legislation 34

DECLASSIFIED

A/ Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems 34
B/ Directive 2011/92/EU on combating sexual abuse and sexual exploitation of children and child pornography 36
C/ *Online card fraud* 36
5.2. Procedural issues 37
5.2.1. Investigative Techniques 37
5.2.2. Forensics and Encryption 47
5.2.3. e-Evidence 48
5.3. Protection of Human Rights/Fundamental Freedoms 49
5.4. Jurisdiction 53
5.4.1. Principles applied to the investigation of cybercrime 53
5.4.2. Rules in case of conflicts of jurisdiction and referral to Eurojust 53
5.4.3. Jurisdiction for acts of cybercrime committed in the 'cloud' 54
5.4.4. Austrian perception of the legal framework to combat cybercrime 55
5.5. Conclusions 55

6. OPERATIONAL ASPECTS 58
6.1. Cyber attacks 58
6.1.1. Nature of cyber attacks 58
6.1.2. Mechanism to respond to cyber attacks 59
6.2. Actions against child pornography and sexual abuse online 62
6.2.1. Software databases identifying victims and measures to avoid re-victimisation 62
6.2.2. Measures to address sexual exploitation/abuse online, sexting, cyber bulling 63
6.2.3. Preventive actions against sex tourism, child pornographic performance and others 64
6.2.4. Actors and measures countering websites containing or disseminating child pornography 66
6.3. Online card fraud 68
6.4. Conclusions 68

7. INTERNATIONAL COOPERATION 72
7.1. Cooperation with EU agencies 72
7.1.1. Formal requirements to cooperate with Europol/EC3, Eurojust, ENISA 72
7.1.2. Assessment of cooperation with Europol/EC3, Eurojust, ENISA 72
7.1.3. Operational performance of JITs and cyber patrols 75

DECLASSIFIED

7.2. Cooperation between the Austrian authorities and Interpol 76
7.3. Cooperation with third states 76
7.4. Cooperation with the private sector 77
7.5. Tools of international cooperation 78
7.5.1. Mutual Legal Assistance 78
7.5.2. Mutual recognition instruments 80
7.5.3. Surrender/Extradition 80
7.6. Conclusions 81

8. TRAINING, AWARENESS-RAISING AND PREVENTION 83
8.1. Specific training 83
8.2. Awareness-raising 93
8.3. Prevention 94
8.3.1. National legislation/policy and other measures 94
8.3.2. Public Private Partnership (PPP) 95
8.4. Conclusions 95

9. FINAL REMARKS AND RECOMMENDATIONS 98
9.1. Suggestions from Austria 98
9.2. Recommendations 98
9.2.1. Recommendations to Austria 99
9.2.2. Recommendations to the European Union, its institutions, and to other Member States 100

Annex A: Programme for the on-site visit and persons interviewed/met 102

Annex B: Persons interviewed/met 104

Annex C: List of abbreviations/glossary of terms 107

Annex D: Austrian legislation 109

DECLASSIFIED

1. EXECUTIVE SUMMARY

The evaluation visit was well prepared by the Austrian authorities and included meetings with the relevant actors with responsibilities in the field of preventing and combating cybercrime as well as in the implementation and operation of European policies e.g. the Federal Chancellery, the Federal Ministry of Justice, the Federal Ministry of the Interior, the Public Prosecutors Office of Vienna, the police. The evaluation team was also given the opportunity to meet private entities involved in combating and preventing cybercrime in Austria such as Saferinternet.at, the Internet Ombudsman, Stopline and others.

During the on-site visit the Austrian authorities did their utmost to provide the evaluation team with complete information and clarifications on legal and operational aspects of preventing and combating cybercrime, cross-border cooperation and cooperation with EU agencies, and cyber strategy.

The Austrian Cyber Security Strategy (ACSS) provides a comprehensive and proactive concept for protecting cyberspace and the people in virtual space while guaranteeing human rights. It aims to enhance the security and resilience of Austrian infrastructures and services in cyberspace. It is a paramount common concern of the State, the economy and society to ensure cyber security in a national and international context.

DECLASSIFIED

The strategy was compiled by National Security Council liaison officers and cyber experts under the direction of the Federal Chancellery. The latter also set up the Cyber Security Steering Group, which also coordinates and supervises implementation of the strategy. The Steering Group compiles an annual report entitled 'Cyber Security in Austria' and advises the Federal Government on cyber security matters. Implementation plans setting out steps to achieve strategy goals are published as well as annual reports on cybercrime in Austria.

The national cybercrime priorities are aligned both with the EU's priorities in the fight against cybercrime and with the strategic guidelines of the ACSS. Measures to combat fraud via the Internet enjoy high priority. National and international cooperation - above all with Europol/EC3 and Eurojust - is being greatly stepped up. At the national level close cooperation with national partners in the business community, such as the credit sector, the Austrian Economic Chambers and the Internet Ombudsman, is being reinforced. It is noted further that the homepage of the Austrian Criminal Intelligence Service (.BK) contains a code of practice should a mass phenomenon occur.

In addition, a Cyber Security Centre (CSC) is currently being set up at the Federal Agency for State Protection and Counter Terrorism (BVT)/BMI and its main objective is to increase resilience against cyber threats both through operational coordination on cyber security incidents (particularly in the critical infrastructure and public administration sectors) and through preventive measures (promotion and coordination of information exchange, awareness-raising measures, involvement in security research, technical analyses and situation reports).

DECLASSIFIED

No prosecutors or judges are designated to deal exclusively or to a large extent with cybercrime cases. Austrian prosecutors and judges are obliged to continuously improve their skills and take part in training. Austria offers them national and international training in the area of cybercrime but in the evaluators' view, given the fact that there are no specialised prosecutors or judges in Austria for cybercrime, this area calls for improvement and more training opportunities.

Law enforcement authorities are well prepared, organised, connected and trained with regard to cybercrime. The structure of law enforcement authorities is robust at federal, regional and local level. Every regional division has a cybercrime-support unit with an appropriate infrastructure ("first responders").

As regards legislation, the European legislation pertaining to cybercrime has been implemented in Austrian law. Austria amended the criminal and procedural laws in criminal matters focusing on cybercrime, introducing penalties and explicitly naming the different types of criminal behaviour in cybercrime. Special sections in the criminal law with regard to cybercrime and special sections in the criminal procedural law regulating investigative measures in the field of cybercrime for the purpose of gathering information and evidence from ISPs are now in place. Austrian law does not provide for the possibility to block compromised websites in criminal proceedings. It is noted that the data retention period by providers e.g. for billing purposes amounts to three months and Austria awaits legislative actions on data retention at the EU level to reform its rules.

Different bodies collect statistics in Austria, however Austria lacks one single body in charge of processing statistics. As a consequence, the Cyber Security Steering Group may not have clear and comprehensive statistical information on the development of cybercrime in Austria. In the opinion of the evaluators it would be useful to take into consideration further development of the already existing and operational statistical systems to help to create a better understanding of dangers posed by criminals to every stakeholder involved in fighting cybercrime.

DECLASSIFIED

ISPA, the association of ISPs in Austria, has 200 members and advises companies with regard to cyber matters. It has established a platform for law enforcement to improve cooperation in the area of communication surveillance, and it is currently working on a security strategy together with companies, law enforcement and the University of Vienna. It is noted however that the financial sector in Austria does not have a mandatory reporting obligation to inform the police of suspicious or criminal behaviour- this leaves some room for improvement and according to the evaluators more mandatory obligations could be considered in that regard.

Austria carries out a number of awareness programmes in the education field, and has a number of bodies charged with monitoring publications and websites in areas of child pornography and national socialism, which facilitate the removal of such material. Many prevention projects are also performed ('Click & Check' project, Cyber.Sicher, or Cyber.Kids' project).

As cybercrime is a relatively new phenomenon, the area of the utmost importance is training and the development of expertise. The judges and prosecutors are not subject to general training on cybercrime and participation in the available courses is not mandatory. On the other hand, Austria has developed tailor-made training for law enforcement. All categories of police officers are trained on cybercrime (basic police training, basic training for mid-level officers and basic training for senior officers). Joint events for the police and judiciary are not organised. The organisation of joint training events including judges and prosecutors, police officers and IT specialists could help to cover the entire process through which a criminal case is finally brought to judgment**.**

Taking into account the ambitious approach in terms of countering cybercrime and its intention to continuously strengthen cybersecurity in Austria, the evaluators consider that the situation in Austria is promising.

DECLASSIFIED

2. INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997[1], a mechanism for evaluating the application and implementation at national level of international undertakings in the fight against organised crime was established. In line with Article 2 of the Joint Action, the Working Party on General Matters including Evaluations (GENVAL) decided on 3 October 2013 that the seventh round of mutual evaluations should be devoted to the practical implementation and operation of the European polices on prevention and combating cybercrime.

The choice of cybercrime as the subject for the seventh Mutual Evaluation round was welcomed by Member States. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. To this end, the evaluation covers three specific areas: cyber attacks, child sexual abuse/pornography online and online card fraud and should provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography[2] (transposition date 18 December 2013), and Directive 2013/40/EU[3] on attacks against information systems (transposition date 4 September 2015), are particularly relevant in this context.

DECLASSIFIED

1 Joint Action of 5 December 1997 (97/827/JHA), OJ L 344, 15.12.1997 pp. 7 - 9.
2 OJ L 335, 17.12.2011, p. 1.
3 OJ L 218, 14.8.2013, p. 8.

Moreover, the Council Conclusions on the EU Cybersecurity Strategy of June 2013[4] reiterate the objective of ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[5] of 23 November 2001 as soon as possible and emphasise in their preamble that 'the EU does not call for the creation of new international legal instruments for cyber issues'. This Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.[6]

Experience from past evaluations show that Member States will be in different positions regarding implementation of relevant legal instruments, and the current process of evaluation could provide useful input also to Member States that may not have implemented all aspects of the various instruments. Nonetheless, the evaluation aims to be broad and interdisciplinary and not focus on implementation of various instruments relating to fighting cybercrime only but rather on the operational aspects in the Member States.

Therefore, apart from cooperation with prosecution services, this will also encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3 and how feedback from the given actors is channelled to the appropriate police and social services. The evaluation focuses on implementing national policies with regard to suppression of cyber attacks and fraud as well as child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to persons who fall victims of cybercrime.

DECLASSIFIED

4 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

5 CETS no. 185; opened for signature on 23 November 2001, entered into force on 1 July 2004.

6 CETS no. 189; opened for signature on 28 January 2003, entered into force on 1 March 2006.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. Austria was the twenty third Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, a list of experts in the evaluations to be carried out has been drawn up by the Presidency. Member States have nominated experts with substantial practical knowledge in the field pursuant to a written request on 28 January 2014 to delegations made by the Chairman of GENVAL.

The evaluation teams consist of three national experts, supported by two members of staff from the General Secretariat of the Council and observers. For the seventh round of mutual evaluations, GENVAL agreed with the proposal from the Presidency that the European Commission, Eurojust, ENISA and Europol/EC3 should be invited as observers.

The experts charged with undertaking the evaluation of Austria were Mr Attila Kökényesi - Bartos (Hungary), Ms Mairead Cotter (Ireland), and Mr Rogério Bravo (Portugal). Two observers were also present: Mr Murat Ayilmaz (Eurojust) together with Mr Sławomir Buczma from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Austria between 18 and 20 May 2016, and on Austria's detailed replies to the evaluation questionnaire together with their detailed answers to ensuing follow-up questions.

DECLASSIFIED

3. GENERAL MATTERS AND STRUCTURES

3.1. National cyber security strategy

Austria indicated the national and international safeguarding of cyberspace as one of its top priorities. On 20 March 2013 the Federal Government adopted the Austrian Cyber Security Strategy (ACSS - *Österreichische Strategie für Cyber Sicherheit / ÖSCS*), a comprehensive and proactive approach to protecting cyberspace and people who use it. The cyber security strategy is based on the principles of the rule of law, subsidiarity, self-regulation and proportionality. An open and free Internet, the protection of personal data and the integrity of interconnected networks are the foundation for global prosperity, security and the promotion of human rights.

The ACSS forms the basis of nationwide cooperation in cyber security. It establishes an operational cyber coordination structure at national level. The aim is to ensure regular exchange of information, continuously monitor and assess the situation in cyberspace and decide on joint actions.

The Cyber Security Steering Group, under the leadership of the Federal Chancellery, is responsible for coordinating measures relating to cyber security at a political-strategic level, monitoring and supporting the implementation of the ACSS, preparing an annual Cyber Security Report and advising the federal government in all matters relating to cyber security. The Steering Group is composed of liaison officers for the National Security Council and cyber security experts of the ministries represented in the National Security Council.

DECLASSIFIED

The Computer Emergency Response Team (CERT), a state agency run by the Federal Chancellery, already operates as the central contact point for cyber incidents. The Austrian Trust Circles set up by Cert.at and the Federal Chancellery link up security experts in the various sectors, thereby ensuring that the right contacts are available if the need arises. The Austrian CERT Association will be expanded and CERT.at will be strengthened to facilitate national cooperation among Austrian CERTs. This will help to promote the establishment of CERTs in all sectors on the one hand and to intensify the exchange of information and experience on CERT-specific issues on the other hand.

The Operational Coordination Structure is coordinated by the Federal Ministry of the Interior (PPP model) by involving the ministries and the operational structures of the business and research sectors. The aim is to facilitate ongoing communication between the State, the private sector and civil society.

3.2. National priorities with regard to cybercrime

The national cybercrime priorities are aligned both with the EU's priorities in the fight against cybercrime and with the strategic guidelines of the ACSS. The Austrian authorities have declared that measures to combat fraud via the Internet enjoy high priority. National and international cooperation - first of all with Europol/EC3 - is being greatly stepped up. With prevention in mind there is close cooperation with national partners in the business community, such as the credit sector, the Austrian Economic Chambers and the Internet Ombudsman. This enables new developments to be made publicly available without delay and special professional groups to be immediately informed about specific events.

DECLASSIFIED

It is further noted that the homepage of the Austrian Criminal Intelligence Service (.BK) contains a code of practice should a mass phenomenon occur. This service, which comes under the Federal Ministry of the Interior (BMI), takes part in the 'Don't look away!' campaign against tourism-related child sexual abuse, in which seven European countries (AT, CH, DE, FR, LUX, NL, PL) participate. This service is also involved in conducting presentations and training courses for ACCOR hotel managers, amongst others.

In combating cybercrime, the priorities of the .BK/5.2 C4 - Cybercrime Competence Centre are guided by the strategic goals of the Austrian Criminal Intelligence Service (.BK) and comprise investigations into cybercrime offences, the preservation of digital forensic evidence and a cybercrime hotline for the public. C4 also covers training, prevention and international police cooperation in the area of cybercrime. Furthermore, Austria supports the EU's international efforts to combat cybercrime by its participation in EMPACT cyber attack working parties and its involvement in J-CAT operations.

At the time of the on-site visit, the Cyber Security Centre (CSC) was being set up at the Federal Agency for State Protection and Counter Terrorism (BVT)/BMI. The centre's main objective is to increase resilience against cyber threats, both through operational coordination on cyber-security incidents (particularly in the critical infrastructure and public administration sectors) and through preventive measures (promotion and coordination of information exchange, awareness-raising measures, involvement in security research, technical analysis and situation reports).

DECLASSIFIED

3.3. Statistics on cybercrime

3.3.1. Main trends leading to cybercrime

Investigations	2011	2012	2013	2014	Grand total
District prosecutor's offices ('DPOs')	**508**	**589**	**596**	**651**	**2 344**
118a Illegal access to a computer system	148	95	152	190	585
119a Illegal interception of data	18	17	22	12	69
126a Damage to data	58	71	76	67	272
126b Disruption of the operational capacity of a computer system	14	50	19	16	99
126c Misuse of computer programs or access data	71	61	82	68	282
148a Fraudulent misuse of data processing	163	243	197	217	820
207a Pornographic representations of minors	4	2	4	3	13
208a Sexual grooming of persons under 14		9	3	7	19
225a Forgery of data	32	41	41	71	185
Public prosecutor's offices ('PPOs')	**1 070**	**1 088**	**1 053**	**1 222**	**4 433**
118a Illegal access to a computer system	42	51	52	71	216
119a Illegal interception of data	12	8	9	9	38
126a Damage to data	47	47	49	42	185
126b Disruption of the operational capacity of a computer system	6	13	6	9	34
126c Misuse of computer programs or access data	26	22	21	36	105
148a Fraudulent misuse of data processing	226	227	275	345	1073
207a Pornographic representations of minors	693	659	554	630	2536
208a Sexual grooming of persons under 14		50	69	66	185
225a Forgery of data	18	11	18	14	61
Grand total	**1 578**	**1 677**	**1 649**	**1 873**	**6 777**

DECLASSIFIED

Total for all types of investigation:

Investigations	2011	2012	2013	2014	Grand total
DPOs	268 097	196 719	195 251	190 444	850 511
PPOs	145 549	146 110	147 300	145 164	584 123
Grand total	**413 646**	**342 829**	**342 551**	**335 608**	**1 434 634**

Statistics collected by the police in the years 2012 -2014 show the decrease in the number of cybercrimes in comparison to the total number of crimes registered in Austria.

	2012	2013	2014
All types of crime in total	548 027	546 396	527 692
Cybercrime in total	10 308	10 051	8 966
Percentage of cybercrime	1.9 %	1.8 %	1.7 %

DECLASSIFIED

3.3.2. Number of registered cases of cyber criminality

The respective figures for the conduct and completion of proceedings by public prosecutors and courts are listed in a justice department database (Verfahrensautomation Justiz - VJ) and may be analysed in anonymised form. The figures for final convictions are sent each year by the Criminal Records Office to Statistics Austria, which in turn publishes the figures annually in its crime statistics (www.statistik.at).

The Federal Ministry of the Interior keeps parallel figures of its own. Cybercrime statistics are recorded under police crime statistics. These are the statistics for complaints and are compiled by the Criminal Intelligence Service. The relevant data are entered in the police records system, forwarded to the database of the Criminal Intelligence Service, and then analysed. They are not connected to the statistics held by the judicial authorities.

