Council of the
European Union

Brussels, 19 May 2017
(OR. en)

7159/1/17
REV 1 DCL 1

GENVAL 20
CYBER 36

DECLASSIFICATION

of document:	7159/1/17 REV 1 RESTREINT UE/EU RESTRICTED
dated:	2 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 Germany

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, 2 May 2017
(OR. en)

7159/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 20
CYBER 36

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 Germany

ANNEX

Table of Contents

1. EXECUTIVE SUMMARY

The evaluation of Germany took place between 24 -27 May 2016 and included meetings with the relevant actors with responsibilities in the field of prevention and combating cybercrime as well as in the implementation and operation of European policies (Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Ministry of Economic Affairs and Energy, Federal Ministry for Family Affairs, Senior Citizens, Women and Youth, Federal Criminal Police Office (BKA), Federal Office for Information Security (BSI), German Competence Centre against Cybercrime, Bitkom (Digital Industry Association)).

Furthermore, a visit to the General Public Prosecution Office in Celle with the participation of prosecutors and police officers from Celle, Verden, Berlin, Cologne, Bamberg and Lüneburg was organised, which provided the team with a practitioner's point of view in the field of cybercrime.

As a general remark, the evaluation team is of the opinion that Germany is very committed and well equipped to tackle cybercrime. To this end a number of initiatives, good practices and measures are in place and might be used as examples for other Member States.

Considering the federal state structure of Germany, preventing and combating cybercrime require close cooperation at federal and *Land* level. Efforts are being made to connect these two levels and to ensure proper communication and coordination.

The national priorities in terms of cybercrime are linked to the EMPACT priorities projects developed as part of the EU policy cycle: prevention, capacity building, international and national cooperation, European strategy. Germany has a strong national cybersecurity strategy that it initiated in 1991 and, since 2009, it has also had a police cybersecurity strategy which was last revised in 2015.

Most of the *Lander*(*s*) have either specialised cybercrime prosecutors or have set up dedicated sections or contact persons for cybercrime in the public prosecutor's offices.

With regard to the police authorities, most of the *Lander*(*s*) have set up special cybercrime departments within their *Land* Criminal Police Offices. Staff in the specialised departments have in–depth IT knowledge and special IT expertise. Furthermore, the Federal Criminal Police Office has a unit responsible for cybercrime (Group SO4).

Regarding legislation, Germany ratified the Council of Europe Convention on cybercrime and has transposed Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography, and Directive 2013/40/EU on attacks against information systems, into national legislation.

Cooperation with the private sector is very good. Germany has set up a reliable and very structured public-private partnership at federal and *Land* level. The BKA entered into an agreement with the German Competence Centre against Cybercrime (G4C), an association composed of a number of banks. There is also good cooperation with BITKOM and Deutsche Telekom.

In the field of cyber-attacks, the BSI (CERT) is responsible for the public administration network and there is very good cooperation with various other bodies (active information, exchange of good practices, common handling of incidents). There is a limited legal obligation incumbent upon critical infrastructure to report cyber incidents to the BSI, but the police try to encourage reporting as much as possible.

In order to combat child sexual exploitation or child abuse on the internet, national authorities don't use the 'blocking access approach' since they prefer the 'deletion approach' which is considered to be more effective.

Germany demonstrates very good international cooperation on cybercrime within Europol/EC3 and Eurojust, as well as with Interpol and other third parties. Some difficulties were reported during the evaluation visit in relation to cooperation with third countries.

Germany provides several awareness-raising and prevention programmes to inform the public and industry about the risks of cybercrime and to encourage the safe use of the internet. The national and *Länder* police are very much involved in these prevention campaigns.

The BKA has developed various initial and further training programmes on cybercrime, including in the field of ICT forensics. At *Länder* level, there are various training initiatives, for example, in *Land* North Rhein-Westfalia which organises a joint training programme for specialists from the *Land* police force and public prosecutors from Lower Saxony. The evaluation team considers this to be a good practice.

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 had been 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 preventing 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 2011/93/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.

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

Therefore, this will encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3, how feedback from the given actors is channelled to the appropriate police and social services, as well as cooperation with prosecution services. The evaluation focuses on implementing national policies with regard to the 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 the victims of cybercrime.

[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. Germany was the (third) Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, a list of experts involved 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 to delegations made by the Chairman of GENVAL on 28 January 2014.

The evaluation teams consist of three national experts supported by two 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 Germany were Mr Pierrick Buret (France), Mr Sven Kivvistik (Estonia) and Mr Timo Piiroinen (Finland). Three observers were also present: Ms Daniela Buruiana (Eurojust), Ms Claudia Warken (European Commission) and Mr Alexander Gutwin (Europol), together with Mr Steven Cras and Ms Carmen Necula 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 Germany between 23 and 27 May 2016, and on Germany's detailed replies to the evaluation questionnaire together with their detailed answers to the follow-up questions.

3. GENERAL MATTERS AND STRUCTURES

3.1. National cybersecurity strategy

The Federal Republic of Germany has a national cybersecurity strategy. It is available here: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf;jsessionid=A7CACE6B709E665A39AB488C5A406778.2_cid364?__blob=publicationFile

The cybersecurity strategy covers ten areas:

- Protection of critical information infrastructures
- Secure IT systems in Germany
- Strengthening IT security in public administration
- National Cyberdefence Centre
- National Cybersecurity Council
- Effective crime control - including in cyberspace
- Effective coordinated action to ensure cybersecurity in Europe and worldwide
- Use of reliable and trustworthy information technology
- Personnel development in federal authorities
- Tools to respond to cyber-attacks

Since 2009 there has also been a police cybersecurity strategy, which was last revised in 2015. It includes areas for improvement and recommendations on the following areas:

- Situation report
- Police cooperation
- Law
- Police-judicial cooperation
- Methods for fighting cybercrime

- Cooperation with third parties (outreach)
- Initial and further training
- Personnel development
- Organisational development
- Prevention
- Technology and logistics

In addition, some of the *Länder* have their own strategies and policies to combat and prevent cybercrime.

Given the wide range of cyber offences, there cannot be any genuinely tried and tested procedures or methods for investigating such offences. Each case is different; investigative procedures and methods must be tailored to the individual case and the investigative leads available. One of the most important investigative approaches is undoubtedly the use of network data tracks generated from communications in the form of personal data linked to IP addresses used, in the form of traffic data or - if an offence listed in the catalogue has been committed - surveillance of internet communications. Other important sources are the seizure and analysis of data carriers and e-mail mailboxes. If the cyber offence involves theft, bank and account details are also essential in order to trace the money. In particular, where phishing in connection with online banking is concerned, the tax administration is involved and covert measures are used to attempt , to obtain evidence of computer fraud carried out by gangs.

If investigations cannot be carried out using technical means, covert investigations must be conducted by officers. These covert police investigations, which can be conducted by deploying undercover officers under the general police regulation, generally take the form of investigations on forums and boards. But investigations of this kind are only likely to yield results if they are carried out over the long term.

In the *Land* of Brandenburg, a video chat system is operated which can be used with a user account once the user has registered, giving a name and e-mail address.

The service makes it possible to take part in group chats, in which images are transmitted in real time. If offences are committed on this video chat platform, e.g. by displaying an image of the erect male member, this is documented by the operator in real time. The operator identifies the IP address stored on the server and faxes it to the Public Prosecutor's Office. The latter swiftly initiates investigative proceedings, identifies the internet service provider from the IP address and - if the provider stores traffic data for a relevant period - orders the provider by fax, pursuant to Section 100j(1)1, first sentence and (2) of the Code of Criminal Procedure, to terminate the subscriber's account.

3.2. National priorities with regard to cybercrime

Prevention

The preventive activities are aimed both at citizens and at the business sector. At both federal and *Länder* level a wide range of measures are in place to draw attention to the current forms of cybercrime and to raise awareness among the population. For example, the competent authorities give prevention and security tips at events and on their websites.

In addition, there is an institutionalised public-private partnership called the 'German Competence Centre against Cybercrime e.V.' involving the Federal Criminal Police Office (*Bundeskriminalamt*, BKA), the Federal Office for Information Security (*Bundesamt für die Sicherheit in der Informationstechnik*, BSI) as well as three financial institutions (so far) and a manufacturer of anti-virus software (for background information see http://www.g4c-ev.org/ – DE only). Its aim is to exchange views on current modus operandi (which are often based on security loopholes) and perpetrator structures and to develop appropriate responses.
Where certain forms of cybercrime (may) affect consumer protection interests, the competent authorities inform the public accordingly and provide targeted advice. Active outreach work is done in this context.

Capacity building

Special emphasis is placed on cybercrime (in the narrower sense) in the fight against crime both at federal level and in the *Länder*, and it continues to be increasingly important.

The Federal Government has set itself the objective of further improving the material and human resources of the security authorities and of adapting technical and legal expertise to their new tasks. The powers of the BKA and the federal police will be strengthened in the fields of cybercrime, cyber espionage and cybersecurity. In the BKA, the Cybercrime Centre, which is responsible for analysis and investigation in this area, is being further expanded.

Training

Training is offered by various types of educational providers, (the Federal Criminal Police Office (*Bundeskriminalamt*, BKA), other *Länder*, the Federation of German Detectives (*Bund deutscher Kriminalbeamter*), universities and Europol) to staff of different professions depending on their level of training and training needs. As regards judges and public prosecutors, please see our comments under 10 B 1 (page 109 et seq.).

International and national cooperation

International cooperation, e.g. with the European IT security agency ENISA and with the Europol Cybercrime Centre, is to be strengthened. In general, international cooperation takes place through the Federal Criminal Police Office (*Bundeskriminalamt*, BKA), as well as directly through the competent authorities in individual cases. The central cybercrime units at federal and *Länder* level have good links to each other. Interdisciplinary cooperation between the specialised authorities at federal level will be improved through the National Cyber Response Centre's platform.

European strategy

The national priorities are consistent with the EU's strategic goals and operational action plans for fighting cybercrime. In line with the EU Policy Cycle 2014-2017, cybercrime has been identified as a priority for Germany and divided into three sub-projects:

- Credit Card Fraud
- Online Child Sexual Exploitation
- Cyber-attacks.

3.3. Statistics on cybercrime

3.3.1. Main trends leading to cybercrime

Cybercrime is a growing social problem. The increasing penetration of IT into almost all areas of life also means that there are more ways for cybercriminals to attack. Owing to the range of professional cybercrime services available in the underground economy ('cybercrime as a service'), the technical possibilities for carrying out cyber-attacks/cyber offences can also be exploited by criminals who lack technical expertise themselves.

In 2014, 246 925 cases of cybercrime committed using the internet ('computer as a tool') were recorded. A large majority of these related to fraud (74.2 %), particularly merchandise fraud (29.2 %). In addition, 49 925 cases of cybercrime in the strict sense[7] ('computer as a target') were recorded, including 11 887 cases (23.8 %) of data espionage and interception of data including preparatory acts, and 5 661 cases (11.3 %) of alteration of data and computer sabotage. The clear-up rate for cybercrime in the strict sense is 29.3 %, but only 17.7 % for alteration of data and computer sabotage. In addition, there were 23 670 cases of fraud using unlawfully obtained debit cards with PIN.

Owing to changes to the rules on the recording of statistics, it is not possible to compare these case numbers and clear-up rates with those of the previous year. It should also be noted that these figures include only cases which involved offences committed in Germany and which were finally dealt with by the police. Some particularly relevant phenomena, such as phishing in the field of online banking, extortion involving targeted DDoS attacks and the many other forms of digital extortion (for example by means of ransomware), are recorded in the Police Crime Statistics (PCS) under the PCS keys for the individual offences rather than under cybercrime. These types of offence are therefore not taken into account here.

In addition, in 2014 damage was recorded only in cases of computer fraud and fraud involving access authorisation to communication services. In 2014 such damage amounted to around EUR 39.4 million, the greater part of which – around EUR 36.9 million – related to computer fraud.

[7] Cybercrime in the strict sense includes all offences targeting the internet, data networks, information technology systems or their data (more specifically the following offences: computer fraud (PCS 517500), fraud involving access authorisation to communication services (PCS 517900), falsification of legally relevant data, deception in legal transactions in connection with data processing (PCS 543000), alteration of data/computer sabotage (PCS 674200), and data espionage and interception of data including preparatory acts (PCS 678000)).

Further details can be found in the Federal Cybercrime Situation Assessment, which is available at the following web address:
http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true

The phenomenon of cybercrime is becoming increasingly relevant to the performance of police duties. The internet allows levels of all types of crime to increase.

3.3.2. Number of registered cases of cyber criminality

The Police Crime Statistics (PCS) for the Federal Republic of Germany provide the basis for a survey of cybercrime offences. Crimes and offences handled by the (criminal) police, including punishable attempts, are recorded in the PCS on the basis of a defined catalogue of offences, together with the suspects investigated by the police. A case is recorded once the police department responsible for finishing the work on the case has completed its investigations and the file has been handed over to the Public Prosecutor's Office or the court. The Federal Criminal Police Office uses the individual data sets supplied to compile the annual Police Crime Statistics for the Federal Republic of Germany. Data from private bodies are taken into account in only a few individual cases to shed light on current phenomena.

Cases that come to the notice of the police are recorded according to where the offence was committed. In accordance with specific recording principles, each suspect is counted only once for the reporting period, regardless of the number of investigations carried out. For example, if a suspect has committed several offences which fall under different key numbers within a statistical domain, he/she is counted only once under each key number, under the next group(s) up and in the total number (genuine counting of suspects).

Regardless of the trends in the net case figures or damage figures, the intensity of criminal activity in the field of cybercrime and the potential risk for each internet user have continued to increase. This is due not least to the increased professionalism of the malware used and the greater specialisation and professionalisation demonstrated by the perpetrators.

In addition, the Police Crime Statistics (PCS) do not reflect cybercrime in its entirety. Cases of cybercrime are included under different offence keys. Cases where the victim lives in Germany but the offence was or may have been committed abroad are not recorded, for example. The presentation of cybercrime offences in the PCS is currently under review. The aim is to be able to give a more comprehensive view of developments in this area.

The PCS are outgoing statistics; cases handled by the police are recorded after conclusion of the investigations when the file is handed over to the public prosecutor's office.

It is not possible to compare the PCS with judicial statistics (see question 1.6 below) because there are sometimes considerable periods between the respective data entry times (PCS handover to the judiciary; final decision), and the recording principles and the legal classification systems differ.

For the area of criminal justice we can report on the numbers of adjudicated persons and convicted persons (see table below). These are recorded in the criminal prosecution statistics. 'Adjudicated persons' are defendants given penalty orders or whose cases were finally closed, after the main proceedings were opened, either by a judgment or by an order that the case be dismissed. They include convicted persons and persons in respect of whom other decisions (e.g. dismissal of the case, acquittal) were taken. "Convicted persons" are accused parties against whom a prison sentence, personal arrest, or a fine has been handed down under general criminal law (including by a penal order that has become non-appealable), or whose deed has been punished under juvenile criminal law by measures such as juvenile custody, disciplinary measures, or educational measures of reform and prevention. The criminal prosecution statistics are based on the provisions of criminal law.

Some provisions of the Criminal Code can be referred to as computer offences in the strict sense, while other offences can be committed by means of computers, the internet or in other ways, and it is not possible to make a statistical distinction in this respect. A distinction is therefore made between 'computer offences in the strict sense' and 'other offences' in the table below. This also has an impact on the convictions for cybercrime as a percentage of the total number of all convictions.

Taking the narrower concept of computer offences as a basis, the proportion was 0.3 % in 2013 (2 728 of 755 938 convictions); based on a broader understanding it was 0.7 % (5 788 of 755 938 convictions). For various reasons it is not possible to compare these percentages with the police figures (see question 1.4 above), not least because, unlike the criminal prosecution statistics, the Police Crime Statistics do not include traffic offences. There have been no significant changes in the conviction figures in the last few years (2011-2014) (see table below).

It should be noted that Section 202d of the Criminal Code establishing the offence of handling stolen data only entered into force in December 2015, and therefore no statistics in this regard have been recorded as yet.

Persons adjudicated for (= "A") and convicted of (= "C") computer offences

	2011		2012		2013		***2014***	
Section ... of the German Criminal Code - offence	A	C	A	C	A	C	***A***	***C***
Computer offences in the strict sense								
202a: Data espionage	80	48	73	41	64	30	***84***	***48***
202b: Phishing	2	1	5	2	3	2	***1***	***1***
202c: Acts preparatory to data espionage and phishing	2	2	2	2	1	1	***4***	***1***
263a: Computer fraud	3.439	2.797	3.393	2777	3.252	2.645	***3.241***	***2.628***
303a: Data tampering	50	27	59	36	53	32	***46***	***24***
303b: Computer sabotage	18	10	28	15	26	18	***22***	***12***
TOTAL COMPUTER OFFENCES IN THE STRICT SENSE	3.591	2.885	3.560	2.873	3.399	2.728	***3.398***	***2.714***
Other Offences								
184: Distribution of pornography	150	116	195	154	213	158	***282***	***222***
184a: Distribution of pornography depicting violence or sodomy	17	11	9	9	10	9	***13***	***11***
184b: Distribution, acquisition and possession of child pornography	1.716	1.611	1.892	1.798	1.795	1.679	***2.170***	***2.022***
184c: Distribution, acquisition and possession of juvenile pornography	109	90	112	100	125	101	***158***	***133***
184d: Distribution of pornographic performances by media services	14	12	13	11	18	13	***15***	***9***
130(2) subpara. 1 and 2: Incitement to hatred by media services	67	53	49	39	32	25	***57***	***43***
131: Dissemination of depictions of violence	15	6	15	12	16	12	***22***	***9***
266b: Misuse of cheque and credit cards	61	40	52	39	41	28	***42***	***20***
269, 270*: Forgery of data intended to provide proof	996	845	1.033	864	1.218	1.035	***1.371***	***1.159***
TOTAL OTHER OFFENCES	3.145	2.784	3.370	3.016	3.468	3.060	***4.130***	***3.628***
TOTAL COMPUTER OFFENCES	***6.736***	***5.669***	***6.930***	***5.889***	***6.867***	***5.788***	***7.528***	***6.342***

* Section 270 of the German Criminal Code is not covered separately in the criminal prosecution statistics.

Sources: Statistisches Bundesamt (Federal Statistical Office), Fachserie (subject-matter series) 10, Reihe (series) 3, Strafverfolgung (Criminal prosecution)

As regards police data, please refer to the Police Crime Statistics (PCS), which are available at the following address, including in English:
http://www.bka.de/DE/Publikationen/PolizeilicheKriminalstatistik/pks__node.html

The federal cybercrime situation assessments are also based on the Police Crime Statistics, and are available here:
http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true

Due to the changes in the statistical recording of cybercrime mentioned above, it is unfortunately impossible to compare the figures for 2014 with those for previous years, even within a publication series.

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

Budget allocations for law enforcement authorities for the fight against cybercrime (preventive and punitive) are based on the federal and *Länder* budgets. Additional external sources of finance are generally not available to police authorities. EU funding is possible only in exceptional cases, for example to finance international (EU-wide) research projects or in the framework of EMPACT measures.

The Federal Criminal Police Office (BKA) currently receives EU funding for the fight against cybercrime under the EU's (now expired) ISEC support programme (internal security, 2007 to 2013). The BKA, together with the Netherlands and Sweden, is implementing the 'Cyber OC – Scope and manifestations in selected EU Member States' project, which covers the period from 1 April 2014 until 31 March 2016 with a project size of around EUR 500 000. The project is being completed and its final report is now available on line at: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/PolizeiUndForshung/1_50_Cyber-OCScopeandManifestationsInSelectedEUMemberStates.html.
In 2014 it was possible once again for projects aimed at preventing and fighting cybercrime within the EU to be financed in part through applications for EU funds. The European Commission made around EUR 5 million available in the 'Internal Security Fund – Police' (ISF central) programme. Project applications can only be made in response to special calls for proposals.

In the *Länder*, funds are allocated as part of the budget for general duties. Additional posts or higher-than-planned expenditure are occasionally authorised. To our knowledge, the *Länder* have not applied for EU funds to date. The *Länder* make financial contributions to the ProPK police prevention programme in accordance with the 'Königstein formula'[8]. Under this programme, materials are produced and developed across the country, including on preventing cybercrime. The materials are accessed and used accordingly.

Germany has a strong national cybersecurity strategy initiated in 1991 and, since 2009, has also had a police cybersecurity strategy which was last revised in 2015.

In addition, some *Länder* have their own strategies and policies to combat and prevent cybercrime.

[8] The Königstein formula determines how the individual *Länder* of the Federal Republic of Germany participate in joint financing. Two thirds of the share to be contributed by a *Land* is based on tax revenue and one third is based on population size.

The aim of the national strategy is to provide an appropriate level of cybersecurity in Germany in connection with what is required by the administration and industry.

The German National Cybersecurity Strategy listed ten priority objectives and measures:

- Protection of critical infrastructure
- Secure IT systems in Germany
- Strengthening of IT security in Public Administration
- National Cyber Response Centre
- National Cybersecurity Council
- Effective measures to counter cybercrime
- Effective cybersecurity cooperation at European level
- Implementation of trustworthy and reliable IT
- Adequate development of personal resources and competences in Federal Government agencies
- Instruments for defending cyber-attacks

The need to have a harmonised protection level of IT security was underlined as was the fact that industry actors should implement security measures in this area.

Further consideration should be given to the following identified issues:

- Deterrence of malicious actors
- Consideration of military aspects within the strategy
- Introduction of concepts of active cyberdefence
- Improvement of the resilience of infrastructure by utilising networks separated from the internet
- Improvement of cooperation between authorities and industry to better deal with attacks
- Effective protection of privacy and informational self-determination in the European Single Market

3.5. Conclusions

- **Germany possesses two cybersecurity strategies, one at federal level and another more specific strategy at the level of the BKA. In addition, there are some cybersecurity strategies in place in some of the *Länder*. The National Cybersecurity Strategy covers a wide range of topics and there are two institutions in charge of cybersecurity (National Cyber Defence Centre and National Cybersecurity Council).**

- **The government involved the private sector in the drafting of the National Cybersecurity Strategy (economy, industry, Bitkom, etc). However, the evaluation team is of the opinion that other key actors, like the General Prosecution Service or law enforcement authorities, could be involved to a greater extent.**

- **The strategy is accompanied by an implementation plan with precise deadlines. The cybersecurity field is considered by the German police as the main challenge for the next 10-15 years.**

- **Protection of critical infrastructure includes state institutions, society and the economy. The National Cybersecurity Council includes relevant public administration representatives who cooperate with industry representatives. BSI cooperates well with ENISA.**

- **The national priorities target the main aspects of the phenomenon, such as prevention, capacity building, training, international and national cooperation, consistent with the EU Policy Cycle 2014-2017.**

- **In Germany, police criminal statistics are collected by BKA and cases of cybercrime may be included under different offences or, if the offender does not reside in Germany, are not included (even if the victim resides in national territory). However, the statistics system of BKA is currently under review in order to be made more comprehensive. The police criminal statistics are not comparable with the judicial statistics due to the fact that collection periods are incongruent (criminal offences are not recorded until the police investigation have been concluded and the respective files can be handed over to the public prosecutor's office or the court), recording principles and the data differ and individual cases may be categorized differently in penal law terms by the judiciary. Therefore there is no added value in combining police and judicial statistics.**

- **The federal and *Länder* budgets provide allocations for the fight against cybercrime. The BKA also received European funds for some projects, for example 'Cyber OC - Scope and manifestations in selected EU Member States'.**

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecutions and courts)

4.1.1. Internal structure

In Germany the following authorities and departments in particular are responsible for preventing, analysing and fighting cybercrime:

- The public prosecutor's offices of the *Länder* (for example the Central Unit for Combating Internet Crime at the Office of the Chief Public Prosecutor in Frankfurt-am-Main)
- The Federal Criminal Police Office (*Bundeskriminalamt*, BKA) (in particular the SO 4 group)
- Criminal police departments of the *Länder*
- The Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*, BfV)
- The criminal police offices of the *Länder* (*Landeskriminalämter*, LKAs)
- The offices of the *Länder* for the protection of the constitution
- The Federal Police (*Bundespolizei*, BPOL)
- The Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI)
- The Customs Criminal Investigation Office (*Zollkriminalamt*, ZKA).

Fighting cybercrime requires close cooperation at federal and *Länder* level. For this purpose, there are central points of contact in the BKA and in the *Länder*. In their work with the competent federal authorities (BKA, BSI, BPOL, BfV, ZKA), the single points of contact and joint expert conferences have proved their value and have led to the establishment of a close information network.

Prosecution is the responsibility of the *Länder*. Most *Länder* have certain public prosecutor's offices which either specialise in combating cybercrime (e.g. the *Länder* of Brandenburg (Cottbus public prosecutor's office), Thuringia (Mühlhausen public prosecutor's office) and Mecklenburg-Western Pomerania (Public Prosecutor's Office specialising in information and communications crime in Rostock)) or have set up dedicated sections or contact persons for cybercrime in the public prosecutor's offices (as in the *Länder* of Baden-Württemberg, Bavaria, Berlin, Bremen, Hamburg, Mecklenburg-Western Pomerania, Lower Saxony, Rhineland-Palatinate, Saarland, Saxony, Saxony-Anhalt and Schleswig-Holstein).