The following table contains statistics of convictions and acquittals:

	2011	2012	2013	2014	Grand total
Acquittal	**45**	**51**	**68**	**50**	**214**
Regional court	**40**	**35**	**44**	**44**	**163**
126a Damage to data	3	1	2	1	7
148a Fraudulent misuse of data processing	15	9	14	20	58
207a Pornographic representations of minors	22	25	28	22	97
208a Sexual grooming of persons under 14				1	1
District court	**5**	**16**	**24**	**6**	**51**
118a Illegal access to a computer system		2	3	1	6
126a Damage to data	2	3	7	1	13
126c Misuse of computer programs or access data	1	1	1		3
148a Fraudulent misuse of data processing	1	8	10	2	21
225a Forgery of data	1	2	3	2	8
Conviction	**336**	**423**	**352**	**330**	**1 441**
Regional court	**308**	**395**	**331**	**315**	**1 349**
118a Illegal access to a computer system		2	1	1	4
126a Damage to data	7	5	4	3	19
126b Disruption of the operational capacity of a computer system	1	1			2
126c Misuse of computer programs or access data	4			1	5
148a Fraudulent misuse of data processing	99	101	95	138	433
207a Pornographic representations of minors	194	286	223	167	870
208a Sexual grooming of persons under 14			5	1	6
225a Forgery of data	3		3	4	10
District court	**28**	**28**	**21**	**15**	**92**
118a Illegal access to a computer system	1		2		3
126a Damage to data	2	3	2		7
126b Disruption of the operational capacity of a computer system				1	1
126c Misuse of computer programs or access data	2		2		4
148a Fraudulent misuse of data processing	20	17	12	9	58
225a Forgery of data	3	8	3	5	19
Grand total	**381**	**474**	**420**	**380**	**1 655**

DECLASSIFIED

Statistics collected by the police in the years 2013 -2014 show the decrease in detecting cybercrime:

Reported cases	2013	2014	Deviation
cybercrime *sensu stricto*	1 737	1 754	1.0 %
cybercrime *sensu largo*	8 314	7 212	-13.3 %
cybercrime in total	10 051	8 966	-10.8 %

Cleared cases	2013	2014	Deviation
cybercrime *sensu stricto*	310	316	1.9 %
cybercrime *sensu largo*	4 234	3 344	-21.0 %
cybercrime in total	4 544	3 660	-19.5 %

Clearance rate	2013	2014	Deviation
cybercrime *sensu stricto*	17.8 %	18.0 %	0.2
cybercrime *sensu largo*	50.9 %	46.4 %	-4.6
cybercrime in total	45.2 %	40.8 %	-4.4

Identified suspects	2013	2014	Deviation
cybercrime *sensu stricto*	334	326	-2.4 %
cybercrime *sensu largo*	3 621	3 278	-9.5 %
cybercrime in total	3 955	3 604	-8.9 %

DECLASSIFIED

The evaluators noticed that the figures provided by the Ministry of the Interior and the Criminal Records Office to Statistics Austria show different numbers regarding the cybercrime detected and registered and investigations carried out.

3.4. Domestic budget allocated to prevent and fight against cybercrime and support from EU funding

There is no budget allocation dedicated to the prevention and fight against cybercrime. However, specific resources were allocated to carry out projects outlined in the table below.

Project promoter	Project title	Planned EU funding	ongoing	planned
.BK Sub-department 5.2 Cyber Crime Competence Centre C4	Cyber.Kids	27 000.00	x	
.BK Sub-department 1.4 Criminal investigation strategy	BK-Radar	270 000.00		x
.BK Sub-department 1.4	New Media	350 000.00	x	
.BK Department 7 Economic crime	Screening System	665 660.70		x
II/BVT/3	Cyber Security Centre	1 134 000.00	x	

DECLASSIFIED

3.5. Conclusions

- On 20 March 2013 the Federal Government adopted the Austrian Cyber Security Strategy (ACSS). It is a comprehensive and proactive approach to protecting cyberspace and forms the basis of nationwide cooperation in this area**.** It expresses the Austrian state's vision for developing the digital economy, whilst preserving the cyber security of its citizens.

- The ACSS was created with the support of the most important private stakeholders, various CERTs - both governmental (GovCERT, MilCERT) and private (CERTs, banks, etc.), as well as the Cyber Crime Competence Centre at the police (Department .BK/5.2 C4). The strategy is a high-level policy, which was drawn up by the Cyber Security Steering Group comprising the most relevant ministries (Ministries of Justice, Interior, Foreign Affairs, and Defence) and headed by the Federal Chancellery. It seems to be a well-placed body which compiles all the important information to create a proper overall strategy and define the main relevant principles, including feedback from the industry.

- The national cybercrime priorities are aligned both with the EU's priorities in the fight against cybercrime and with the strategic guidelines of the ACSS. National and international cooperation is being greatly stepped up. With prevention in mind there is close cooperation with national partners in the business community, such as the credit sector, the Austrian Economic Chambers and the Internet Ombudsman. The initiative to set up an Office of the Internet Ombudsman deserves special mention as this person represents customers aggrieved as a consequence of transactions made online and suspicious behaviour observed thereon.

- Statistics are collected in Austria by different bodies. The respective figures for the conduct and completion of proceedings by public prosecutors and courts are listed in a justice department database. The figures for final convictions are sent each year by the Criminal Records Office to Statistics Austria which in turn publishes the figures annually in its crime statistics.

DECLASSIFIED

- The Federal Ministry of the Interior keeps parallel figures of its own. Cybercrime statistics are recorded under police crime statistics. These are statistics for complaints and are compiled by the Criminal Intelligence Service. The relevant data are entered in the police records system and forwarded to the database of the Criminal Intelligence Service.[7]

- Furthermore, statistics are collected by hotlines due to a parallel reporting possibility. Since the statistics cover both public and private hotlines this may create an obstacle for proper collection of statistics due to multiple reports of the same incident. It is currently unknown how many reported incidents were registered simultaneously and in such a way potentially doubled the number of reports.

- Moreover, it appears that statistical data of the Ministry of Interior, the police and the Ministry of Justice are different. There was no direct explanation for the differences, just the fact that the various organisations use different kinds of approach to define the base number of their statistics, and also to define the phenomenon of cybercrime. The different approaches to the base numbers derive from the different roles of the stakeholders referred to in the Austrian system. As a consequence, the Cyber Security Steering Group may not have clear and comprehensive statistical information which may undermine its effort due to lack of a clear picture of how cybercrime develops. It is the opinion of the evaluators that it would be useful to consider further development of the already existing and operational statistical systems to help create a better understanding of the dangers posed by cyber criminals to every stakeholder.

- Furthermore, the statistical differences can also cause conflicts, for example between the police and the Ministry of Interior in analysing the budgetary and human resource necessities of the cybercrime units of the police or distorting international/EU statistics.

- Austria has not allocated any specific budget for cybercrime, although bodies referred to in the report have their own budgets allocated by the government. It is noted however that Austria actively uses EU funding to support its own budget in cybercrime matters, which is a recommended practice.

[7] The evaluation team was informed after the on-site visit that new reporting software is being developed for the regional police departments. Obtaining meaningful statistical data is an important aspect of this work. Where technically and legally possible, it will deal with known shortcomings.

DECLASSIFIED

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecutions and courts)

4.1.1. Internal structure

The main proceedings are held in court on the basis of charges with legal effect. All judges, public prosecutors and criminal investigation bodies are required to carry out their duties impartially and with an open mind, and to avoid any semblance of bias. They must devote the same care to investigating circumstances that incriminate or exonerate the person under investigation.

The criminal investigation department of the police and the public prosecutor's office are required to launch a criminal investigation of their own motion on the basis of any initial suspicion of a criminal offence that comes to their knowledge, except for offences which are only to be prosecuted at the request of a person authorised to make such a request. Unless otherwise provided by law, charges are brought by the public prosecutor's office, which leads the investigation. It is noted however, that the criminal investigation department and the public prosecutor's office should, as far as possible, be in full agreement over the conduct of the investigation. Where such full agreement is not secured, the public prosecutor's office should issue the necessary orders, to be followed by the criminal investigation department.

The Central Public Prosecutor's Office for the Prosecution of Economic Crimes and Corruption (WKStA) is responsible for prosecuting computer-related fraud causing particularly high damage. Otherwise, the general powers of the public prosecutor's offices and courts apply in the case of cybercrime. For those matters which come within its substantive jurisdiction the WKStA has nationwide competence.

The evaluation team did not notice judges or prosecutors specialised in fighting cybercrime, in particular at regional level.

DECLASSIFIED

4.1.2. Capacity of and obstacles for successful prosecution

While there is no special team of staff deployed solely to deal with cybercrime, recent years have seen a significant increase in the number of public prosecutors - in particular at the Central Public Prosecutor's Office for the Prosecution of Economic Crimes and Corruption. This development is perceived by the Austrian authorities as beneficial also in relation to cybercrime. Over the past ten years the pattern for the number of public prosecutors in full-time posts has been as follows (actual numbers, establishment posts):

Procurator-General's Office + Judicial authorities in the Länder	TARGET NUMBER	ACTUAL NUMBER
04/ 1995	208	203.00
04/ 1996	208	206.00
04/ 1997	209	204.00
04/ 1998	209	207.00
04/ 1999	210	208.00
04/ 2000	220	215.00
04/ 2001	218	219.00
04/ 2002	218	216.00
10/ 2003	216	217.50
04/ 2004	213	220.50
04/ 2005	212	216.68
04/ 2006	216	218.50
04/ 2007	283	221.50
10/ 2008	340	341.50
01/ 2009	340	335.75
07/ 2010	367	363.00
07/ 2011	376	345.75
09/ 2012	382	370.75
01/ 2013	393	373.50
05/2014	406	380.00
04/2015	406	395.30

DECLASSIFIED

Central Public Prosecutor's Office for the Prosecution of Economic Crimes and Corruption (WKStA)	TARGET NUMBER	ACTUAL NUMBER
01/2009	5	1.00
07/2009	5	5.00
01/2010	5	7.00
07/2010	7	8.00
01/2011	12	8.00
07/2011	21	10.50
01/2012	21	15.00
07/2012	21	16.00
01/2013	29	20.00
07/2013	30	21.50
01/2014	35	21.50
07/2014	40	25.50
01/2015	40	27.25
07/2015	40	30.50

DECLASSIFIED

The competent public prosecutor's offices mentioned the following obstacles for successful prosecution of cybercrime:

- the international dimension of cybercrime;
- the lengthy process of executing MLA requests and/or the fact that such requests prove unsuccessful;
- the offenders' high level of expertise, often surpassing that of law enforcement personnel; new forms of cybercrime are constantly emerging;

- concealment tactics by offenders involving the use of fake call numbers and IP addresses or false identities, as well as money transfers via companies such as Western Union; anonymous Internet access; use of anonymisation programs; difficulties in proving that the computer has in fact been used;
- limited scope for consulting social networks;
- large quantities of data =) police capacities are exceeded, meaning that experts sometimes have to be called in (very costly);
- problems in cases in which data are stored in the 'cloud' or on foreign servers;
- short storage periods, ban on data retention;
- in the mobile phone sector, allocation of IP addresses to several subscribers simultaneously, meaning that an address can no longer be attributed to a device;
- overburdening of all investigating officials (police, public prosecutor's office) with activities unrelated to law enforcement;
- the fact that telecommunications providers are sometimes unwilling to cooperate at weekends to the extent required.

4.2. Law enforcement authorities

BK

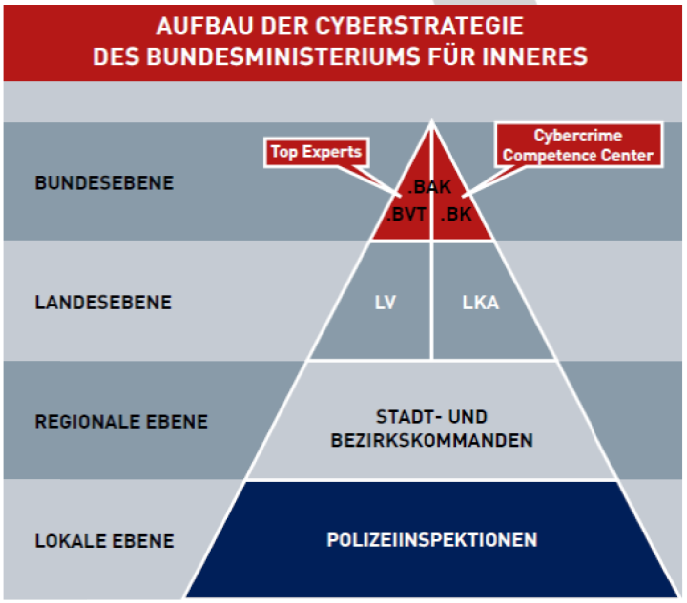
Pursuant to Section 4 of the Criminal Intelligence Service Act (Federal Law Gazette I No 22/2002, as amended on 6.2.2015) the .BK is responsible at the federal level for directing, coordinating and steering work on Internet fraud, international coordination and investigations, and reporting offences to the public prosecutor's office. Responsibility for directing, coordinating and steering work at Land level, national coordination and investigations, and reporting offences to the public prosecutor's office, lies with the criminal intelligence services of the Länder (Landeskriminalämter, LKAs). The police inspectorates are in charge of receipt of complaints, investigations and reporting offences to the public prosecutor's office.

DECLASSIFIED

The Cybercrime Competence Centre (C4)

The Cybercrime Competence Centre (Department .BK/5.2 C4) is responsible for all investigations aimed at combating cybercrime in the narrower sense (Sections 118a, 119a, 126a-c, 148a, 225a StGB) and for the securing of electronic evidence. It was established as part of the Service in 2011. The centre comprises a hotline, the Central Tasks Unit, the IT preservation of evidence Unit and the Investigations Unit. It is the national and international central unit for the fight against cybercrime in Austria. In addition to C4 at federal level there are similar units in all the criminal intelligence services of the Länder (LKAs). These organisational units have technical and criminal investigation experts working on cybercrime and IT forensics at Land level. At local level the police are supported by district IT investigators in the police inspectorates - so-called "first responders". There are currently 300 first responders in Austria. It is intended to allocate more time for the practical and theoretical training of first responders. This will be introduced in 2017.

By way of illustration the cyber strategy organisation chart shows the entire administrative structure dealing with the fight against cybercrime. Unit II/BK/5.2.3 of the Austrian Criminal Intelligence Service (.BK) is responsible for conducting investigations. The Austrian Criminal Intelligence Service's forensic IT specialists are based in Unit II/BK/5.2.2.



RESTREINT UE/EU RESTRICTED

In addition, Office 3.2 of the Austrian Criminal Intelligence Service contains the child pornography and child sex tourism hotline.

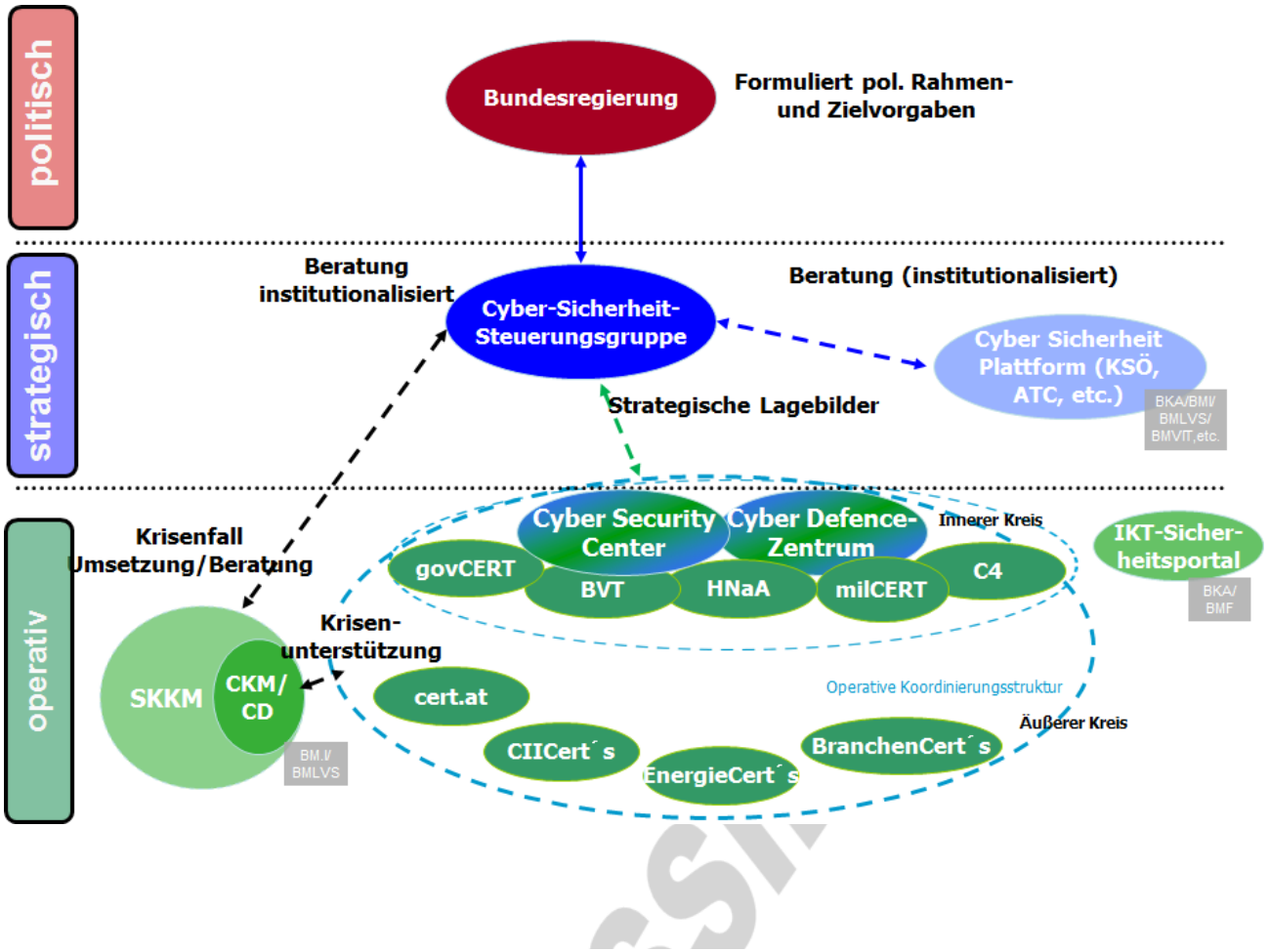
The Federal Agency for State Protection and Counter Terrorism has departments the job of which is to prevent cybercrime, and others which deal with the prosecution of offences already committed.

4.3. Other authorities/institutions/public-private partnership

In the process of adopting the Austrian Cyber Security Strategy an additional operational structure for coordinating cybersecurity incidents was established to bring together relevant public sector and business stakeholders. The Cyber Security Centre (CSC) chairs this structure (as well as the Cyber Defence Centre (CDZ) in the Federal Ministry of Defence and Sport, for cyber defence cases). The CSC is set up at the Federal Agency for State Protection and Counter Terrorism (BVT)/BMI to increase resilience against cyber threats both through operational coordination on cybersecurity incidents (particularly in the critical infrastructure and public administration sectors) and through preventive measures (promotion and coordination of information exchange, awareness-raising measures, involvement in security research, technical analyses and situation reports).

From the public sector the following bodies are represented in the 'Inner Circle': C4, govCERT, milCERT and the Army Intelligence Office. The 'extended circle' is expected in the future to include CERT.at, sector-specific CERTs and other relevant stakeholders in the field of cybersecurity. The aim is to ensure regular coordination and joint situation assessments.

The Austrian private sector has established the CERT.AT. Members of this CERT.AT are private cyber-specialists paid by the private and the public sector aiming to fight cybercrime. It supports the private and the public sector in this matter, analyses current dangers, proposes solutions, coordinates in situations of crisis, is the point of contact for the private sector, publishes current danger analysis, and works together with ISPs.



Pursuant to Section 4 of the Criminal Intelligence Service Act (Federal Law Gazette I No 22/2002, as amended on 6.2.2015), the Criminal Intelligence Service, in its capacity as superordinate central body, is responsible for the national coordination of cross-regional and international official action. It has the power to give instructions to subordinate departments. The fight against cybercrime is coordinated by the Cybercrime Competence Centre (C4).