In 2011 Baden-Württemberg established a Central Unit for Combating Information and Communications Crime at the Office of the Chief Public Prosecutor in Stuttgart. For Lower Saxony, there is a central coordination and support unit (Central Organised Crime and Corruption Unit) at the Office of the Chief Public Prosecutor in Celle.

The Central Organised Crime and Corruption Unit, whose remit includes internet crime and crime in the field of information and communications technology, acts as coordinator and central contact point for cybercrime, including for the three public prosecutor's offices in Lower Saxony which specialise in combating information and communications technology crime (the public prosecutor's offices in Göttingen, Osnabrück and Verden). The Central Organised Crime and Corruption Unit's remit also includes providing training and advice. On 1 October 2014 Rhineland-Palatinate established the *Land* Central Cybercrime Unit at the Office of the Chief Public Prosecutor, with responsibility for prosecuting cybercrime throughout the *Land*. On 1 January 2015 Bavaria established a central unit for combating computer and internet crime (Bavarian Central Cybercrime Unit) at the Office of the Chief Public Prosecutor in Bamberg. On 15 March 2016, Saxony established a Saxon Central Counter-Cybercrime Department in the Dresden Office of the Director of Public Prosecutions, which serves as a contact point both for the offices of public prosecutions in Saxony and for the central departments in other states in cybercrime proceedings. It also coordinates education and continuing professional development for public prosecutors from Saxon on cybercrime. In addition, the Central department also investigates serious and complex cybercrime cases itself with the Saxon Cybercrime Competence Center (SN4C) in the State Criminal Investigation Department.

As of 11 April 2016, the Land of North Rhine-Westphalia has established a central Cybercrime Unit and Contact Point at Cologne public Prosecution Office. This unit deals with significant cybercrime proceedings, acts as a central contact point for police, judiciary, industry and academia and is involved in regional and cross-regional basic and further training programmes. Schleswig-Holstein ha established a central unit to coordinate the investigation of cybercrime at the Office of the Chief public Prosecutor.

In Mecklenburg-Vorpommern, pursuant to an instruction from the Office of the Chief Public Prosecutor, the investigation of cyber offences was transferred, as of 1 July 2012, to the specialised Public Prosecutor's Office for Information and Communications Crime in Rostock. The specialised team currently consists of a team leader and three specialists. The *Land* of Hessen has created a Central Unit for Combating Internet Crime at the Office of the Chief Public Prosecutor. Schleswig-Holstein has established a central unit within the Office of the Chief Public Prosecutor which coordinates the prosecution of cybercrime offences.

There are no courts with specific jurisdiction in most of the *Länder*. In North Rhine-Westphalia, however, Cologne regional court has a criminal division with special jurisdiction on account of the Central Cybercrime Unit and Contact Point located at Cologne Public Prosecution office.

4.1.2. Capacity and obstacles to successful prosecution

Separate cybercrime units have been set up at Federal and *Länder* level. In some cases, special departments for dealing with cybercrime have also been created within the services responsible for crime-fighting at some of the branch stations of *Länder* police forces.

At both Federal and *Länder* level, improvements to security agencies' equipment and human resources are continuing, and technical and legal competences are being adapted to the relevant tasks.

The capabilities of the Federal Criminal Police Office (BKA) and the Federal Police relating to cybercrime are to be boosted. The Cybercrime Centre in the BKA is to be expanded, and work on internet activities that span various different phenomena will be grouped together.

Interdisciplinary cooperation between specialist authorities will be improved through the National Cyber Response Centre's platform.
The law that entered into force on 18 December 2015 made handling stolen data a criminal offence.

The following (non-exhaustive) information has been reported with regard to the *Bundesländer*:

Baden-Württemberg
To step up the fight against cybercrime and optimise ICT user and investigative support in the area of digital evidence, at the beginning of 2012 the units of the *Land* Criminal Police Office of Baden-Württemberg (LKA BW) were merged into a new Cybercrime and Digital Evidence Department. Additional staff have joined the department since then, most recently as part of the implementation of the police reform on 1 January 2014, and it now counts 98 members.

As part of the implementation of the police reform, Criminal Police Inspectorates No 5 (cybercrime and digital evidence) were also set up at regional police headquarters. These inspectorates mirror the tasks of the Cybercrime and Digital Evidence Department (Department 5) in the LKA BW. Exceptions to this rule are *Land*-wide services such as operation of the telecommunications surveillance centre, mobile phone surveillance or network forensics, as well as internet research and the child pornography contact point. Those tasks are performed solely by the LKA BW.

In addition to a new department, new *Land*-wide bodies were set up such as the cybercrime/digital evidence steering group and working groups for individual thematic areas, such as investigations, digital evidence and data analysis.

Police prioritisation of the fight against cybercrime, in particular since the establishment of Department 5 in the LKA BW, has raised awareness among all staff not only of cybercrime in the narrower sense, but also of the fight against internet crime (cybercrime committed using the internet) in general. Overall, a significant improvement in the fight against cybercrime can be observed throughout Baden-Württemberg.

Berlin

The following departments in the Berlin police deal with cybercrime:
Land Criminal Police Office (*Landeskriminalamt*, LKA) 75: Forensic information and communications technology (ICT), including responsibility for the hotspots in the local directorates.

LKA 72: Central internet unit (investigative support in processing internet investigations which go beyond the normal duties of a case worker).

LKA 33: Department conducting investigations, with responsibility for data offences (Sections 202a to 202c, 303a to 303b, 269 to 271, 274(1) Subsections 2 and 348 of the Criminal Code) and phishing in connection with money laundering (Sections 263a and 261 of the Criminal Code).

LKA 33 is responsible for the thematic area ‘cybercrime’ at the federal and *Länder*-level Leaders’ Cybercrime Conference. The Berlin LKA’s central cybercrime contact point for businesses is based there. Both tasks require cooperation with the other *Bundesländer*. The central cybercrime contact point organises networking activities in Berlin and is by its nature the contact point for all matters relating to cybercrime.

In the area of cybercrime in the broader sense, jurisdiction lies with a large number of departments, depending on the offence. These include the following, by way of example:

LKA 13 – child pornographic images on the internet.

LKA 23/25 – infringement of copyright (using the internet).

LKA 33 – fraudulent goods or claims (online).

LKA Prev. – responsible for managing, coordinating and – in selected cases – initiating preventive measures.

Brandenburg

At police headquarters, the fight against cybercrime is carried out at three levels: by the specialised directorate of the *Land* Criminal Police Office, by the criminal police of the police directorates and by the inspectorates' criminal police commissariats.

The police headquarters has set up an 'anti-cybercrime network', with the collaboration of the specialised Public Prosecutor's Office, among others, 'to combat computer and data network crime, as well as violent, pornographic and other texts harmful to minors'. In addition, it pursues close national and international cooperation, for example by participating in the northern cybercrime network, cooperating with other federal and *Länder* police departments (including work shadowing and exchanges of experience), in order to extend cooperation with other authorities and institutions.

Saarland

In the *Land* Criminal Police Office, responsibilities in the area of cybercrime are divided between the LPP 222 cybercrime department (central unit) and nine criminal investigation services/police inspectorates. The LPP 222 cybercrime department is the Saarland police's central cybercrime unit within the meaning of the Act on the Federal Criminal Police Office (BKA) and on Cooperation between the Federation and the *Länder* in Criminal Matters. As such, the department serves as a link between the Saarland police departments and the LKAs or the BKA. In its capacity as the 'central cybercrime contact point for businesses and other public and non-public bodies', the specialised department develops and maintains contacts with companies and associations, scientific organisations and other bodies.

Saxony

In the Saxony police both the police directorates and the *Land* Criminal Police Office (*Landeskriminalamt*, LKA) are responsible for fighting cybercrime.

The *Land* Criminal Police Office handles cybercrime cases, including by order of the Saxony State Ministry of the Interior, upon assignment by the Federal Criminal Police Office to Saxony, provided that the Saxony State Ministry of the Interior does not declare any other police department as competent, or upon assignment by the Office of the Chief Public Prosecutor or at the request of a public prosecutor's office.

In addition, the *Land* Criminal Police Office may take over the running of police investigations if inter-directorate investigations are necessary and consistent prosecution seems appropriate, or if another police department requests it to do so because of the volume, regional nature or high visibility of the investigations.

A key element of the reorientation of the fight against cybercrime in the Saxony police was the establishment of a Cybercrime Competence Centre (SN4C) in the LKA on 10 June 2014. The SN4C pools the information and communications technology (ICT) expertise that was previously 'dispersed' across different departments into one unit under unified management.

Schleswig-Holstein

In Schleswig-Holstein, the investigations and central unit tasks in cybercrime cases and for offences connected to child pornography are carried out at different levels of the police:

Land Criminal Police Office:

- 'Central Cybercrime Unit' project
- Central unit (central contact point for federal and *Land* departments, businesses and public and non-public institutions)
- Investigations aimed at combating offences classified as cybercrime under the restricted definition
- Central preservation of computer evidence for the *Land* Criminal Police Office (*Landeskriminalamt*, LKA) and at *Land*-level
- Point of contact for child pornography.

District criminal police inspectorates:

- Regional preservation of computer evidence for the regional court districts.

Criminal police inspectorates/criminal police units:

- All offences that cannot be classified as cybercrime under the restricted definition, including:
- Goods/commercial credit fraud
- Child pornography.

In addition, the anti-cybercrime strategy working group is currently conducting an analysis of the present situation in the Schleswig-Holstein police as regards organisational and substantive requirements for effectively combating cybercrime.

The 'Central Cybercrime Unit' project was launched on 1 February 2014 at the *Land* Criminal Police Office (*Landeskriminalamt*, LKA). The project involves merging the LKA's central preservation of computer evidence group, investigations into 'restricted definition' cybercrime cases, the point of contact for child pornography and the single point of contact for cybercrime.

Thuringia

In the Thuringian police, the institutions for preventing and combating cybercrime and for forensic analysis/assessment in that field are organisationally separate.
Due to the different thematic areas involved, the prevention of cybercrime falls within the sphere of activity of various state and non-state bodies. In addition to the police and the judiciary, educational establishments in particular should be mentioned here. Cooperation takes place on an ad hoc basis, but there is no coordination between the institutions at present.

Criminal investigations in the area of cybercrime are handled by both the Thuringia *Land* Criminal Police Office (*Landeskriminalamt*, LKA) and the local competent departments, depending on the type of offence.

On 1 September 2014, Department 64 (Cybercrime) was set up in the Thuringia LKA to increase the effectiveness of the fight against cybercrime. The department is subdivided into units for analysis of and combating cybercrime, and the central technical analysis unit for combating child and youth pornography. Special cybercrime cases, criminal investigations in connection with the dissemination of child and youth pornography, and criminal investigations carried out where there is a suspicion of child sexual abuse, where the criminal act consists in producing child pornographic publications, are handled by the Thuringia LKA.

All other offences in the area of cybercrime are handled by the local competent departments in the *Land* Police Inspectorates.

The backing up and processing of data secured in cybercrime proceedings for analysis by case workers is carried out both by Department 43 of the Thuringia LKA and by the regional evidence preservation units attached to the individual *Land* Police Inspectorates. In cases where a technically complex analysis is necessary, data analysis is carried out entirely by members of Department 43. Reports are also drawn up exclusively by that department. Special IT investigators work in the regional evidence preservation units and Department 43.

Department 33 of the Thuringia LKA performs technical operations and provides investigative support for Thuringia (e.g. implementation of telecommunications surveillance measures).

Expert conferences are held to exchange experience and expertise between the departments concerned. Department 64 is available to answer technical queries from the Thuringian police authorities with regard to cybercrime.

According to the division of powers between the Federal level and the *Länder* as provided for in the Basic Law, the exercise of state powers and the discharge of state functions is a matter for the *Länder*, unless otherwise provided for or permitted by the Basic Law. In accordance with that principle, responsibility for criminal prosecution basically lies with the prosecution authorities of the *Länder*, i.e. the Public Prosecutor's Offices and their investigative staff. In special cases, namely in matters relating to protection of the state, powers lie with the Federal Prosecutor-General's Office and the Federal Criminal Police Office. The Federal Criminal Police Office has a unit responsible for cybercrime (Group SO4). Prevention programmes are developed by the '*Länder* and Federal Police Crime Prevention' project lead, aimed at various target audiences, depending on the type of cybercrime offence .

Most of the *Länder* have set up special anti-cybercrime departments within their *Land* Criminal Police Offices. Staff in the special departments have in-depth IT knowledge and special IT expertise.

4.2. Law enforcement authorities

The following non-exhaustive information was received from the *Bundesländer*:

Berlin:

In Berlin, cybercrime in the strict sense (not including online card fraud) is dealt with by the police in the *Land* Criminal Police Office (LKA) LKA 33, more specifically by units LKA 336 (phishing relating to online banking) and LKA 335 (data offences including computer sabotage). There are a number of stations which deal with cybercrime in the broad sense. The physical use of payment cards (including skimming) is dealt with by LKA 36. LKA 37 is responsible for the fraudulent obtention of services and goods using payment card data. LKA 13 is responsible for images of child abuse on the internet (child pornography).

These stations are also responsible for prevention as part of the tasks assigned to them. If stations belonging to the Berlin police need support for internet investigations (including live forensics), LKA 722 stands ready to act as the central internet office to provide assistance throughout the process. LKA 75 is responsible for the forensic analysis of confiscated data carriers or copies of them. At the branch directorates (Directorate 1-6), specialist departments for ICT investigation support have been established in the *Ref VBs* (crime departments). In addition to the analysis of mobile phones, these departments deal with a whole series of ICT issues to assist in the process (e.g. adapting the data format of surveillance cameras for evaluation in a case).

Mecklenburg-Western Pomerania

Depending on the basic offence, cybercrime offences in Mecklenburg-Western Pomerania (M-WP) are usually dealt with by the Criminal Police Commissariats, the Criminal Police Inspectorates in Special Commissariats No 5 (Finance, Environment and Cybercrime), or by the M-WP *Land* Criminal Police Office.

In addition, the Criminal Police Inspectorates are responsible for offences against the confidentiality, integrity and availability of computer data and systems (in particular Sections 202a-d, 263a, 303a, b of the Criminal Code) and other offences which it takes special IT expertise to process.

Furthermore, when a case requires central processing because, for instance, more in-depth IT knowledge, special IT expertise and/or considerable national or international coordination are necessary, it is the M-WP *Land* Criminal Police Office which is responsible.

Unit 45/Cybercrime was set up in the M-WP *Land* Criminal Police Office with effect from 1 March 2011. Unit 45 is divided into the following departments: general/analysis; investigations; investigative support, and the child pornography contact point. Unit 45 also acts as the central cybercrime contact point and supports the Criminal Police Commissariats and Criminal Police Inspectorates in investigations.

Saxony-Anhalt

Such offences are usually dealt with by the police stations with local jurisdiction. The *Land* Criminal Police Office (LKA) has jurisdiction over investigations into cases of cybercrime in the strict sense (criminal acts against state institutions and bodies or prominent public figures) and, for example, when new *modi operandi* appear, especially when extensive damage to a number of persons or to medium or large businesses has already occurred or is likely to occur as a result of the offences. In some cases, responsibility for dealing with a case is sometimes coordinated between the LKA and the police directorate with jurisdiction.

The fields of information and communications technology (ICT) forensics are covered in the LKA and in the three police directorates and, in terms of organisation, are kept separate from the investigative fields.

As already mentioned, unit 4C was set up in the LKA on 1 June 2012 to fight cybercrime. It has departments for ICT forensics (collection and analysis of computer evidence, encryption experts, mobile phone forensics, forensic ICT), ICT investigative support (telecommunications surveillance, technical operational unit, IT investigative support) and cybercrime investigations with the Analysis and Coordination Centre for Child and Youth Pornography.

Thuringia

Specialised staff are deployed at all levels. The *Land*'s central prevention centre comes under the *Land* Police Directorate (HQ), department SG 12/Crime. Each *Land* Police Inspectorate has a criminal police advice centre and each police station has two prevention officers.

Both the Federal Criminal Police Office (BKA) (Group SO4) and the 16 *Land* Criminal Police Offices (LKAs) of the *Bundesländer* have set up anti-cybercrime services or are making concrete preparations to do so. The structure of each individual service varies considerably due to Germany's federal structure. There are also forensic special services which are used for the collection and analysis of evidence. Each criminal police station has an IT evidence analysis section.
The following information (indicative) was received from the *Bundesländer*:

Baden-Württemberg

At the beginning of 2012 the existing Inspectorates in the Baden-Württemberg (BW) *Land* Criminal Police Office (LKA) were merged into a new Cybercrime and Digital Evidence Department to improve law enforcement in the field of cybercrime. New staff have joined the Department since then, and it now counts 98 members.

In addition, Criminal Police Inspectorates No 5 were set up in the regional police headquarters. Their tasks mirror those of Department 5 of BW's LKA. Exceptions to this rule are national services such as the telecommunications surveillance centre operations, mobile phone surveillance or network forensics, as well as internet research and the child pornography contact point. Those tasks are performed solely by the LKA.

In addition to the 'investigative' department, specially trained officers work in IT forensics in both the LKA and the local Criminal Police Inspectorates. Capabilities will be strengthened further thanks to the creation in 2014 of the cybercrime detective career path (recruitment of IT and engineering graduates followed by shortened police training).

Berlin

Berlin *Land* Criminal Police Office (LKA 75) is responsible for the forensic examination of digital evidence. Some of the members of staff there have completed training as experts. The other members also have a high level of expertise. Several IT specialists also work in the department. LKA 72, including the central internet unit, also has a number of highly qualified and expert members. They also 'research', in the broad sense, cybercrime. Their tasks include network forensics. Some members of LKA 33 inspect confiscated evidence or secure and analyse data in accordance with forensic principles. They also conduct investigative proceedings.

Brandenburg

At Brandenburg Police Headquarters, the fight against cybercrime is organised in three stages. Fighting cybercrime is also part of every police officer's tasks when acting as first responder. In order to continue to meet the growing challenges of cybercrime, Brandenburg police has recruited specialised IT staff and, depending on their qualifications, is offering them special development and career opportunities.

Mecklenburg-Western Pomerania

Unit 55 (ICT Forensics and Special Photography) of the M-WP *Land* Criminal Police Office is responsible for the forensic analysis of digital evidence for all types of crime. Forensic analysis for a specific type of offence can also be conducted in Unit 45. There are posts for ICT Forensics Experts in Unit 55.

Saarland

Land Police Headquarters (LPP) Unit 222 Cybercrime is responsible for this in Saarland. The Unit is the central cybercrime department in the Saarland police: it acts as contact point for IT investigative support for the police stations in Saarland, is responsible for investigations in prominent cybercrime cases, and acts as Central Cybercrime Contact Point (*ZAC*) for businesses and other public and non-public entities. Two IT posts in Unit LPP 222 and, in LPP 4.7, IT forensics posts for IT forensic experts, have been set up as special posts for IT forensic experts.

Saxony

In Saxony, depending on the aim of the analysis, the workload in the competent public prosecutor's office and the timeline, (forensic) analysis in the field of cybercrime is outsourced for evaluation and preparation. In some cases analysis is conducted directly in SN4C or at the forensic institute of the *Land* Criminal Police Office.

Bavaria

The Bavarian *Land* Criminal Police Office (LKA) has had a special department for the investigation of cybercrime in the form of Section 54 since 1 January 2014. It consists of Unit 541, which is the Central Cybercrime Unit (*ZAC*); Unit 542, which includes several special investigation teams; and Unit 543 for network investigations. Special investigation departments have also been established at the Munich Police Headquarters and the Mittelfranken Police Headquarters, all of which have specialised investigators with IT training (known as 'cybercops'). Investigative measures in the telecommunications field (telecommunications surveillance, traffic data collection, IMSI catchers, etc.) are carried out by Unit 633, the Bavarian Telecommunications Surveillance Centre.

All local *Präsidiums* have cybercrime departments and regional Evidence Collection and Analysis Centres (*RBA*) to carry out forensic analysis and the coordination of telecommunications surveillance measures. Unit 210, which is the Forensic ICT Unit in the Bavarian *Land* Criminal Police Office, provides another service which evaluates confiscated documents.

Hamburg

Hamburg police force has a specialised department in which investigative officers and computer forensics officers have been brought together for investigative tasks (LKA 54-Cybercrime). Police officers work alongside employees (computer scientists) in investigations and forensics alike.

Thuringia

The future structure of the recently created Unit 64 in Thuringia Criminal Police Office (LKA) was mentioned in point 1.3 (Annex 1).

In the field of ICT forensics in Thuringia, each of the seven *Land* Police Inspectorates has a Regional Evidence Collection Unit (*RBE*) which secures and prepares electronic data for case work, and deals with simple IT problems within its area of competence.

In Thuringia, Unit 43 ICT Forensics performs these tasks. Unit 43 is also responsible for coordinating training, writing reports and handling more difficult cases. The staff in Unit 43 have been specially trained for this purpose.

4.3. Other authorities/institutions/public-private partnerships

Federal and *Länder* offices for the protection of the constitution

Federal and *Länder* offices for the protection of the constitution perform specific, legally defined tasks. The main task is to observe conduct referred to as 'activities'. Under Section 3(1) of the Federal Act on the Protection of the Constitution (*Bundesverfassungsschutzgesetz*) observation is focused on:

- Activities directed against the free democratic basic order, the existence or the security of the Federation or *Länder*
- Activities aimed at unlawfully damaging the administration of the constitutional organs of the Federation or *Länder* or their members
- Activities constituting a threat to security or secret service activities falling within the scope of this law undertaken for a foreign power
- Activities within the scope of this Act which endanger interests of the Federal Republic of Germany abroad through the use of violence or preparatory acts to that end, or
- Activities which are counter to the principles of international understanding (Article 9(2) of the Basic Law) and, in particular, which are incompatible with the peaceful coexistence of nations.

Activities outside this context are not covered by the statutory allocation of tasks even if they are harmful to individuals, society or the state. The wide scope of cybercrime is therefore relevant for the protection of the Constitution only if the activities described are connected to it. The Office for the Protection of the Constitution has no executive powers. Prevention of specific threats and law enforcement are therefore outside its remit.

The Federal Office for Information Security (BSI)

The Federal Office for Information Security (BSI) was set up on 1 January 1991 and falls within the remit of the Federal Ministry of the Interior. The BSI is responsible for safeguarding the IT of Germany's federal administration and critical infrastructure and, in its capacity as a neutral agency, also performs advisory, warning and information functions related to IT security issues in the information society. It currently employs some 600 IT staff, physicists, mathematicians and other employees. There are plans to recruit more staff. The BSI's headquarters are in Bonn.
Pursuant to the Act on the Federal Office for Information Security (BSI Act - BSIG), the BSI's tasks include:

- protecting federal networks, detecting and thwarting attacks on government networks
- testing, certifying and accrediting IT products and services
- acting as the central agency for IT security in the field of IT of critical infrastructures
- warning about malware or security gaps in IT products and services
- providing IT security advice for the federal administration and other target groups
- making citizens more aware of IT issues and information security and providing them with information
- developing uniform and mandatory IT security standards
- developing cryptosystems for federal government IT.

Cyberdefence Centre

Under the leadership of the Federal Office for Information Security (BSI), the Federal Office for the Protection of the Constitution (BfV), the Federal Office of Civil Protection and Disaster Assistance (BBK), the Federal Criminal Police Office (BKA), the Federal Police (BPol), the Customs Criminal Investigation Office (ZKA), the Federal Intelligence Service (BND) and the German military together make up the National Cyberdefence Centre (Cyber-AZ).

All these authorities cooperate while strictly observing their statutory tasks and powers. The Cyber-AZ is linked up to the situation centres and the relevant bodies of the participating authorities where the operational work is performed.

All information on cyber-attacks that authorities gather within their remit is pooled at the Cyber-AZ. Accordingly, the BSI assesses cyber-attacks from a technical point of view, the BfV deals with the question of whether the attack possibly emanates from a foreign intelligence service and the BBK assesses the consequences of possible attacks for infrastructures. The other participating authorities add their knowledge on new attack methods and tools, so that an up-to-date, comprehensive situation assessment is available as soon as possible.

The fight against cybercrime is coordinated by the police nationwide through Federation/*Länder* cooperation, in particular by the Working Group of Heads of the *Länder* Criminal Police Offices and the Federal Criminal Police Office (AG Kripo) and its subordinate bodies, the (punitive) Fight Against Crime Committee (KKB) and the (preventive) Police Crime Prevention Committee. In addition to the above- mentioned bodies, the State Protection Committee (K-ST), deals with this matter in a Federation/ *Länder* working group on 'politically motivated cybercrime'.
In addition, the Leaders' Cybercrime Conference takes place at the Federal Criminal Police Office twice a year. Participants include the decision-making heads of the *Länder* central cybercrime departments and the BKA.

In the *Länder*, the coordination is carried out in accordance with the organisational rules laid down in the laws of the *Länder*.

4.4. Cooperation and coordination at national level

4.4.1. Legal or policy obligations

The Act increasing the security of information technology systems (IT Security Act), which entered into force on 25 July 2015, introduced tighter IT security requirements for critical infrastructure operators and introduced a requirement to report certain IT security incidents.

Specifically, operators are required to report security incidents that affect the IT of a critical infrastructure. The requirement to report incidents should facilitate a quicker, complete situation assessment and faster implementation of targeted countermeasures in the event of an attack.

Pursuant to Article 1(2) of the IT Security Act, the systems, equipment or components that constitute critical infrastructure within the meaning of the law should be laid down by legal regulation.

If critical infrastructure operators fall under specific laws such as the Act on electricity and gas supply (EnWG) or the Act on the peaceful use of nuclear energy and the protection against its hazards (Atomic Energy Act - AtG), then those operators' obligations are regulated separately in those laws.

The requirements for telecommunications operators to report incidents are being extended in conjunction with the new provisions for critical infrastructure; they must now also report to the Federal Network Agency damage which could lead to considerable security breaches. Previously, a report was only required once the security breach had occurred. Moreover, the reporting requirement is being extended to malfunctions which might lead to reduced ability or to unauthorised access to the users' telecommunications and data processing systems. If the reported security breaches affect IT, the Federal Network Agency always notifies the BSI. Extending the reporting requirements makes for a better and more accurate assessment of attacks on telecommunications networks and services.

Furthermore, telecommunications companies must inform users if they become aware of incidents emanating from users' systems. This applies in particular to botnets which have installed themselves on users' computers. However, this notification requirement applies only if the telecommunications provider already knows the user.

The IT crisis management structures have taken on the task of managing serious cyber-attacks.

Germany's IT crisis management is undertaken essentially at the National IT Crisis Response Centre (IT-KRZ), at the Federal Office for Information Security (BSI). The IT-KRZ is evolving progressively out of the National IT Situation Centre and the Federal Computer Emergency Response Team (CERT-Bund). The so-called 'particular situation' or IT crisis can thus be managed by drawing on the BSI's relevant experts and support staff based on a scalable approach. The IT-KRZ is managed using a staff cell model, similar to general crisis and disaster protection cells, where all the relevant people are grouped together to manage organisational and technical tasks. Tactical/technical tasks such as situation awareness and assessment and prioritisation are carried out and measures recommended. Specialists from the whole BSI are brought together according to the situation and provide wide-ranging technical expertise. Through the staff cells, communication is established with the BSI's target groups e.g. authorities and critical infrastructure companies and appropriately coordinated crisis management processes are implemented.

The press office and the legal team are likewise involved, as are, where applicable, liaison persons from other authorities - e.g. the BKA - in their respective domains. This includes in particular representatives of the National Cyber Response Centre who help maintain contact with the German security authorities. The IT-KRZ is supported by the organisational staff cells for tasks such as personnel management, logistics and the internal service.

If the scope of the technical crisis has the potential to extend to other areas of public life or a political dimension is added, the crisis cell of the Federal Ministry of the Interior (BMI) is activated. This cell is responsible for crisis management in general, for IT crisis aspects, and for other aspects of public life which might possibly be affected owing to interdependencies e.g. civil protection (security of supply) or counter-terrorism (identification of perpetrators). A specific staff unit within the BMI crisis team is responsible for IT-related ministerial crisis management. This unit takes the IT assessment compiled and drawn up in the IT Crisis Response Centre, processes it at ministerial level and presents it to the BMI crisis cell. The unit is essentially the interface between the general, strategic-administrative team in the BMI and the operative-tactical (staff) IT-KRZ cell at the BSI.

To complete the situation report, there are naturally exchanges between the BSI IT Situation Centre, the BMI Situation Centre and the Joint Information and Situation Centre (GMLZ). Other situation centres are involved depending on the circumstances.

Moreover, there is communication and cooperation at both national and international level with specialised communities, especially through the IT-KRZ. CERT networks have formed worldwide, with the aim of cooperating on cyber incidents, including mutual support for the management of IT situations. CERT networks have a similar focus to some extent e.g. government/authorities' CERTs and others, e.g. with teams from business, science and the authorities.

The differentiated set-up of teams and their partially multidisciplinary composition should be explicitly seen as an advantage since they can draw on broad expertise. The international dimension further supports this. In addition to day-to-day business, these networks contribute to IT crisis management since they carry out regular exercises.

Successful civilian-military cooperation on IT incident processing and CERT tasks has existed for years at national level between the BSI and the German armed forces. The BSI is listed at NATO as the National Cyber Defence Authority and is, in the event of a major cyber-attack perpetrated by a state, the primary contact point for Germany. The emphasis of the German armed forces' CERT (*CERT-Bundeswehr*) is on the protection of their own military networks and it focuses on that work together with the other international military CERTs.

IT-KRZ has long-established and tested crisis management channels in the public administration, in particular the federal administration and for German businesses in the field of critical infrastructure. A range of BSI mechanisms and cooperation can cover a wide spectrum, reach most German businesses and also the public.

In the area of online card fraud, there is wide-ranging cooperation between the Federal Criminal Police Office and the private sector. Examples include cooperation with the 'Debit- und Kreditkarten in Deutschland' ('the Debit and Credit Card') security working group and the National Cybercrime Cooperation Unit, in particular the 'institutionalised Public-Private Partnership' (**iPPP**). As regards increased payment card security, there is cooperation with companies in order to prevent the tampering of POS (point-of-sale) terminals and ATMs, and on the switch from magnetic strip to chip card technology.

In addition, law enforcement authorities in the *Länder* work in various ways with companies, particularly with banks, so as to combat and solve crimes involving online fraud. Set out below, for instance, is an indicative outline of the cooperation between law enforcement authorities and companies in Brandenburg and Saxony-Anhalt:

In **Brandenburg**, the central cybercrime contact point for companies, agencies and citizens was set up in the specialised directorate of the Criminal Police Office (police headquarters). This also functions as a single point of contact.

The specialised directorate of the Criminal Police Office regularly takes part in events such as those held by the Brandenburg's chambers of commerce and industry, so as to pass on cybercrime information known to the police, establish contacts in the business and IT fields or exchange information on IT security within companies.

In **Saxony-Anhalt,** the police work closely with EURO-Kartensysteme GmbH (a services and competence centre) in the area of card-based payments within the German banking industry. Queries are also sent to individual credit card companies. However, these credit card companies do not always send a response.

Every year the working group 'sicherheit der Kartenorganisationen in Deutschland' (card organisation security working group) holds a practice-based symposium on payment card crime, a forum for the latest security strategies and approaches in the field. Participants include crime investigators from specialised units in the German *Länder* and the Federal Criminal Police, as well as representatives from credit card and security companies. In addition, the above meet on a voluntary basis four times a year in order to exchange information.

There is intensive information exchange between the police, credit card companies and ATM/terminal industry representatives. Specially trained or skilled credit card company employees develop industry-specific security concepts. They work closely with the police authorities which can contact them at any time. Public awareness is raised through relevant prevention material provided by the police. For example, security awareness is raised through short films. When requested, police officers run training sessions in financial institutions. The introduction across Europe of EMV card chip technology and the general phasing out of debit card magnetic strips by financial institutions has greatly improved security against skimming attacks on German ATMs. This has made it more difficult to use counterfeit cards.

Law enforcement authorities do not have any powers as regards authorisation of online transactions. Again, when it comes to prevention, emphasis is placed on the need to exercise caution when making online payments. As a rule, banks do not always report incidents, as the damage caused by the misuse of card data accounts for only a fraction of the total turnover.

An obligation to surrender evidence exists under the Code of Criminal Procedure (*Strafprozessordnung* – StPO). Cooperation with the private sector is supported and improved by establishing appropriate institutions for cooperation between the private sector and public administration/law enforcement bodies (for example, the 'German Competence Centre against Cybercrime e.V. ' (G4C) between the BKA/BSI and several institutions from the private sector). Similar efforts have also been seen in the *Länder*, with the German police being organised at this level due to Germany's federal structure. Germany transposed the provisions of the E-Commerce Directive on the liability of internet providers by means of Sections 7 to 10 of the Telemedia Act (Telemediengesetz – TMG). In principle, it is initially the respective content provider who has made content available on the internet that has criminal law responsibility for its own content. Pursuant to Sections 7 to 10 of the Telemedia Act, providers of telemedia services are in principle not responsible for third party information that they transmit or store on behalf of their users, nor are they obliged to monitor the transmitted or stored information in the absence of any reason or to examine it for indications of unlawful activities. Specifically, Section 10 of the Telemedia Act provides that host providers that store third party information for their users are not responsible for that information, provided that they:

- are not aware of any illegal act or information, or
- act immediately to remove or block illegal content as soon as they become aware of it.

As a rule, service providers immediately comply with police instructions (this is usually the responsibility of the *Land* police) by promptly removing the content as requested. If host providers fail to take appropriate measures, their responsibility for the relevant illegal content is governed by the general provisions. However, the provisions of the Telemedia Act do not give rise to direct criminal liability on the part of internet providers.

4.4.2. Resources allocated to improve cooperation

Most *Länder* consider that staffing levels and technical equipment in law enforcement agencies are adequate. Challenges remain in particular in respect of the analysis of large volumes of data. In many cases, the data stored on suspects' computers is in the order of terabytes. The analysis of this data is both technically very difficult and often fairly time-consuming, with the result that investigative proceedings can be delayed.

A large number of training sessions give public prosecutors and judges the requisite expertise.

The Federal Criminal Police Office has an annual budget for cybercrime training of approximately EUR 200 000. These costs consist of instructors' fees, travel costs and the purchase of hardware and software.

In 2014, the German Judicial Academy spent EUR 151 844 on instructors' fees alone at its conference site in Trier, while at its Wustrau conference site, instructors' fees amounted to EUR 178 591.

The following (non-exhaustive) information was reported with regard to the *Bundesländer*:

Baden-Württemberg:

Approximately EUR 20 000 annually from the judicial budget for the training of public prosecutors.

Brandenburg:

Approximately EUR 7 000 - EUR 10 000.

Saarland:

Approximately EUR 20 000.

Saxony-Anhalt:

Approximately EUR 40 000.

Bavaria:

Approximately EUR 10 000.

Bremen:

Approximately EUR 10 000 annually.

Hamburg:

Annual external training costs are estimated at approximately EUR 15 000. The total annual budget averages around EUR 180 000.

Hessen:

About EUR 15 000 is spent each year on conferences organised by Hessen's Judicial Academy.

Lower Saxony:

Approximately EUR 10 000 (public prosecutor training provision).

Rhineland-Palatinate:

Approximately EUR 10 000 (for police training measures) annually.

Thuringia:

About EUR 20 000 in 2013 and about EUR 36 000 in 2014.

4.5. Conclusions

- **Germany has a Federal structure composed of 16 *Länder*. According to the division of powers between Federal level and the *Länder,* as stipulated in the Basic Law, the exercise of state power and the discharge of state functions is a matter for the *Länder* unless otherwise provided for or permitted by the Basic Law. As a consequence the responsibility for criminal prosecution basically lies with the prosecution authorities of the *Länder* (the public prosecutor's offices and their investigative staff). In special cases (e.g.protection of the state) powers lie with the Federal Prosecutor-General's Office and the Federal Criminal Police.**

- **There are several national structures responsible for preventing, analysing and fighting cybercrime: public prosecutor's offices of the *Länder*, police, both at federal and *Länder* levels, the office for the protection of the constitution, both at federal and *Länder* levels, the customs criminal investigation office, as well as the Federal Office for Information Security.**

- **Most of the *Länder* have either specialised cybercrime prosecutors or have set up dedicated sections or contact persons for cybercrime in the public prosecutor's offices.**

- **With regard to the police authorities most of the *Länder* have set up special cybercrime departments within their *Land* Criminal Police Offices. Staff in the specialised departments have in–depth IT knowledge and special IT expertise. Furthermore, the Federal Criminal Police Office has a unit responsible for cybercrime (Group SO4).**

- **There is also a National Cyber Defence Centre (Cyber-AZ), composed of several institutions responsible for cyber-attacks, under the administration of the BSI. This structure coordinates the fight against cyber-attacks, especially with focus on attacks against infrastructure and also performs operational work.**

- **The fight against cybercrime is coordinated by the Cybercrime Department of the Federal Criminal police Office, the *Länder* Criminal Police Offices, the federal Police and some other bodies, such as the Fight Against Crime Committee, the police Crime Prevention Committee and the State Protection Committee.**

- **At federal level there is an 'institutionalised Public-Private Partnership' in the area of cybercrime, named "German Competence centre against Cybercrime - G4C. Besides that law enforcement authorities have a very good relationship with the financial sector in relation to combating crimes involving online fraud. The evaluation team considers that there is a good level of cooperation and coordination at national level.**

- **The police implemented its own Cyber Defence Strategy, which established contact points for industry in case of cybercrime incidents, a coordination mechanism and a single contact point to exchange information. There is also a cooperation platform with industry. The strategy contains 11 fields of action, including measures to be taken by private actors.**

- **Some practitioners explained to the evaluation team that the division of competences between the specialised units for combating cybercrime cases is organised on a case by case basis after informal consultation between the prosecution units. Account is also taken of the legal category of the offence; in case of a serious offence the responsibility for the investigation falls to the cybercrime offices for fighting serious cybercrime.**

- **The Federal Criminal Police Office has an annual budget for cybercrime training and some of the Länder reported that they have resources allocated for training as well.**

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

5.1.1. Council of Europe Convention on Cybercrime

Germany signed the Convention on 23 November 2001 and ratified it on 9 March 2009. It entered into force in Germany on 1 July 2009.

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

Acts unique to information systems, in particular those related to cyber-attacks: Sections 202a, 202b, 202c, 202d, 303a and 303b of the German Criminal Code.

- Pursuant to Section 202a of the Criminal Code, whosoever unlawfully obtains data for himself or another that were not intended for him by circumventing any special protection in place to prevent unauthorised access thereto is liable to imprisonment not exceeding three years or a fine.
- Section 202a(2) of the Criminal Code defines data as those stored or transmitted electronically or magnetically or otherwise in a manner not immediately discernible.
- Pursuant to Section 202b of the Criminal Code, whosoever unlawfully intercepts data not intended for him for himself or another by technical means from a non-public data processing facility, or from the electromagnetic broadcast of a data processing facility, is liable to imprisonment not exceeding two years or a fine.
- Pursuant to Section 202c of the Criminal Code, whosoever prepares to commit an offence under Section 202a or Section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible passwords or other security codes enabling access to data, or software for the purpose of committing such an offence, is liable to imprisonment not exceeding two years or a fine.

- Pursuant to Section 202d of the Criminal Code, whosoever acquires for himself or another, supplies to another, disseminates or makes otherwise accessible data which are not generally accessible and which another has obtained through an unlawful act, with the intent of enriching himself or a third person or of harming another is liable to imprisonment not exceeding three years or a fine. However, the penalty must not be more severe than that laid down for the predicate offence (Section 202d(2) of the Criminal Code). An exception is made for acts that exclusively serve the fulfilment of lawful official or professional duties.
- Pursuant to Section 303a of the Criminal Code, whosoever unlawfully deletes, suppresses, renders unusable or alters data is liable to imprisonment not exceeding two years or a fine.
- Pursuant to Section 303b of the Criminal Code, whosoever interferes with data processing operations which are of substantial importance to another by committing an offence under Section 303a(1), or entering or transmitting data with the intention of causing damage to another, or destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier, is liable to imprisonment not exceeding three years or a fine.
- In all cases, only intentional conduct attracts criminal liability (Section 15 of the Criminal Code).
- Aggravating/mitigating factors: Under Section 303b of the Criminal Code, if the data processing operation is of substantial importance for another's business, enterprise or a public authority (Section 303b(2) of the Criminal Code), the penalty is imprisonment not exceeding five years or a fine. In especially serious cases, custodial sentences of between six months and ten years may be imposed. Examples of especially serious cases (Section 303b(4) of the Criminal Code): if the offender causes major financial loss, acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or, through the offence, jeopardises the population's supply of vital goods or services or the national security of the Federal Republic of Germany.

- Recidivism: This is a factor in the determination of penalties (Section 46 of the Criminal Code). If the offender acts on a commercial basis, this is an especially serious offence, pursuant to Section 303b(4) of the Criminal Code. Any person who wishes to procure a non-temporary, substantial source of revenue through the continued commission of an offence will be deemed to be acting on a commercial basis.
- The attempt is punishable under Sections 303a and 303b of the Criminal Code (see Section 303a(2) and Section 303b(3)). Pursuant to Section 202c of the Criminal Code, preparation is punishable in the cases referred to under Section 202a, Section 202b, Section 303a(1)(2) and Section 303b (1)(5).
- Aiding and abetting are punishable pursuant to the provisions of Sections 26 and 27 of the Criminal Code

Acts where computer/IT systems were involved as tool or target: Sections 263a, 269 and 270 of the Criminal Code

- Pursuant to Section 263a of the Criminal Code, computer fraud is punishable by up to five years' imprisonment or a fine. An offence within the meaning of Section 263a of the Criminal Code is committed where the perpetrator, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing.
- Pursuant to Section 269 of the Criminal Code, whosoever for the purposes of deception in legal commerce stores or modifies data intended to provide proof in such a way that a counterfeit or falsified document would be created upon their retrieval, or uses data stored or modified in such a manner, shall be liable to imprisonment not exceeding five years or a fine.
- The acts must have been committed intentionally. Commission by negligence is not a punishable offence.

- Aggravating/mitigating factors: pursuant to Section 263a(2) in conjunction with Section 263(3)(2) of the Criminal Code, if the offender acts on a commercial basis or as a member of a gang, or causes a major financial loss, or, through the continued commission of fraud, acts with the intention of placing a large number of persons in danger of financial loss, or if another person has been placed in financial hardship, or if the offender abuses his powers or his position as a public official, or pretends that an insured event has happened after he or another has for this purpose set fire to an object of significant value or caused the sinking or beaching of a ship, this shall be considered to be especially serious case of computer fraud. Where the perpetrator on a commercial basis commits the offence as a member of a gang, whose purpose is the continued commission of offences under sections 263 to 264 or sections 267 to 269, he or she shall be liable to imprisonment from one to ten years, in less serious cases to imprisonment from 6 months to five years. The same applies *mutatis mutandis* to the forgery of data intended to provide proof pursuant to Section 269(3) in conjunction with Section 267(3) of the Criminal Code. For those especially serious cases, the law provides for a term of imprisonment of between six months and ten years.
- Recidivism: this is a factor in the determination of penalties (Section 46 of the Criminal Code). Pursuant to Section 263a(2) in conjunction with Section 263(3) to (5) and Section 269(3) in conjunction with Section 267(3)(4) of the Criminal Code, if the offender acts on a commercial basis this is considered to be an especially serious offence. Any person who wishes to procure a non-temporary, substantial source of revenue through the continued commission of an offence will be deemed to be acting on a commercial basis.
- An attempt is punishable: Section 263a(2) in conjunction with Section 263(2) and Section 269(2) of the Criminal Code. Pursuant to Section 263a(3) of the Criminal Code, whosoever prepares an offence of computer fraud by writing computer programs the purpose of which is to commit such an act, or procures them for himself or another, offers them for sale, or holds or supplies them to another is liable to imprisonment not exceeding three years or a fine.
- Aiding and abetting are punishable pursuant to the provisions of Sections 26 and 27 of the Criminal Code.

Encouraging the commission of a serious violent offence endangering the state (Section 91 of the Criminal Code)

- Pursuant to Section 91(1) of the Criminal Code ('Encouraging the commission of a serious violent offence endangering the state'), 'whosoever (1) displays or supplies to another written material (Section 11(3)) which by its content is capable of serving as an instruction to commit a serious violent offence endangering the state (Section 89a(1)), if the circumstances of its dissemination are conducive to awakening or encouraging the preparedness of others to commit a serious violent offence endangering the state, (2) obtains written material within the meaning of no. 1 above for the purpose of committing a serious violent offence endangering the state will be punished [...]'. Pursuant to Section 11(3) of the Criminal Code, audiovisual media, data storage media, illustrations and other depictions will be equivalent to 'written material'.
- Pursuant to Section 91 of the Criminal Code, the penalty is imprisonment not exceeding three years or a fine. If the degree of guilt is of a minor nature, the court may order a discharge for the offence in question (Section 91(3) of the Criminal Code).
- The offence in question is an intentional offence (Section 15 of the Criminal Code).
- The attempt is not punishable (Section 23(1) of the Criminal Code).
- The criminalisation of aiding and abetting is governed by the general provisions (Sections 26 and 27 of the Criminal Code).

The offences referred to above may be committed only by natural persons. A fine not exceeding EUR 10 million may be imposed on associations (legal persons and partnerships) in cases where a person in a managerial position has committed a business-related criminal or administrative offence (Sections 30 and 130 of the Administrative Offences Act). The maximum fine which may be imposed on associations for criminal offences and breach of the duty of supervision was increased in 2013 from EUR 1 million to EUR 10 million (Section 30(2)(1) and Section 130(3), third sentence of the Administrative Offences Act). This upper limit may be exceeded if it does not suffice for the purposes of recovering the economic benefit derived from the offence (Sections 30(3) and 17(4) of the Administrative Offences Act).

Pursuant to Section 46 of the Criminal Code, criteria such as the amount of damage are taken into account when sentencing.

The Public Prosecutor's Office may dispense with the prosecution of minor cases pursuant to Sections 153(1) and 153a of the Code of Criminal Procedure (StPO). With regard to Section 153a(1) of the Code of Criminal Procedure, the offender must comply with a condition before the proceedings are definitively dropped.

There are currently no plans for new specific legislative measures on cybercrime.

There are guidelines for criminal and monetary fine proceedings (RiStBV). Those guidelines are intended primarily for public prosecutors. However, certain advice is also directed at judges. Pursuant to No. 208 RiStBV (guidelines on criminal proceedings and fines), the public prosecutor must notify the Federal Criminal Police Office in proceedings involving written material endangering the state. Pursuant to No. 224 RiStBV, the Federal Criminal Prosecution Office indicates whether written material (Section 11(3) of the Criminal Code) has already been the subject of criminal proceedings pursuant to Sections 184, 184a, 184b or 184c of the Code. In order to avoid diverging decisions, the principles laid down in No. 224(2) RiStBV must be adhered to in investigations involving pornographic written material. Pursuant to No. 228 RiStBV, if a court finds in a final judgment that written material has a content as defined in Sections 184, 184a or 184b of the Criminal Code, the central unit must send a copy of that judgment to the Federal Review Body for Media Harmful to Minors for inclusion in the list of media harmful to minors pursuant to Section 18(5) of the Protection of Minors Act.

Under the Act increasing the security of information technology systems (IT Security Act), the Federal Criminal Prosecution Office has jurisdiction regarding all offences which are directed against public authorities, pursuant to Sections 202a, 202b, 202c, 263a, 303a and 303b of the Criminal Code. The public prosecutor may transfer the investigations to another authority (cf. Section 4 of the Act on the Federal Criminal Prosecution Office and on Cooperation between the Federation and the *Länder* in Criminal Matters (BKAG)). In addition, No. 30(1) RiStBV provides that a public prosecutor who becomes aware of a case which justifies a suspicion of one of the offences referred to in Section 4(1)(1) BKAG must notify the Federal Criminal Prosecution Office and the *Land* Criminal Police Office immediately, if necessary by telex or telephone.

Sabotage against the constitution (Section 88(1)(2) of the Criminal Code)

- With regard to 'offences unique to computers and information systems, in particular attacks against information systems' (category 1 of Annex 2 to the questionnaire), point 2 of Section 88(1) of the Criminal Code ('sabotage against the constitution') is of relevance. According to that provision, 'whosoever as ringleader or instigator of a group or individually without acting with or for such a group intentionally causes, by acts of interference within the territorial scope of this Act [...] telecommunications facilities which serve public functions [...] to cease to function, in whole or in part, or to be deprived of their assigned functions and thereby intentionally supports efforts against the continued existence or security of the Federal Republic of Germany or against its constitutional principles [...] will be punished'.
- The penalty is imprisonment not exceeding five years or a fine. The offence in question is an intentional offence (Section 15 of the Criminal Code).
- The attempt is punishable (Section 88(2) of the Criminal Code).
- The criminalisation of aiding and abetting is governed by the general provisions (Sections 26 and 27 of the Criminal Code).

The legal situation in Germany already complied with almost all the requirements in Directive 2013/40/EU on attacks against information systems. The only change necessary was to raise the upper limit for the offence of acts preparatory to data espionage and phishing (Section 202c of the German Criminal Code) from one year to two years' imprisonment, which occurred with the entry into force of the anti-corruption law on 26 November 2015.