In addition, there is an international research project financed by KIRAS (in addition, the Criminal Intelligence Service (Sub-department 3.2) provides two advisers for the private hotline 'Stopline' (www.stopline.at). Sub-department 3.2 is also a permanent member of the 'Round Table on Ethics in Tourism' set up at the Federal Ministry of Economic Affairs, the Family and Youth. There is also regular participation in international meetings organised by ECPAT.

Furthermore, many NGOs such as ECPAT, Stopline (provider organisation) and Safer Internet explicitly refer to the Criminal Intelligence Service hotline, meldestelle@interpol.at, on their homepages and in various videos and publications.

Within the national programme for critical infrastructure protection, the public-private partnership model was chosen in order to increase the resilience of strategically important companies. This concerns preparatory measures against both physical risks and cybercrime. This public-private partnership is implemented through the provision of information (e.g. risk management guides), events, advice on security-related issues, an early-warning system and a 24/7 contact point and hotline.

4.4. Cooperation and coordination at national level

4.4.1. Legal or policy obligations

Currently the private sector is not under any obligation to report cyber attacks in Austria.

The Austrian authorities reported sufficient and effective cooperation between industry, banks, the private sector and LEAs to prevent and fight online card fraud in general terms. Private companies generally have no objection to providing access to the servers if requested to do so through a court order.

As part of the implementation of the Austrian Cyber Security Strategy, a 'cyber crisis mechanism' (CKM) is being set up, which will be integrated into the National Crisis and Disaster Protection Mechanism (SKKM).

DECLASSIFIED

4.4.2. Resources allocated to improve cooperation

The research project 3B3M financed by the Austrian Security Research Programme (KIRAS) as part of the project 'Social Media Crime', which is a comprehensive study, was carried out with the aim of creating a scientifically sound categorisation of social media-related crimes. By means of scientific research and surveys, individual social media crime phenomena and activities were analysed, shedding light not only on types of crime but also on the causes and consequences and victim and offender characteristics. The results were structured and categorised in accordance with the needs of the police. This categorisation is used to draw attention to preventive and corrective measures which are already being implemented or planned internationally. Based on these findings, specific recommendations were drawn up to help the police to reduce social media crime in the long term.

According to the Austrian authorities specialised units have sufficient equipment and competence. However, in the opinion of the evaluators, Austria has not allocated a dedicated budget for improving cooperation referring to cybercrime, although the bodies described above have budgets derived from the government. Moreover, the evaluation team was informed by the Austrian representatives met during the on-site visit that there is a need for more funding for digital forensics, for both tools and human resources.

4.5. Conclusions

- There are no specialised courts and judges dealing with cybercrime in Austria. There are no specialised prosecutor's offices or specialised prosecutors. The Central Public Prosecutor's Office for the Prosecution of Economic Crimes and Corruption in Vienna presented one prosecutor who supervised a large-scale international investigation and cooperated in the JIT operation called 'Mozart'.

DECLASSIFIED

- The evaluation team was informed that the prosecutors are trained well and can cope with such issues as child pornography, but not in the narrower area of cybercrime. In the evaluators' view better training and specialisation could improve prosecutors' capacity with regard to cybercrime in the narrower sense.

- The evaluators believe that fighting cybercrime requires not only knowledge and understanding regarding how the crime was committed but also how to investigate different types of cybercrime. Especially in the field of cybercrime the modus operandi, the software and tools that were used change constantly and at short intervals. The investigating measures need to be updated (for example with special investigating computer software), which requires constant attention to these areas, also with regard to legal impacts. Furthermore, fighting cybercrime often requires mutual legal assistance from other countries, which makes networking necessary. The evaluators believe that Austria should either appoint specialised prosecutors in charge of fighting cybercrime and/or improve the level and the number of expert prosecutors and judges in the area of cybercrime.

- In contrast to the judges and prosecutors, the police have a very well-developed central unit - the Cybercrime Competence Centre (C4) handling cybercrime. The centre comprises a hotline, the Central Tasks Unit, the IT preservation of evidence Unit and the Investigations Unit. It is the Austrian national and international central unit for the fight against cybercrime in Austria. In addition to the C4 level there are similar units at the federal level in the criminal intelligence services of the Länder (LKAs). These organisational units have technical and criminal investigation experts working on cybercrime and IT forensics. At local level the police are supported by district IT investigators in the police inspectorates.

DECLASSIFIED

- Furthermore, the central structure of the police is supported at the regional and local level by a line of first responders, a 300-person strong staff, with 1-3 persons located in almost every single local police office. This staff of first responders have proper equipment and frequent training which makes them geared to perform on site live forensics or data recording tasks. The local police officers are given a short training course on cybercrime (4-8 hours) to prepare them in general.

- Although the C4 has been established as a multi-disciplinary centre for intelligence gathering and policing it seems to be short-staffed and the experts met expressed desire for more funding and resources. Another issue is the need to provide more funding to digital forensics, for both tools and human resources that would reduce the 'backlog' in digital forensics examinations.

- The police have a good partnership with the private hotline called 'Stopline' and also with the representatives of the project 'Safer internet' which is co-funded by the EU. C4 also has its own crime prevention project (Cyber.Kids) which is funded by the EU. In the project the help of psychologists is used to ensure that the information given to the minors is understandable for them.

- The Federal Agency for State Protection and Counter Terrorism has departments the job of which is to prevent cybercrime, and others which deal with the prosecution of offences already committed.

- In general Austria has developed some cooperation between the public and private sector in the fight against and prevention of cybercrime. In March 2015 the Cyber Security Platform was established, in which the private and public sector are represented, but which is chaired by the private sector.

DECLASSIFIED

- It was noted by the evaluation team that there are some difficulties relating to establishing public-private partnership in specific areas. Gathering information from the financial institutions and the data request procedure to execute it is long and complicated. There are no clear or mandatory reporting obligations for the private sector in general, which leaves the decision whether or not to investigate/prosecute a crime partly in the hands of private industry. In the opinion of the evaluators, it would be useful to strengthen cooperation between the police and the financial sector with regard to certain cases for mandatory reporting**.**

- It is thought that the 24/7 contact point could be significantly improved by more resources, to tackle the massive increase of information traffic.

DECLASSIFIED

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

5.1.1. Council of Europe Convention on Cybercrime

The Convention on Cybercrime (CETS No 185) was subject to the ratification process via Criminal Law Amendment Act 2002, Federal Law Gazette I No 134/2002.

5.1.2. Description of national legislation

A/ Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems

Framework Decision 2005/222/JHA on attacks against information systems has been incorporated into Austrian law via Criminal Law Amendment Act 2008, Federal Law Gazette I No 109/2007. The provisions of the Criminal Law Amendment Act 2015 that entered into force on 1 January 2016 transpose Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

There is extensive legislation in place in Austrian law regarding cybercrime[8]. The following acts are criminalised in the Austrian Criminal Code (CC): illegal access to information system (Article 118a), illegal system interference/illegal data interference (Article 126a - 126b), illegal interception of computer data (Article 119a), misuse of devices - production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools (Article 126c), fraudulent misuse of data processing (Article 148a), falsification of data (Article 225a), breach of telecommunications secrecy (Section 119 StGB).

DECLASSIFIED

[8] Due to the large number of pages involved, its description has not been included in the report. For more information see Annex D.

Illegal access to information system (Section 118a of the Criminal Code) and illegal interception of computer data (Section 119a of the Criminal Code) are prosecuted only with the consent of the aggrieved party.

Sending or controlling the sending of spam is not defined specifically as an offence.

The criminal law powers laid down in Federal Law Gazette I No 108/2010 provided for a reorganisation and a tightening-up of provisions regarding property law measures in order to enable the State to recover (large amounts of) illicit proceeds more effectively, particularly where organised crime is involved.

The law stipulates that attempts are punishable as regards these offences. Incitement, aiding and abetting are also criminalised under Austrian law. The criminal liability of legal entities is laid down in the *Verbandsverantwortlichkeitsgesetz* (Corporate Criminal Liability Act). Legal persons may be held criminally liable for offences committed by individuals in management positions (decision-makers) or by individuals under their authority (employees). However, in the latter case, they may be held liable only if they failed to provide sufficient supervision or control. In order for a legal person to be held liable for a criminal offence, the offence must have been committed for its benefit or in breach of its duties. If the constituent elements described are present, it is therefore also possible for legal persons to be held criminally liable for cybercrime. The penalty imposed generally takes the form of a fine, which is calculated by multiplying the number of daily rates imposed (from 40 to 180) by the amount of the applicable daily rate (calculated on the basis of revenue).

Moreover, the offences 'damage to data' and 'disruption of the operational capacity of a computer system' will in future comprise aggravated offences of causing serious damage or damage to the essential components of critical infrastructure. The use of several computer systems ('botnets') to commit a criminal offence is under consideration by the Austrian authorities. The law is also intended to penalise new manifestations of computer crime hitherto not fully covered by criminal law (e.g. payment card fraud involving 'phishing' and 'skimming' - Section 241h Criminal Code). Further legislative steps are not envisaged at present.

DECLASSIFIED

B/ Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography

Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA; Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA; the recommendations of the Council of Europe's GRETA experts group concerning the transposition of the Council of Europe Convention on action against trafficking in human beings and those of the UN Committee on the Rights of the Child in regard to the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography have been transposed into substantive law by the Criminal Law (Sex Offences) Amendment Act 2013, Federal Law Gazette I No 116/2013.

As regards the Internet, aggravated offences have been included under 'pornographic representations of minors' and a new offence of 'grooming' has been introduced.
Currently computer-related production, distribution or possession of child pornography (Article 207a), computer-related solicitation or 'grooming' of children (Section 208a of the Criminal Code 'Sexual grooming of persons aged under 14') are criminalised (please refer to Annex D).

C/ Online card fraud

Austrian law counters any fraudulent financial operations made online. In accordance with Article 241h of the CC (Reconnaissance of data of non-cash means of payment) the following actions are punishable:
§ 241h. (1) Any person who reconnoitres data of non-cash means of payment with the intention that

1. The person or a third person gains an undue advantage from their use in legal dealings, or
2. To enable himself, herself, or another to counterfeit non-cash means of payment (§ 241)

is liable to imprisonment for up to one year or a fine not exceeding 720 penalty units.

DECLASSIFIED

(2) Any person who commits the offence commercially or as a member of a criminal association is liable to imprisonment for up to three years.
(3) The person is not liable if the person freely and before the data within the meaning of para. 1 subparas. 1 or 2 are used eliminates the risk of their use by alerting the authorities, the rightful user, or in any other way. A person is not liable if there is no risk that data be used or if that risk has been eliminated without the person's involvement, but if the person unaware of these circumstances freely and genuinely endeavours to eliminate these risks.

5.2. Procedural issues

5.2.1. Investigative Techniques

The following investigative measures may be applicable under the Austrian law:

Confiscation (Section 115 StPO - general rules, no special reference to computer data, hence also applicable to computers, servers and all forms of data media):
Section 115(1) Confiscation shall be permitted if it is likely that the items seized

1. will be required as evidence in subsequent proceedings;
2. are subject to private-law claims; or
3. will be needed to secure a judicial decision on the confiscation of instrumentalities and proceeds [*Konfiskation*] (Section 19a StGB), on forfeiture (Section 20 StGB), on extended forfeiture (Section 26 StGB), on removal (Section 26 StGB) or on any other property-related order provided for by law whose execution would otherwise be endangered or made considerably more difficult.

DECLASSIFIED

The court must decide on confiscation without delay, on application of the public prosecutor's office or of a person affected by the seizure. Confiscation shall be limited to records and copies listed there, as required. In a decision permitting confiscation in order to secure a judicial decision on forfeiture (Section 20 StGB) or extended forfeiture (Section 20b StGB) an amount of money has to be determined that covers the assets to be declared forfeit. If, or as soon as, the conditions for confiscation do not exist or no longer exist or an amount of money as referred to in paragraph 5 is deposited, the public prosecutor's office or, after charges have been brought, the court, must terminate the confiscation.

Search (Sections 119 to 122 StPO - general rules, no special reference to computer data):

Section 117(2) 'Searches of places and objects' the searching

a. of a parcel of land, a space, a vehicle or a container that is not generally accessible;

b. of a dwelling or another place protected by domiciliary rights and of the objects therein;

Searches of places and objects and of persons

Section 119(1) Searches of places and objects (point 2 of Section 117) shall be permitted if certain facts give reason to believe that a person suspected of a criminal offence is hiding there or that there is evidential material there to be seized or analysed.

(2) Search of a person (point 3 of Section 117) shall be permitted if the person

1. was arrested or caught in the act;

2. is suspected of a criminal offence or certain facts give reason to believe that they have items subject to seizure with them or bear traces;

3. might have suffered injuries or experienced other bodily changes as a result of a criminal offence that need to be verified for the purpose of criminal proceedings.

Section 120(1) Searches of places and objects pursuant to point 2.b of Section 117 and of persons pursuant to point 3.b of Section 117 must be ordered by the public prosecutor's office on the basis of a court authorisation; if delay poses a threat, however, the criminal investigation department shall be entitled to undertake these searches provisionally without an order or an authorisation. The same shall apply in the cases mentioned in point 1 of Section 170(1) to searches of persons pursuant to point 3.b of Section 117. However, the victim may under no circumstances be compelled to undergo a search against his or her will (point 3 of Section 119(2) and Section 121(1), last sentence).

DECLASSIFIED

(2) Searches pursuant to point 2.a and point 3 of Section 117 may be carried out by the criminal investigation department on its own initiative.

Section 121(1) Before any search the person concerned, having been informed of the reasons for the search, must be requested to permit it or to voluntarily surrender the items sought. This requirement may be waived only if delay poses a threat and under point 1 of Section 119(2). The use of coercion (Section 93) in the case of a search of a person pursuant to point 3 of Section 119(2) shall be unlawful.

(2) The person concerned shall have the right to be present during a search pursuant to point 2 of Section 117 and to bring in a person whom he or she trusts during such a search or a search pursuant to point 3.b of Section 117; in such cases Section 160(2) shall apply mutatis mutandis. If the owner of the dwelling is absent, an adult person living there may exercise his rights. If that too is impossible, two trustworthy, uninvolved persons must be brought in.

This requirement may be disregarded only if delay poses a threat. In the case of a search of premises used solely for professional purposes by persons as referred to in points 2 to 4 of Section 157(1) a representative of the respective professional association and/or the media owner or a representative identified by the latter must be brought in ex officio.

(3) When a search is conducted, visibility, inconvenience and disturbance must be reduced to a minimum. Property and personality rights of all persons concerned must be protected as far as possible. A search of persons pursuant to point 3.b of Section 117 must in all cases be carried out by a person of the same gender or by a doctor with regard for the dignity of the person to be examined.

Section 122(1) The criminal investigation department must report to the public prosecutor's office as soon as possible (point 2 of Section 100(2)) on every search pursuant to the second half of the first sentence of Section 120(1). The public prosecutor's office must apply retrospectively for a court decision on the admissibility of the search (Section 99(3)). If authorisation is not granted, the public prosecutor's office and the criminal investigation department must use the legal means at their disposal to restore the legal situation in accordance with the court decision.

DECLASSIFIED

(2) If items are found during a search which point to the commission of an offence other than that which is the reason for carrying out the search, they must be seized; however, they must be the subject of a special report and the public prosecutor's office immediately notified.
(3) In any event the person concerned must be issued or served with, immediately or at the latest within 24 hours, a confirmation of the search and its outcome and, if applicable, the order from the public prosecutor's office together with the judicial decision.

Seizure (Sections 110 to 114 StPO - general rules, no special reference to computer data; therefore also applicable to computers, servers and all forms of data media):
Section 110(1) Seizure is permissible where it appears necessary
1. for evidential reasons,
2. to secure private-law claims, or
3. to secure confiscation of instrumentalities and proceeds (Section 19a StGB), forfeiture (Section 20 StGB), extended forfeiture (Section 20b StGB), removal (Section 26 StGB) or another property-related order provided for by law.

(2) Seizure must be ordered by the public prosecutor's office and carried out by the criminal investigation department.
(3) The criminal investigation department shall be authorised to seize items (point 1.a of Section 109) on its own initiative
1. if
   (a) the items are not subject to anyone's power of disposal,
   (b) the victim was deprived of the items as a result of the offence,
   (c) the items were found at the scene of the crime and may have been used or intended to be used in commission of the criminal act, or
   (d) the items are of low value or can easily be replaced temporarily,
2. if possession of the items is subject to a general prohibition (Section 445a(1)),

DECLASSIFIED

3. that are found in the course of a search pursuant to Section 120(2), or that are discovered on a person who has been arrested for the reason referred to in point 1 of Section 170(1), or that are found in the course of a search of that person pursuant to Section 120(1), second sentence, or

4. in the cases referred to in Article 18 of Regulation (EU) No 608/2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003, OJ L 181, 29.6.2013, p. 15.

(4) The seizure of items for evidential reasons (point 1 of subsection (1)) is not permissible, and must in any case be revoked at the request of the person concerned, to the extent that and as soon as the evidential purpose can be attained by means of video, audio or other recordings, or by copies of written records or electronically processed data, and it can be assumed that there will be no need for the seized items themselves or the originals of the seized information to be inspected during the main proceedings.

Section 111(1) Anyone who has the power of disposal over items or assets that are to be seized is obliged (Section 93(2)) to surrender them to the criminal investigation department on request or otherwise enable them to be seized. Where necessary, this obligation can also be enforced by means of a search of persons or dwellings; in such a case, Sections 119 to 122 shall be applied mutatis mutandis.

(2) Where information recorded on data media is to be seized, every person is required to grant access to that information and, when requested, must hand over an electronic data medium in a widely-used file format or have one made. Furthermore, that person must permit the making of a back-up copy of the information that is recorded on the data media.

(3) Persons who are not themselves suspected of having committed the offence shall, at their request, have their reasonable costs reimbursed at a customary local rate where these have necessarily been incurred by them as a result of having documents or other evidentiary items detached from others or as a result of the handing over of copies.

DECLASSIFIED

(4) In any event the person concerned by the seizure must be issued or served with confirmation of the seizure immediately or at the latest within 24 hours and be informed about the right to object (Section 106) and to request a judicial decision on the revocation or continuation of seizure (Section 115). In the event of a seizure to secure a decision on private-law claims (point 2 of Section 110(1)), the victim shall, where possible, also be informed.

Section 112 (1) If the person concerned or present, even if he himself is suspected of having committed the offence, opposes the seizure of written records or data media by invoking a legally recognised right to remain silent that may not be circumvented by seizure on pain of nullity, the documents in question must be protected by appropriate means from unauthorised inspection or alteration and deposited with the court. If requested by the person concerned, however, the items must be deposited with the public prosecutor's office, where they must be stored separately from the investigation file. In either case, the documents may not be inspected by the public prosecutor's office or the criminal investigation department until a decision on inspection has been taken pursuant to the following subsections.