B/ Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography

Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography was incorporated into German law by the 49th Criminal Code Amending Act (transposition of European rules on the law governing sexual offences), which came into force on 27 January 2015. **Child abuse (Section 176 of the Criminal Code)**

- "Pursuant to Section 176(1) of the Criminal Code, whosoever engages in sexual activity with a person under fourteen years of age (child) or allows the child to engage in sexual activity with himself will incur a penalty. Whosoever induces a child to engage in sexual activity with a third person or to allow third persons to engage in sexual activity with the child will incur the same penalty (Section 176(2) of the Criminal Code). Pursuant to Section 176(4) of the Criminal Code, whosoever engages in sexual activity in the presence of a child (no. 1); induces the child to engage in sexual activity, unless the act is punishable under subsection (1) or subsection (2) above (no. 2); presents a child with written materials (section 11(3)) to induce him to engage in sexual activity with or in the presence of the offender or a third person or allow the offender or a third person to engage in sexual activity with the child (no. 3, letter a) or commit an offence pursuant to section 184(1) (no.3) (Producing of child pornography) or pursuant to section 184b (3) (obtain possession or possession of child pornography) - (no.3 letter b); or influences a child by showing pornographic illustrations or images, by playing audio recordings with pornographic content accessible by way of information and communication technology, or by corresponding speech (no. 4), is liable to imprisonment from three months to five years. Pursuant to Section 176(5) of the Criminal Code, whosoever supplies or promises to supply a child for an offence under Section 176 (1) to (4) of the Code or who agrees with another to commit such an offence is liable to imprisonment from three months to five years.

- Definitions: Pursuant to Section 184h(1) of the Criminal Code, sexual acts and activities are only those which are of some relevance in relation to the protected legal interest in question. Pursuant to Section 184h(2) of the Criminal Code, sexual acts and activities in the presence of another are those which are committed in the presence of another who observes them. Pursuant to Section 11(3) of the Criminal Code, audiovisual media, data storage media, illustrations and other depictions are equivalent to written material. The concept of pornography is not legally defined, but is determined by the case-law (for child and juvenile pornography see below, section 184b(1) no. 1 and 184c(1) no. l of the Criminal Code).
- Only intentional conduct attracts criminal liability (Section 15 of the Criminal Code).
- Aggravating/mitigating factors: Aggravating factors: Section 176a (Aggravated child abuse), Section 176b (Child abuse causing death) of the Criminal Code.
- Scale of penalties: Custodial sentence of between six months and ten years (Section 176(1) and (2) of the Criminal Code); custodial sentence of between three months and five years (Section 176(4) and (5) of the Code); custodial sentence of between one year and 15 years (Section 176a(1) of the Code); custodial sentence of between two years and 15 years (Section 176a(3) of the Code); life imprisonment or custodial sentence of between ten and 15 years (Section 176b of the Code).
- Recidivism: According to section 176a(1) of the Criminal Code the sexual abuse of children under section 176(1) and (2) shall entail a sentence of imprisonment of not less than one year if the offender was convicted of such an offence by final judgement within the previous five years.
- Aiding and abetting are punishable pursuant to the provisions of Sections 26 and 27 of the Criminal Code.
- The attempt is punishable pursuant to Section 176(6) of the Criminal Code, with the exception of offences under Section 176(4), No. 3 and No. 4 and Section 176(5) of the Code.

Distribution, acquisition and possession of child pornography (Section 184b of the Criminal Code)

- Pursuant to Section 184b(1) of the Criminal Code, whosoever disseminates or otherwise makes accessible child pornography (points 1 and 2 EN version; no. 1, first half sentence DE version), or whosoever undertakes to obtain possession for another of child pornography representing an actual or realistic activity (no. 2), or whosoever produces child pornography representing an actual activity (no. 3), or whosoever produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export child pornography in order to use it or copies made from it or facilitates such use by another is liable to imprisonment from three months to five years, insofar as the offence is not liable to a penalty pursuant to subsection 3 (no. 4). Pursuant to Section 184b(3) of the Criminal Code, whosoever possesses or undertakes to obtain possession of child pornography reproducing an actual or realistic activity is liable to a penalty.

- Definitions: pursuant to Section 184b(1), no. 1 (DE version) of the Criminal Code, pornographic written materials (Section 11(3) of the Code - see above) are regarded as child pornography if they (a) relate to sexual activities performed by, on or in the presence of a person under fourteen years of age (child), or (b) relate to the depiction of a child either fully or partially unclothed in an unnaturally sexually explicit posture or (c) relate to the sexually provocative depiction of the child's naked genitalia or buttocks. Pursuant to Section 184d(1), first sentence of the Criminal Code (EN version - section unnumbered), whosoever makes pornographic content accessible to another person or the public via broadcasting or telemedia shall incur the penalty under sections 184 to 184c of the Criminal Code. Pursuant to Section 184d(2), first sentence of the Criminal Code, whosoever undertakes to access child pornography via media shall incur the penalty under Section 184b(3) of the Criminal Code.
- Only intentional conduct attracts criminal liability (Section 15 of the Criminal Code).
- Aggravating/mitigating factors: Section 184b(2) of the Criminal Code provides for a more severe penalty in the cases covered by subsection 1 where the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences, and where, in the cases referred to under Section 184b(1)(1), (2) and (4), the pornography reproduces an actual or realistic activity.

- Scale of penalties: dissemination, production, possession, procurement etc. (184b(1) and (2)): imprisonment from three months to five years. Qualification for subsection 1 (184b(2): EN subsection 3): imprisonment from six months to ten years. Undertaking to obtain possession and possession 184b(3): subsection 4 EN version): imprisonment not exceeding three years or a fine.
- Recidivism: this is a factor in the determination of penalties (Section 46 of the Criminal Code).
- Aiding and abetting are punishable pursuant to the provisions of Sections 26 and 27 of the Criminal Code.
- The attempt is punishable pursuant to Section 184b(4) of the Criminal Code, with the exception of offences under184b(1) no. 2 and 4 and 184b(3). However, insofar as the law refers to the undertaking of an offence in Section 184b(1)(no.2) and Section 184b(3) of the Criminal Code, the attempt and completion of such an offence is covered by point 6 of Section 11(1).
- Other: Pursuant to Section 184b(5) of the Criminal Code, Section 184b(1)no. 2 and Section 184b(3) do not apply to acts that exclusively serve the lawful fulfilment of state functions or that result from an agreement with a competent government body (no. 2 DE version) or that serve the fulfilment of official or professional (no. 3).

Distribution, acquisition and possession of juvenile pornography (Section 184c of the Criminal Code)

- Pursuant to Section 184c(1) of the Criminal Code, whosoever disseminates or otherwise makes accessible juvenile pornography (no. 1DE version; EN version points 1 and 2), or undertakes to obtain possession for another of juvenile pornography representing an actual or realistic activity (no.2), or produces juvenile pornography representing an actual act (no. 3 DE version, point (4) EN), or produces, obtains, supplies, offers, announces, commends or undertakes to import or export such pornographic written materials in order to use them or copies made from them or facilitates such use by another person is liable insofar as the offence is not punishable pursuant to point 3 (no. 4) (DE version). Pursuant to Section 184c(3) of the Criminal Code, whosoever possesses or undertakes to obtain possession of juvenile pornography representing an actual activity is liable to a penalty.
- Definitions: pursuant to Section 184c(1), no. 1 of the Criminal Code, pornographic written materials constitute juvenile pornography (Section 11(3) of the Code - see above) if they (a) relate to sexual activities performed by, on or in the presence of persons between the ages of fourteen and eighteen years or (b) relate to the depiction of persons between the ages of fourteen and eighteen years either fully or partially unclothed in an unnaturally sexually explicit posture. Pursuant to Section 184d(1), first sentence (EN version: unnumbered subsection) of the Criminal Code, whosoever makes pornographic content accessible to another person or the public via broadcasting or telemedia shall incur the penalty under Sections 184 to 184c of the Criminal Code. Pursuant to Section 184d(2), second sentence (EN version: unnumbered subsection) of the Criminal Code, whosoever undertakes to access juvenile pornography via telemedia shall incur the penalty under Section 184c(3) of the Criminal code.
- Only intentional conduct attracts criminal liability (Section 15 of the Criminal Code).
- Aggravating/mitigating factors: Section 184c(2) of the Criminal Code provides for a more severe penalty in cases under paragraph 1 where the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences, and where, in the cases referred to under Section 184c(1)(1), (2) and (4), the pornography reproduces an actual or realistic activity.

- Scale of penalties: dissemination, production, possession, procurement etc. (184c (1) and (2)): imprisonment not exceeding three years or a fine. Qualification for subsections 1 (184c(2): imprisonment from three months to five years. Undertaking to obtain possession (184c (3): imprisonment not exceeding two years or a fine.
- Recidivism: This is a factor in the determination of penalties (Section 46 of the Criminal Code).
- Aiding and abetting are punishable pursuant to the provisions of Sections 26 and 27 of the Criminal Code.
- The attempt is punishable pursuant to Section 184c(5) of the Criminal Code, with the exception of offences under subsection 184c(1) no. 2 and no. 4 and 184c(3). However, insofar as the law refers to the undertaking of an offence in Section 184c(1) no. 2 and no. 4 and 184c(3) of the Criminal Code, the attempt and completion of such an offence is covered by no. 6 of Section 11(1) of the Code.
- Other: Section 184c(4) of the Criminal Code, point 3 of Section 184c(1), Section 184c(5) and Section 184c(3) do not apply to acts of persons related to juvenile written pornography produced by them solely for personal use and with the consent of the persons therein depicted. Pursuant to Section 184c(6) (EN version: subsection 5) of the Criminal Code, Section 184b(5) of the Code applies *mutatis mutandis*.

C/ Online card fraud

As a rule, citizens who fall victim to online card fraud offences report them. Private companies do not always report such offences and card providers almost never.
The reasons are as follows:

When an individual discovers unauthorised transactions on a personal credit card/bank account, he/she starts by contacting the financial institution in question in order to resolve the matter. As a rule, he/she is asked by the bank to report the incident to the police. Members of the public see the misuse of personal data as a significant and serious threat.

Private companies report card fraud a lot less frequently as they are generally only indirectly affected by card fraud. In their case, goods and services are ordered by means of illegally obtained card data. As these companies are often compensated by credit card companies, they are not very interested in criminal proceedings. Nevertheless, the losses incurred are costed in exactly the same way as retail store
thefts.

Card providers, whether banks or credit card companies themselves, almost never report such incidents. Reported incidents would generate negative publicity, which is not in the interests of bank and credit card companies.

This is a grey area and there are no reliable details available on these incidents, although a regional study from Lower Saxony shows that only 9 % of cybercrime offences are reported.
Possible reasons for victims not reporting incidents are:

- the purchase of online access to illegal or pornographic material
- the purchase of illegal goods (for instance, pharmacy-only medicine)
- the low value of the sum involved
- reputational damage in the case of private companies

In the area of online card fraud, there is wide-ranging cooperation between the Federal Criminal Police Office and the private sector. Examples include cooperation with the 'Debit- und Kreditkarten in Deutschland' ('the Debit and Credit Card') security working group and the National Cybercrime Cooperation Unit, in particular the 'institutionalised Public-Private Partnership' (**iPPP**). As regards increased payment card security, there is cooperation with companies in order to prevent tampering with POS (point-of-sale) terminals and ATMs, and on the switch from magnetic strip to chip card technology.

In addition, law enforcement authorities in the *Länder* work in various ways with companies, particularly with banks, so as to combat and solve crimes involving online fraud. Set out below, for instance, is an indicative outline of the cooperation between law enforcement authorities and companies in Brandenburg and Saxony-Anhalt:

In **Brandenburg**, the central cybercrime contact point for companies, agencies and citizens was set up in the specialised directorate of the Criminal Police Office (police headquarters). This also functions as a single point of contact.

The specialised directorate of the Criminal Police Office regularly takes part in events such as those held by Brandenburg's chambers of commerce and industry, so as to pass on cybercrime information known to the police, establish contacts in the business and IT fields or exchange information on IT security within companies.

In **Saxony-Anhalt,** the police work closely with EURO-Kartensysteme GmbH (a services and competence centre) in the area of card-based payments within the German banking industry. Queries are also sent to individual credit card companies. However, these credit card companies do not always send a response. Every year the working group 'sicherheit der Kartenorganisationen in Deutschland' (card organisation security working group) holds a practice-based symposium on payment card crime, a forum for the latest security strategies and approaches in the field.

Participants include crime investigators from specialised units in the German *Länder* and the Federal Criminal Police, as well as representatives from credit card and security companies. In addition, the above meet on a voluntary basis four times a year in order to exchange information. There is intensive information exchange between the police, credit card companies and ATM/terminal industry representatives.

Specially trained or skilled credit card company employees develop industry-specific security concepts. They work closely with the police authorities, the representatives of which can contact them at any time. Public awareness is raised through relevant prevention material provided by the police. For example, security awareness is raised through short films. Upon request, police officers run training sessions in financial institutions. The introduction across Europe of EMV card chip technology and the general phasing out of debit card magnetic strips by financial institutions has greatly improved security against skimming attacks on German ATMs. This has made it more difficult to use counterfeit cards. Law enforcement authorities do not have any powers as regards authorisation of online transactions. Again, when it comes to prevention, emphasis is placed on the need to exercise caution when making online payments. As a rule, banks do not always report incidents, as the damage caused by the misuse of card data accounts for only a fraction of their total turnover.

D/ Other cybercrime phenomena

Most German states consider that staffing levels and technical equipment in law enforcement agencies are adequate. Challenges remain in particular in respect of the analysis of large volumes of data. In many cases, the data stored on suspects' computers is in the order of terabytes. The analysis of this data is both technically very difficult and often fairly time-consuming, with the result that investigative proceedings can be delayed.

The Federal Criminal Police Office (BKA) endeavours to reduce obstacles to cross-border cooperation, particularly in the field of online card fraud, by strengthening international bilateral cooperation and involving central agencies (Interpol/Europol).

In Saxony-Anhalt and other *Länder*, cooperation with foreign police authorities takes place in the context of international judicial cooperation. In addition, the Euro-Kartensysteme GmbH's payment card security service collects all data relating to ATM / POS terminals that have been targeted across Europe and makes this data available to the investigating authorities.

Hessen provided information on an approach that has proved effective in recent years as regards the preservation of evidence across borders. This concerns cases in which information has been passed on from abroad concerning criminal offences that also affect individuals in Germany. The approach comprises launching parallel investigative proceedings, taking preliminary measures to secure evidence and transmitting information obtained to foreign investigative authorities in a timely manner pursuant to Section 61a of the IRG (Act on International Legal Assistance in Criminal Matters) on preparing an MLA request.

As the formal MLA procedure has often proved too difficult for effective law enforcement, bilateral cooperation (especially in the form of joint investigation teams or JITs) has proved in recent years to be another effective tool in combating cross-border online card fraud.

In this context Germany is also involved in a number of European and international projects. These include:

- the European Network and Information Security Agency (ENISA) which aims to promote increased cooperation and information exchange between Member States in the area of network and information security
- the European Commission's AGIS programme, which is designed to help legal practitioners, law enforcement authorities and representatives of victim assistance services from the EU Member States and candidate countries to set up Europe-wide networks and exchange information and best practice.
- the Interpol European Working Party on IT Crime (EWPITC), a platform for the exchange of information to combat IT crime

5.2. Procedural issues

5.2.1. Investigative techniques

The following investigative techniques are permissible*:*

- search and seizure of information system/computer data;

In accordance with Sections 94 et seq., 102 et seq. and 110 of the Code of Criminal Procedure, search and seizure of objects on which data are stored (e.g. hard disks or servers) are possible, provided that such objects constitute evidence in investigative proceedings.

- real-time interception/collection of traffic/content data;

In the context of the interception of telecommunications under Sections 100a and 100b of the Code of Criminal Procedure, the removal of traffic/content data in real time is possible. However, this presupposes that a serious criminal offence listed in Section 100a(2) of the Code is suspected and that interception pursuant to Section 100b has been ordered by the court in accordance with the usual procedure. Traffic data such as the numbers or identifiers of the connections involved or of the terminals and location data of a mobile phone may also be obtained in accordance with Section 100g CCP. This is done only when a criminal offence of significant importance, even in an isolated case (including, in particular, those offences listed in Section 100a(2) of the Code of Criminal Procedure, or a criminal offence using telecommunications), has been committed.

If the measure refers to traffic data which must be stored by the telecommunications undertakings over a certain period in accordance with the Act introducing a storage obligation to store data and a maximum retention period for traffic data, which entered into force on 18 December 2015, collection is permitted only in the case of particularly serious criminal offences within the meaning of the offences listed in Section 100g(2) of the above Code. In all cases of traffic data collection, a court order is normally required.

- preservation of computer data;

Stored data may be secured by seizing the storage media. In accordance with Sections 94 and 98 of the Code of Criminal Procedure this requires that a criminal offence is suspected and, in general, that a court order has been issued. In addition, the fact that the data may be of importance as evidence for the investigation must be substantiated. Where circumstances require, seizure may also be ordered by the public prosecutor's office and the police (first sentence of Section 98(1), Code of Criminal Procedure). Collection by way of an 'online search' – i.e. access to the stored data using communications networks by infiltrating the target system by means of special spyware - is not permitted for criminal prosecution purposes.

- order for stored traffic/content data;

Pursuant to Sections 100b and 101a of the Code of Criminal Procedure, measures under Sections 100a and 100g of the Code may be ordered by the court only at the request of the public prosecutor's office. Where circumstances require, the order may also be given by the public prosecutor's office. However, this does not apply to the retrieval of compulsorily stored traffic data (second sentence of Section 101a(1), Code of Criminal Procedure). If the order is not confirmed by the court within three working days, it ceases to have effect.

- order for user information.

The collection of user information in the form of customer data, including a subscriber's name and address and assigned subscriber numbers and identification codes, is permitted in the case of telecommunications undertakings, provided that this is required for investigation of the case or determination of the suspect's whereabouts (Section 100j, Code of Criminal Procedure). This applies only if - as in the case of all criminal procedural measures - there is an initial suspicion of a criminal offence; a court order is not required.

The relevant police investigation measures (covert and/or overt) are carried out as far as the law allows.

The following specific methods of investigation are used:

- obtaining user data and traffic data from providers (this is one of the most commonly used investigation methods);
- telecommunications surveillance (surveillance of data traffic on computers with internet access or internet servers);
- traditional telephone interception;
- seizing e-mails from the service provider;
- IP tracking (e.g. Skype and other messaging services);
- open-source searches on the internet;
- investigations in forums, personalising nicknames and
- backing up data from data carriers and from the internet (websites, log files).

It is increasingly often the case that extensive server surveillance or individually programmed surveillance measures are required in order to successfully prosecute cyber-offences. However, a successful investigation strategy always includes a number of different investigation measures, some of them traditional.

In combating child pornography, the most common investigation methods are proactive searches in file-sharing networks to identify persons disseminating and downloading child pornography, but also analysis of login data to identify users of child pornography websites and analysis of the contacts of previously identified offenders.

Law enforcement authorities can also obtain investigative leads from, for instance, internet searches, evidence obtained from physical searches, covert measures or questioning of persons charged with offences or witnesses.

Given the wide range of cyber-offences, there cannot be any generally tried and tested procedures or methods for investigating such offences. Each case is different; investigative procedures and methods must be tailored to the individual case and the investigative leads available. One of the most important investigative approaches is undoubtedly the use of network data tracks generated from communications in the form of personal data linked to IP addresses used, in the form of traffic data or - if an offence listed in the catalogue has been committed - surveillance of internet communications. Other important sources are the seizure and analysis of data carriers and e-mail mailboxes. If the cyber-offence constitutes a property offence, bank and account details are also essential in order to trace the money. In particular, where phishing in connection with online banking is concerned, the tax administration is involved and an attempt is made, using covert measures, to obtain evidence of computer fraud carried out as part of a gang.

If investigations cannot be carried out using technical means, covert investigations must be conducted by officers. These covert police investigations, which can be conducted by deploying - 9undercover officers under the general police regulation, generally take the form of investigations on forums and boards. But investigations of this kind are only likely to yield results if they are carried out over the long term.

In the *Land* of Brandenburg, a video chat system is operated which can be used with a user account once the user has registered, giving a name and e-mail address. The service makes it possible to communicate in group chats, with images transmitted in real time. If offences are committed on this video chat platform, e.g. by displaying an image of the erect male member, this is documented by the operator in real time. The operator identifies the IP address stored on the server and faxes it to the public prosecutor's office. The latter swiftly initiates investigative proceedings, identifies the provider from the IP address and - if the provider stores traffic data for a relevant period - orders the provider by fax, pursuant to Section 100j(1)1, first sentence and (2) of the Code of Criminal Procedure, to terminate the subscriber's account.

5.2.2. Forensics and encryption

For example, the examination of a seized hard disk takes place electronically. The analysis of a seized functional mailbox takes place via an internet connection and may thus be categorised as a 'remote forensic examination'. Surveillance of computer-based telecommunications (e.g. via smartphones) by means of a previously infiltrated Trojan horse is not currently practised in Germany.

Computer systems used today are equipped with the latest hardware and software as well as constantly expanding storage media. In order to be able to analyse these devices for a broad range of information such as SMS messages, emails, documents, photos, videos, call procedures and deleted data, high-quality software and hardware systems are also used for forensic police analysis and examination of data carriers and storage systems. The police regard the growing market share of mobile terminals, such as smartphones, tablets und laptops, as constantly gaining in importance when securing evidence and carrying out forensic assessments. A central aspect of IT forensics is the electronic analysis of digital data which have been forensically backed up in accordance with the process explained in point 2.B.4. The analysis is performed by a handler in charge of the case, in such a way that each step is documented and tampering with the source data is ruled out. Remote examinations in the strict sense do not take place but, according to requirements, backups of remote data sources (e.g. cloud data, websites) may also be made. This always takes place under responsible guidance from the case handler or the designated body (e.g. by way of a mutual assistance request). In the context of network forensics, root servers leased from professional providers can be monitored by offenders on the internet. The root servers are generally used by the offenders as 'drop zones', i.e. to receive data pirated on compromised host computers (bank data, etc.).

Encryption should not only be seen as a problem: In consideration of all the requirements, the Federal Government also actively promotes the broader use of 'encryption and other safeguard mechanisms'. In the Digital Agenda the mandate reads:

'We support the use of more and better encryption. and aim to become the world's leading country in this area. To achieve this goal, the encryption of private communication should be adopted as standard across the board.'

'We promote business models that use anonymisation and pseudonymisation measures.'

The Federal Government therefore supports the use by citizens of encryption techniques and does not intend to restrict them. The availability of secure and trustworthy encryption technologies is an essential precondition for both the protection of citizens' privacy and effective data protection. After all, as things stand at present, the confidentiality of internet communications can only be ensured by using encryption technologies. Their use is therefore essential for the protection of privacy in cyberspace. However, particularly in the field of serious and organised crime, the use of encryption can make law enforcement considerably more difficult.

Access to information relevant to investigations is made difficult or prevented completely by the unconscious or targeted use of encryption. In the field of serious and organised crime, telecommunications surveillance measures are generally the only promising investigative measures. Failing this, many serious to very serious offences cannot be prosecuted.

The encryption of telecommunications, in connection with the dynamic development and spread of information and communication technologies, has gained further relevance, inter alia because encryption technology can now be deployed by anyone, without any need for technical expertise, using free software. In addition to active encryption of data and connections by the user (e.g. use of encryption tools for email or IP telephony), this is also frequently effected unknowingly by the user through the use of products already comprising data stream encryption as an integral component (e.g. Skype, Google Mail). It is anticipated that the implementation of encryption mechanisms will in future be mandatory in new telecommunications services. In the examination and evaluation of recorded telecommunications data, even the detection of encrypted telecommunications quite often poses a problem, as the high level of market dynamics constantly leads to new or modified telecommunications services appearing, which initially require a usually very time-consuming manual examination before automated processing and classification are possible. In the case of offence-related data carriers, it can increasingly be observed that these are encrypted by the offenders in order to deprive the law enforcement authorities of evidence.

Anonymisation and encryption are sometimes deployed deliberately to make investigations or law enforcement difficult or to prevent them from taking place. In this context, one of the challenges is to detect encrypted content, as it is not always indicated as such. For example, it is possible to store further hidden and encrypted content inside a data file encrypted with TrueCrypt (hidden container). Opening the content of encrypted data files using purely technical means is difficult, extremely laborious and likely to be unsuccessful. Provided that algorithms are carefully selected and implemented, encryption is nowadays considered to be an effective means of safeguarding confidentiality and integrity. Attack mechanisms do not exist for all instances of encryption. The development of such attack mechanisms is extremely time-consuming. It is pointless to carry out a brute-force attack on strong encryption - i.e. trying out all possible codes - because of the very long time it would take in virtually all cases. Even dictionary attacks using terms devised for password mining can last for months or years. Some encryption methods cannot currently be decoded.

There is no standard solution either for encrypted data or for encrypted communications. After examination of the individual case, targeted measures such as special telecommunications surveillance measures or decryption measures are deployed, if necessary.

Whether these solutions succeed generally depends on the offender's handling of the encryption software. Only if the offender does not use the possibilities offered by the software to their full extent would the security authorities be able to access content data. Otherwise, in the case of communications, there remains only analysis of the raw data or metadata, which is technically demanding and requires specialised IT knowledge. In the case of fully encrypted data carriers no other approaches may be possible. In many work domains it is therefore not yet possible to solve the problem of encryption effectively.

By deploying specialised computer scientists, it has been possible in some cases to decode offenders' encryptions. For more effective processing of dictionary attacks, efficient servers with high-performance graphics cards can be helpful for decryption.

By stepping up research and development, good cooperation between the authorities and development of new methods, the challenges posed by encryption can be partially offset. Thus, as far as investigative tactics are concerned, encryption of data carriers can for example be circumvented, subject to strict observance of the rules of procedure and the principle of proportionality, as long as there is access to operational computers and the main memory is backed up.