(2) The person concerned must be requested to indicate specifically, within an appropriate time limit of not less than 14 days, those parts of the records or data media the disclosure of which would constitute a circumvention of his silence; for this purpose he is entitled to inspect the deposited documents. If the person concerned fails to make such an indication, the documents shall be added to the file and evaluated. In all other cases, the court or, in the event of a request pursuant to the penultimate sentence of subsection (1), the public prosecutor's office, in consultation with the person concerned and, if necessary, suitable assistants or an expert, shall examine the documents and order whether and to what extent they may be added to the file. Documents which are not added to the file shall be handed over to the person concerned. Should the seizure be otherwise declared null and void, information gained from the examination of the latter items may not be used for further investigations or as evidence.

DECLASSIFIED

(3) The person concerned may file an objection against the order of the public prosecutor's office, in which case the documents are to be submitted to the court, which shall decide whether and to what extent they may be added to the file; the last sentence of subsection 2 shall apply. An appeal against the decision of the court shall have suspensory effect.

Section 113(1) Seizure shall end

1. when the criminal investigation department revokes it (subsection 2),
2. when the public prosecutor's office orders its revocation (subsection 3),
3. when the court orders confiscation.

(2) The criminal investigation department must report any seizure to the public prosecutor's office without delay and at the latest within 14 days (point 2 of Section 100(2)), unless it has previously revoked a seizure pursuant to Section 110(3) on the grounds that the conditions were not or no longer fulfilled. This report can, however, be combined with the one immediately following it, if this does not prejudice any significant interests of the proceedings or of persons, and if the items seized are of low value, are not subject to anyone's power of disposal, or possession thereof is subject to a general prohibition (Section 445a(1)). In the case described in point 4 of Section 110(3), the criminal investigation department shall act in accordance with the provisions of Sections 3, 4 and 6 of the Act on Product Piracy 2004, Federal Law Gazette I, No 56/2004.

(3) The public prosecutor's office must, in the case of a seizure pursuant to point 1.b of Section 109, immediately apply to the court for confiscation or, if the conditions for this are not fulfilled or are no longer fulfilled, order revocation of the seizure.

(4) In the case of seizure of items (point 1.a of Section 109), confiscation shall not take place even on application if the seizure relates to items within the meaning of point 1.a and d or point 2 of Section 110(3), or if the safeguarding purpose can be achieved by means of other measures of the public authorities. In these cases, the public prosecutor's office shall make the necessary orders concerning the seized items and their continued safekeeping and, if appropriate, revoke the seizure.

Until the report is made concerning seizure (Section 113(2)), the criminal investigation department shall see to the safekeeping of seized items, and thereafter the public prosecutor's office (Section 114 (1)).

DECLASSIFIED

Disclosure of data concerning transmission of communications (pursuant to point 2 of Section 134 StPO, this includes the disclosure of information on traffic data (point 4 of Section 92(3) of the Telecommunications Act (TKG)), on access data (point 4a of Section 92(3) TKG) not subject to an order pursuant to section 76a(2), and on location data (point 6 of Section 92(3) TKG) of a telecommunications service or an information society service (point 2 of Section 1(1) of the Notification Act) is permissible under Section 135(2) StPO,

1. where and for as long as a strong suspicion exists that a person concerned by the disclosure has kidnapped a person or otherwise taken a person under his control, and the disclosure is limited to data concerning a communication which it can be assumed is being transmitted, received or sent by the suspect during the deprivation of liberty,
2. if it can be expected that this will contribute to clarifying the facts of a criminal offence committed with intent that is punishable by a term of imprisonment of more than six months and the owner of the technical device to or from which the communication was or will be transmitted has given their express consent to the disclosure, or
3. if it can be expected that this will contribute to the clarification of the facts of a criminal offence committed with intent that is punishable by a term of imprisonment of more than one year, and if it can be assumed on the basis of certain facts that the suspect's data can thereby be determined.
4. if it can be expected, on the basis of certain facts, that the location of a fugitive or absent suspect who is strongly suspected of having committed, with intent, a criminal act punishable by a term of imprisonment of more than one year, can thereby be determined.

Surveillance of communications (defined in point 3 of Section 134 of the Code of Criminal Procedure as the investigation of the content of communications (point 7 of Section 92(3) TKG) exchanged or conveyed via a communications network (point 11 of Section 3 TKG) or an information society service (point 2 of Section 1(1) of the Notification Act)) is permissible under Section 135(3) StPO:

DECLASSIFIED

1. in the cases referred to in point 1 of Section 135(2),

2. in the cases referred to in point 2 of Section 135(2), provided that the owner of the technical device to or from which the communications were or will be transmitted gives their consent to the surveillance,

3. if such surveillance appears to be necessary to clarify the facts of a criminal offence committed with intent that is punishable by a term of imprisonment of more than one year, or if the investigation or prevention of criminal acts committed or planned in the context of a criminal or terrorist association or a criminal organisation (Sections 278 to 278b StGB) would otherwise be significantly impeded, and

(a) the owner of the technical device to or from which the communications were or will be transmitted is strongly suspected of the criminal offence committed with intent that is punishable by a term of imprisonment of more than one year or of an offence under Sections 278 to 278b StGB, or

(b) certain facts give reason to believe that a person strongly suspected of the offence (point (a)) will use or establish a connection with the technical device;

'**Communication**', within the meaning of point 7 of Section 92(3) TKG 2003, means any information exchanged or conveyed between a finite number of parties by means of a publicly available communications service. This does not include any information conveyed as part of a broadcasting service to the public over a communications network, except to the extent that the information can be related to the identifiable subscriber or user receiving the information (see 'content data' immediately below).

DECLASSIFIED

In principle, investigations are conducted on the instructions of the public prosecutor's office, as defined by the Code of Criminal Procedure, or in accordance with the Security Police Act.
Techniques: Identifying IP addresses, monitoring communications, analysing electronic evidence, rigorously tracking money trails via the Internet for fraud offences. Special forensic analysis software may be used in house searches and the seizure of data. This allows data to be made visible and the committed offence to be proved and brought before a court. However, data traffic retention is possible for the period of 3 months by providers e.g. for billing purposes.

The competent public prosecutors mentioned the following most frequently used investigative techniques:

- Disclosure of master data and access data;
- Disclosure of bank accounts and banking transactions;
- Disclosure of data concerning transmission of communications;
- Initiation of foreign correspondence by the police;
- Mutual legal assistance (MLA) requests;
- Seizure and analysis of data carriers by police officers and experts;
- Electronic data comparison (computerised profile searches).

The following technique has proved effective in investigating fraud: Identifying and monitoring communication channels as far as possible while rigorously tracking money trails. Where there are concrete leads, setting up teams comprised of IT specialists, analysts and experienced fraud investigators.

DECLASSIFIED

5.2.2. Forensics and Encryption

The Austrian authorities reported that encryption remains an unresolved issue in the context of server surveillance. Experts have repeatedly pointed out that decryption is very labour-intensive and, even where possible, would probably take several years. The cooperation of the data subject (the person under investigation) has thus far been indispensable. Encryption is a growing problem for forensic data backup.

The following problems have been encountered with encryption:

All or part of a data medium has been encrypted by the data subjects. In most such cases the data subjects are unwilling to cooperate with the authorities, which means that the data cannot be decrypted. The usual result of this is that only encrypted data can be secured, meaning ultimately that no analysis can be carried out on them. Even if the key has been disclosed or is otherwise known, more often than not it is not possible to make a physical copy of the data medium, which means that empty sectors may not be adequately secured. As regards the transmission of data to the authorities competent in this area, data volumes remain a major problem, given the resources required for data storage.

On the other hand, some success has been achieved in areas in which very simple encryption methods are used, and it has been possible to ascertain or back-calculate keys using appropriate software. Simple passwords can be 'cracked' using the appropriate hardware and tools.

DECLASSIFIED

According to the Austrian authorities, cooperation between the various authorities is indispensable since not every department or authority can afford to purchase password recovery hardware and software due to the costs resulting therefrom. Dividing responsibilities between authorities allows savings to be made and also opens up more possibilities in this area. Austria's specialist centre is in the Criminal Intelligence Service with its Cybercrime Competence Centre (C4). However, there are also special departments within the Ministry of Defence which are competent in this field. Services such as Europol and Interpol generally also serve as competent contact points in this area. For legal reasons, private companies intervene only on the instructions of the public prosecutor's office.

5.2.3. e-Evidence

No specific definition exists under Austrian law for e-evidence and there are no specific rules for its classification. E-evidence is generally secured as a support service for the investigating units within the framework of the Code of Criminal Procedure. All electronic data which could be relevant in the context of judicial investigations are considered e-evidence. E-evidence is stored only on the instructions of the public prosecutor's office. If such an instruction is given, the data is backed up and analysed in accordance with international standards. The results are transmitted to the department in charge of the investigation, which is then responsible for forwarding them to the public prosecutor's office.

There are no specific admissibility rules for e-evidence. It is therefore fully admissible and subject to the free assessment of evidence. The admissibility rules are no different if e-evidence is obtained in a different country.

DECLASSIFIED

5.3. Protection of Human Rights/Fundamental Freedoms

All coercive investigative measures involve a restriction of the fundamental rights and freedoms of those concerned by them. Therefore, the Austrian authorities indicated that implementing such measures is necessary to respect the requirement of proportionality, the right to a hearing, the right of defence, the presumption of innocence, and the requirement to provide a decision within a reasonable time. The principles of orality, publicity, immediacy and *in dubio pro reo* must also be respected. No one can be tried again for the same offence, and law enforcement authorities are required to be objective. An effective, wide-ranging legal protection system is in place to ensure that these principles are complied with (citations taken from the StPO [Code of Criminal Procedure]):

Objectivity and establishment of the truth

The criminal investigation department, the public prosecutor's office and the court shall be required to establish the truth and to elucidate all the facts relevant to the judgment of the offence and the person under investigation. All judges, public prosecutors and criminal police bodies shall be required to carry out their duties impartially and with an open mind, and to avoid any semblance of bias. They must devote the same care to investigating circumstances that incriminate and exonerate the person under investigation (Section 3).

DECLASSIFIED

Legality and proportionality

In the exercise of their powers and when gathering evidence, the criminal investigation department, the public prosecutor's office and the court may interfere with the rights of persons only to the extent that is expressly laid down by law and is necessary to perform their tasks. Any restriction of legal rights brought about by this must be proportionate to the gravity of the offence, the degree of suspicion and the intended outcome. Where several suitable investigative acts and coercive measures are available, the criminal investigation department, the public prosecutor's office and the court shall be required to use those which interfere least with the rights of those concerned. Legal powers shall, at every stage of the proceedings, be exercised in a manner that avoids attracting unnecessary attention, upholds the dignity of the persons concerned and protects their rights and legitimate interests. It shall not be permitted to incite suspects or other persons to commit, continue or complete an offence, nor shall it be permitted to use an undercover agent to induce a confession (Section 5).

Right to a hearing

The person under investigation shall have the right to participate in all stages of the proceedings, and shall be obliged to be present at the main trial. The person under investigation shall be treated with respect for his personal dignity. Any person involved in proceedings or subject to coercive measures shall have the right to an adequate hearing and to be informed of the reason for and the purpose of the proceedings in which he is involved, and of his fundamental rights in the proceedings. The person under investigation shall have the right to be informed of all the grounds for suspicion, and to be given full opportunity to eliminate those grounds and to defend himself (Section 6).

DECLASSIFIED

Right of defence

The person under investigation shall have the right to defend himself and, at any time during the proceedings, to enlist legal counsel. The person under investigation may not be compelled to incriminate himself. He shall be free to testify or to remain silent at any time. He may not be compelled or induced to make a statement by coercive measures, threats, promises or false representation (Section 7).

Presumption of innocence

Every person shall be presumed innocent until convicted by a final judgment (Section 8).

Requirement to proceed with due dispatch

Every person under investigation shall be entitled to see proceedings completed within a reasonable time. The proceedings shall in all cases be conducted swiftly and without undue delay. Proceedings during which a person under investigation is held in custody shall be conducted with particular dispatch. Every person under investigation held in custody shall be entitled to the earliest possible delivery of judgment or to release during the proceedings. All authorities, institutions and persons active in criminal proceedings shall be required to ensure that detention is as brief as possible (Section 9).

Orality and publicity

Judicial proceedings in the main trial and the appeal shall be conducted orally and publicly. The investigation shall not be public. When giving judgment, the court must confine its considerations to what took place in the main proceedings (Section 12).

DECLASSIFIED

Immediacy

The main proceedings shall form the focal point of the trial. The evidence that forms the basis for delivering the judgment must be taken at this stage. The evidence that is essential for bringing charges must be taken during the investigation, as well as any evidence which it will probably not be possible to take in the main proceedings for reasons of fact or law. Where evidence can be taken directly, it may not be replaced by indirect evidence. The content of dossiers and other written documents may be used as evidence only insofar as it is reproduced in a manner permitted pursuant to this law (Section 13).

Free assessment of evidence

The court must decide on the evidence, on the basis of its freely formed opinion, whether the facts are proven; in case of doubt, it must always rule in favour of the accused or otherwise aggrieved party (Section 14).

Ne bis in idem

Once criminal proceedings have been finally concluded, the same suspect may not be prosecuted again for the same offence. This shall be without prejudice to the provisions on the continuation, resumption, reinstitution and renewal of criminal proceedings and on actions for annulment to uphold the law (Section 17).

DECLASSIFIED

5.4. Jurisdiction

5.4.1. Principles applied to the investigation of cybercrime

Austrian criminal law applies to all offences committed in Austria.
For offences committed abroad (other than those described in Sections 63 and 64) provided that these offences are also punishable under the law of the place where the offence was committed, Austrian criminal law applies, if:

1. the offender was Austrian at the time of the offence or subsequently acquired Austrian citizenship and still holds it when the criminal prosecution commences;
2. the offender was a foreign national at the time of the offence, is apprehended in Austria and cannot be extradited to a foreign country for a reason other than the type or nature of the offence.

The offender shall be deemed to have committed a punishable act at the time that he or she acted or should have acted. The time when the result occurs is irrelevant. The offender shall be deemed to have committed a punishable act in every place where he or she acted or should have acted or in which a result corresponding to the offence occurred in whole or in part or should have occurred according to the intention of the offender.

5.4.2. Rules in case of conflicts of jurisdiction and referral to Eurojust

Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings was transposed by Austria through Sections 59a to 59c of the Federal Law on Judicial Cooperation in Criminal Matters with the Member States of the European Union (EU-JZG).

DECLASSIFIED

Austria does not have any practical experience with conflicts of jurisdiction in criminal cases involving cybercrime, though the Austrian law enforcement authorities also use the instrument for the transfer of criminal proceedings for cybercrime offences if the suspect permanently resides abroad and criminal proceedings may be conducted more effectively there. If criminal proceedings are taken over by the requested State, the proceedings in Austria are suspended until the outcome is communicated. If a final conviction is delivered abroad, the proceedings in Austria must be discontinued if the punishment has been executed in full or has been remitted (Section 74(4) Extradition and Mutual Assistance Act (ARHG)).

5.4.3. Jurisdiction for acts of cybercrime committed in the 'cloud'

A corresponding link has to be found to access data in the 'cloud'. During seizures, links have in fact been found to such stored data (Dropbox, Sendspace, etc.), which are then downloaded and backed up accordingly. However, an order from the public prosecutor's office is always required. Problems arise in practice because such data are password-protected or even encrypted. In such cases it is not possible to obtain access without the cooperation of the data subject.

A further problem is that the MLA process is subject to long waiting times. Data stored in the 'cloud' consistently cause problems. Depending on the volume of data and the transfer rate, it is not always possible to perform a full forensic backup of the cloud memory. Furthermore, remote data storage can usually only be accessed logically. This makes it virtually impossible to physically back up the data, which means empty sectors or similar cannot be included in a backup. The time factor of analyses consistently poses a major problem. Usually the validity of the data sought is much shorter than the time it takes to find them. In malware analysis in particular this consistently poses a problem. The data volumes in this area are also becoming increasingly problematic. Data volumes in the realm of terabytes entail long analysis periods, which again ultimately affects the timeliness of the data. Hidden services on the darknet consistently cause problems during prosecution, because the technical possibilities usually cannot be used due to the legal framework conditions.

DECLASSIFIED

5.4.4. Austrian perception of the legal framework to combat cybercrime

The Austrian authorities pointed out that the Internet is a very fast-moving medium, which requires swift reactions by the police. However, existing legal rules mean that in the vast majority of cases users can only be identified through MLA requests. The time taken to complete such MLA requests leads to delays that are often a decisive factor in whether a crime is solved. In addition, national and international investigations lead to negative outcomes due to the lack of retention obligations (data retention). Basic information about IP addresses and data subjects, such as an excerpt from the header protocol, need to be made available through fast-track international information exchange (administrative assistance). Unfortunately such matters are often referred to the legal assistance channel.

5.5. Conclusions

- Austria has ratified the Budapest Convention. Council Framework Decision 2005/222/JHA on attacks against information systems has been transposed into Austrian law. Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA has been transposed by the Criminal Law Amendment Act 2015. The offences provided for both in the Convention and the European legislation exist in the national legislation.

- Illegal access to information system (Section 118a of the Criminal Code) and the illegal interception of computer data (Section 119a of the Criminal Code) are prosecuted only with the consent of the aggrieved party. Although these are common requirements, not unique to the legal background of Austria, it was the understanding of the evaluation team that this requirement can cause difficulties in cybercrime cases, as the number of the possible victims appearing in a single case during mass data leaks or other big volume incidents tends to be high and it can cause an administrative difficulty for the investigation.

DECLASSIFIED

- Austria amended the criminal and procedural laws in criminal matters focusing on cybercrime, introducing penalties and explicitly naming the different types of criminal behaviour in cybercrime. Before this change cybercrime was subsumed under the general fraud section. Austria now has special sections in the criminal law with regard to cybercrime and special sections in the criminal procedural law regulating investigative measures in the field of cybercrime for the purpose of gathering information and evidence from ISPs. As a result, Austria has brought in the criminal regulations clarifying competences among those empowered to carry out investigations and the investigative measures.

- Directive 2011/92/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography has been implemented. Combating credit card fraud is provided for in the Criminal Code but it is also based on cooperation with the private sector.

- Private industry in Austria is not under any obligation to retain and furnish data material for policing purposes. This is worrying, given the potential to save lives or prevent torture (child sex abuse), which are absolute rights under Articles 2 and 3 of the European Convention on Human Rights - unlike the right to privacy which is a qualified right under Article 8 of the said Convention.

- Telecommunication data is retained by providers, e.g. for billing purposes for a period of three months. The lack of any European instrument regulating this issue after invalidation of Directive 2006/24/EC seems to be a problem across the EU. In the evaluators' view, it may have an impact on criminal investigations and Austria is not an exception. It is clear that this is a fracturing issue among civil society, where for historical reasons there is still strong opposition to data traffic access by police and other authorities. Nonetheless, it could be useful if more debate among civil society was launched so that data traffic could be perceived as a need both for the Austrian authorities and also to help other countries' investigations in the global fight against cybercrime.

DECLASSIFIED

- The Austrian prosecutors indicated that whilst they had not previously dealt with the bit-coin issue, they felt their legislation allowed for the search and seizure of bit-coin as an asset.