In association with the federal and *Länder* police authorities, there is ad hoc cooperation in problem-solving and in providing intelligence for overcoming the encryption mechanisms.

Through joint bodies, working parties and project groups, fundamental approaches to resolving problematic topics such as the encryption of communications and data relevant to investigations are worked out at *Land* and federal level. As all law enforcement authorities are faced with similar challenges with regard to encryption, an exchange of information and knowledge involving experts has developed, which is coordinated by the BKA and has been institutionalised in the form of an annual meeting of officials responsible for cryptanalysis. At this workshop topical problems are discussed, and participants seek practical approaches, exchange experience (attack mechanisms) and - where possible - offer mutual assistance.

In addition to police forums, cooperation takes place at various established and institutionalised seminars and meetings of experts. Information is regularly exchanged via an electronic cooperation platform (Wiki-TKÜ (telecommunications surveillance)). At federal level cooperation also takes place in research.

In the BKA and in some of the *Länder*, centres of excellence exist or are under development. The BKA is currently examining in depth the subject of cryptanalysis. All authorised bodies entrusted with implementing telecommunications surveillance measures may be referred to as specialised institutions in the broadest sense. These may also include the manufacturers and suppliers of telecommunications facilities and of special software and specialised research establishments (e.g. universities, Fraunhofer Institutes).

The decryption is not carried out in cooperation with private companies as a rule. In individual cases the task can theoretically be contracted out to external firms. The decision as to whether decryption should be contracted out to private companies is taken by the public prosecutor's office conducting the proceedings. There are a few commercial providers offering fee-based encryption - but with no guarantee of success. The BKA does not currently use private companies. In the field of telecommunications surveillance, private companies' software products are also used, but decryption is not effected in cooperation with or by such companies.

Decryption is very resource-intensive in any case; consequently, if strong encryption has been used properly, there is no real solution. A range of encryption programs, which currently guarantee secure encryption, are available on the market. Given greater awareness among the public, these programs are attracting growing attention, with the result that citizens who are concerned are making increasing use of such applications to protect data and communications against unauthorised access.

In some cases, this development has resulted in offenders using these programs to prevent law enforcement authorities from accessing their data which could incriminate them or serve as evidence. Analysing data which have been encrypted using procedures which are known to be secure is problematic. The choice of password also affects the solution of problems.

If traditional methods of investigation (searching the area around the computer workstation, establishing the social environment of the person under investigation, questioning) or live forensics (backing up the main memory, analysis) do not yield any firm indications as to passwords, or fragments of passwords, decryption generally cannot be carried out successfully, or only in a few cases and then with considerable investment of time. The crucial factor here is the processing power of the decryption system used: passwords of a certain length and complexity can pose exorbitant demands in terms of time (months or years). There is no known standard solution for this.

For communications, the security services can generally compensate by having recourse to source telecommunications surveillance.

Assuming that the security concerns relate to the possible loss of information of relevance to proceedings as a result of encryption, the competent authorities generally adopt the following approaches to resolve the problem:

- Intensifying research and development in this area
- Exchange of experts and of methods
- Developing technical capabilities
- Expanding cooperation between security services

Specific problem-solving approaches in the area of encryption are envisaged as follows:

- developing the authorities' capabilities in terms of decoding and analysis;
- researching, (further) developing and flexibly deploying innovative methods to circumvent encryption and/or capture telecommunications data, e.g. via source telecommunications surveillance and other special forms of telecommunications surveillance;
- obtaining meta-/traffic data from encrypted telecommunications in order to ascertain at least the immediate circumstances of the telecommunication, if its contents cannot be accessed;
- intensifying cross-border cooperation, pooling skills, cooperation with outside institutions.

5.2.3. -E-evidence

Under point 30 of Section 3 of the Telecommunications Act (TKG), 'traffic data' are data collected, processed or used in the provision of a telecommunications service. Under point 3 of Section 3 of the Act, 'customer data' are data of a subscriber collected for the purpose of establishing, framing the contents of, modifying or terminating a contract for telecommunications services.

Under Section 202a(2) of the Criminal Code, 'data' are only those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.

Pursuant to Section 184b(1) no. 1 of the Criminal Code, pornographic written materials (Section 11(3) of the Code - see above) are regarded as child pornography if they (a) relate to sexual activities performed by, on or in the presence of a person under fourteen years of age (child), or (b) relate to the depiction of a child either fully or partially unclothed in an unnatural sexually explicit posture or (c) relate to the sexually provocative depiction of the child's naked genitalia or buttocks. Under no. 1 of Section 184c(1) of the Criminal Code (DE version), 'pornographic written materials' (Section 11(3) of the Code - see above) are regarded as juvenile pornography if they (a) relate to sexual activities performed by, on or in the presence of a person of fourteen to seventeen years of age inclusive, or (b) relate to the reproduction of a person fourteen years of age but not yet eighteen years of age in a state of full or partially undress in a posture unnaturally displaying sexual characteristics.

The other terms are not legally defined in Germany.

Under Section 110(3) of the Code of Criminal Procedure, the examination of an electronic storage medium at the premises of the person concerned by the search may be extended also to cover physically separate storage media insofar as they are accessible from the storage medium if there is reason to fear that the data sought would otherwise be lost. The aim of the provision is to prevent the loss of data constituting evidence which, although accessible from the examined computer, are on a physically separate storage medium such as the server on the intranet or internet. This also includes emails which are stored on the provider's server. Examination is permitted if there is reason to fear that data or evidence would otherwise be lost, i.e. if the external storage medium cannot be secured in good time. If data relevant to the proceedings are found, they may be secured pursuant to the second sentence of Section 110(3) of the Code of Criminal Procedure.

All evidence produced or stored using digital technology is classified as e-evidence. Objects in question are all those on which digital data potentially relevant to the proceedings may be stored, e.g. computers, laptops, external data carriers, mobile phones/smartphones, game consoles, but also e.g. databases and email stocks in the company context and data in the network, in cloud storage or on the internet (e.g. fora, etc.). They are secured or seized under the expert guidance of the public prosecutor's office in accordance with Sections 94 and 98 of the Code of Criminal Procedure. Where there is reason to fear a loss of the data sought (e.g. because they are physically separated in a cloud store, the connection to which would be interrupted in securing the exhibit), those data may first be provisionally seized pursuant to Section 110(3) of the Code of Criminal Procedure in order to carry out an examination (on remote data carriers as well) for data relevant to the proceedings. From a technical point of view, the digital data are secured in order to maintain the chain of evidence and rule out any manipulation. The competent police authorities prepare a backup from original investigation data received (including exhibits such as log files, complete hard disk images). In this process a forensic backup is made of the e-evidence in accordance with recognised standards. For this purpose a bit-by-bit 1:1 copy of the data, including the forensic check sum, is produced in a standardised format, in such a way that a write-protect module specifically used for this process ensures that access to the source data is always read-only. Following this duplication process ('imaging'), a further verification takes place by means of the stored check sums. The integrity of the secured data is thereby ensured by calculating a cryptographic check sum.

In this way a forensic backup that is usable in court is produced, which serves as the basis of all further investigations. These investigations take place exclusively on the forensic copies and never on the original data.

The copy of the investigation data is forensically processed. The content of the forensically processed data carriers is evaluated by the investigating police officers.

As work takes place only with copies of the data to be evaluated, it is always clear that the data to be examined are not tampered with by staff of the *Land* Criminal Police Office (LKA) or the police. If they are relevant to the criminal proceedings, the storage medium and/or duplicate is also kept in a proper manner. They are made available to the courts and to the public prosecutor's office. For the transmission of data, CDs/DVDs or external hard disks are used, according to the volume of data. The decision as to what quantity of the secured data will ultimately be used in proceedings is the responsibility of the public prosecutor's office or the investigators who assess the content of the data.

In Germany there are no special provisions concerning the collection of e-evidence. There is no legal definition of the concept of electronic evidence. The Code of Criminal Procedure in Germany does not contain any explicit rules governing e-evidence. The general rules apply. Stored data are generally copied (mirrored) on to another storage medium (e.g. DVD, hard disk) and made available in this form to the public prosecutor's office and the court. In addition, readable data (e.g. text messages) or image files are printed out and made available at least in paper form as well. In the current legal situation, it is not possible to read electronic documents directly for the purpose of taking evidence via their content, as they are not considered to be 'documents' or 'records;. They must therefore first be printed out. In the context of a current legislative proposal, direct reading of electronic documents is also to be made possible by an amendment to the relevant provision.

5.3. Protection of human rights/fundamental freedoms

The basic rights guaranteed by the Basic Law bind the legislature, the executive and the judiciary as directly applicable law. Pursuant to Article 1(3) of the Basic Law, the exercise of any state authority is bound by the basic rights. Insofar as, under the Basic Law, a basic right may be restricted by or pursuant to a law, such law must comply with the principle of proportionality. The law must apply generally and not merely to a single case. In addition, the law must specify the basic right affected and the article in which it appears. In no case may the essence of a basic right be affected. The basic rights also apply to domestic legal entities to the extent that the nature of such rights permits. Should any person's rights be violated by a public authority, he may have recourse to the courts. Union law has effect in Germany in accordance with the provisions of the treaties and within the limits of Article 23 of the Basic Law.

The Telecommunications Act, the Code of Criminal Procedure (StPO) and the relevant police acts contain provisions setting out specific substantive and procedural rules for the collection of internet-related data, in particular contract data and traffic data. The collection of communication content is permissible only in the context of telecommunications monitoring measures pursuant to a court order.

Fundamental rights can generally be limited on the basis of general laws, which include rules governing powers in investigative proceedings, provided that the principle of proportionality is maintained. This applies both to the right to information privacy and to the fundamental right guaranteeing the confidentiality and integrity of IT-based systems (see Article 2(1) in conjunction with Article 1(1) Basic Law, the fundamental right to freedom of expression (Article 5(1) and (2) Basic Law) and the fundamental right ensuring privacy of telecommunications (Article 10 Basic Law).

Example: under Article 5(2) of the Basic Law, freedom of expression finds its limits in the provisions of general laws, in provisions for the protection of young persons, and in the right to personal honour. The provisions of investigative proceedings may constitute general laws and laws for the protection of minors within the meaning of such provisions. For instance, for the prosecution of the dissemination of child pornography (Section 184b of the German Criminal Code) data carriers, such as hard disks and servers, used to disseminate it on the internet may be seized as evidence pursuant to Sections 94 and 110 of the Code of Criminal Procedure (StPO), although the acts committed by the person concerned could possibly fall within the protection conferred by the fundamental right to freedom of expression.

5.4. Jurisdiction

5.4.1. Principles applied to the investigation of cybercrime

In order for German law enforcement authorities to act, German criminal law must apply. This is determined pursuant to Sections 3 to 9 of the Criminal Code. German criminal law always applies to offences committed in Germany (territoriality principle, Section 3 of the Criminal Code). Under Section 9 of the Criminal Code, an offence is committed in the locality where the perpetrator acted or, in the case of omission, should have acted, or where the outcome entailed by the offence occurred, or was intended by the perpetrator to occur.

Irrespective of the law of the locality where the offence was committed, German criminal law also applies to offences committed on a ship or in an aeroplane which is entitled to fly or carry the federal flag or national emblem of the Federal Republic of Germany (flag principle, Section 4 of the Criminal Code). If an offence committed abroad is punishable there, or the locality where the offence was committed is not subject to any criminal jurisdiction, German criminal law also applies to any offence committed abroad against (passive personality principle, Section 7(1) of the Criminal Code) or by a German national (active personality principle, Section 7(2)(1) of the Criminal Code). In addition, point 2 of Section 7(2) of the Criminal Code provides that German criminal law also applies to offences committed abroad by foreign nationals if the offence is punishable in the locality where it was committed or is not subject to any criminal jurisdiction, and the perpetrator is found in Germany; another condition to be met is that the perpetrator is not extradited, although this is admissible under the Act on International Cooperation in Criminal Matters (IRG), depending on the nature of the offence (whether because an extradition request has not been submitted within an appropriate period of time or has been rejected, or because extradition cannot be carried out).

German law also applies, under Section 5 of the Criminal Code, to offences committed abroad which have a particular connection with Germany, regardless of the law of the locality where the offence was committed. In addition, Section 6 of the Criminal Code sets out a list of offences committed abroad against internationally protected legal interests, to which German law also applies regardless of the law of the locality where the offence is committed (universal jurisdiction principle) - for instance, the dissemination of child pornography in text form (Section 184b(1) to (3) of the Criminal Code in point 6 of Section 6 of the Criminal Code).

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

In Germany there is no mandatory, legally binding rule for resolving conflicts of jurisdiction.

The yardstick for dealing with cross-border conflicts of jurisdiction is the ne bis in idem principle as laid down inter alia in Article 54 of the Schengen Convention and Article 50 of the EU Charter of Fundamental Rights.

For offences where there may be a conflict of jurisdiction regarding prosecution, information from the other state involved is essential.

Where several competing jurisdictions have been recognised, the conflict can be resolved in a number of different ways. If one state's proceedings are clearly more comprehensive and likely to achieve a better outcome, the other states will be able to suspend or abandon their proceedings in favour of these main proceedings In Germany, this can be done inter alia under Sections 153 and 154 et seq. of the Code of Criminal Procedure. If none of the states is willing to take over the conduct of the proceedings, or if several states wish to do so, there is the possibility of transferring proceedings by agreement. There are no mandatory provisions on the transfer of proceedings in Germany, but it seems an obvious solution in view of, for instance, Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings.

If agreement cannot be reached on where proceedings are to be conducted, the German authorities (and the authorities of the other Member States) can turn to Eurojust. In this case, Eurojust plays the role of mediator, but cannot take a binding decision.

The EU decisions on mutual assistance are passed on to the *Länder*. Consequently, national central authorities have no practical details to provide related to the Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings in relation to cybercrime cases. The Federal Government does not keep official statistics on other forms of mutual assistance.

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

When law enforcement authorities access data in cloud storage, there is the practical problem that it is often not clear on which state's territory the data are stored, making it impossible to determine the addressee of a possible mutual assistance request to the state in which the data storage facility is located.

5.4.4. Perception of Germany with regard to the legal framework for combating cybercrime

As regards the issue of the applicability of German criminal law, national authorities consider the existing legal framework to be sufficient, given the numerous rules in place (the territoriality, flag and passive/active personality principles, offences which have a particular connection with Germany and the universal jurisdiction principle).

German law enforcement authorities' powers when carrying out investigative measures such as access to data are essentially limited, in accordance with the sovereignty principle, to the territory of the Federal Republic of Germany. However, the normal mutual assistance procedure, as generally applied, is often too protracted to yield results. Consequently, direct cross-border access to data, e.g. as permitted under Article 32 of the Cybercrime Convention, regularly proves to be the only productive option. Otherwise, international mutual assistance has to be sought. One of the practical challenges is that e.g., under Article 31(1) of the Cybercrime Convention, mutual assistance requests are to be addressed to the state in which the data storage facility is located. But this often cannot be determined, or is not the same as the state in which the provider has its registered office.

Improved international police and judicial mutual assistance can only be achieved by an international legal framework extending beyond the EU and based on the Cybercrime Convention. Improved and faster communication between the competent judicial authorities would also be helpful, in particular. In addition, differences in national criminal law can give rise to difficulties, for instance where dual criminality is required.

5.5. Conclusions

- **Germany ratified the Council of Europe Convention on Cybercrime in 2009.**

- **The Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems have been transposed into national law.**

- **The Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography has also been transposed into national law.**

- **The Criminal Code was recently amended in order to fully implement the Lanzarote Convention and Directive 2011/93/EU. On this occasion Section 176(4) no. 3 of the Criminal Code, which covers grooming, had been improved.**

- **In the same legislative field an Act to increase security of information technology was recently adopted. There are new provisions on data retention related to the ISPs' obligation to store traffic data for 10 weeks and location data for 4 weeks, subject to strict conditions (serious and listed offences) intended to protect the privacy of the citizens. The new law was adopted in December 2017, after the evaluation visit; the storage obligation will enter into force on 2017.**

- **However, data retention is still considered an issue by practitioners and cooperation with other countries in this matter is problematic. A solution should probably be found at EU level.**

- **Some practitioners reported practical problems related to Article 202a Criminal Code because they consider that there are no appropriate legal instruments to investigate those cases. They expressed the idea that this provision should be amended in order to have aggravated forms for possessing huge amounts of stolen data. On the other hand, representatives of the Ministry of Justice said that they had reviewed this issue and considered that it would not be appropriate to change the legal situation for the time being.**

- **Mere possession of malware or credentials is not incriminating. The national legislation incriminates these facts only when a person commits them with the intention of enriching himself or a third person or of harming another person.**

- **Concerning procedural law, investigative measures are provided by German law on criminal procedure. E-evidence is described as: 'many different types of data produced or stored using digital technology'.**

- **Evidence obtained illegally is not rejected *ab initio* but is evaluated in the court.**

- **Under German law, direct access by German authorities to foreign providers for subscriber information is allowed and depends on how far it is allowed by the law of the state of the provider's seat, and this works quite well. However, some practitioners expressed a wish for a harmonised mechanism for exchanging subscriber data and new approaches at EU level on establishing jurisdiction.**

- **Problems in gathering evidence from the cloud were also underlined and the wish to address them at EU level was mentioned.**

- **Other challenges regarding encryption and cross border access to data were touched upon. Decryption is very time-consuming (months, even years sometimes) and with strong encryption there is no real solution.**

- **Concerning the investigation of botnets, a view was expressed to the effect that there should be some legal provisions to give power to judicial authorities to infiltrate the botnet in order to gather evidence and to carry out the take-down after that. The possibility of monitoring botnet traffic is not enough to combat cybercrime effectively.**

- **According to some practitioners, there is a need to introduce legal provisions into the Criminal Procedural Code to allow the use of tools to access criminal infrastructure (hacking). Police officers consider that they are one step behind the offenders.**

- **The necessity to establish a secure way to exchange information was also underlined, especially in the field of cyber-crime.**
  In Germany, the 18 contact points of the EJTN are provided with secured email addresses.

6. OPERATIONAL ASPECTS

6.1. Cyber attacks

6.1.1. Nature of cyber attacks

The BSI state of IT security for 2014 shows the following parameters:

Vulnerabilities:

- In 2014 there were around 700 critical vulnerabilities in the most used software products.
- For this group of widely-used products alone, the detection of an average of two critical vulnerabilities per day can be expected.
- By July in 2014 five zero-day exploits had been identified.

Malware:

- The total number of PC-based malware variants is now estimated at more than 250 million.
- The number of malware variants increases at a rate of about 300 000 a day.
- In Germany there are at least one million malware infections a month.
- Windows is the most frequently affected application, accounting for around 95 per cent of all cases.
- At least three million malware programs exist for smartphones or tablets.
- 98 per cent of these affect the Android operating system.

Botnets:

- In Germany more than a million computers are part of a botnet.

Identity theft:

- Millions of cases in January and April: a total of 34 million stolen identities.
- Every day thousands of digital identities are stolen.
- The number of identity-theft malware programs is steadily increasing. The BSI alone analyses 11 000 malware programs a month which are implicated in identity theft in Germany.

DDoS

- In 2014 there were over 32 000 DDoS attacks in Germany alone.
- Over a third of companies have been targets of DDoS attacks on their websites during the past three years.
- A quarter of the companies surveyed had suffered DDoS attacks on their network infrastructure.

Government networks/federal administration:

- There have been thousands of untargeted attacks on the government network.
- Special security measures have intercepted up to 60 000 additional infected e-mails a month in the federal administration's networks.
- In 2014, between 15 and 20 high-quality attacks on the government network were detected every day.
- An average of one attack per day is a targeted attack attributable to an intelligence agency.

6.1.2. Mechanism to respond to cyber-attacks

The IT crisis management structures have taken on the task of managing serious cyber-attacks. Germany's IT crisis management is undertaken mainly at the National IT Crisis Response Centre (IT-KRZ), at the Federal Office for Information Security (BSI). The IT-KRZ is evolving progressively out of the National IT Situation Centre and the Federal Computer Emergency Response Team (CERT-Bund). The so-called 'particular situation' or IT crisis can thus be managed by drawing on the BSI's relevant experts and support staff based on a scalable approach. The IT-KRZ is managed using a staff cell model, similar to general crisis and disaster protection cells, where all the relevant people are grouped together to manage organisational and technical tasks.

Tactical/technical tasks such as situation awareness and assessment and prioritisation are carried out and measures recommended. Specialists from the whole of the BSI are brought together according to the situation and provide wide-ranging technical expertise. Through the staff cells, communication is established with the BSI's target groups, e.g. authorities and critical infrastructure companies, and an appropriate coordination of crisis management processes is implemented. The press office and the legal team are likewise involved, as are, where applicable, liaison persons with other authorities - e.g. the BKA - in their respective domains. This includes in particular representatives of the National Cyber Response Centre who help maintain contact with the German security authorities. The IT-KRZ is supported by the organisational staff cells for tasks such as personnel management, logistics and the internal service.

If the scope of the technical crisis potential extends to other areas of public life or a political dimension is added, the crisis cell of the Federal Ministry of the Interior (BMI) is activated. This cell is responsible for crisis management in general, for IT aspects of crises, and for other aspects of public life which could be affected owing to interdependencies, e.g. civil protection (security of supply) or counter-terrorism (identification of perpetrators). A specific staff unit within the BMI crisis team is responsible for IT-related ministerial crisis management. This unit takes the IT assessment compiled and drawn up in the IT Crisis Response Centre, processes it at ministerial level and presents it in the BMI crisis cell. The unit is essentially the interface between the general, strategic-administrative team in the BMI and the operational-tactical (staff) IT-KRZ cell at the BSI.

To complete the situation report, there are naturally exchanges between the BSI IT Situation Centre, the BMI Situation Centre and the Joint Information and Situation Centre (GMLZ). Other situation centres may be involved, depending on the circumstances.

Moreover, there is communication and cooperation at both national and international levels with specialised communities, especially through the IT-KRZ. CERT networks have formed worldwide, with the aim of cooperating on cyber incidents, including mutual support for the management of IT situations. CERT networks have partly similar focuses, e.g. government/authorities' CERTs, and partly different, e.g. with teams from business, science and the authorities. The differentiated set-up of teams and their partially multidisciplinary composition should be explicitly seen as an advantage, since they can draw on broad expertise. The international dimension further supports this. In addition to day-to-day business, these networks contribute to IT crisis management, since they carry out regular exercises.

Successful civilian-military cooperation on IT incident processing and CERT tasks has existed for years at national level, between the BSI and the German armed forces. The BSI is listed at NATO as the National Cyber Defence Authority and is, in the event of a major cyber-attack with a state origin, the primary contact point for Germany. The focus of the German armed forces CERT (*CERT-Bundeswehr*) is the protection of their own military networks and it works on that together with the other international military CERTs.

IT-KRZ has long-established and tested crisis management channels in the public administration, in particular the federal administration and German businesses in the field of critical infrastructure. A range of BSI mechanisms and cooperation can cover a wide spectrum, reach most German businesses and also the public.

The existing international communication channels (Interpol, Europol, G7 and numerous bilateral contacts) are used. In the case of judicial requests, the formal channels for mutual legal assistance are used; however, in the fast-moving area of cybercrime, the formal rules make these channels generally impracticable and ineffective, in particular because the process is protracted and execution of the request takes time. Here, the G7-24/7 network of contact points is proving useful. It cannot, however, make up for all the shortcomings of the channels for mutual legal assistance. Efforts are therefore being made to extend the quick information exchange that exists at police level to the judicial level, through direct cooperation by the competent public prosecutor's offices.

6.2. Actions against child pornography and sexual abuse online

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

The Federal Criminal Police Office is the central unit for combating the sexual abuse of children and young people and the production and dissemination of pornographic images/video material depicting children/young people; as part of its role, it manages a national image comparison collection that enables information relating to these offences to be collated and analysed. Apart from the national image reference collection which is being operated at the BKA, the BKA being the National central Bureau of Federal Republic of Germany, also uses the "International Child Sexual Exploitation database" (ICSE-DB) which is being administrated by the Interpol General Secretariat.

The collection is designed to:

- link previously identified offenders with the pornographic images/video material of children/young people produced by those offenders
- distinguish pornographic depictions of young people from those of, for example, young adults
- compare stored images/video material with freshly seized material
- avoid multiple investigations by identifying known offenders and/or victims of sexual abuse
- help to marshal evidence by enabling previously seized material to be used in current proceedings

It is possible to establish whether a minor is already known to have been the victim of a sexual offence by comparison with existing images of children/young people.
In order to avoid re-victimisation, media that are harmful to minors will be included by the German Agency for the Examination of Harmful Media for Minors (*Bundesprüfstelle für jugendgefährdende Medien* - BPjM) in the index of media deemed harmful for minors (the 'Index'). The decision to include a website in the Index is taken in a procedure that resembles court proceedings. The proceedings include a non-public hearing before a body of 12 persons. Any person directly concerned by the decision (i.e. editor, author or distributor) will have the opportunity to take part and to defend their position.

The BPjM starts the proceeding (as described above) and – if the website is considered harmful to minors - the BPjM puts the website on the list/index.
The Protection of Young Persons Act (*Jugendschutzgesetz*) provides for foreign websites that have been indexed to be filtered by user-autonomous filter programs. To comply with its statutory duty the BPjM uses the 'BPjM module'. The 'BPjM module' contains the indexed URLs disseminated from other countries. Although not an independent filter program, it can be integrated into user-autonomous filter programs as a blacklist for youth protection. The BPjM makes the module available to manufacturers of user-autonomous filter programs in collaboration with the FSM self-regulating system. The module enables foreign websites indexed by the BPjM to be filtered in schools, for example.

Major search engine operators that offer their services in Germany have made a voluntary undertaking not to show websites indexed by the BPjM in their lists of results. They have been fulfilling that promise for several years now.

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

The following indicative information was received from the *Bundesländer* :

Berlin

The address, telephone number and e-mail address of LKA department 13 are published on the internet, together with a flyer telling people what to do if they come across child pornography on the internet.

The sexual offences department regularly organises events in schools and nurseries on how to prevent sexual abuse. The Berlin police also has an online service for sending in information or reporting offences at any time.

Tip-offs about possible child pornography on the internet are often received here too. Various information tools on the topic can be found on www.polizei-beratung.de, the website of the *Länder* and Federal Police Crime Prevention programme (ProPK). These include the short film: '*Chatten. Aber sicher*!' [Chat. But keep it safe!] which gives children rules for keeping safe when chatting on-line, and the short film '*Surfen. Aber sicher*!' [Surf. But keep it safe!], another element in the campaign '*Kinder sicher im Netz*' [Children safe on the net]. The TV presenter Rudi Cerne gives parents tips on how to protect their children from the dangers of the internet. Both films are available on a DVD for use on the spot and also as internet content. The comic '*Hallo - jetzt reicht's*' [Hi - that's enough] depicts children's day-to-day experiences in a child-friendly fashion, dealing especially with violence, bullying, blackmail, property damage and online chatting, and gives them rules on how to behave in these situations. Primary schoolchildren are the target group.

The flyer '*Das Netz vergisst nichts*' [The Net never forgets] features a comic strip describing why people should reveal as little personal information as possible about themselves and others on the internet. Children and young people are the target group. The internet portal 'time4teen' (Internet address www.time4teen.de) is designed especially for young people. It contains information about the risks of many different types of crime, including child abuse, bullying and sexual violence. Further information tools can be requested on the web page.

Brandenburg

Amongst other things, police inspectorates' prevention departments hold events on the subject of 'New Media' for schoolchildren in years 6 and 7 and their parents and teachers. This preventive measure is designed to inform target audiences about the potential risks of using 'new media' and to equip them to deal critically and responsibly with the range of different opportunities offered by the internet. Topics are to include victim avoidance strategies and perpetrator strategies, in particular in online grooming. These events also make use of the various media provided by the nationwide Police Crime Prevention programme.

Mecklenburg-Western Pomerania

The online platform 'Safe Internet Initiative' was first launched in Mecklenburg-Western Pomerania in 2001, in cooperation with the *Land* data processing centre. The platform was developed further in 2010 and is now available under www.netzverweis.de as a reporting platform for cases of suspected child pornography and cybercrime, so that Mecklenburg-Western Pomerania LKA's department 45/Cybercrime can now be contacted directly.

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

Two legislative amendments introduced in 1993 and 1998 provide the framework for Germans who commit sexual abuse against foreign children or young people while abroad to be prosecuted in Germany, even if their actions are not punishable in the country concerned. Certain forms of sexual abuse of children (1993) and young people (1998) have been added to the list in Section 5 of the Criminal Code ('Offences committed abroad against domestic legal interests'). The basic prerequisites for comprehensive prosecution are thus in place, at least for Germans suspected of committing sexual offences against children (irrespective of nationality and regardless of the law of the country where the offence is committed).

The working party for the implementation of the code of conduct on child sex tourism has been dealing with this particular type of sexual abuse of children and young people for some time; it works under the auspices of the DRV (*Deutscher ReiseVerband* - German Travel Association) with major involvement from ECPAT Germany (an (NGO) alliance working to protect children from sexual exploitation). Some years ago it drew up a joint flyer to raise awareness among holidaymakers, which is distributed worldwide by the police and by its partners on the working party.

In 2010 it also brought out a video targeted at private and business travellers, designed to raise awareness among German speakers travelling to destinations where they might observe suspected cases or even witness cases of so-called child sex tourism, leading to police checks in the country concerned and where necessary to actual criminal investigations.

Thanks in particular to the efforts of ECPAT Germany, the German federal authorities have followed their Austrian and Swiss counterparts in setting up and publicising a central online reporting site for holidaymakers abroad which can take reports of such cases and launch or assist further action in the foreign country involved. In September 2010, at the same time as the working party for the implementation of the code of conduct on child sex tourism brought out its video to mark World Tourism Day 2010, the BKA set up a central e-mail address to make it easier to report observations/suspected cases of child sex tourism. In addition, a contact form was posted on the BKA website (ww.bka.de) under the section 'Citizens' contact for child sex tourism'. The form can easily be found by searching on relevant terms and has the advantage that the reporter is 'prompted' and so does not forget any important details.

At European level, the European reporting platform was launched at the International Travel Trade Show (ITB) on 5 March 2014; it allows travellers to pass on information on sexual abuse to the relevant national authorities. There is also a link to the corresponding German reporting platform; alternatively, this can be reached directly under 'www.nicht-wegsehen.net'. There is also a link to the BKA's information page on child sex tourism and the contact form on that page.

The BKA monitors information sent to the central e-mail address or via the BKA contact form 24/7, so that it can launch emergency measures if necessary.

Measures to counteract real-time pornographic depictions of children are based on the relevant legal bases in the code of criminal procedure or, on a case-by-case basis, on the Telecommunications Act or the Telemedia Act, which allow inventory data to be collected from internet service providers.

In the course of patrolling the internet, the police can track down pornographic content involving children and young people (chat rooms, swap sites, etc.) and establish who is responsible, if necessary with the help of the internet service provider.

In addition, clues to the sexual abuse of children and young people or the dissemination of pornographic written material involving children and young people may also be found in the course of other procedural measures (e.g. telecommunications monitoring, or searches) and then pursued further.

The internet search department of the Baden-Württemberg LKA has self-programmed software which enables it to track the dissemination and downloading of child pornographic content on file-sharing platforms and document it for evidential purposes.

Automated processes mean that IP requests can quickly be sent to providers, enabling suspects to be identified in many cases.

Germany has three hotlines:
Jugendschutz.net (Cross-federal-state Office for Youth Media Protection)
eco e.V. (Association of the German ISPs)
fsm e.V. (Voluntary Self-Regulation of German Multimedia Companies)
All three hotlines are members of INHOPE.
Reporting to the three hotlines as well as to the police may be done anonymously and online.

A wide range of measures has been implemented in order to achieve high visibility for the hotlines in Germany. These measures include websites, flyers, brochures, press releases, annual reports, presentations on hotline work at national and international level and promotion by the project coordinator, Klicksafe.

When internet users conduct a search with terms that relate to the sexual abuse of children Google refers them to the hotlines of FSM and jugendschutz.net.

Child-abuse material which is reported to one of the three hotlines will be processed in accordance with an MoU between the Federal Criminal Police Office (BKA) and hotlines as follows:
a) Hotline receives information from the public or partner hotlines about child-abusive content.
b) Hotline reviews the content and verifies if it is illegal or not.
c) If the hotline comes to the conclusion that the material is of criminal relevance it produces a report about the content (with links) and sends it to German Federal Criminal Police Office (BKA) via email.
d) If the material is hosted in Germany the hotline may contact a provider who is a member of the hotline only after it has reported the content to the BKA. This sequence avoids creating risks for the criminal investigation. If necessary BKA seizes the relevant content for the purpose of criminal proceedings.
e) If the material is hosted abroad, the hotline will report simultaneously to its relevant INHOPE partner in order to achieve removal of the material as fast as possible. Furthermore, the hotlines may directly contact a foreign provider if the reporting over the police channel and the INHOPE hotline has not led to removal of the relevant material.
f) BKA receives all reports from all three hotlines and national police forces, and also directly from the public.

g) BKA double-checks with regard to all incoming reports whether content is illegal and still online.

h) If content is illegal, online and hosted in Germany the proceedings to achieve elimination of the content continue as follows:

- The relevant ISP is informed by the BKA, asked to remove the content and supply the subscriber data of the responsible uploader etc.
- BKA checks availability of content hosted in Germany on a daily basis and contacts the responsible ISP in order to initiate the removal of the relevant content.
- Average processing time for German content in 2014: 1.88 days (receipt of report by BKA until removal of content by ISP)

i) If the content is illegal, online and hosted abroad, the proceedings to achieve elimination of the content continue as follows:

aa) National police of the hosting country is informed by BKA via the Interpol I24/7 network in order to undertake take-down measures in its own jurisdiction.

bb) Via the German hotlines, all foreign content is also forwarded to the INHOPE hotline of the hosting country parallel to the I24/7 police channel.

cc) BKA checks availability of content reported abroad on a weekly basis for three weeks after reporting and will send reminders to the police of the hosting country if the material is still available. After four weeks of availability BKA will seek personal contact (e.g. via phone) with the foreign agency in charge in order to discuss the case.

dd) Furthermore, the hotlines may directly contact a foreign provider if the reporting over the police channel and the INHOPE hotline has not led to removal of the relevant material.

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

Germany seeks to ensure the prompt elimination of child sexual abuse material (CSAM). German law does not require access providers or hosting providers to apply filters for child pornographic material. Such a requirement would not be in line with Article 15 of Directive 2000/31/EC.

As a general rule, access providers, caching providers and hosting providers are not required to monitor the content of stored or transmitted information (§ 7 para. 2 Telemedia Act). However, if a host provider is informed about illegal content which is stored on his service, he may be held responsible for illegal content if he does not take measures for the immediate removal of such content. The reporting system described under 5.A.5 is based on this mechanism.

In 1995 the Federal Criminal Police Office set up the Central Child Pornography Unit to analyse child pornographic content on a coordinated nationwide basis. Since 2009 offences relating to child abuse and the possession, dissemination and production of child pornography have been among the priority crimes targeted by the Federal Criminal Police Office, which means that the initial Central Child Pornography Unit has become a department of approx. 20 police officers.

At the same time as the Central Child Pornography Unit was set up at the Federal Criminal Police Office, the federal *Länder* set up child pornography contact points at the *Land* Criminal Police Offices (LKAs), firstly in order to provide a specialised response to the phenomenon, given the growing use of technology, and secondly to provide full and direct information sharing at national level. Below the level of the LKA child pornography contact points there are specialised units at local police headquarters, which also have expertise in handling relevant criminal investigations. The *Länder* have supplied the following details, although this information is not exhaustive:

Baden-Württemberg:

As regards public prosecutor's offices, each authority has a number of officials dealing mainly, but not exclusively, with child pornography. With regard to No 223 RiStBV, one public prosecutor's office has special jurisdiction, in particular in respect of proceedings concerning the possession and dissemination of child pornography, with two units based in the youth department (both have reciprocal representation). It is estimated that around 30-40 % of staff are allocated to this task in both cases. At another public prosecutor's office, a special unit has sole responsibility for child pornography cases. It also handles other sexual offences against children and adolescents, along with environmental crimes and offences under the Animal Protection Act. The senior desk officers of these specialised units at the public prosecutor's office each have the general powers of a public prosecutor. The central unit for combating violent, pornographic and other material harmful to minors is based at the Office of the Chief Public Prosecutor in Stuttgart.

Operations aimed at combating child pornography on the internet are regularly carried out by specialised officers in Inspectorate 510 at the Baden-Württemberg Criminal Police Office (LKA). This also has a child pornography contact point. A detective at one Criminal Police Commissariat currently deals exclusively with cases relating to child pornography. This detective is sometimes assisted by other officers from that unit. The backing up of storage media seized during searches and the copying of data files on to appropriate storage media for evaluation purposes is the responsibility of a separate unit ('ITB') within the Criminal Police's Inspectorate 5. This unit comprises a total of 11 people. It is responsible not only for dealing with such offences but for the analysis of storage media in general.

Currently, approximately seven months are needed for such analysis. The Criminal Police also has special competence within the sexual offences unit vis-à-vis police working for another public prosecutor's office. Following the current police reform, four Criminal Police officials (three working full-time and one half-time) cover this area for the police headquarters as a whole. In addition, this Criminal Police department has an ITB (internet /preservation of evidence) department which handles the analysis of data carriers. A detective chief inspector in the department has primary responsibility for child pornography.

Bavaria:

There are no specialised units dealing solely with child pornography. The Bavarian Central Cybercrime Unit established at the Office of the Chief Public Prosecutor in Bamberg on 1 January 2015 handles internet-related investigations presenting particular legal and technical difficulties. A special unit at the police headquarters deals with child pornography offences for a public prosecutor's office. The unit comprises 15 investigative officers and is responsible for other sexual offences against children, young people and adults, too.

Berlin:

The Berlin Criminal Police Office has a department with exclusive responsibility for investigations into child and youth pornography, documented cases of sexual abuse of children and young people, as well as investigations into the dissemination of pornography. Currently, the Criminal Police Office comprises 23 employees (18 detectives, one administrative official and four salaried employees). A specialised unit at the Berlin public prosecutor's office prosecutes offences pursuant to Sections 184 to 184d of the Criminal Code.

Bremen:

The Bremen public prosecutor's office has two specialised child pornography units. The Bremen police force's sexual offences department has a specific competence for this area. The department has four police officers dealing with child pornography investigations together with general cases involving sexual offences.

Hamburg:

The Hamburg Criminal Police Office has special department LKA 541 (cybercrime, investigations) which inter alia has overall competence for offences relating to the dissemination of child pornography. LKA 541 acts as a central contact point for child pornography cases (with reporting and analysis tasks) and as a police investigative service handling criminal cases. It has six detectives and one employee to cover this area.

The specialised unit of the Hamburg public prosecutor's office is also responsible for cases linked to the fight against child pornography.

Hessen:

Hessen does not have specialised anti-child-pornography units. However, every public prosecutor's office has one or more special experts, who in their units deal partly with youth media protection cases.

The Central Unit for Combating Internet Crime (ZIT) also deals with a significant number of large-scale proceedings involving child pornography. In these cases, the central unit functions as a direct contact point for the Federal Criminal Police Office and as the public prosecutor's office responsible for identification. Once the perpetrator has been identified, it transfers a case against an accused person not resident in Hessen to the competent local public prosecutor's office. Overall, since its establishment in 2010, the Central Unit has conducted several thousand cases against persons accused of possession and dissemination of child pornography. The Unit also regularly carries out searches to identify victims and offenders of sexual abuse shown in child pornography. Such measures - in particular those that involve alerting the public - have resulted in the identification of a number of offenders. Since its establishment in 2010 the Central Unit has launched several thousand proceedings against persons accused of possession and dissemination of child pornography.

Mecklenburg-Western Pomerania:

The judicial system in the state of Mecklenburg-Western Pomerania has no specialised units that deal solely with the prosecution of child pornography. Special youth department units in public prosecutor's offices treat criminal investigations and proceedings relating to the production, dissemination and possession of child pornography as offences related to the protection of minors. The specialised public prosecutor's office for information and communications crime provides investigative support, where there is a need for IT expertise as regards the dissemination of such material on the internet.

Lower Saxony:

Lower Saxony's Central Unit for combating violent, pornographic and other material harmful to minors, based at Hannover public prosecutor's office, handles cases concerning the possession and criminal distribution of pornography (Section 184 of the Criminal Code), pornography depicting violence or sodomy (Section 184a of the Criminal Code) and depictions of violence (Section 131 of the Criminal Code). However, its main area of responsibility is the prosecution of criminal offences concerning the possession and dissemination of pornographic written material involving children and young people. The Central Unit covers child pornography cases for the whole of Lower Saxony. It has the powers normally attributed to a central unit. The Central Unit has a head of department and five senior desk officers. However, only half are assigned to the unit, with the other half working on other sexual offences. In 2013, the Unit worked on more than 3 500 cases against known suspects. By far the largest number of these cases were criminal offences relating to the suspected possession and dissemination of pornographic written material involving children and young people.

Rhineland Palatinate:

All public prosecutor's offices in Rhineland Palatinate have specialised units. As a rule, the senior desk officers work on other subject areas, too. Accordingly, senior desk officers attached to the sexual offences and pornography unit' sometimes handle internet-related child pornography cases. Their remit also covers all offences against sexual self-determination.

In addition, the state's Central Unit for combating material harmful to minors is at the Office of the Chief Prosecutor in Koblenz. The senior desk officer responsible for this area has additional tasks. The Central Unit does not carry out its own investigations but has a monitoring function in matters of overriding importance, collates decisions and performs a specific coordinating role between public prosecutor's offices.

Furthermore, the Rhineland Palatinate police force does not have any specialised unit that deals exclusively with child pornography. The Central Unit's Unit 44 (violent crime, offences against women and children) at the Rhineland Palatinate Criminal Police Office is the child pornography contact point. Unit 44 is responsible for handling murder, violent and weapons-related crime and sexual offences, violence in close social relationships, stalking, violence against police officers, as well as for cases concerning missing persons and unidentified dead persons.

In addition, child pornography offences in Rhineland-Palatinate are dealt with by Unit 2 at the regional criminal police inspectorates (sexual offences/offences against women and children).

Saxony:

There are several senior desk officers at public prosecutor's offices who handle child pornography cases. Their number depends on the volume of cases and varies between one and three per office. The specialists do not handle child pornography cases alone. They are also responsible for other criminal investigations.

Saxony-Anhalt:

The Ministry of Justice and Gender Equality established a central department fighting the display of violence, pornography and other endangerment of minors in the media, attached to the public prosecutor's office at Halle (Saale). This department is competent for the whole Land.

Thuringia:

The central technical analysis department for combating child and youth pornography is based in Unit 64 of the Thuringia *Land* Criminal Police Office. It comprises 6 posts. The powers and responsibilities as regards combating child and youth pornography offences in Thuringia are set out in the Thuringia police force's strategy document.

6.3. Online card fraud

6.3.1. Online reporting

As a rule, citizens who fall victim to online card fraud offences report them. Private companies do not always report such offences and card providers almost never.

The reasons are as follows.

When an individual discovers unauthorised transactions on a personal credit card/bank account, he/she starts by contacting the financial institution in question in order to resolve the matter. As a rule, he/she is asked by the bank to report the incident to the police. Members of the public see the misuse of personal data as a significant and serious threat.

Private companies report card fraud a lot less frequently, as they are generally only indirectly affected by card fraud. In their case, goods and services are ordered by means of illegally obtained card data. As these companies are often compensated by credit card companies, they are not very interested in criminal proceedings. Nevertheless, the losses incurred are costed in exactly the same way as retail store thefts.

Card providers, whether banks or credit card companies themselves, almost never report such incidents. Reported incidents would generate negative publicity, which is not in the interests of bank and credit card companies.

This is a grey area and there are no reliable details available on these incidents, although a regional study from Lower Saxony shows that only 9 % of cybercrime offences are reported.

Possible reasons for victims not reporting incidents are:

- the purchase of online access to illegal or pornographic material;
- the purchase of illegal goods (for instance, pharmacy-only medicine);
- the low value of the sum involved;
- reputational damage in the case of private companies.

6.3.2. Role of the private sector

In the area of online card fraud, there is wide-ranging cooperation between the Federal Criminal Police Office and the private sector. Examples include cooperation with the *Debit- und Kreditkarten in Deutschland* ('Debit and Credit Cards in Germany') security working group and the National Cybercrime Cooperation Unit, in particular the 'institutionalised Public-Private Partnership' (**iPPP**). As regards increased payment card security, there is cooperation with companies in order to prevent tampering with POS (point-of-sale) terminals and ATMs, and on the switch from magnetic-strip to chip-card technology.

In addition, law enforcement authorities in the *Länder* work in various ways with companies, particularly banks, to combat and solve crimes involving online fraud. Set out below, for instance, is an indicative outline of the cooperation between law enforcement authorities and companies in Brandenburg and Saxony-Anhalt:

In **Brandenburg**, the central cybercrime contact point for companies, agencies and citizens was set up in the specialised directorate of the Criminal Police Office (police headquarters). This also functions as a single point of contact.

The specialised directorate of the Criminal Police Office regularly takes part in events such as those held by Brandenburg's chambers of commerce and industry, so as to pass on cybercrime information known to the police, establish contacts in the business and IT fields and exchange information on IT security within companies.

In **Saxony-Anhalt,** the police work closely with *EURO-Kartensysteme GmbH* (a services and competence centre) in the area of card-based payments within the German banking industry. Queries are also sent to individual credit card companies. However, these credit card companies do not always send a response. Every year the working group *Sicherheit der Kartenorganisationen in Deutschland* (card organisation security working group) holds a practice-based symposium on payment card crime, a forum for the latest security strategies and approaches in the field. Participants include crime investigators from specialised units in the German *Länder* and the Federal Criminal Police, as well as representatives from credit card and security companies. In addition, the above meet on a voluntary basis four times a year to exchange information. There is intensive information exchange between police, credit card company and ATM/terminal industry representatives. Specially trained or skilled credit card company employees develop industry-specific security concepts. They work closely with the police authorities, which can contact them at any time. Public awareness is raised through relevant prevention material provided by the police. For example, security awareness is raised through short films.

When requested, police officers run training sessions in financial institutions. The introduction across Europe of EMV card chip technology and the general phasing-out of debit card magnetic strips by financial institutions has greatly improved security against skimming attacks on German ATMs. This has made it more difficult to use counterfeit cards. Law enforcement authorities do not have any powers as regards authorisation of online transactions. Again, when it comes to prevention, emphasis is placed on the need to exercise caution when making online payments. As a rule, banks do not always report incidents, as the damage caused by the misuse of card data accounts for only a fraction of total turnover.

6.4. Other cybercrime phenomena

Most German states consider that staffing levels and technical equipment in law enforcement agencies are adequate. Challenges remain in particular in respect of the analysis of large volumes of data. In many cases, the data stored on suspects' computers are in the order of terabytes. The analysis of these data is both technically very difficult and often fairly time-consuming, with the result that investigative proceedings can be delayed.

Specific measures taken by the Federal Criminal Police Office include cooperation with the manufacturers and operators of POS and ATM terminals.

For instance, warnings are issued via the Saarland *Genossenschaftsverband* (cooperative federation) to all Saarland banks. As this functions as a central point, the competent stations in Saarland are also given information on and made aware of developments at national level.

6.5. Conclusions

- **In relation to cyber-attacks, the national authorities reported that the RANSOMWARE threat is very high in Germany. There are massive attacks using SPAM, exploit kits and the vulnerabilities of servers, especially for mobile operators. Approximately 60% of the industry have been victims of cyber-attacks in the last few years.**

- **BSI (CERT) has a 24/7 operating service and other reporting channels (phone, email, fax, webpages).**

- **BSI (CERT) is responsible for the public administration network and there is a very good cooperation with different other bodies (active information, exchange of good practices, common handling of incidents).**

- **BSI informs BKA on a voluntary basis about incidents that could constitute cybercrime offences and when it does so BKA and/or Police of the Länder have the legal obligation to start an investigation.**

- **BKA and BSI established an iPPP named G4C with private partners from banking sector and AV-Industry in order to combat cybercrime.**

- **BKA maintains 24/7 quick reaction personnel in case of cybercrime attacks/incidents towards critical infrastructure and/or federal institutions.**

- **Every two years a national cyber-exercise is organised on specific topics. Police can take part as observers in these cyber-exercises.**

- **National companies are sometimes reluctant to report cybercrime incidents to the police, as they fear that this might affect their trust or reputation. In order to encourage reporting, police authorities highlight the fact that the investigations can be secret and good results can be achieved without affecting their reputation.**

- **In the field of online card fraud, there is an informal group based on personal contacts, which has operational meetings with various relevant actors (BKA, private partners).**

- **In order to combat child abuse material on the internet Germany does not use the access-blocking approach. The deletion approach is preferred as being more effective. Every year the national parliament receives a report on the effectiveness of the deletion of websites containing child abuse material.**

- **Referring to measures to avoid revictimisation, the national authorities mentioned the existence of a memorandum of understanding on hotlines for combating child sexual exploitation.**

- **At national level there is a database project in place that focuses on the grey area in child sexual abuse. The project is based on hotlines, and works with the private sector as well.**

- **The national authorities use key-words for automated picture recognition in order to recognise child abuse content. There is currently a project which will be finalised in two years that will make it possible to automatically recognise sexual postures, not the person themselves (physical identity), but this will be checked with Interpol's database and the private sector.**

- **As a good practice it should be underlined that if the police cannot identify the victim using the database but have reasonable suspicions about the possible identity of a child, they share one or more pictures of the victim with schools for identification.**

- **There is a Central Point in charge of the prevention of sex child tourism, which organises awareness campaigns as well.**
  In 2010, a project including NGOs, law enforcement authorities and representatives of the tourism industry from AT, DE, IT, FR, NL, PL, and Switzerland was developed with the aim of providing a cross-border coordination mechanism. There is a national network which makes possible exchanges of information between major stakeholders (BKA, industry of tourism associations) and awareness-raising measures.