- E-evidence is not defined by the national legislation, with the result that the general provisions are applicable to this kind of evidence as well. Encryption is considered a challenge and is perceived as an unresolved issue in the context of server surveillance. Moreover, experts met repeatedly pointed out that decryption was very labour-intensive and, even where possible, would probably take several years. The cooperation of the data subject (the person under investigation) has thus far been indispensable. Encryption is a growing problem for forensic data backup. The evaluation team was informed that there were no legal provisions to give criminal investigators access to advanced evidence acquisition such as remote forensics.

- There are no special provisions in Austrian jurisdiction concerning cybercrime. Should conflicts of jurisdiction occur, provisions transposed to the Austrian law based on Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings would apply.

DECLASSIFIED

6. OPERATIONAL ASPECTS

6.1. Cyber attacks

6.1.1. Nature of cyber attacks

The nature and number of cyber attacks are given in the following statistics:

Reported cases	2013	2014	Deviation
cybercrime *sensu stricto*	1 737	1 754	1.0 %
cybercrime *sensu largo*	8 314	7 212	-13.3 %
cybercrime in total	10 051	8 966	-10. 8%

Cleared cases	2013	2014	Deviation
cybercrime *sensu stricto*	310	316	1.9 %
cybercrime *sensu largo*	4 234	3 344	-21.0 %
cybercrime in total	4 544	3 660	-19.5 %

Clearance rate	2013	2014	Deviation
cybercrime *sensu stricto*	17.8 %	18.0 %	0.2
cybercrime *sensu largo*	50.9 %	46.4 %	-4.6
cybercrime in total	45.2 %	40.8 %	-4.4

Identified suspects	2013	2014	Deviation
cybercrime *sensu stricto*	334	326	-2.4 %
cybercrime *sensu largo*	3 621	3 278	-9.5 %
cybercrime in total	3 955	3 604	-8.9 %

DECLASSIFIED

6.1.2. Mechanism to respond to cyber attacks

Austria is in the process of building up its cyber resilience. As part of the implementation of the Austrian Cyber Security Strategy, a 'cyber crisis mechanism' (CKM) is being set up, which will be integrated into the National Crisis and Disaster Protection Mechanism (SKKM).

Austria claims to have an efficient infrastructure that can provide a high level of security as regards the supply of food, transport services, telecommunications services, energy and financial services, in addition to the secure provision of social and healthcare services. Both the public services provided to citizens and the attractiveness of Austria as a business location rely on the permanent availability and smooth functioning of a variety of infrastructure systems. The proper functioning of infrastructure systems is therefore increasingly important.

For this purpose the Federal Government adopted on 4 November 2014 a new master plan based on the 2008 programme for the protection of critical infrastructure. The 2014 Austrian Programme for Critical Infrastructure Protection (the APCIP master plan) details the work which has already been completed and further develops the previous master plan on the basis of lessons learned in recent years. It was drawn up jointly by the Criminal Intelligence Service and the Federal Ministry of the Interior, and agreed with the relevant departments, the Länder and professional associations and selected strategic companies. The APCIP master plan is founded on the principles of cooperation, subsidiarity, complementarity, confidentiality and proportionality and is based on an all-hazards approach. The main focus of the plan is on helping strategic companies to develop a comprehensive security architecture (risk management, business continuity management and safety management), so as to reinforce Austria's resilience and security. Operators of critical infrastructure are also encouraged to ensure that their facilities remain state-of-the-art as regards cyber security.

DECLASSIFIED

The national programme for critical infrastructure protection (based on the European programme for critical infrastructure protection (EPCIP)) requires operators of strategic infrastructure to put in place sufficient and appropriate safeguards in cooperation with the authorities. This cooperation takes the form of a public-private partnership, with no legal obligations. With the exception of possible certifications such as ISO 27001, there are also no generally applicable rules for all critical infrastructure sectors. One problem is the inability to analyse large volumes of data, apart from which there are the problems of lengthy procedures, different data retention periods, preserving evidence and limited knowledge, skills and/or capacity.

Basically there is no legal obligation to report alleged cyber attacks by critical infrastructure. As a consequence, service providers may be held liable only where the right-holder has drawn attention to the legal infringement and where the breach is also immediately apparent to a non-lawyer. The liability rules for Austrian providers are regulated in the E-Commerce Act (ECG) which is itself based on the provisions of Directive 2000/31/EC (the E-Commerce Directive). It gives the overall picture of situations where service providers are exempt from liability. This occurs in the following situations:

1) an access provider is not liable for the information transmitted across its networks provided that it has not initiated the transmission, and so has not decided itself that the transmission should be made (Section 13 of the ECG). The basic grounds for exempting the provider from liability are that the transmitted information has been provided by the user of the service, not by the provider;

2) a service provider that makes a search engine or other electronic tools available to users for the purposes of searching for external information is not responsible for the information that is requested provided that it does not initiate the transmission of the requested information, does not select the recipient of the requested information, and does not select or modify the requested information (Section 14 of the ECG);

DECLASSIFIED

3) a service provider that transmits in a communication network information provided by a recipient of the service is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the onward transmission of the information to other recipients of the service upon their request, provided that it does not modify the information; complies with conditions on access to the information; complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement (Section 15 of the ECG);

4) a hosting service provider is not liable if it stores illegal information entered by a user as long as it does not have actual knowledge of the illegal activity or information. Also, in respect of claims for damages, the provider must not be aware of any facts or circumstances that make the illegal activity or information clearly apparent. This exemption from liability applies only if a provider that becomes aware of illegal information takes immediate measures to remove the information or to block access to it (Section 16 of the ECG);

5) a service provider that uses an electronic link to provide access to external information is not responsible for that information provided that it does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent, or upon obtaining such knowledge or awareness, acts expeditiously to remove the electronic link (Section 17 of the ECG).

However, Austrian courts may rule on the (hosting service) provider's responsibility for disseminating any content that infringes personal rights and justifies a prohibitory injunction and an eliminatory injunction in civil proceedings. In such cases the hosting service provider must be aware of the content that is the subject of the alleged illegal behaviour, or be in breach of a duty to monitor it. However, the latter only applies to serious and blatant breaches.

DECLASSIFIED

The Austrian Supreme Court of Justice has ruled in two relatively recent decisions (4 Ob 71/14s and 4 Ob 22/15) that access providers must block access to websites whose main activity consists of disseminating illegal copies of copyright-protected material. These court decisions were taken in the light of a preliminary ruling by the European Court of Justice on Article 8(3) of Directive 2001/29/EC: the European Court of Justice ruled in its judgment on Case C-314/12, UPC Telekabel ('kino.to judgment'), that EU law requires access providers, in certain circumstances, to prevent their customers from accessing Internet services containing infringing content.

So far, all the providers have only implemented the required blocking measures after being obliged to do so through an interim injunction. The interim injunctions issued on the basis of the 'kino.to judgment' do not specify what type of blocking measure is to be used by the provider. The network blocking measures currently in use are DNS blocks. The Austrian authorities are in the process of analysing whether a DNS block is an adequate measure for preventing an access provider's customers from accessing infringing websites.

6.2. Actions against child pornography and sexual abuse online

6.2.1. Software databases identifying victims and measures to avoid re-victimisation

There are no software databases specifically designed to identify victims in Austria. Perpetrators and victims are identified using the ICSE (database operated by INTERPOL). Victim identification is also the subject of very close international cooperation. Austria is currently working with the German authorities on a national victim identification database.

Measures to prevent re-victimisation mainly take the form of guidance and counselling provided for victims by NGOs (e.g. Weißer Ring, etc.). And again, there is the 'Click & Check' project.

The Austrian legal process uses psychologists to execute the hearings of the witnesses/victims who are minors, while the suspect and the defence counsel are not present, yet they can continue the process of the hearing and initiate questions to the witness through the judge.

DECLASSIFIED

6.2.2. Measures to address sexual exploitation/abuse online, sexting, cyber bulling

On 1 January 2016 provisions of the Criminal Law Amendment Act 2015, Federal Law Gazette I No 112/2015, entered into force to establish 'Continued Harassment using Telecommunications or Computer Systems' including cyber bullying as a criminal offence as an unreasonable interference in another person's life and/or damaging another's reputation in the eyes of a large number of people or bringing to the notice of a large number of people facts or images of a highly personal nature without the permission of the person concerned).

As the law stands, the taking of naked photographs is not deemed to damage a person's reputation so cannot be subsumed under the definition of the offence of 'dangerous threat' pursuant to Section 107 of the Criminal Code. As regards the publication of naked photographs, according to the case-law there is deemed to be damage to reputation if the victim does not want them to be published and the threat is connected to refusing the victim due respectful treatment and so diminishing his or her public reputation. The definition of 'dangerous threat' was recently extended to include the threat of disclosing facts or of making available images of a highly personal nature in the following way:
Section 74(1) point 5: 'dangerous threat: threat of injury to body, freedom, reputation, property or highly personal private life by making available, disclosing or publishing facts or images in a way that is likely to cause the threatened person justified concerns considering the circumstances and his or her personal disposition or the seriousness of the threat, irrespective of whether that threat is directed against the threatened person, his or her family, or other persons under his or her protection or closely related to him or her.'

DECLASSIFIED

In addition, the Austrian Criminal Intelligence Service (.BK) and domestic Internet service providers cooperate closely. If one of those services is being misused, data are transferred promptly to the Criminal Intelligence Service, so that it can launch investigations to trace the suspects. The incriminating image or video material is removed by the respective providers after it has been seized.

In addition, close cooperation with the private hotline 'STOPLINE' has led to a marked decrease in Internet websites containing representations of child abuse.

6.2.3. Preventive actions against sex tourism, child pornographic performance and others

There are legislative measures in place which legislate against advertising abuse opportunities and child sex tourism include the following offences/rules of jurisdiction set out in the Criminal Code:

- Announcement provoking obscene behaviour (an announcement intended to provoke obscene behaviour which in terms of its content is likely to cause legitimate offence - Section 219)
- Incitement to commit punishable acts and endorsement of punishable acts (incitement to commit a punishable act using printed matter, a radio broadcast or otherwise via a medium that makes the message accessible to a mass audience - Section 282)

DECLASSIFIED

- Criminal offences abroad punished without regard for the laws of the State in which they were committed (Section 64), such as:

genital mutilation within the meaning of Section 90(3), kidnapping with extortion (Section 102), handing over a person to a foreign power (Section 103), slave-trading (Section 104), trafficking in human beings (Section 104a), extreme intimidation pursuant to point 3 of Section 106(1), prohibited adoption placement (Section 194), rape (Section 201), sexual assault (Section 202), sexual abuse of a defenceless or mentally impaired person (Section 205), serious sexual abuse of persons under 14 (Section 206), sexual abuse of persons under 14 (Section 207), pornographic representations of minors pursuant to Section 207a(1) and (2), sexual abuse of young persons (Section 207b), abuse of a position of authority pursuant to Section 212(1), procuring and facilitating pornographic presentations of minors (Section 215a), or cross-border trafficking of prostitutes (Section 207), if

a) the offender or the victim is Austrian or habitually resides in Austria;

b) other Austrian interests have been damaged by the offence; or

c) the offender was a foreign national at the time of the offence, resides in Austria and cannot be extradited.

Moreover, the child pornography hotline at the Austrian Criminal Intelligence Service was extended to cover child sex tourism so that indications are obtained on this kind of offence, and a BM.I liaison officer for South East Asia was posted to Bangkok.

The existing 'Click and Check' project, which has been rolled out to target the 12 to 14 age group in schools and youth facilities, highlights the dangers of cyber grooming and the preparation of criminal acts in chat rooms, social networks and fora. However, if providers offering pornographic presentations of children in real time are outside Austria, the national authorities cannot intervene.

As an example of preventive actions undertaken to prevent sex tourism, a hotline for child pornography and sex tourism has been set up, meldestelle@interpol.at

- developing information tools for children for safe use of Internet,
- developing information tools on harmful/illegal behaviour online.

DECLASSIFIED

Information folders are also produced, not only on special areas of criminal activity such as cyber grooming but also on other Internet dangers, with general tips for children, parents, teachers and attachment figures. The 'Click and Check' project also helps to raise awareness with regard to the Internet. Furthermore, in the context of prevention, particular attention is focused on the issue of 'sexting' and its attendant risks. NGOs operating in Austria have an important part to play in this area.

6.2.4. Actors and measures countering websites containing or disseminating child pornography

The provisions of Sections 13 to 17 of the federal law regulating certain legal aspects of e-commerce and e-justice (E-Commerce Act - ECG), Federal Law Gazette I No 152/2001, give rise to an obligation to delete illegal content from websites. The law makes no provision for access to particular websites to be blocked in general. Nevertheless, a ban on disseminating certain content on the Internet can be inferred from individual legal provisions, for example concerning the dissemination of pornographic representations of minors (Section 207a StGB), or from the National Socialism Prohibition Act 1947. In addition, in accordance with the case-law of the European Court of Justice on Article 8(3) of Directive 2001/29/EC (Case C-314/12, UPC Telekabel), right-holders have a civil-law right to demand that access providers deny their customers access to Internet services with content that structurally infringes copyright. Moreover, there is no legal basis to filter websites for child pornographic materials.

The public prosecutor's office (Section 110(3)) can order and execute the seizure of servers. The seized servers can be confiscated by the court on application by the public prosecutor's office (Sections 115 et seq. StPO).

DECLASSIFIED

Although there is no legal basis for blocking access to the Internet, the private sector is under obligation to remove the content in the following cases:

a) National procedure: if criminal proceedings are pending, the host or provider is called upon to remove the website with the harmful or illegal content from the Internet. In practice it is usually sufficient to make the provider aware of the fact that websites it maintains online infringe its own company guidelines/standards. It is noted by the evaluators that, if needed, a judicial order can also be used to force a provider to take websites down.

b) International procedure: criminal proceedings are necessary to apply for an MLA request and then notify the foreign provider via the competent judicial authorities abroad. There is no provision for direct coercive measures abroad; these may only be taken by the domestic judicial and security authorities in accordance with national legislation.

The Austrian Criminal Intelligence Service has a specialist division for combating child pornography in Unit 3.2.1 (violent crimes) of Sub-department 3.2. The division is currently composed of two investigators.

The ISPA operates Stopline, which is an Austrian hotline for combating child pornography and national socialism on the Internet. Stopline can be contacted by Internet users directly, anonymously and without bureaucratic formalities if they discover web pages that include the following content:

- child pornography within the meaning of Section 207a of the Austrian Criminal Code or
- national socialism within the meaning of the Austrian laws prohibiting national socialism and the wearing of associated regalia and symbols.

When Stopline receives a report, the staff check whether the material is actually illegal within the meaning of Austrian law. If so, the competent Austrian executive authority, the Austrian provider that is affected and the foreign partner hotlines within INHOPE, a network of hotlines dealing with illegal content online, are immediately informed so that the content can be removed as quickly as possible. In such cases, 90 % of the illegal content across Europe is removed within 72 hours.

DECLASSIFIED

6.3. Online card fraud

The Austrian authorities reported that citizens and private companies usually report online card fraud offences to LEAs and there is sufficient cooperation between the financial sector and LEAs to prevent and fight online card fraud.

However, the evaluation team observed that private industry in Austria does not have a mandatory reporting obligation. The Ministry of the Interior indicated that the Directive on security of network and information systems (the NIS Directive), adopted on 6 July 2016, will have an impact on the situation in Austria and certain bodies will have to report in the future under planned domestic legislation.

6.4. Conclusions

- The Cyber Security Centre (CSC) is currently being set up at the Federal Agency for State Protection and Counter Terrorism (BVT)/BMI. Its main objective is to increase resilience against cyber threats, both through operational coordination on cyber-security incidents (particularly in the critical infrastructure and public administration sectors) and through preventive measures (promotion and coordination of information exchange, awareness-raising measures, involvement in security research, technical analyses and situation reports).

- Austria has set up both a Cyber Crisis Management group which is a cross-organisational group that takes charge of any emergency cyber crisis that may arise for Austria.

DECLASSIFIED

- In general critical infrastructure entities are not legally obliged to report cybercrime attacks to the police. However, the evaluation team was informed that this will change once the NIS Directive is implemented. According to the evaluators, this situation calls for developments, as without a reporting obligation and trust in law enforcement, there is a real danger that most of the cases remain outside the notice of the authorities. This can cause not just a lack of proper law enforcement notification, but also a risk of misunderstanding at the strategic level as statistics may not cover certain incidents.

- In combating cybercrime, the priorities of the .BK/5.2 C4 - Cybercrime Competence Centre are guided by the strategic goals of the Austrian Criminal Intelligence Service (.BK) and comprise investigations into cybercrime offences, the preservation of digital forensic evidence and a cybercrime hotline for the public.

- The Austrian police have a specialised unit dealing with child pornography, which consists of two members. It also has a liaison officer in Bangkok for handling child sex tourism cases. Moreover, Austria is currently developing a common database with Germany on identifying the victims of child pornography. This service, which comes under the Federal Ministry of the Interior (BMI), takes part in the 'Don't look away!' campaign against tourism-related child sexual abuse, in which seven European countries (AT, CH, DE, FR, LU, NL, PL) are currently participating. This also involves conducting presentations and training courses for ACCOR hotel managers, among others.

- The Austrian legal system provides for use of psychologists to perform the hearings of witnesses/victims who are minors, while the suspect and the defence counsel are not present. The defence team can participate in the process of the hearing and initiate questions to the witness through the judge. According to the evaluators, this seems to be a well developed system to protect the interests of the victim and the right of the defendant at the same time.

DECLASSIFIED

- There is no general rule in criminal procedure allowing LEAs to block websites containing child pornography or national socialism or material infringing the rights of right-holders. In these cases there is a civil-law right to demand that access providers deny their customers access to services with infringing content.

- The public sector works together with NGOs such as saferinternet.at. This NGO has focused on fighting cyber mobbing, malware, fraud in the internet, spam, and data protection. This NGO is financed by the EU and its main target is schools and work with minors, parents and teachers. It is a hotline and a helpline. The same applies to the project 'Cyber.Kids'. Project Stopline operated by the ISPA is also worth mentioning, as an Austrian hotline for combating child pornography and national socialism on the Internet. In the opinion of the evaluators, the way the public authorities cooperate with the private sector in the field of combating child pornography and child abuse online is an example of best practice.

- The financial sector in Austria does not have mandatory reporting obligations to inform the police of suspicious or criminal behaviour. This leaves some room for improvement and, according to the evaluators, more mandatory obligation needs to be considered.

- During the on-site visit, the evaluation team received information on the culture and history of strong privacy requirements on the part of Austrian citizens. It stated that the tragic events of World War II, when the personal data of citizens were used against them, made Austrian citizens cautious with regard to any data request on the part of the authorities. In 1997, when the authorities resolved a data request by seizing the systems of a telecommunication provider, there was a big uproar from society. This was the starting point also for the creation of the association of internet service providers of Austria, which tries to give information as far as possible to the requesting authorities, yet on the other hand protecting the privacy of the customers.