- **On the BKA website a link is available where people can report sexual tourism cases.**

- **Awareness campaigns on child sexual abuse are also organised by the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth and the Federal Ministry of Education and Research.**

- **Another good practice is that police officers can consult a psychologist or equivalent counsellor, anonymously or in group sessions. All applicants are assessed before being appointed as specialised officers for combating child sexual abuse, there are annual psychological examinations, and strategies have been developed to cope with the specific stresses involved.**

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

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

Cooperation between the national authorities and Eurojust on investigation of cybercrime offences is based on the Act transposing Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, under the same terms as the cooperation on investigations into other criminal offences. There are no formal requirements or specific procedures provided for under national law regarding cooperation with Eurojust.

As a matter of principle, any public prosecutor, court or police authority that has questions concerning the handling of an offence of international concern may address them directly – in German, of course – to the German Desk at Eurojust. This may be done by phone, fax, e-mail, post or in person.

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

Eurojust has been involved several times as a coordinating body in the handling of transnational investigations.

For example, having been asked by the Hessen Central Unit for Combating Internet Crime to get involved in a case Eurojust provided assistance with coordination, thereby enabling a succession of concerted procedural measures to be taken across the world on a single day (http://www.eurojust.europa.eu/press/PressReleases/Pages/2014/2014-05-19.aspx).

This was achieved thanks to Eurojust's holding of three coordination meetings. By and large, cooperation with Eurojust has been exemplary. Eurojust also provided assistance in a case before a German public prosecutor (fraud investigation following the sending of phishing e-mails), and held a coordination meeting involving the EC3 which decided how cooperation in the matter was to continue and who would carry out the further investigation on which of the accused persons. In another case (investigation into fraud using ransomware/banking trojans), Eurojust coordinated a large number of MLA requests and the possibility of setting up a joint investigation team was also discussed.

In Baden-Württemberg, data were exchanged with Europol and the European Cybercrime Centre (EC3) in three ongoing cases, with case-related discussions and corresponding exchanges of information and data that in turn led to the discovery of links between the different cases following the use of cross-match reports. In one case a joint investigation team (JIT) was set up.

In the national collective case brought by the NERD investigation team at the Niedersachsen *Land* Criminal Police Office, three meetings were held by the EC3 concerning the Europe-wide problem of ransomware. The meeting was attended by police officers and public prosecutors from the countries affected by the problem, together with representatives of companies and employees of state and private institutions that deal with internet security.

The EC3 analysed the discussions at the meeting, which provided useful input for the investigations, and sent a written report to the participants. As well as these working meetings at Europol, a meeting of Spanish and German investigators was held at Eurojust's instigation, at which the two countries exchanged their latest knowledge concerning perpetrators.

The German law enforcement authorities cooperate with the EC3 in both operational and strategic areas. Case-related operational cooperation takes place on an ad hoc basis, and since 1 September 2014 the work has been coordinated by the Joint Cybercrime Action Task Force (J-CAT) launched by the EC3.

The EC3 is regarded as an active partner, and its establishment has boosted the fight against cybercrime. The approach pursued to date should be continued and developed consistently (see answer to question 8.A.2). Eurojust is held in high regard by the German law enforcement bodies. As cybercrime offences generally entail international investigations, Europol/EC3 and Eurojust regularly provide valuable input. The involvement of these bodies is vital, in particular for organising multinational operations, though also for facilitating exchange of information.

Baden-Württemberg has reported that job-shadowing at Europol by its own employees has led to better understanding of Europol procedures, which in turn has helped establish more precisely targeted investigations. Baden-Württemberg has also expressed its desire to involve the EU agencies in investigations. So far they have only been operating as supranational coordination bodies.

Hessen gave the following recommendation:
The agencies should have closer relations with the lower levels of the justice systems in the *Länder*, i.e. they should approach the public prosecutors directly to explain their own role and the benefits to be derived from involving them.

Lower Saxony gave the following recommendation:
Access to the EC3 analysis unit should be simplified and made directly accessible to the *Land* authorities. The key is to link up EC3 and Eurojust so that coordination between the law enforcement authorities can be accompanied by the provision of a comprehensive, Europe-wide analysis of data. It would also be helpful to increase the EC3's role as a provider of forensic services, e.g. by enabling it to test new types of malware and how they function in certain operating system environments, focusing on how they work and ways of recognising them.

As regards Eurojust, it would be helpful to make even more progress on the synchronisation of investigation measures, since it remains impossible in practice to perform simultaneous monitoring of servers in several Member States. Eurojust would however also be the right body for giving due consideration to the various demands of individual countries and establishing, on a case-by-case basis, competence networks in the Member States which can then provide direct input to the investigating law enforcement authority in specific cases, e.g. following prior approval of the envisaged measures by the national competent bodies.

Rhineland Palatinate gave the following recommendation:
Where the investigating department involves Europol from the start of an investigation the relevant analysis work file (AWF) can be used at an early stage. This means, however, that the data collected during the case - on people, vehicles, statements, phone numbers, nicknames, etc. - is provided by the investigating department at a later stage in the proceedings, which generates a corresponding workload. By entering the personal details of suspects in the Europol Information System (EIS) in parallel with the above procedure, the added value of both the EIS and the AWF could be significantly enhanced, not least owing to the resulting or increased probability of obtaining hits. EUCTF meetings are attended by a representative of the Federal Criminal Police Office (BKA).

7.1.3. Operational performance of JITs and cyber-patrols

The Stuttgart public prosecutor's office which participated in a JIT reported that the experience had been unsatisfactory, as the other Member State concerned had failed, for ultimately unsound reasons, to provide the evidence needed to transfer a particular offender. On the other hand, the ZIK (Central Unit for Combating Information and Communications Crime at the Stuttgart Office of the Chief Public Prosecutor) in **Baden-Württemberg** had had some entirely positive experience of the JIT arrangements.

Hessen reported positive experiences, saying that the reasons for establishing this instrument had been confirmed, as the procedures had been speeded up and could now be run more efficiently.
In **Saxony** too, the Office of the Director of Public Prosecutions and most of the offices of public prosecutions are already involved in joint investigation teams, primarily too investigate organised crime. Their experience in internationally coordinated investigations, which can be of benefit in effectively prosecuting cybercrime, has largely been positive.

The other *Länder* have so far had no experience of joint investigation teams.
Baden-Württemberg reported that the translation and travel costs for the JIT meeting in The Hague had been covered. Hessen reported that EU funds had been allocated to cover travel costs for coordination meetings at Eurojust.

There is no reported experience with joint cyber-patrols.

In order to improve international cooperation, in 2014 Germany, through the Federal Criminal Police Office (BKA), set up an international coordination group under the EMPACT Operational Action Plan on cyber-attacks. The aim of the coordination group is to create a platform for improving exchanges of experience between search units in the participating countries, simplifying contact arrangements and making more effective cooperation possible in any future joint activities.

7.2. Cooperation between Germany's authorities and Interpol

The international image database (ICSE DB) at Interpol's General Secretariat in Lyon has been up and running since March 2009. The relevant national ICPO-Interpol bureaus search the database and supply it online. In Germany it is the Federal Criminal Police Office which performs this role. Searches of the database can establish whether child pornographic material is new or already known and, if so, whether it has already been identified. Any image downloads are usually stored in the database with the relevant case data so that they are ready for future queries from any other state.

The potential added value of the ICSE DB thus grows steadily as the number of participating states increases and they make more active use of the database. The Federal Criminal Police Office has had online access to the ICSE DB since it started. It carries out database searches and inputs material into the database centrally, for the whole of Germany. The ICSE DB is an indispensable component of so-called 'perpetrator/victim identification'.

Cooperation between the Federal Criminal Police Office (*Bundeskriminalamt* – BKA) and third countries takes place where necessary via Interpol channels. There are high expectations of the INTERPOL Digital Crime Centre, currently under development at INTERPOL, as a central cybercrime contact point within the INTERPOL Global Complex for Innovation (IGCI, located in Singapore).

According to Saxony-Anhalt, cooperation is satisfactory. For a large number of countries, a formal request for mutual legal assistance must be made at judicial level in order to obtain subscriber data and traffic data for IP addresses or e-mail account data that can be used as evidence in court proceedings.

7.3. Cooperation with third states

Existing bilateral contacts are used when indicating investigative lines of enquiry abroad. Where no such contacts are available, the standard communication channels (Europol, Interpol and G7) for exchange of police information are used. Where necessary, information needed for use in court is provided through the standard legal assistance procedures.

With regard to combating child pornography, which is treated as a cybercrime by Europol EC3, our experience of investigations that have had to be coordinated at international level has been positive. Cooperation between third countries, Europol / EC3 and the Member States has also proven useful in the context of combating conventional cybercrime.

In **Baden-Württemberg**, initial experience with EC3 is currently being gathered in the course of ongoing investigations. In proceedings conducted by Baden-Württemberg *Land* Criminal Police Office (*Landeskriminalamt Baden-Württemberg* – Baden Württemberg LKA) it has been possible for links to proceedings in other Member States to be made via EC3 using what are called cross-match reports. Efforts are currently being made to exchange information with these countries. With the aim of further developing cooperation with Europol, an official was seconded to The Hague for a three-month work-shadowing visit. A further three-month work-shadowing visit took place at the beginning of 2015.

Hessen cited the following link:
http://www.eurojust.europa.eu/press/PressReleases/Pages/2014/2014-05-19.aspx
They also reported that all coordination meetings had been attended by the representatives of the US LEA. Eurojust and Europol/EC3 were said to be the ideal partners for involving non-EU Member States in ongoing investigations.

Lower Saxony reported that it has brought an added value. In particular, there was reported to be one case in which the involvement of the USA via Eurojust had been helpful, and the degree of cooperation had in certain respects been greater than in bilateral relations.

7.4. Cooperation with the private sector

In the BKA's experience, local branches of foreign service providers are always sales/marketing subsidiaries that do not have access to data of the parent undertaking. In this regard there has to our knowledge been no cooperation, nor have any coercive measures been taken.

Private-sector companies contribute to the costs that arise in connection with institutionalised cooperation. For example, funds are being made available for the establishment of the G4C.

The Federal Criminal Police Office (BKA) endeavours to reduce obstacles to cross-border cooperation, particularly in the field of online card fraud, by strengthening international bilateral cooperation and involving central agencies (Interpol/Europol).

In Saxony-Anhalt and other *Länder*, cooperation with foreign police authorities takes place in the context of international judicial cooperation. In addition, the Euro-Kartensysteme GmbH's payment card security service collects all data relating to ATM / POS terminals that have been targeted across Europe and makes these data available to the investigating authorities.

Hessen provided information on an approach that has proved effective in recent years as regards the preservation of evidence across borders. This concerns cases in which information has been passed on from abroad concerning criminal offences that also affect individuals in Germany. The approach comprises the launching of parallel investigative proceedings, the taking of preliminary measures to secure evidence and the timely transmission of information obtained to foreign investigative authorities pursuant to Sections 61a and 92c of the IRG (Act on International Legal Assistance in Criminal Matters) on preparing an MLA request.

As the formal MLA procedure has often proved too difficult for effective law enforcement, bilateral cooperation (especially in the form of joint investigation teams JITs) has in recent years proved to be another effective tool in combating cross-border online card fraud.

In this context Germany is also involved in a number of European and international projects. These include:

- the European Network and Information Security Agency (ENISA), which aims to promote increased cooperation and information exchange between Member States in the area of network and information security;
- the European Commission's AGIS programme, designed to help legal practitioners, law enforcement authorities and representatives of victim assistance services from the EU Member States and candidate countries to set up Europe-wide networks and exchange information and best practice;
- the Interpol European Working Party on IT-Crime (EWPITC), a platform for the exchange of information to combat IT crime.

7.5. Tools of international cooperation

7.5.1. Mutual legal assistance

With the exception of the provisions set out in the Convention on Cybercrime, there is no specific legal basis in Germany for the provision of mutual legal assistance in cybercrime investigations. The same conditions and rules apply to mutual legal assistance in cybercrime investigations as in the investigation of other offences.

Mutual legal assistance in cybercrime investigations works in exactly the same way as it does in other criminal matters. As a rule, the federal authorities in Germany are responsible for dealing with mutual legal assistance. In that regard, the Federal Office of Justice functions as the central unit. Approval decisions are taken with the consent of the Federal Foreign Office. In contrast to the use of diplomatic channels, which involves requests sent via the Federal Foreign Office, international agreements can go through the Ministry of Justice.

To a large degree, an agreement between the Federal Government and the *Länder* governments has transferred competence mainly in EU- MLA matters to the justice ministries in the *Länder*. As a rule, the justice ministries in the *Länder* have further delegated the decision in matters relating to mutual legal assistance between EU member State to the public prosecutor's offices.
Urgent requests for data preservation measures can be sent through the 24/7 Network pursuant to Article 35 of the Convention on Cybercrime or the G7 Network of Contact Points, in which the Federal Criminal Police Office is the national contact point.

The Federal Government and the *Länder* do not keep official statistics on mutual assistance.

Under German law there are no specific procedures or conditions that need to be fulfilled as regards the various categories of MLA requests related to cybercrime. As a general rule, mutual legal assistance under German law is based on a requirement to accelerate the handling of requests; see point 19(1) of the German guidelines for relations with foreign countries in criminal matters ('with immediate effect' RiVASt - *Richtlinien für den Verkehr mit dem Ausland in Strafrechtlichen Angelegenheiten*).

Any measures covered by criminal procedure law may be requested under an MLA request concerning cybercrime. On this point, please see our comments on question 2.B.2. Additionally, pursuant to Section 110(3) of the Code of Criminal Procedure, examination of an electronic storage medium may, under certain conditions, also be allowed to be extended to storage media that are physically separate from the initial storage medium.This includes the securing of data on the separate storage medium. However, since there are complex issues related to cloud computing, as it is called, it is not necessarily clear whether the data are physically stored in the country or abroad (and, in some cases, in which foreign country).

According to information held by the Federal Government, third countries regularly issue requests relating to computer sabotage. Outgoing requests quite often concern fraud and child pornography.

In urgent cases, requests for immediate assistance are sent via the 24/7 Network provided for under Article 35 of the Convention on Cybercrime or the G7 Network of Contact Points; however, such requests are always followed by formal requests for legal assistance.

In appropriate cases, a prior consultation may be helpful, either directly between the relevant authorities or through the European Judicial Network or Eurojust. This is particularly useful where requests need to be handled simultaneously in a number of different states, or where there is uncertainty regarding the requisite format and content of a request.

When issuing requests for backing up and releasing of data in the 'cloud', it is often not clear which state the request should be addressed to.
The Federal Republic of Germany is a signatory to the Council of Europe's Convention on Cybercrime of 23 November 2001. The Convention on Cybercrime has already been used in several cases as a basis for MLA requests with third countries. The requests in question were sent to and received from the United States of America and Canada.

The United States generally attaches strong formal and content-related requirements to such requests, particularly as regards the link between the criminal offence and the specific element of proof that is the subject of the request for transmission. Efforts are made to understand and comply with these requirements through training and detailed discussions with the US Department of Justice on general issues and individual cases.
In addition, the provisions in Section 67(1) of the Act on International Legal Assistance in Criminal Matters (IRG), together with Sections 59 and 73, enable the competent German authorities and courts to provide legal assistance even where there is no international legal basis.

The existing international communication channels (Interpol, Europol, G7 and numerous bilateral contacts) are used. In the case of judicial requests, the formal channels for mutual legal assistance are used; however, in the fast-moving area of cybercrime, the formal rules make these channels generally impracticable and ineffective, in particular because the process is protracted and execution of the request takes time. Here, the G7-24/7 network of contact points is proving useful. It cannot, however, make up for all the shortcomings of the channels for mutual legal assistance. Efforts are therefore being made to extend the quick information exchange at police level to the judicial level too, through direct cooperation of the competent public prosecutor's offices.

7.5.2. Mutual recognition instruments

Germany has transposed all the framework decisions in mutual recognition matters. The Federal Government basically has no knowledge of numbers of cases as competence vis-à-vis the EU in this area has been transferred to the *Länder*. Neither the Federal Government nor the *Länder* record general statistics on legal assistance. The Federal Government only has competence for the application of the law implementing the Framework Decision on financial penalties, in respect of which the emphasis has so far been placed on road transport fines.

7.5.3. Surrender/extradition

Extradition to other Member States of the EU for prosecution purposes is permissible under Section 81 IRG, which transposes Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, only where the offence is punishable under the law of the requesting Member State by a maximum sentence of imprisonment or an alternative penalty lasting at least 12 months. Extradition for the purposes of enforcing a sentence is permissible where the sentence imposed by the requesting Member State provides for a prison term of at least four months.

A surrender or extradition does not require a double-criminality check where the offence is one of those listed in Article 2(2) of the Council Framework Decision of 13 June 2002 on the European arrest warrant.

Requests sent/received for surrender or extradition are to be found in the attached 'Record of statistics on extradition for 2013' dated 14 January 2015 and published on 25 February 2015. The statistics on extradition for 2014 have also been published after the evaluation visit: http://www.bmjv.de/DE/Service/Statistiken/Statistiken_node.html .

There are basically no specific procedures or conditions that need to be complied with as regards requests related to cybercrime. The general call to accelerate the handling of such requests is based on point 19(1) of the German guidelines for relations with foreign countries in criminal matters (*Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten, RiVASt)*. Incoming requests are processed as a priority. Support from the European Judicial Network, Eurojust, and the 24/7 Network established by Article 35 of the Convention on Cybercrime, helps speed up the processing further.

Provisional arrests may also be used in the context of fighting cybercrime.

The average duration of processing is only recorded statistically for surrenders effected under the European arrest warrant. The statistics do not distinguish between individual types of offence. In 2013, surrender procedures with the consent of the person under investigation took 15.94 days to process, whilst those without the person's consent took 38.4 days. In 2014, surrender procedures with the consent of the person under investigation took 15,15 days to process, whilst those without the person's consent took 41,74 days.

The Federal Criminal Police Office's responsibility in relation to the worldwide Interpol wanted-person searches does not entail any specific procedures and there are no special requirements for cyber-offences. The standard Interpol wanted-person search procedures are used for dealing with such crimes. The legal basis for issuing German requests for wanted-person searches (covering all types of crime) to foreign states is Section 14 of the Act on the Federal Criminal Police Office and on Cooperation between the Federation and the *Länder* in Criminal Matters (BKAG), whilst the legal basis for the processing of wanted person search requests from abroad (covering all types of crime) in Germany is Section 15 BKAG. Additional types of procedure and/or requirements relating to requests on combating cybercrime are covered by the Convention on Cybercrime or the general rules governing legal assistance. We cannot provide universally valid and reliable statistics on response times on requests for legal assistance.

Requests sent/received for surrender or extradition are to be found in the attached 'Record of statistics on extradition for 2012' of 13 January 2014, which was published on 11 February 2014. Meanwhile statistics for 2014 have been published as well. Typical cybercrime offences are cited in the following sections of the German Criminal Code: Section 202a ('data espionage'), Section 202b, Section 202c ('acts preparatory to data espionage and phishing'), Section 263a ('computer fraud'), Section 269 ('forgery of data intended to provide proof'), Section 303a ('data tampering') and Section 303b ('computer sabotage').

Here too the principal legal basis is the Convention on Cybercrime. In addition, the Federal Government may act on a non-contractual basis.

7.6. Conclusions

- **Cooperation with EU Member States was assessed as generally good, and practitioners make use of all the available channels: bilateral relations, liaison officers and magistrates or EU agencies. Cooperation with third states is sometimes difficult and responses are delayed.**

- **During the visit, practitioners several times mentioned the need for a secure channel to exchange information between prosecutors and other law enforcement authorities.**

- **Germany has made efforts to establish a reliable and very structured private–public partnership at federal and *Land* level.**

- **BKA has entered into an agreement with the German Competence Centre against Cybercrime (G4C), an association composed of a number of banks which is especially important from the perspective of online card fraud.**

- **Good cooperation with BITKOM (Germany's digital association, set up in 1999 as a merger of individual industry associations in Berlin and representing more than 2 300 companies in the digital economy) and Deutsche Telekom was also underlined. These companies offer a range of software and IT, telecommunications and internet services, manufacture hardware and consumer electronics, and operate in the digital media and internet industries.**

- **Deutsche Telekom must comply with the right to secrecy of telecommunications and with data protection legislation. It does not respond to direct inquiries from authorities outside Germany. Any inquiry should be received via the relevant German authority (process of MLAs). Deutsche Telekom is of the opinion that cross-border procedures between providers and law enforcement authorities should be harmonised, since every country currently has different requirements regarding lawful interception and data provision. This makes it difficult for them to operate and to ensure compliance with the law.**

- **The main stakeholders in international cooperation mentioned during the visit were: specialised cybercrime prosecutor's offices, general prosecutor's offices (contact points EJN and ENCS), the Federal Office of Justice (contact points EJN, ENCS and further networks), the Federal Criminal Police Office (BKA), the German Liaison Bureau at Europol, and the German Desk at Eurojust. Eurojust is very well known by practitioners and used when necessary. A good example of the use of Eurojust in a complex cybercrime case dealt with by PPO Verden was presented. Europol is known as well and used by law enforcement authorities, which participate in the activities carried out by all three focal points dealing with cybercrime issues (Cyborg, Twins and Terminal) and in EMPACT projects developed under the EU policy cycle. Europol (EC3) has been involved in concrete cases and information is exchanged via the corresponding channels (SIENA).**

Germany has no separate provisions to regulate international cooperation on cybercrime, with the exception of the provisions set out in the Convention on Cybercrime. Provisions in international treaties apply directly (e.g. Act on International Cooperation in Criminal Matters, section 1(3) [Article 29 Budapest Convention]). The general rules on mutual legal assistance apply to all investigations, regardless of the type of crime. This also includes cybercrime investigations. As a rule, the federal authorities are responsible for dealing with mutual legal assistance, specifically the Federal Office of Justice, which functions as a central unit. There are no specific procedures to speed up the handling of MLA requests in cybercrime investigations. There is, however, a general requirement under German law to accelerate the handling of MLA requests. It was emphasised that subscriber information can be obtained quite quickly, if the MLA process was considered too slow. There are high hopes that practical solutions will be found to speed up the process following the discussions at EU level.

- **In some cases German authorities have not decided to set up a JIT because they considered that evidence could be obtained and exchanged very quickly on a bilateral basis.**

- **There are no statistics on MLA requests due to the fact that they fall under the jurisdiction of the *Länder*.**

- **The Europol national desk includes 10 representatives and its organisation reflects both federal and *Land* levels. The national authorities also emphasised the close cooperation with EC3.**

- **The team was informed of the idea of putting in place a measure similar to 'hot pursuit' in cybercrime investigations, which will allow investigators to cross national jurisdictions in urgent cases and access data directly.**

- **In terms of practical tools used in international cooperation, Germany uses Eurojust, EJN, Europol (EC3) and BKA as a 24/7 contact point.**

- **As a good practice, Germany has guidelines on international cooperation in criminal matters ('RiVASt').**

- **Germany is a member of J-CAT and the work of this target group was considered very efficient.**

- **Germany welcomes discussions at EU level concerning improvements to criminal justice in cyberspace, and supports the establishment of the European Judicial Cybercrime Network.**

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

The **Federal Criminal Police Office (BKA)** has contributed substantially to the development of various national initial and further training programmes. These meet the requirements for initial and further training formulated by the Federation and the *Länder*. Pursuant to the 'uniform federal initial and further training approach for ICT crime', specialists – classified either as 'first responders', 'specialists in the broader sense' or 'specialists in the narrower sense' – are offered targeted training courses based on their qualifications and intended deployment. This approach has been implemented by the *Länder* after being adapted to local circumstances. To ensure uniformity and avoid duplication of efforts, multipliers have been used in the *Länder*. Coordination of these multipliers is ensured by means of annual further training events for multipliers organised and run by the BKA.

In cooperation with the specialised units of the Serious and Organised Crime Department (*Abteilung Schwere und Organisierte Kriminalität; SO*), the KI Department offers the following specialised courses drawn from this approach on an annual basis: 'Child pornography on the internet', 'Pharmaceutical crime via the internet', and the 'Special training course for members of central internet research units'. In addition, the BKA is responsible for the central expert training in the field of ICT forensics for the Federation and the *Länder*. As part of this training it is possible to specialise in Windows, Linux, Macintosh, networks/internet, mobile forensics and cryptology. All modules that form part of the expert training course are offered once a year. Within the BKA, an internal basic training course on cybercrime consisting of two modules is made available once a year.

Training courses for which there is an urgent need are organised at short notice both exclusively for the specialised units of the BKA and in the form of needs-based courses for the Federation and the *Länder* . For example, in 2013 it was established that there was a nationwide need for courses in Windows 8 forensics. In response to this need, a large-scale Windows 8 event was held in June 2014, at which more than 50 officials from the Federation and the *Länder*, as well as from Switzerland and Luxembourg, received training. This course was run again in November 2014 due to the continued high demand. Similar training courses are being planned for Macintosh forensics, mobile forensics and Windows 10.