DECLASSIFIED

- To facilitate this process, the Austrian government created a common system to share data with law enforcement, but cooperation is limited to the very basic needs of an investigation, the data retention periods are relatively short, and sometimes the requested information (such as IP addresses) is not recorded in a useful way because of technical reasons (the use of the NAT procedure). This potentially leads to a difficult situation concerning the identification and apprehension of suspects in cybercrime cases and could be improved.

DECL

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

7.1.1. Formal requirements to cooperate with Europol/EC3, Eurojust, ENISA

Austrian domestic law does not lay down any formal conditions or specific procedures for cooperation between the Austrian authorities and Eurojust for the investigation of cybercrime cases. The general rules on cooperation with Eurojust apply (Sections 63 to 68a of the Federal Act on Judicial Cooperation in Criminal Matters with the Member States of the European Union (EU-JZG)).

The legal bases for cooperating with Europol are the EU Police Cooperation Act; Federal Act on police cooperation with the Member States of the European Union and the European Police Office, Federal Law Gazette I No 132/2009, as last amended by Federal Law Gazette I No 161/2013, transposing Framework Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol). Cooperation with Europol is focused on preventing and fighting serious cross-border crime, including terrorism. Information exchange with Europol is conducted through the national Europol office in the Criminal Intelligence Service (.BK) or through the .BK's liaison officer unit in The Hague via the SIENA channel.

7.1.2. Assessment of cooperation with Europol/EC3, Eurojust, ENISA

The Austrian authorities declared that the support and coordination provided by Europol/EC3 and Eurojust are essential for facilitating international cooperation. Their wide-ranging work includes producing analyses of trends and risks, with Europol having begun to look into the threats posed by cybercrime as early as 2010 in its IOCTA (Internet Organised Crime Threat Assessment). Furthermore, they draft 'early warning messages' and work with the private sector (in public-private partnership) to develop models for crime prevention and strategic planning.

DECLASSIFIED

The operational support provided by Europol/EC3 comprises: operational analysis; forensic support, thanks to new technologies developed by Microsoft such as PhotoDNA, which uses photo comparison for speedy identification, particularly of victims of child pornography; rapid reaction to cybercrime attacks by setting up emergency response teams; support for investigations into financial and economic crime, as well as online child pornography; and, lastly, protection of critical IT infrastructure in the EU within Europol's remit. In carrying out these tasks, Europol processes and collates flows of information to and from law enforcement authorities and institutions in the EU and private organisations, and coordinates the work on IT by the investigating teams responsible.

Austria participates in the European Union Strategic Group of the Heads of National High-Tech Crime Units at Europol. Austria has been involved since the former AWF (analysis work file) was set up in 2009. 'Check the web' was transformed into the 'EU IRU' (EU Internet Referral Unit) in July 2015. However, this relates to the prevention and combating of terrorism.

Austria has sent a liaison officer to the EC3 J-CAT. Since the EC3 was set up, six operations have been carried out in the framework of the 'Cyborg' FP, including one led by Austria. J-CAT (the Joint Cybercrime Action Taskforce) was launched in September 2014 following the JIT Mozart as an EC3 pilot project aiming to intensify cooperation in the field of cybercrime. The main broad types of offence it seeks to combat are:

- High-tech crime (malware, botnets, intrusion, etc.)
- Aiding cybercrime (bulletproof hosting, counter anti-virus services, infrastructure leasing and rental, money laundering including virtual currencies, etc.)
- Online fraud (online payment systems, carding, social engineering, etc.)
- Sexual exploitation and sexual abuse, particularly of children.

DECLASSIFIED

Responsibility for these tasks lies within the Austrian Criminal Intelligence Service. Austria is convinced that it is necessary to pool its own resources and use synergies effectively and efficiently. J-CAT is one way of achieving that, which is why the J-CAT liaison officer has a key role to play. Experience to date has shown that the main specific requirements and tasks associated with the position of J-CAT liaison officer are as follows:

- having in-depth knowledge of this highly complex, swiftly changing field and the multiple phenomena involved, together with the extensive specialist terminology used;
- keeping abreast of ongoing investigations in all J-CAT cases and the nature and extent of Austria's involvement;
- working on several J-CAT cases simultaneously while devoting particular attention to issues relating to Austria;
- dealing with urgent investigative action quickly, in both directions, without creating unnecessary bureaucracy;
- attending weekly J-CAT coordination meetings consistently;
- maintaining regular contact with other Europol countries' J-CAT liaison officers to ensure everyone works together in a spirit of trust and in accordance with the law;
- making direct contact with non-Europol J-CAT members (e.g. USA, Canada, Australia, Colombia);
- working towards closer contact with the private sector, particularly internationally (e.g. Microsoft, Symantec, Kaspersky, Google, Facebook, PayPal, eBay);
- seeking improved ways of working together with Russia through contacts with Russian IT security companies;
- informing national units about the knowledge and experience gained from J-CAT;
- forwarding international requests correctly to the relevant national units via SIENA;
- reducing the burden on national units during international investigations, i.e. saving time and resources.

DECLASSIFIED

The Austrian authorities indicated that the limits of traditional systems became abundantly clear in the course of the investigations. Constant sharing of information and short reaction times are key factors for fighting cybercrime effectively. While other liaison officers generally act as extensions of various investigating units and carry out largely administrative tasks, the J-CAT liaison officer is an integral part of the investigating organisation. To perform this role to the required standard, the J-CAT liaison officer must actively pursue training. Treating the J-CAT liaison officer as an on-the-spot expert enables operational meetings to be scheduled at short notice and cuts down on work-related travel. Operational experience has shown that any well-designed efforts to fight cybercrime should include a J-CAT liaison officer with the necessary specialist knowledge. The job involves a wide range of complex tasks, requiring a full-time member of staff.

J-CAT provided the framework for the international police operation Onymous, which spanned 15 countries and led to the arrest of 17 suspects, searches of 13 premises, and the seizure of cash and bit-coins worth over USD 1 million. 414 illegal websites were taken down.

7.1.3. Operational performance of JITs and cyber patrols

At the operational level the 'Mozart' joint investigation team (JIT Mozart) was set up in 2013 to combat Internet fraud. It is headed by Austria and supported by Europol/Eurojust. Apart from Austria, other States participating are: FI, UK, NL and Norway. The fraudulent acts took place when the Internet banking system was infected with malware. This prompted the victim to authorise fraudulent money transfers. The investigation succeeded when the perpetrators' covert means of communication via virtual private networks and proxy servers which hid the actual IP address were discovered. Between 2013 and 2015 eleven members of an internationally active Russian-Ukrainian organised crime group were traced, and eventually in the spring of 2015 the founder and head of the organisation was also tracked down and placed under arrest in the USA. The investigations conducted by the special investigation commission or JIT Mozart led to 60 arrests in four countries. The JIT is still operating as the evidence seized will contain indications for solving crimes worldwide.

DECLASSIFIED

Austria was also involved in another cross-border case in which a group of offenders operating online used malware to access victims' accounts via their active Internet connection and transfer funds to money mules throughout Europe. The victims who suffered losses were in Germany, the UK, Italy, the Netherlands, Finland, Norway, the USA and Australia. The Austrian public prosecutor's office responsible for the matter responded by setting up a multinational JIT by way of an agreement among AT, FI, BE, UK and Norway. Originally planned to last a year, the JIT's mandate has been extended and it continues its work today. The Netherlands has recently also joined. Within the JIT, evidence is exchanged without any further formal requests for mutual legal assistance, and some coordination meetings are held at Eurojust. The investigators and prosecutors from the countries involved meet in person, which makes coordinating the investigations easier and facilitates direct communication. Eurojust JIT funding was claimed to help finance the JIT's work.

7.2. Cooperation between the Austrian authorities and Interpol

The Austrian Criminal Intelligence Service's contact point for combating Internet child pornography is connected to the ICSE (database in Lyon).
Cooperation regarding cybercrime issues takes place through the I-24/7 Network.

7.3. Cooperation with third States

Austria cooperates with third countries with regard to cybercrime on the basis of an international agreement or, in the absence thereof, by the Austrian Extradition and Mutual Assistance Act (ARHG). Cooperation takes place through the national central bureaus of ICPO-Interpol (I-24/7 Network) and/or with the third countries' authorities under police cooperation agreements (combating cybercrime is included in around 30 agreements).

DECLASSIFIED

The central body in the Federal Ministry of Justice is chiefly responsible for relations with third countries, and Eurojust is only involved where the central body is not able to establish satisfactory contacts. In such cases the Austrian authorities mainly rely on the contact points established by Eurojust with the third countries. They reported that the involvement of Eurojust and Europol/EC3 generally means that cases are dealt with more quickly. Europol has always been an important strategic partner. Europol/EC3 has organised meetings, covered travel costs and provided staff for deployment in the field. This speeds up investigations.

7.4. Cooperation with the private sector

Cooperation with the private sector is performed exclusively via official institutions.
MLA requests addressed to Facebook are sent to Facebook USA. At present the mutual legal assistance agreement with the USA is the only channel available in this regard. Owing to the lack of a legal basis, it is currently not possible to refer matters directly to Facebook. The issue is dealt with at EU level (rules on the transfer of data to private entities in third countries have already been included in the new Data Protection Directive for police and judicial cooperation in criminal matters).

The Austrian authorities indicated that participation in the Global Airport Action Day (joint international operations) serves as a means to overcome obstacles to cross-border cooperation specifically regarding online card fraud.

DECLASSIFIED

7.5. Tools of international cooperation

7.5.1. Mutual Legal Assistance

There is no specific legal basis for providing mutual legal assistance (MLA) in terms of cybercrime. The Austrian authorities apply general rules provided for in the applicable instruments (in particular the EU Mutual Assistance Convention of 2000 and its Protocol, the European Convention on Mutual Assistance in Criminal Matters and its Additional Protocol, and the Convention on Cybercrime). Where there is no international agreement, mutual assistance in accordance with the Austrian Extradition and Mutual Assistance Act (ARHG) can also be provided on the basis of reciprocity.

The framework of the relevant agreement (diplomatic channels, communication between the ministries of justice, or direct communication with the authorities) determines which authorities are responsible for receiving/sending requests for MLA. In principle, the public prosecutor's offices are responsible for executing requests for MLA. However, the trial court is responsible for providing information on the main proceedings or the execution of custodial sentences. The same applies to the formal questioning of persons and the provision of information if a national case is pending where charges have already been filed and the subject of the foreign request for MLA is related to the subject matter of the national case.

There are no specific procedures or conditions that need to be fulfilled as regards the various categories of MLA requests related to cybercrime. Urgent requests are marked as such and given priority. The average response time is approximately three months, depending on the type of MLA requested.

DECLASSIFIED

All measures provided for in the Austrian Code of Criminal Procedure can be requested via MLA (including requests relating to cybercrime). Most MLA requests relating to cybercrime concern master data and traffic data in the area of telecommunications (under Austrian law, this term also includes the Internet) or bank data, when the Internet has been used to commit fraud.

If the legal and factual conditions for the required MLA are not sufficiently clear to the requesting authority, pre-MLA consultations are held with the authorities of the requesting State; in addition to direct communication, these can also involve the contact points of the EJN and in individual cases Eurojust.

Due to the direct communication between the Member States of the EU in MLA matters, central statistics on all MLA requests are not yet available. However, the Federal Ministry of Justice is working to enable a future statistical evaluation of the computerised central case registry, which should also make it possible to classify and compile statistics on MLA requests according to the offence on which they are based.

Problems providing/requesting MLA assistance for offences committed in the 'cloud' can be encountered if the provider is a multinational company and it is not immediately obvious from which office in which country the data stored in the 'cloud' should be accessed. That is why MLA requests are sometimes sent to the 'wrong' State, but generally Austria is informed in return on the third State jurisdiction for the provision of MLA.

Communication with non-EU States is mainly based on the European Convention on Mutual Assistance of 20 April 1959. Austria also has bilateral mutual assistance treaties with individual countries such as Australia, Canada and the United States of America. Incoming requests are also based on the Convention on Cybercrime of 23 November 2001.

DECLASSIFIED

In cases relating to cyber attacks involving criminals from outside the EU requests for the transfer of criminal prosecution or mutual assistance are sent by the competent public prosecutor's offices. In the case of Africa, mutual assistance requests are generally not made, as they are unlikely to be successful. Within the EU, the public prosecutor's offices reported problems with mutual assistance requests to the UK.

7.5.2. Mutual recognition instruments

The Austrian authorities used the relevant provision of the Directive on the European protection order, the Framework Decision on mutual recognition of custodial sentences and measures involving deprivation of liberty and the Framework Decision on mutual recognition of financial penalties in relation to prevention, investigation and prosecution of cybercrime.

7.5.3. Surrender/Extradition

Under Article 2(2) of the Framework Decision on the European Arrest Warrant, 'computer-related' crime is listed generally as an offence which, if it is punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years (and the other conditions are met), gives rise to surrender without verification of the double criminality of the act. In cases where the competent authority of the issuing State has ticked the relevant box on the EAW form, the competent Austrian authorities do not therefore have to verify double criminality in principle.

If the Framework Decision on the European Arrest Warrant does not apply, whether or not the offence is extraditable is determined by the relevant agreement. Pursuant to Article 2(1) of the European Convention on Extradition, for instance, the offence motivating the extradition request must be punishable under both the law of the requesting State and Austrian law by a custodial sentence or a detention order of at least one year or by a more severe penalty. If extradition is requested for the purpose of executing a custodial sentence it must be a sentence of at least four months.

DECLASSIFIED

Responsibility for sending surrender/extradition requests lies with the public prosecutors and - after the indictment has been filed - with the court. The Regional Courts are competent for decisions on such requests. Responsibility for receiving such requests is determined by the relevant agreement (diplomatic channels, communication between ministries of justice, or direct communication between authorities).

There are no specific procedures or conditions that need to be fulfilled as regards requests related to cybercrime. Urgent requests are marked as such and given priority. The average reply time for a request is around three to six months depending on whether or not the person concerned consents to the surrender/extradition (simplified surrender/extradition).

7.6. Conclusions

- Austria cooperates closely with the EU agencies, especially with Europol/EC3 and Eurojust. Eurojust is frequently used in the area of cybercrime via the Austrian desk. Requesting financial support to fund projects and also using Eurojust's powers to its advantage seems, in the evaluators' view, to be an example of best practice.

- The Austrian authorities perceive Europol as an important strategic partner helping cases to be dealt with more quickly. Europol/EC3 has organised meetings, covered travel costs and provided staff for deployment in the field. This speeds up investigations.

- Austria participates in a number of international cybercrime operations and has good cross-border relations with the neighbouring countries (e.g. Germany), including bilateral training. It is thought that CEPOL exchange programmes could also be explored.

DECLASSIFIED

- As regards investigations, Austria supports the EU's international efforts to combat cybercrime by its participation in EMPACT cyber attack working parties and its involvement in J-CAT operations.

- Cooperation with private companies located in Austria is generally assessed as positive by the Austrian authorities, but some concerns were expressed to the evaluation team by representatives of various stakeholders. The Austrian authorities reported some difficulties with regard to cooperation with private companies that have their main headquarters in third countries (e.g. Facebook).

- The Austrian authorities stated that mutual assistance was slow. The prosecutors expressed concerns with regard to real-time translations of content data, such as the example given in the JIT Mozart case regarding downloaded telephone calls/internet communications in Russian language.

- Austria has no special national provisions that regulate international cooperation on cybercrime. The legal basis for such cooperation lies within international conventions to which Austria is party and the Austrian Extradition and Mutual Assistance Act. Practitioners make use of all available channels: liaison officers and magistrates or EU agencies.

- The Austrian authorities view cooperation with Member States positively. However, it was reported that cooperation with third countries was sometimes difficult and responses might be late. Communication with non-EU States is mainly based on the European Convention on Mutual Assistance of 1959. Austria also has bilateral mutual assistance treaties with individual countries such as Australia, Canada and the United States of America.

DECLASSIFIED

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

Judiciary

Cybercrime-related training is on offer for all representatives of the judicial authorities (judges and public prosecutors) and for individuals whose duties involve international cooperation. The topic of cybercrime was addressed at the following events in recent years:

- in April 2013 Innsbruck Higher Regional Court held a course (for the entire sector) entitled 'computer crime - areas of difficulty in connection with the forensic analysis of data media and Internet investigations';
- a workshop held in 2014 brought together public prosecutors and lead investigators to discuss measures to combat child pornography and sexual abuse of minors;
- on the occasion of the Judges' Week 2015, lectures were organised on the media in civil and criminal law covering not only the misuse of new media (such as Facebook and Twitter) for dissemination of illegal content, fraud or indeed targeted defamation, but also the use of those same technologies by the law enforcement authorities to obtain relevant information or to contact citizens;
- in 2016 a few events are being carried out, *inter alia* the workshop for public prosecutors and lead investigators on measures to combat child pornography and sexual abuse of minors held from 9 to 11 May 2016 (in cooperation with the Criminal Intelligence Service) referring to the following topics: Facebook and Twitter; the Criminal Intelligence Service's new investigation tools; Bitcoin and other cryptocurrencies; darknets; online investigations; issues with investigative procedures on the Internet. Other seminars on cybercrime and the darknet are organised from 19 to 21 September and on 10 and 11 November 2016.

DECLASSIFIED

Judges and public prosecutors attended many events regarding cybercrime organised by ERA, the EJTN and other organisations. The department of the Federal Ministry of the Interior responsible for international affairs (Department I/4, Unit I/4/a, - Attaché Matters) works with the ZIA (centre for international affairs) at the SIAK (the Ministry's security academy) to provide training for Austrian liaison officers (police attachés) that is tailored to their needs.

Cooperation also takes place with Austrian universities, under the KIRAS Programme (Austrian programme to support security research). C4 and the Federal Ministry of Justice have cooperated closely since 2014 to run mutually available training for judges and public prosecutors.

Nonetheless, the evaluators noticed that participation in training is not mandatory for judges and prosecutors and the number of seminars organised in Austria and abroad in which they have participated does not allow a sufficient number of professionals dealing with criminal cases to be trained.

Law Enforcement

The Security Academy (SIAK) is responsible for providing and conducting basic training for employees within the Federal Ministry of the Interior. For the police service, a specific regulation lays down and regulates:

- basic police training;
- basic training for category E 2a police officers (mid-level officers);
- basic training for category E 1 police officers (senior officers).

DECLASSIFIED

As a general rule, the topics and content of the courses provided are drawn up in close cooperation with the Directorate-General for Public Security and the competent departments and units of the Federal Ministry of the Interior. In the basic police training, cybercrime is taught as a cross-curricular topic and is dealt with from the point of view of the legislation and operational guidance applicable to police work (particularly criminal law, the Code of Criminal Procedure, operational security police training and criminalistics, etc.). The aim is to incorporate more core knowledge on cybercrime into the basic police training through the modules on criminal law, criminalistics and operational security police training and related courses given by the police service's full-time teachers.

No specific training on the topic is currently provided as part of the basic police training (except for the 8-hour basic training on cybercrime).

In the basic training for category E 2a police officers (mid-level officers), specific training on computer crime is provided as part of the module on criminalistics. The main topics and content covered include the legal framework for and manifestations of computer crime, the principles of securing e-evidence, and the possibilities for data analysis and processing.

The basic training for category E 1 police officers (senior officers) does not currently include any specific modules on cybercrime or computer crime. As part of the specialised training for the criminal investigation service (FAB-KD) added to the Federal Ministry of the Interior's training offer in 2010, participants are expected to extend and develop the essential skills required to carry out their professional tasks within the criminal investigation service, on the basis of need and provided that the training links in effectively with the practical requirements of their work. This training builds on the content of the basic police training and the basic training for category E 2a police officers (mid-level officers).

DECLASSIFIED

A module on computer crime has been included in this specialised training since its inception. The main topics and content covered include the legal framework for and manifestations of computer and network crime (cybercrime in the narrower and wider sense), general principles for dealing with e-evidence, methods of seizing e-evidence, the execution of seizures, the possibilities for data analysis and processing, and practical procedures.

In the framework of the ongoing cycle of further training weeks (standardised, mandatory training for members of the Federal Police, who are predominantly uniformed officers), the Länder of Burgenland, Lower Austria and Salzburg provide training on cybercrime or computer crime as part of the module on regional priorities.

The Federal Ministry of the Interior's training arrangements, which are based on the principle of lifelong learning, provide, among other things, for a structured interaction between centralised and decentralised training. This is in view of the complexity of the duties and areas of activity of the Ministry's staff and the sometimes widely differing needs and target groups to which training courses must be tailored, and also in light of the size of the general active target group, which comprises over 32 000 staff. Training is planned, organised and/or conducted either centrally, for the whole country, or on a decentralised basis, by training bodies which span all the Länder, regional police departments, or local district or city police forces, depending on the training content and subject areas, the target group, the available resources (in terms of staff, logistics, infrastructure/premises and budget) and the applicable organisational conditions. In addition, a distinction is made, among other things, between general and specialised training courses, which, depending on their classification, involve different organisational and/or structural competencies within the Federal Ministry of the Interior.

DECLASSIFIED

The Security Academy is responsible for steering and coordinating training courses for the Ministry of the Interior's staff, but this does not imply any responsibility for the specific planning, organisation and/or implementation of all training courses within the Ministry or of training for all of the Ministry's staff.

Specialised training (training courses related to a specific field, post or task which, in view of their content or subject area, are relevant only to a limited group of participants) is provided by the competent departments or units of the Federal Ministry of the Interior, in particular to allow courses to be tailored to specific needs and target groups and linked as efficiently as possible to the practical working requirements of the participants' tasks and posts (practical orientation). The following are examples of cybercrime training courses offered by the competent departments or units of the Federal Ministry of the Interior:

- Training for district IT investigators

In the last few years, police inspectorates and district and city police forces have appointed district IT investigators, who carry out IT-related criminal investigations and secure and analyse relevant data, as far as their training and equipment allow, working under the technical supervision of the auxiliary teams established at the criminal intelligence service of their Land (LKA AB 06 IT-B). Under the current rules, training for district IT investigators comprises a one-week theory module and two months of hands-on training at the relevant Land-level criminal intelligence service. Together, the department of the Federal Ministry of the Interior responsible for operational affairs (Department II/2, unit II/2/a - police service) and the Criminal Intelligence Service (Sub-departments 5.2 (C4 Cybercrime Competence Centre) and 1.2 (initial and further criminal investigation training) conducted a total of 19 one-week training modules for district IT investigators between 2012 and 2014, which were attended by 276 staff members. The topics covered in these training courses included the basic principles of computer crime, a practical overview of network crime and data backup, the basic principles of mobile phone analysis, online property crime, Internet child pornography, cybercrime and undercover investigations.

DECLASSIFIED

- Initial and further training for specialists at Land level (LKA AB 06 IT-B)

In accordance with the KDFR (rules on training for the criminal investigation service), specialists at Land level, specifically the staff of the auxiliary teams for the preservation of IT evidence set up at the criminal intelligence services of the Länder, are provided with further specialised training. The organisation of this training is managed by the department of the Federal Ministry of the Interior responsible for operational affairs (Department II/2, unit II/2/a - police service), with the involvement of the Criminal Intelligence Service (Sub-departments 5.2 (C4 Cybercrime Competence Centre) and 1.2 (initial and further criminal investigation training)). Staff assigned to the auxiliary teams are obliged to participate in one of the relevant seminars or workshops offered during each further training cycle (the current cycle runs from 2014 to 2016). No specific training is currently provided to staff members when they are first assigned to the auxiliary teams.

- Initial and further training for specialists at federal level (Criminal Intelligence Service, Federal Agency for State Protection and Counter Terrorism, and Federal Bureau of Anti-Corruption)

Initial and further training for specialists at federal level - specifically at the Criminal Intelligence Service (.BK), the Federal Agency for State Protection and Counter Terrorism (.BVT) and the Federal Bureau of Anti-Corruption (.BAK) - is organised according to individual priorities on the basis of the relevant national and international training courses and specialist courses offered.

Where possible, specialists at both Land (LKA AB 06 IT-B) and federal level (.BK, .BVT and .BAK) are also given the opportunity to attend the relevant training courses in this field offered by universities of applied sciences and institutes of higher education, such as the St Pölten University of Applied Sciences, the University of Applied Sciences Technikum Wien and the Hagenberg campus of the University of Applied Sciences Upper Austria. Universities of applied sciences and institutes of higher education also occasionally assist with in-house Ministry of the Interior training courses, in particular by providing relevant speakers and trainers.

DECLASSIFIED

Training for the criminal investigation department includes a course to become a specialised IT investigator, which is held from time to time at all levels. Further training is governed by the KDFR (rules on training for the criminal investigation service). Any training required in addition to that is planned and carried out on an ad hoc basis. Higher education institutions are involved in close cooperation on training. The Federal Ministry of the Interior also runs a course on economic crime and cybercrime in cooperation with a university of applied sciences.

In the criminal intelligence services of the *Länder*, staff working in auxiliary teams for the preservation of IT evidence attend courses as part of regular training in criminal investigation (the courses take around three to five days and are run for around 10-20 staff at a time; eight such courses were held in 2014 covering specialist forensic know-how).

At district and city police headquarters, district IT investigators (numbering around 300 throughout Austria) have been trained. Under the supervision of the auxiliary team for the preservation of IT evidence (AB 06 ITB) at the criminal intelligence service of their Land, they carry out IT-related police investigations at district and city level and, to the extent their training and equipment permit, preserve and analyse data. Training to become a district IT investigator comprises a one-week basic theory course and a two-month hands-on training placement, followed by in-service training (for up to two days a year).

DECLASSIFIED

When deciding what the main content and core topics of the training should be, the emphasis is on what the liaison officers' duties and tasks will be and what skills they will need for their future work; as far as possible, all the relevant specialist departments within the Federal Ministry of the Interior are included in the process. There are also plans to have experts from the Federal Ministry of Europe, Integration and Foreign Affairs and the Federal Ministry of Justice provide complementary input, building on the themes and content covered. The Criminal Intelligence Service was specifically in charge of one week of the course starting in November 2015 (taking the form of three blocks of three weeks each); part of that week's course content was cybercrime.

To the extent possible, staff attend the relevant international training measures and specialist courses in this field, particularly as part of the initial and further training for specialists at the level of the Länder (auxiliary teams for the preservation of IT evidence at Länder criminal intelligence services) and at federal level (Criminal Intelligence Service, Federal Agency for State Protection and Counter Terrorism, and Federal Bureau of Anti-Corruption).

From the Federal Ministry of the Interior downwards, courses at CEPOL are advertised by the ZIA (centre for international affairs) at the SIAK (Security Academy). Under the KDFR (rules on training for the criminal investigation service), the Ministry appoints training coordinators from the staff of the Länder criminal intelligence services. They put together a programme of initial and further training for one training cycle (currently three years), which all IT investigators from the Länder criminal intelligence services are then required to follow. All district IT investigators must attend training in their Land every year.

DECLASSIFIED

The Criminal Intelligence Service (Departments 5 and 1) puts together the content of additional basic training for current and new IT investigators (the existing basic training programme is currently being reworked) and works with the Ministry's security academy to offer courses for the various parts of the police force. Subject-specific training on current topics (software, hardware, new offences) is planned and provided by the Criminal Intelligence Service (Departments 3, 5, and 7 in cooperation with the Service's training office). As regards the international dimension of training, the Criminal Intelligence Service is part of the International Association of Computer Investigative Specialists (IACIS), an organisation that brings together forensics experts. IACIS provides basic training and specialist modules in the context of European projects. The Criminal Intelligence Service is also involved in the European Cybercrime Training and Education Group (ECTEG), a European training programme on high-tech crime. There are also external national courses to provide ongoing training on operating systems, analysis software, servers and networks. In addition, courses and workshops are organised as the need arises with partners including Microsoft and the Computer Emergency Response Team (CERT).

A total of EUR 1 380 762.15 was spent on all training activities for the judicial authorities (judges and public prosecutors) in 2013. This comprised speakers' fees, accommodation expenses, travel costs and travel allowances, as well as other costs.

DECLASSIFIED

Centre of Excellence

Department 5 of the Criminal Intelligence Service, which deals with cybercrime, is home to C4 Austria's centre of excellence. New developments are quickly brought to light and information about them distributed via newsletters. If it is considered necessary, training measures are quickly put in place via the established channels. The KLF (criminological guidelines), maintained by Department 1 of the Criminal Intelligence Service, serve as an information platform and can be accessed from any part of the police force. The KLF is always kept up to date.

Academia

At Vienna University courses are organised in 'IT-related criminal law' and 'current cybercrime issues' in alternate semesters as part of the group of optional modules on criminal justice and crime studies. There are groups of optional modules designed to offer a specialised programme that students can choose to complete in addition to the compulsory content of their law studies.

Wiener Neustadt University of Applied Sciences has offered a continuing vocational training course on economic crime and cybercrime since March 2015. The course is designed to address the challenges of that nature faced by practitioners in the fields of business, finance, law, IT, investigations, criminal prosecution or administration. Participants attend on a part-time basis alongside their professional work. The course takes three semesters and culminates in the award of a Master of Science (MSc) in Business and Cyber Crime Control.

Course content relating to cybercrime includes the legal bases for computer crime offences, the technical foundations of computer systems (particularly IT systems, system software, hardware, data media, user software, databases etc.), preservation of digital evidence, data analysis and data mining, as well as modules on IT forensics, IT security and mobile forensic devices.

DECLASSIFIED

8.2. Awareness-raising

Austria has adopted a multi-stakeholder approach to cybersecurity, with businesses kept on board. Contact between businesses and representatives of internal security authorities began with the KSÖ Cyber Initiative. This developed into Austria's Cybersecurity Platform, which now facilitates ongoing communication with all stakeholders from the administration, business and academia.

The KSÖ Initiative also gave rise to the Cyber Security Forum, which is composed of business representatives. They come from a core group of companies operating in sectors including banking, telecommunications and technology. They exchange information about cyber weaknesses that would otherwise probably be kept secret for fear of reputational damage, for example. At an operational level, close cooperation takes place in a spirit of trust: information is exchanged, risks assessed and measures discussed.

The Federal Ministry of Defence and Sport has domestic jurisdiction in the field of cyber defence. It holds annual ICT security conferences (most recently in St. Pölten in November 2015) which also help to raise awareness externally and internally.

Among the Criminal Intelligence Service's awareness-raising measures are the preventive Cyber.Kids project for children aged between 8 and 12, and the Click & Check project for young people aged over 14.

DECLASSIFIED

8.3. Prevention

8.3.1 National legislation/policy and other measures

In crime prevention distinctions are made between areas such as protection of property, prevention of violence, prevention of drug addiction and prevention of sexual offences. Although cybercrime cuts across all of these areas, a government circular has been issued to the effect that it should be recognised as a separate issue. Measures to combat cybercrime are found in target-group-oriented information campaigns and projects.

The following preventive measures are being implemented or planned by the Crime Prevention Office of the Criminal Intelligence Service:

- periodic and ad hoc publications on the subject on the homepage, official Facebook page and police app;
- 'Click & Check' project – training programme for 12 to 14-year-old children on social media, cybercrime, bullying, etc.;
- 'Prevention against Cybercrime – Cyber.Sicher' ('Cyber.Safe') project: e-learning module on Internet use for adults in cooperation with, among others, the University of Vienna, the Austrian Economic Chambers and saferinternet.at (not yet released);
- 'Cyber.Kids' project: preparing children from primary-school age upwards to use the Internet (under preparation);
- 'Sicher in den besten Jahren' ('Safe in the prime of life'), a comprehensive booklet for senior citizens which includes a chapter on Internet safety.

The Federal Ministry of Defence and Sport has domestic jurisdiction in the field of cyber defence.

DECLASSIFIED

8.3.2 Public Private Partnership (PPP)

There is the international research project financed by KIRAS. In addition, the Criminal Intelligence Service (Sub-department 3.2) provides two advisers for the private hotline 'Stopline' (www.stopline.at). Sub-department 3.2 is also a permanent member of the 'Round Table on Ethics in Tourism' set up at the Federal Ministry of Economic Affairs, the Family and Youth. There is also regular participation in international meetings organised by ECPAT.

Furthermore, many NGOs such as ECPAT, Stopline (provider organisation) and Safer Internet explicitly refer to the Criminal Intelligence Service hotline, meldestelle@interpol.at, on their homepages and in various videos and publications.

8.4. Conclusions

- Some events on cybercrime were organised for representatives of the judiciary in the years 2013-2016. However, training of judges and prosecutors is based on voluntary participation. Thus, it is addressed to a limited number of practitioners and this does not guarantee a general knowledge by those dealing with cybercrime and cyber-enabled crime cases. Judges and prosecutors are entitled to participate in training programmes organised by external resources, such as ERA or the EJTN and they should be actively encouraged to avail themselves of those opportunities.

- Taking into account the number of events and participants involved in the training of judges and prosecutors in the past years, the evaluators take the view that there is not sufficient training available in the area of cybercrime. Specifically more funding for prosecutors could be considered, given that the vision stated in the security strategy statement cannot be achieved, if the prosecution does not successfully enforce cybercrime cases in courts.

DECLASSIFIED

- On the other hand, there is basic training addressed to all categories of police officers on selected aspects of cybercrime. There are courses and seminars for first responders. There are currently 300 first responders in Austria, located at the district and city level. It is intended to allocate more time for the practical and theoretical training of first responders. This will be introduced in 2017.

- The basic-level training of police officers involves a total of eight hours in the initial phase of instruction. Moreover, the local police also lack adequate training for handling cybercrime cases properly. In the opinion of the evaluators, improvement of these training components deserves consideration in the future and, specifically, the time allotted to such training of police officers at basic level should be increased.

- Bearing in mind the impressive level of training on cybercrime addressed to police officers, the evaluators consider that an integrated approach for common training of judges, prosecutors and representatives of LEAs as a platform for discussing obstacles relating to admissibility of evidence and exchanging experiences could step up the resilience of the Austrian system to fight cybercrime.

- According to the opinion expressed by the prosecutors met by the evaluation team, law enforcement should have more digital forensic analysts for cybercrime and more specialised investigators. This seems to be a widespread problem across the EU. Well-trained and specialised forensic analysts in the area of cybercrime are popular in the private sector. It is difficult for the public sector to compete with the financial possibilities offered by the private sector.

DECLASSIFIED

- The evaluation team would like to give special mention to the cooperation between C4 and academia aiming to develop new investigating tools in the area of fighting cybercrime. The team also notes the many public-private partnerships which cover awareness-raising (e.g. the Click & Check project), training for LEAs and prevention ('Prevention against Cybercrime – Cyber.Sicher' ('Cyber.Safe') project). This type of cooperation organised jointly with the private sector is, in the evaluators' opinion, an example of best practice.

- Austria also has a number of excellent awareness programmes in the fields of both education and cyber defence, and a number of bodies charged with monitoring publications and websites in the areas of child pornography and national socialism, which facilitate the removal of such material**.**

DECLASSIFIED

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Austria

The Austrian authorities believe that cyberspace opens up a wide range of opportunities and possibilities. In order to take advantage of the potential benefits of the globalised world, the digital infrastructure must work reliably and safely. Guaranteeing cyber security therefore presents the State, the economy and society with a key common challenge.

One of the methods of providing cyber security is to step up international cooperation once cybercrime is involved. The JIT Mozart demonstrated that coordinated cross-border cooperation is the only way to combat cybercrime. The knowledge and experience gained during the JIT Mozart investigations shed light on the criminal structures underlying Internet fraud and their modus operandi. The JIT Mozart investigations helped to solve hundreds of cases of Internet fraud globally. In addition, the knowledge gained and lessons learned from the investigation are being passed on to staff of the law enforcement authorities in training courses, particularly for public prosecutors and staff at Europol, the FBI and the USPIS (United States Postal Inspection Service).

9.2. Recommendations

As regards the practical implementation and operation of the Framework Decision and the Directives, the expert team involved in the evaluation of Austria was able to satisfactorily review the system in Austria.

Austria should conduct a follow-up on the recommendations given in this report 18 months after the evaluation and report on progress to the Working Party on General Affairs, including Evaluations (GENVAL).

The evaluation team thought it fit to make a number of suggestions for the attention of the Austrian authorities. Furthermore, based on the various good practices, some relevant recommendations to the EU, its institutions and agencies, Europol in particular, are also put forward.

DECLASSIFIED

9.2.1. Recommendations to Austria

1. Should work on reliable and comprehensive statistics from various stakeholders involved in fighting cybercrime (such as the Ministry of Interior, the Ministry of Justice, the police, and hotlines concerning the same reporting topics) to have a clearer view of the development of this phenomenon in Austria; (cf. 3.3.2 and 3.5)

2. Should consider appointing prosecutors specialised in fighting cybercrime and/or improving the level and the number of expert prosecutors and judges in the various types of cybercrime**,** e.g. by developing a cybercrime network in which all the relevant information and best practices of cybercrime investigations are collected; (cf. 4.1.1 and 4.5)

3. Should consider involving more digital evidence analysts in the police to ensure fast response and a shorter timeframe for reports on forensics; (cf. 4.2 and 4.5)

4. Should analyse whether the necessity of having criminal liability for illegal access to an information system subject to the consent of the aggrieved party should cause administrative problems in large cases involving a high number of victims; (cf. 5.1.2 and 5.5)

5. Should be encouraged to work on a new data retention law following the ongoing discussion at the EU level; (cf. 5.2.1 and 5.5)

6. Should consider implementing a possibility in criminal proceedings to block access to the Internet containing criminal content, for example in child pornography cases where Interpol set up a black list of pages; (cf. 6.2.4 and 6.4)

DECLASSIFIED

7. Should consider further improving cooperation with the financial sector, for example by developing other methods to ensure that cybercrime activities undetected by the financial sector will be referred to, considered and, if needed, handled by law enforcement authorities; (cf. 6.1.1 and 6.4)

8. Should enhance training opportunities for judges and prosecutors, by organising more events or training modules, and expand basic training for police officers; (cf. 8.1 and 8.4)

9. Should consider creating an integrated approach for common training of judges, prosecutors and representatives of LEAs as a platform for discussing obstacles relating to admissibility of evidence and exchanging experiences and best practice with regard to cybercrime; (cf. 8.1 and 8.4)

9.2.2. Recommendations to the European Union, its institutions, and to other Member States

1. Member States are encouraged to consider setting up a service supporting aggrieved customers concerning transactions made online or other suspicious actions spotted on the Internet, along the lines of the Internet Ombudsman developed by Austria; (cf. 3.2 and 3.5)

2. Member States should consider setting up well-trained and equipped units within LEAs to combat cybercrime more effectively at the regional/local level, like the first responders for cybercrime set up within the police structure in Austria; (cf. 4.2 and 4.5)

3. Member States are recommended to develop tools and measures aimed at protecting children and minors from secondary victimisation in the trial process, as witnessed in the Austrian criminal process, by using psychologists when hearing victims of child sexual abuse; (cf. 6.2.1 and 6.4)

DECLASSIFIED

4. Member States are recommended to enhance their cooperation with neighbouring countries to strengthen their policy to fight cybercrime, as carried out by Austria with Germany or Switzerland; (cf. 6.4 and 7.6)

5. Member States are recommended to use public-private partnerships to develop or strengthen cooperation with private organisations when tackling child pornography and child abuse online, as practised with ISPs in Austria; (cf. 6.2.4 and 6.4)

6. Member States are encouraged to explore the possibility of making more frequent use of Eurojust and the tools available through Eurojust in order to obtain faster responses to MLA requests or its financial support; (cf. 7.1.3, 7.2 and 7.6)

7. The EU institutions should address the issue of data retention as soon as possible; (cf. 5.1.2 and 5.5)

DECLASSIFIED

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

7th Round of Mutual Evaluations ("Cybercrime")

Evaluation Visit to Austria, Vienna (18 – 20 May 2016)

DECLASSIFIED

Wednesday, May 18th, 2016:

10 00 – 12 30 a.m. (with coffee break): discussions of the evaluation team with representatives of the Austrian Ministry of Justice *(Ministry of Justice, Neustiftgasse 2, 1070 Vienna [Room Nr. 615]);*

12 45 – 14 15 p.m.: lunch at the *Justizcafé* (offered by the AT Ministry of Justice);

14 30 – 17 00 p.m. (with coffee break): discussions of the evaluation team with representatives of the Vienna Public Prosecutor's Office;

Thursday, May 19th, 2016:

10 00 – 12 30 a.m. (with coffee break): discussions of the evaluation team with representatives of the Austrian Ministry of the Interior *(Ministry of the Interior Minoritenplatz 9, [Room Nr. 588]);*

- *Presentation Bundeskriminalamt - C4 (Manfred PINNEGGER / Gert SEIDL)*
- *Presentation Bundesamt für Verfassungsschutz und Terrorismusbekämpfung – CSC (Philipp BLAUENSTEINER)*

12 30 – 14 30 p.m.: working lunch (offered by the AT Ministry of the Interior);

14 30 – 17 00 p.m.: (with coffee break): meeting with representatives of the Austrian Ministry of the Interior (including experts for awareness raising campaigns) and the national CERT *(Ministry of the Interior);*

- *14.30-15.00: presentation Austrian Cyber-Security Strategy (Kurt HAGER/BMI)*
- *15.00-15.30: presentation national CERT (Otmar LENDL/CERT)*
- *15.30-16.00: presentation project "Safer Internet" (Bernhard JUNGWIRTH/OIAT)*
- *16.00-16.30: presentation project "Cyberkids" (Gert SEIDL/BK)*
- *16.30-17.00: presentation on countering child abuse online by STOPLINE (tbc)*

Friday, May 20th, 2016:

10 00 – 12 00 a.m. (with coffee break): wrap-up session with representatives of the Austrian Ministry of Justice and the Austrian Ministry of the Interior *(Ministry of Justice [Room Nr. 542]);*

12 00: end of the meeting

DECLASSIFIED

ANNEX B: PERSONS INTERVIEWED/MET

Meetings on 18 of May, 2016

Venue: Ministry of Justice

Person interviewed/met	Organisation represented
Ms. Irene Gartner	Expert (Department for multilateral instruments on cooperation in criminal matters, including mutual recognition
Mr. Johannes Martetschläger	Expert (Department for individual cases of cooperation in criminal matters, including mutual recognition)
Mr. Clemens Burianek	Expert (Departments for Penal Law and for Criminal Procedural Law)
Ms. Sondra Fornather-Lentner	Expert (Department for training of the judiciary
Ms. Linda Mittnik	Expert (Department for Personnel)
Ms. Brigitte Süssenbacher	Expert (Department responsible for the E-Commerce-Directive)
Ms. Andrea Rohner	Expert (Department for individual cases of cooperation in criminal matters, including mutual recognition)

Venue: Vienna Public Prosecutors' Office

Person interviewed/met	Organisation represented
Ms. Maria Luise Nittel	Head of the Public Prosecutor's Office
Mr. Gerd Hermann	Department for sexual offences
Mr. Florian Kranz	Organized Crime and Terrorism
Ms. Nina Bussek	Legal Assistance Department

DECLASSIFIED

Meetings on 19 of May, 2016

Venue: Ministry of Interior

Person interviewed/met	Organisation represented
Mr. Philipp Blauensteiner	Expert (BVT - Federal Agency for State Protection and Counter Terrorism)
Mr. Bernhard Jungwirth	Expert and director (OIAT – Austrian Institute for Applied Telecommunications)
Mr. Otmar Lendl	Expert (cert.at – Computer Emergency Response Team)
Mr. Antonio-Maria Martino	EU policy matters and coordination (Head of Unit - Federal Ministry of the Interior)
Mr. Manfred Pinnegger	Expert (Federal Criminal Agency)
Mr. Paul Schliefssteiner	Assistant to Mr. MARTINO (Federal Ministry of the Interior)
Ms. Barbara Schloszbauer	Head of project „Stopline“ (nic.at – Austria’s domain administration)
Mr. Maximilian Schubert	Secretary General of ISPA (Internet Service Providers Austria - governing body of Austria’s Internet industry
Mr. Gert Seidl	Expert (Federal Criminal Agency)

DECLASSIFIED

Meetings on 20 of May, 2016

Venue: Ministry of Justice

Person interviewed/met	Organisation represented
Ms. Irene Gartner	Expert (Department for multilateral instruments on cooperation in criminal matters, including mutual recognition
Mr. Johannes Martetschläger	Expert (Department for individual cases of cooperation in criminal matters, including mutual recognition)
Mr. Clemens Burianek	Expert (Departments for Penal Law and for Criminal Procedural Law)
Mr. Gert Seidl	Expert (Federal Criminal Agency)

DECLASSIFIED

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	AUSTRIAN OR ACRONYM IN ORIGINAL LANGUAGE	AUSTRIAN OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
ACSS	*ÖSCS*	Österreichische Strategie für Cyber Sicherheit	Austrian Cyber Security Strategy
APCIP	*APCIP*		Austrian Programme for Critical Infrastructure Protection
ARHG	*ARHG*		Austrian Extradition and Mutual Assistance Act
BMI	*BMI*		Federal Ministry of the Interior
BVT	*BVT*		Federal Agency for State Protection and Counter Terrorism
CKM	*CKM*		cyber crisis mechanism
CDZ	*CDZ*		Cyber Defence Centre
CSC	*CSC*		Cyber Security Centre
ECG	*ECG*		E-Commerce Act
IOCTA	*IOCTA*		Internet Organised Crime Threat Assessment
KIRAS	*KIRAS*		Austrian Security Research Programme
LKAs	*LKAs*	Landeskriminalämter	Regional Criminal Offices

DECLASSIFIED

SIAK	*SIAK*		The Security Academy
SKKM	*SKKM*		National Crisis and Disaster Protection Mechanism
StPO	*StPO*	Strafprozessordnung	Code of Criminal Procedure
TKG	*TKG*		Telecommunications Act
VJ	*VJ*	Verfahrensautomation Justiz	Justice department database
WKStA	*WKStA*		The Central Public Prosecutor's Office for the Prosecution of Economic Crimes and Corruption

DECLASSIFIED

ANNEX D: AUSTRIAN LEGISLATION

The content of the provisions cited in chapter 5.1.2

1. Illegal access to information system:

Covered by Section 118a of the Criminal Code ('Illegal access to a computer system'):

Section 118a (1) Anyone who, by overcoming a specific security measure, gains access to a computer system or to part of such a system, without being authorised to access it, or to access it alone, with the intention of:

1. procuring knowledge of personal data, for himself or another unauthorised party, thereby breaching the data subject's legitimate confidentiality interests; or

2. causing harm to another party by the use of data of which he has procured knowledge, which were saved in the system and not intended for him, shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.

(2) Anyone who commits the offence in relation to a computer system that is an essential component of critical infrastructure (point 11 of Section 74(1)) shall be liable to imprisonment for a term of up to two years.

(3) The perpetrator shall be prosecuted only if the aggrieved party has given his consent.

(4) Anyone who commits an offence under subsection (1) as a member of a criminal organisation shall be liable to imprisonment for a term of up to two years; anyone who commits an offence under subsection (2) as a member of a criminal organisation shall be liable to imprisonment for a term of up to three years.

DECLASSIFIED

2. Illegal system interference/illegal data interference:

Covered by Sections 126a and 126b of the Criminal Code ('Damage to data', 'Disruption of the operational capacity of a computer system):

Section 126a (1) Anyone who damages another by altering, deleting or otherwise making unusable or suppressing electronically processed, transmitted or supplied data without being authorised to access it, or to access it alone, shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.

(2) Anyone who causes damage to data exceeding EUR 5 000 by committing the offence shall be liable to imprisonment for a term of up to two years.

(3) Anyone who, by committing the offence, damages many computer systems using software, a computer password, an access code or comparable data providing access to a computer system or part thereof, if it is evident from their particular characteristics that those devices were created or adapted for the purpose, shall be liable to imprisonment for a term of up to three years.

(4) Anyone who:

1. causes damage exceeding EUR 300 000 by committing the offence;
2. damages essential components of critical infrastructure (point 11 of Section 74(1)) by committing the offence;

or

3. commits the offence as a member of a criminal organisation

shall be liable to imprisonment for a term of between six months and five years.

Section 126b (1) Anyone who severely disrupts the operational capacity of a computer system without being authorised to access it, or to access it alone, by entering or transmitting data shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates, unless the offence is punishable under Section 126a.

(2) Anyone who causes long-lasting disruption to the operational capacity of a computer system by committing the offence shall be liable to imprisonment for a term of up to two years.

DECLASSIFIED

(3) Anyone who, by committing the offence, severely disrupts many computer systems using software, a computer password, an access code or comparable data providing access to a computer system or part thereof, if it is evident from their particular characteristics that those devices were created or adapted for the purpose, shall be liable to imprisonment for a term of up to three years.
(4) Anyone who:

1. causes damage exceeding EUR 300 000 by committing the offence;
2. commits the offence against a computer system that is an essential component of critical infrastructure (point 11 of Section 74(1)); or
3. commits the offence as a member of a criminal organisation

shall be liable to imprisonment for a term of between six months and five years.

(2a. Excursus: Critical infrastructure:
Definition in point 11 of Section 74(1) of the Criminal Code:
'critical infrastructure: establishments, facilities, systems or parts thereof, that are of significant importance for maintaining public security and national defence, for the proper functioning of public information and communication technology, for preventing or combating disasters, for the public health service, for the public water supply, energy supply or supply of essential goods, for the public waste collection system and wastewater system, or for the public transport system.')

3. Illegal interception of computer data:
Covered by Section 119a of the Criminal Code ('Illegal interception of data'):
Section 119a (1) Anyone who uses a device that has been attached to a computer system or has otherwise been enabled to receive a signal, or who intercepts electromagnetic emissions from a computer system, with the intention to procure, for himself or another unauthorised party, knowledge of data transmitted by means of that computer system and not intended for him, and, by using those data himself, making them accessible to another person for whom the data are not intended or publishing those data, to obtain a pecuniary advantage for himself or another person or to cause harm to another person, shall, unless the offence is punishable under Section 119, be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.
(2) The perpetrator shall be prosecuted only if the aggrieved party has given his consent.

DECLASSIFIED

4. Misuse of devices - production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools:

Covered by Section 126c of the Criminal Code ('Misuse of computer programs or access data'):

Section 126c (1) Anyone who produces, imports, markets, sells, otherwise makes available, procures or possesses

1. a computer program or comparable device of this nature that, given its particular characteristics, has evidently been created or adapted to commit the offence of unlawfully accessing a computer system (Section 118a), of breaching the privacy of telecommunications (Section 119), of illegal interception of data (Section 119a), of causing damage to data (Section 126a), of disruption of the operational capacity of a computer system (Section 126b) or of fraudulent misuse of data processing (Section 148a), or
2. a computer password, an access code or comparable data providing access to a computer system or a part thereof,

   with the intention of using them to commit one of the punishable acts referred to in point 1, shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.

(2) Anyone who, of their own volition, prevents the computer program referred to in subsection (1), the comparable device, or the password, the access code or the comparable data being used as described in Sections 118a, 119, 119a, 126a, 126b or 148a shall not be liable to punishment. If there is no risk of such use or if the risk was eliminated without any involvement of the perpetrator, he shall not be liable to punishment if, unaware of this fact, he made serious efforts of his own volition to eliminate the risk.

DECLASSIFIED

5. Computer-related production, distribution or possession of child pornography:

This comes under the general provision of Section 207a of the Criminal Code ('pornographic representations of minors'); there is no specific reference to commission of the offence by means of a computer:

Section 207a (1) Anyone who

1. produces pornographic representations of minors (subsection (4)) or
2. who offers to, obtains for, passes on to, shows to or otherwise makes available to another person such pornographic representations of minors (subsection (4)),

shall be liable to imprisonment for a term of up to three years.

(2) Anyone who produces, imports, transports or exports a pornographic representation of a minor (subsection (4)) for the purpose of dissemination or who commits an offence under subsection (1) on a commercial basis, shall be liable to imprisonment for a term of six months to five years. Anyone who commits the offence as a member of a criminal organisation or who does so in such a way that the minor suffers particularly serious harm as a result of the offence, shall be liable to imprisonment for a term of one to ten years; the same punishment shall be incurred by anyone who produces a pornographic representation of a minor (subsection (4)) using serious violence or who, when producing the representation, endangers the life of the minor depicted, either with intent or with gross recklessness (Section 6(3)).

(3) Anyone who obtains or possesses a pornographic representation of a minor who is aged over 14 but under 18 (points 3 and 4 of subsection (4)), shall be liable to imprisonment for a term of up to one year or to a fine of up to 720 daily rates. Anyone who obtains or possesses a pornographic representation of a person aged under 14 (subsection (4)) shall be liable to imprisonment for a term of up to two years.

(3a) Anyone who knowingly accesses pornographic representations of minors on the Internet shall be liable to the same punishment as provided for in subsection (3).

DECLASSIFIED

(4) Pornographic representations of minors are

1. realistic depictions of a sexual act on a person aged under 14 or by a person aged under 14 on themselves, on another person or with an animal,
2. realistic depictions of events involving a person aged under 14, the observation of which creates the impression, in the circumstances, that a sexual act is taking place on a person aged under 14 or is being performed by the person aged under 14 on themselves, on another person or with an animal,
3. realistic depictions

a) of a sexual act within the meaning of point 1 or of events within the meaning of point 2, but with minors aged over 14 but under 18 years, or

b) of the genitals or the genital area of minors,

to the extent that these are provocatively distorted depictions that are reduced solely to this content and are devoid of any indication of another context, which are intended to be used for the sexual arousal of the viewer;

4. images whose viewing - as a result of modification of a representation or without the use of such - creates the impression, in the circumstances, that they are depictions as described in points 1 to 3.

(5) Liability to punishment under subsections (1) and (3) shall not be incurred by anyone who

1. is in possession of a pornographic representation of a minor aged over 14 but under 18 with their consent that was produced for that minor's or the person's own use, or

1a. produces or possesses a pornographic representation of a minor aged over 14 but under 18 of themselves, or offers, procures, passes on, shows or otherwise makes available to another person such representation for their own use, or

2. produces or possesses, for their own use, a pornographic representation of a minor aged over 14 but under 18 as described in point 4 of subsection (4), as long as this act does not give rise to a risk of dissemination of the representation.

DECLASSIFIED

6. Computer-related solicitation or "grooming" of children:

Section 208a (1) Anyone who,

1. by means of telecommunications or using a computer system, or
2. by other means involving concealment of his or her intention,

suggests or agrees to a face-to-face meeting with a person aged under 14 and takes specific preparatory action to carry out the face-to-face meeting with that person, and does so with the intention of committing a criminal act against that person as defined in Sections 201 to 207a (1), point (1), shall be liable to imprisonment for a term of up to two years.

(1a) Anyone who establishes contact with a person aged under 14 by means of telecommunications or using a computer system, with the intention of committing a criminal act as defined in Section 207a (3) or (3a) concerning a pornographic representation (Section 207a (4)) of that person, shall be liable to imprisonment for a term of up to one year or to a fine of up to 720 daily rates.

(2) Anyone who, of their own volition and before the authority (Section 151(3)) has learned of that person's wrongdoing, renounces his intended action and confesses his wrongdoing to the authority, shall not be liable to punishment under Sections (1) and (1a).

7. Computer-related fraud or forgery

In the general definitions of fraud and forgery offences, there is no specific reference to commission of the offence using a computer. Offences the definition of which does include such a reference:

'Fraudulent misuse of data processing':

Section 148a (1) Anyone who, with the intention of unlawfully enriching himself or a third party, causes material loss to another person by influencing the results of an automated data processing operation, by means of programming; entering, altering, deleting or suppressing data; or otherwise affecting the course of the processing operation, shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.

DECLASSIFIED

(2) Anyone who commits the offence on a commercial basis, or causes a loss exceeding EUR 5 000 by committing the offence, shall be liable to imprisonment for a term of up to three years; anyone who causes a loss exceeding EUR 300 000 by committing the offence shall be liable to imprisonment for a term of between one and ten years.

'Falsification of data'

Section 225a Anyone who, by entering, altering, deleting or suppressing data, intentionally creates false data or falsifies genuine data for use in legal transactions to prove a right, a legal relationship or a fact, shall be liable to imprisonment for a term of up to one year.

8. Computer-related identity offences

Generally included in any case in the definition of the basic offence. General aggravating factor in identity fraud (point 8 of Section 33(1) StGB):

Section 33 (1) An aggravating factor shall be held to exist, in particular, if the offender

8. has, in the process of committing the offence, fraudulently used another person's personal data in order to gain the trust of a third party, and in so doing caused prejudice to the lawful owner of the identity.

Section 119 StGB - 'Breach of telecommunications secrecy'

Section 119 (1) Anyone who uses a device that has been attached to a telecommunications or computer system or otherwise enabled to receive a signal with the intention of procuring, for himself or for another unauthorised party, knowledge of a communication transmitted by means of that telecommunications or computer system which is not intended for him shall be liable to imprisonment for a term of up to six months or to a fine of up to 360 daily rates.

(2) The perpetrator shall be prosecuted only if the aggrieved party has given his consent.

DECLASSIFIED