At the **German Judicial Academy** in Trier and Wustrau a total of seven conferences/further training courses are offered for **judges and public prosecutors from across Germany** who are involved in combating internet crime: '**Investigative measures in the field of telecommunications**', '**Forms of internet crime and how to combat them**', '**Criminal law and the internet**', '**Current developments in criminalistics (forensic science) and criminal justice**', '**Developments and trends in criminal law**', '**Criminal proceedings in cases involving counterfeiting and piracy**' and '**The fight to protect copyright in the digital age**'.

The conference on '**Criminal proceedings in cases involving counterfeiting and piracy**' deals in particular with copyright infringements through illegal downloading on the internet. During the five-day event, substantive law provisions from trademark, copyright and patent law as well as the relevant criminal law provisions are discussed, and an insight is given into the practical work of customs and police authorities. The focal point of the four-day event entitled '**The fight to protect copyright in the digital age**' also covers the prosecution of copyright infringements on the internet, and features an examination of civil and criminal law issues in this context, with particular emphasis on new digital media. One of the presentations given during the nine-day training course entitled '**Current developments in criminalistics and criminal justice**' deals with the subject of 'Identifying perpetrators and victims from child pornography media – also in the context of international cooperation'. It thus relates to one of the specific areas to which the Member States wish to devote particular attention.

The conference on '**Investigative measures in the field of telecommunications**' runs over six days and is aimed at helping to fight offences committed by means of telecommunications, inter alia by conveying knowledge concerning the structure and functioning of the internet, the legal bases in terms of substantive law, and a description of the practical implementation of covert investigative measures. The conference on '**Forms of internet crime and how to combat them**', which runs over five days, deals with the question of the applicability of German criminal law, covering questions of jurisdiction, mutual legal assistance, provider accountability, search methods and forms of internet crime. The German Judicial Academy also offers the six-day further training course '**Criminal law and the internet**' on an annual basis.

This course looks at the different forms of crime connected with the internet, such as phishing, the underground economy, cyber-war, copyright infringements and the dissemination of child pornography in data networks, and at the possibilities for conducting investigations using technology. The current programme of the one-week conference on '**Developments and trends in criminal law**', which also takes place on a yearly basis, covers inter alia substantive law issues of internet crime.

The conferences on '**Forms of internet crime and how to combat them**' and '**Criminal proceedings in cases involving counterfeiting and piracy**' also feature in the **European Judicial Training Network (EJTN)** list. This also offers judges and public prosecutors the possibility of participating in events organised by other Member States. In addition to these events, the EJTN offered 12 further training sessions in 2014 in connection with the subject of cybercrime:

Five events hosted by **various countries (Scotland, France, Portugal and Belgium)** were entitled '**Cybercrime**'. Four of these events were one-day sessions, while one was held over five days. The three courses offered this year entitled 'Basic training course on legal and technical aspects of cybercrime for judges and prosecutors' (each of two days' duration) are aimed at teaching skills for dealing with cybercrime. The course on 'Countering the illegal use of the internet: legal and policy developments at international and European level four years after Stuxnet' (two days) is one of a series of seminars dealing with the fight against internet crime. This event covers large-scale cyber-attacks such as the Stuxnet computer worm attack, and goes into current developments concerning the possibilities for fighting such attacks. The two-day course on 'Justice and cybercrime' focuses on online payment systems, one of the main subjects agreed on in the GENVAL Working Party. The two-day seminar on 'The validity and admissibility of electronic evidence in cybercrime cases' deals with the evidentiary value and admissibility of electronic evidence in cases of cybercrime. The conference on 'Online financial crimes and fraud committed with electronic means of payment' (two days) deals with fraud crimes on the internet, for example in connection with internet auctions or phishing.

In addition, the individual *Länder* offer the following internal further training programmes/courses:

Baden-Württemberg

All police officers in Baden-Württemberg attend courses on the subject of cybercrime as part of their training programme. The training programme for intermediate-level police officers currently includes learning content on cybercrime amounting to 41 hours of tuition. There are plans to upgrade this subject area and to incorporate 50 hours of tuition into the training programme. As regards the training programme for senior police officers, the Police Training College organises courses on this subject (in the areas of criminalistics (forensic science) and information technology) to roughly the same extent as for the intermediate-level police service.

In terms of content, the courses provide instruction in the fundamental principles of hardware and software, the operation and structure of the internet, an overview of malware and an explanation of its function, terminology and nature, relevant offences and information concerning the establishment of suspicion and the preservation of evidence. Depending on an employee's career progression within the organisation, their knowledge of the basic principles is then subsequently supplemented and expanded by means of further training courses, as required. The training programmes in Baden-Württemberg are based on the 'General concept of cybercrime / Digital evidence' (status as of 22 January 2013) developed by the Baden-Württemberg *Land* Criminal Police Office.

The training framework is divided into three levels:

- Level 1 - First responders:

The level of knowledge required by a police officer on patrol for dealing with the issue at the 'first point of intervention'. This knowledge is imparted within the framework of the training course.

- Level 2 - Cybercrime specialist:

The level of knowledge required by a police officer specialising in cybercrime in a broad sense (internet crime), and in simple cases also by those specialising in cybercrime in a narrower sense (computer crime). Such specialists also act as contact points for first responders. This knowledge is imparted within the framework of training courses currently amounting to 26 training days, and builds on the first responder knowledge.

- Level 3 - Highly specialised police officers:

The level of knowledge required by police officers dealing with complex cases of cybercrime, who must have extensive know-how in the field of digital forensics.
Such officers are found only in Criminal Police Inspectorate No 5 of the police headquarters and in Department 5 of the LKA BW.
The aim of the training at levels 2 and 3 is to impart the necessary degree of knowledge to combat all aspects of cybercrime across the board.

In parallel with the training courses, each law enforcement officer in the Baden-Württemberg police force has permanent access to an electronic learning application (ELA), which provides extensive up-to-date information on this topic. The ELA serves as a reference work for the subject area of cybercrime and, by providing updates as needed, aims to ensure that police officers maintain a high level of knowledge.

Berlin

With regard to Berlin, mention should be made of the joint training programme for specialists from the *Land* police force and public prosecutors from Lower Saxony.
Training for first responders (level 1 of the federal ICT training model) is provided in accordance with the 'multiplier model'. For cybercrime specialists in the broad sense (level 2), the *Land* Police Academy offers a four-day course on the subject of 'Selected technical aspects of internet-based investigations'. For the level 3 target group in the ICT training model, the Berlin Criminal Police Office relies on courses offered by other providers (Federal Criminal Police Office [BKA], other *Länder*). In 2012, all police officers in LKA departments 335 and 336 attended a special two-week course.

A two-day course on 'internet child pornography for police officers, public prosecutors and judges' is organised by Dunkelziffer e.V. at various locations in Germany several times a year. Within the Berlin public prosecutor's office, police officers responsible for investigating cybercrime follow special training programmes. The aim is to equip them with the specialised technical and legal knowledge necessary for their day-to-day work in terms of file handling and courtroom representation. A course of this type was held recently, comprising a total of six whole-day training sessions. In addition, efforts are being made to hold annual sessions to consolidate existing knowledge.

Brandenburg

In principle, every police officer is offered an opportunity to attend training courses on cybercrime. The aim is to provide all police officers with a basic level of knowledge by means of training, study and refresher training. An e-learning application comprising a total of four modules enables police officers to acquire a knowledge of the basic principles through self-study on a PC. The modules cover subjects such as hardware, software, social networks, cloud computing, phenomenology, criminal law and criminal procedural law. Building on that, a three-day on-site seminar is held at the Police Academy to consolidate the basic knowledge already acquired by means of practical exercises. Further add-on and specialised modules are offered as required, depending on the target group. The content of all the seminars offered within the training programme is adapted to the Federal Training Plan for the Reorientation of the Criminal Police.

Brandenburg Judicial Academy organises regular training sessions for the senior judiciary that deal with measures to combat cybercrime. In 2013, for example, a one-day course was held on the subject of internet crime which included both an introduction to internet crime and a special training session on ‘phishing and money mules’. In 2014 there were two one-day sessions which dealt primarily with technical principles and possible investigative measures in the field of cybercrime and with the decision of the EU Court of Justice concerning data retention. The events served to convey the requisite basic knowledge in particular to judges and public prosecutors dealing with the phenomenon of ‘cybercrime’ in the context of volume crime and petty crime.

In addition, in 2014, within the framework of ‘training in the field of IT crime’, the Joint Judicial Examination Office of the *Länder* of Berlin and Brandenburg, which is responsible for training the senior judiciary, organised a special six-day course for specialists on combating IT crime, to cater to the continually growing technical and legal requirements in the field of ‘cybercrime’. The subjects covered included the preservation of computer evidence, data network investigations, including with a foreign dimension, the challenges presented by big data and problems relating to data protection.

In addition, case-worker conferences on specialist subjects (e.g. WebMoney) are organised once a year by the specialised directorate of the *Land* Criminal Police Office and are open to members of the specialised unit of the public prosecutor's office.

Saarland

In Saarland, training courses are organised at *Land* level in the following areas:

- comprehensive basic training ('Cybercrime - first responders')
- special training for members of departments LPP 222 (cybercrime) and LPP 4.7 (IT forensics)

The subjects, frequency and duration of the courses are determined on an individual basis, as required.

Saxony

In Saxony, 81 training courses on the subject of cybercrime are organised at central level for police officers. Courses are offered in the field of investigations (ICT 0700) and in the various service areas (e.g. mobile telephony, computer and internet network forensics). Given the overlaps (in particular in relation to information security) with other areas of ICT operations (e.g. the operation of networks and databases), such subjects are also included.

Until 2012, the Saxony Criminal Police Office used to organise an annual four-day "modular complex course" which was also open to specialists at the public prosecutor's offices. topics included a "presentation of techniques for investigating ICT offences, in particular internet crime", "possibilities and limitations in terms of the forensic analysis od data carriers" and a "presentation of the capabilities of the Saxony police force in the field of combating ICT crime with a view to the proper planning of future investigative measures". The course ceased to run in 2013 as the Saxony police force had to carry out a major overhaul of the course concept.

For several years now, the Saxon public prosecutor's offices have been involved in a successful joint venture with an undertaking specialising in IT forensics. Every year, the undertaking in question offers a two-day training course for up to ten participants. The content of the workshops is guided by the current requirements of those involved in combating cybercrime. In the past, the subjects discussed have included the following: ‘chat software analysis of social networks’, ‘investigation of IP addresses’, ‘analysis of mobile telephones’, ‘problems in the field of cloud computing’, ‘technical possibilities and limitations in terms of monitoring internet data traffic’, ‘technical approaches to investigation in cases involving spoofing’ and ‘functioning of the bitcoin payment system’.

Since 15 March 2016, the Saxon Central Counter-Cybercrime department at the Dresden office of the Director of Public Prosecutions has been coordinating education and continuing professional development for Saxon public prosecutors on cybercrime. For this purpose, it developed a basic qualification training concept for all Saxon public prosecutors and also offers in-depth continuing professional development measures for specialised cybercrime department officers.

In addition, the central unit for combating computer and internet crime (Saxon Central Cybercrime Unit) is seeking to engage in close long-term cooperation with a university in Saxony. As part of that cooperation, training courses will be organised at regular intervals focusing on topical IT-related subjects. The first workshop, dealing with general subjects relating to data analysis, took place in September 2014.

Saxony-Anhalt

The area of criminal police training follows the precepts outlined in the federal training plan for special further training in criminal police matters, for which a federal/regional project group has been set up. Under the plan, all police officers are offered training on the subject of cybercrime. Training is divided into three areas (police first responders, cybercrime specialists and specialists in forensic cybercrime). The course frequency is determined by the requirements of the departments concerned. For criminal court judges and public prosecutors, training is offered in the field of cybercrime. Once a year, Saxony-Anhalt's Ministry of Justice and Gender Equality organises a three-day training course on the subject of 'special investigations and multi-media communication - challenges for law enforcement'. Since 2004, the Saxony-Anhalt Media Authority has organised a three-day course on 'the protection of minors on the internet - investigation, preservation of evidence and establishment of the facts', aiming to make those taking part more familiar with the functioning of the internet, internet-related legislation, legally robust documentation techniques and specialised IT tools for internet searches. Training courses on the subject of 'information security and data protection' - in some cases extending over several days - are offered to employees of units involved in various spheres of activity (systems support, public and private sector management, judges, judicial assistants and members of the mid-level judiciary, judicial workers). They aim to provide information on the relevant laws on information security and the secure handling of IT equipment and data.

Schleswig-Holstein

Specialists responsible for conducting criminal investigations in the area of cybercrime acquire their expert knowledge through courses organised by the police directorate for further training within the framework of Schleswig-Holstein's ICT training plan. The aim of the IT training programme and the accompanying cybercrime sub-programme is to enable all trainees and students to qualify as 'cybercrime first responders in accordance with the federal cybercrime training concept' via the police directorate for further training within the framework of their career development.

The IT training cybercrime sub-programme comprises a range of seminars corresponding to the federal cybercrime training framework which enable all employees of the Schleswig-Holstein police force to acquire the skills necessary to qualify as cybercrime first responders. In addition, the police directorate for further training offers a continuously developing, updated and adapted programme of seminars whereby other target groups can also gain qualifications in the field of cybercrime.

On top of the regular programme of seminars, additional seminars are developed and run on request and according to need, in particular for target groups in the Schleswig-Holstein Criminal Police Office involved in the preservation of computer evidence and cybercrime-related activities, to cater to special needs and requirements. For such seminars, external lecturers are employed, cooperation is entered into with other police training providers and any free places available are published via the Federal Criminal Police Office to encourage an exchange of expertise at federal level. The IT training cybercrime sub-programme, together with the accompanying programme of seminars published inter alia via Extrapol, is regularly checked and updated by the police directorate for further training and adapted to the requirements of a professional regional police force. CEPOL contributes to the educational and training programme, to the extent that a representative of the *Land* Criminal Police Office is taking part in the 'Cybercrime forensics and digital evidence' course at the Estonian Forensic Institute this year.

Bavaria

Special training courses on the subject of cybercrime for staff of the specialised departments and the IT contact points of the public prosecutor's offices and Chief Public Prosecutor's Offices were first held in Bavaria in 2012. The basic courses took place over a two-week period, and were divided into several segments. In addition to technical issues and issues relating to investigative tactics, the courses focused primarily on legal matters and aspects of IT forensics. These courses are supplemented by an annual exchange of information on topical issues extending over several days. The basic courses are repeated every three years. In addition, special week-long training sessions for investigating judges are held in Bavaria once a year with a view to providing information on technical and legal issues in connection with investigative measures in the field of cybercrime.

Hamburg

Hamburg Police Academy currently offers four courses for the various target groups in its permanent training catalogue. They are divided into the following levels based on the requirements of the specific tasks involved:

I + II. Courses for first responders (beginners and beginners' basic course)

The beginners' course lasts for one day. The aim is to provide course participants with computer and internet skills. Once they have completed the course, their newly acquired skills should give them greater confidence in their computing and internet-related work. The beginners' basic course lasts for two days. Participants should acquire further, more extensive knowledge of various internet services in addition to the WWW service. They should become confident in handling offences relating to the internet. They should also be able to recognise what action needs to be taken and initiate the necessary measures, attain proficiency in the use of internet-specific technical jargon and extend their skills and investigative competencies in internet-related matters.

III. Investigators in standard cybercrime-related cases (advanced training course)
Participants in the three-day advanced training course should acquire further, more extensive knowledge of various internet services in addition to the WWW service.

They should become confident in handling offences relating to the internet. They should also be able to recognise what action needs to be taken and implement the necessary measures, attain proficiency in the use of internet-specific technical jargon and extend their skills and ability to retrieve information in internet-related matters.

IV. Special investigators in technically challenging cybercrime cases and forensic scientists

(X-Ways)
This five-day course teaches specialists how to effectively analyse secure data using the X-Ways Investigator application, and how to document the results. The courses are divided into modules and must be followed in strict order. They are organised and run according to need, depending on the resources available.

Since August 2014, students of Hamburg Police Academy undergoing basic training have spent one day of their course learning about the internet/cybercrime.

Employees of the cybercrime unit at the Hamburg *Land* Criminal Police Office (LKA 54) undergo training based on their personal requirements and the available funding. Some employees take part in training programmes on an official basis, while others attend on their own initiative and sometimes also at their own expense. The courses cover a broad spectrum of topics in the field of computer forensics (with the technical depth of knowledge depending on the organisation concerned) and deal with a very wide range of specific areas (operating systems, applications, hardware [e.g. mobile telephone forensics]). The training ranges from one-day courses and courses extending over several weeks to long-term measures such as studies at (open) universities leading to academic degrees.

Training on the subject of 'cybercrime' was last organised at regional level for judges and public prosecutors in Hamburg in 2012. The course focused on those provisions of the Criminal Code, Code of Criminal Procedure, Telecommunications Act and Telemedia Act which are of relevance to this area of crime, with reference to cases of special significance for IT-related offences.

Hessen

Hessen Judicial Academy offers the following courses:

(1) Basic training course on internet investigations and internet crime

This one-day course, which was first included in the Judicial Academy's programme in 2014, aims to impart a basic level of knowledge concerning internet investigations. It provides an introduction to the full range of possible intervention measures in internet investigations. The conference is directed at specialists responsible for or interested in handling criminal offences relating to the internet and/or youth media safeguarding procedures.

(2) Internet investigations/internet crime

This three-day course uses seminars followed by discussions to address the possibilities and limitations in terms of internet investigations, together with topical issues of substantive law relating to internet crime and youth media protection (sections 202a ff., 263a, 131 and 184 ff. of the Criminal Code). It presents the full range of possible intervention measures in internet investigations. It also covers measures to combat internet-related child pornography with regard to current case law and the development of telecommunications surveillance. The course is attended by investigators from Hessen *Land* Criminal Police Office in Wiesbaden, the police headquarters, the Federal Criminal Police Office in Wiesbaden, external experts and representatives of internet service providers. It has been held regularly - once a year - since 2008 and is targeted at public prosecutors and judges involved in investigations relating to the internet and/or youth media safeguarding procedures (including child pornography).

(3) Hessen Judicial Academy - Cybercrime

This one-day symposium is held twice a year for postgraduate trainee lawyers. It is also advertised in the framework of the European Judicial Training Network (EJTN). It is especially suitable for foreign participants.

Lower Saxony

Tailored training is offered on procedural law, substantive law, operational tactics and mutual legal assistance. The relevant training courses last for several days and are held at least once a year. There is also a whole range of specially tailored training courses and exchange opportunities for specialised personnel. The range of training available at the *Land* Police has been expanded further and includes continuing training in a modular system, which is sometimes also completed by staff from the prosecutors' offices. The subject of computer crime is also dealt with as one of many subjects in other training courses. The conference on 'International cooperation in criminal matters' offered by Lower Saxony includes a component on 'Foreign investigations into computer and internet crime'. The conference on 'The victim in the criminal justice system', which is also organised by Lower Saxony, also covers 'The needs of victims in the field of computer-related crime'.

Rhineland-Palatinate

The training offered by the Police Faculty of the *Land* Police Academy/University of Public Administration (LPS/FHöV) includes its own training modules, as well as modules in cooperation with other *Länder* and courses offered in collaboration with external providers. The training modules are designed mainly for members of the Rhineland-Palatinate police force. They include training courses on the significance of digital media for police casework, on internet investigations, on the relevant legal bases, on internet investigations and web 2.0 for investigators and on cybercrime multiplier training.

The LPS/FHöV also offers further training on specific subjects for public prosecutors and judges within the jurisdiction, with the support of the Rhineland-Palatinate *Land* Criminal Police Office. Subjects include, for example, general information on internet investigations, the legal scope for internet investigations, dealing with weblogs, Facebook, Twitter and so on, fraud methods, data manipulation and subscription traps.

The LPS/FHöV also holds joint seminars for the police and the judiciary. A seminar on police powers and the law and telecommunications/internet was planned for 2014. Types of data, evidence-gathering powers, monitoring the content of telecommunications, tracking locations, investigations on the internet and the relevant legal bases are some of the subjects dealt with in this seminar.

As a rule, seminars and training courses last for one to three days. Depending on what is on offer, each training activity takes place once a year or more. The specialist staff working in ICT forensics receive special cybercrime training. The aim of such training is to enable staff to examine compromised systems *post mortem* for any relevant digital evidence. Training in live forensics is in the pipeline.

Thuringia

Cybercrime training for the Thuringia police is based on the federal initial and further training plan for combating ICT crime.

For first responders, the content has been incorporated into the general training for intermediate police law enforcement officers.

Building on these basic courses, further advanced training events are also organised for specialists in ICT crime in the broad sense (yellow colour code) and specialists in ICT crime in the strict sense, investigative support specialists (regional evidence collection) and forensic ICT specialists (blue colour code).

For example, the following further training activities were organised in 2013:

- 1x operating systems/applications seminar (I-510.21)
- 1 x UFED-PA seminar (I-531.1)
- 1 x WK internet seminar (I-513.1)
- 1 x Windows 8 and forensics (I-540.1)
- 1 x GK cryptography (I-530.1)
- 1 x EnCase forensic analysis tool workshop (I-532.1).

1. Are there any specialised education modules targeted at IT-forensic examiners and cybercrime investigators?

See also the reply to question 10.B.1.

The Federal Criminal Police Office (BKA) offers central expert training in the field of ICT forensics at federal and *Land* level. This special training is exclusively for experts. In addition, special courses are organised on an ad hoc basis according to need. Special courses for cybercrime investigators are as follows: child pornography on the internet; pharmaceutical crime on the internet; and a special course for members of central internet research units. Cybercrime investigators in the BKA can also attend the cybercrime basic training course.

The following information was reported with regard to the *Bundesländer*:

Baden-Württemberg

The further training plan is divided into four modules which are adapted to the needs of the highly specialised staff at level 3 mentioned in the reply to question 10.B.1. Each component of level 3 is given individual further training tailored to specific needs.

Brandenburg

The advanced and special modules on offer are primarily for cybercrime investigators. The modules cover subjects such as the internet, law, crime scene management, data security, data examination and analysis methods. Seminars for more specialised groups, including IT forensic scientists, are covered by external providers or under the national further training offered by the Federal Criminal Police Office.

Saxony

Special further training and qualifications that go beyond the requirements of centralised further training are organised by specialised departments (e.g. SN4C and Saxon Central Counter-Cybercrime Department) either in-house or with external experts.

Saxony-Anhalt

The special training modules for forensic cybercrime specialists are provided either internally within the *Land* at the Police Academy, or in conjunction with other *Länder* as part of security cooperation between the Free States of Saxony and Thuringia, and the *Länder* Brandenburg, Saxony-Anhalt and Berlin, or at federal level under the auspices of the Federal Criminal Police Office.

Bavaria

Special training modules for IT forensic examiners and cybercrime investigators are offered by the Bavarian police's Further Training Institute.

Berlin

IT forensic scientists who handle the analysis of devices and data carriers work at the *Land* Criminal Police Office in Berlin. To our knowledge, relevant training exists for the staff concerned.

Hamburg

Now that the forensic analysis of data carriers has been decentralised thanks to the deployment of the X-Ways Investigator application, criminal police caseworkers are given a one-week course of training at Hamburg Police Academy in how to use the application (see reply to question 10.B.1.).

In the field of computer forensics, there is a standardised training course at the BKA to qualify as an analyst. The training is permanently on offer to staff of the Hamburg police, who complete it before actually starting work as analysts. There is no fixed, coordinated, permanently available path of modules to be completed by investigators. Content is taught depending on availability.

Rhineland-Palatinate

The LPS/FHöV regularly offers separate training modules for IT forensic examiners (e.g. in network forensics with Wireshark, virtualisation in forensics) and cybercrime investigators (e.g. police powers and the law and telecommunications/internet).

The groups mentioned are also able to attend relevant training modules as part of cooperation with other *Länder* (through the LPS/FHöV), such as ‘’Digital forensics VI: evaluation of internet artefacts’ and ‘Digital forensics V: live forensics’. Participation in events organised by external providers is also possible through the LPS/FHöV, such as ‘ICT expert training - module 2.1.1 Probability’, cybercrime multiplier training, and the basic training course entitled ‘Internet investigations and web 2.0’.

A certification programme under the Open C3S Project is also offered, in collaboration with Albstadt-Sigmaringen University. The programme, which consists of 17 modules, teaches subjects ranging from the basics of digital forensics to specialised subjects such as data carriers or mobile telecommunications forensics.

Rhineland-Palatinate also allows highly qualified police officers to take a Master's in digital forensics at the University of Albstadt-Sigmaringen. In the future, they will be deployed in selected management posts from the fourth starting grade upwards.

There are no special training modules. Some of the further training courses are, however, offered as advanced courses in cooperation with the cybercrime department of the *Land* Criminal Police Office.

Thuringia

The national initial and further training plan for ICT forensics experts has a modular structure. Annual further training activities teaching complex software tools for IT forensics are organised in the field of ICT forensics in Thuringia (Unit 43 of Thuringia *Land* Criminal Police Office and the regional evidence collection units in the *Land* Police Inspectorates). They include courses as well as joint workshops organised by Unit 43. Experts in ICT Forensics Unit 43 also participate in special courses and annual national seminars and workshops, when available, in several specialised subjects.

The Federal Criminal Police Office's Criminology Institute coordinates initial and further cybercrime training for the police services at federal and *Land* level. The Criminology Institute works in close cooperation with national and international centres of initial and further training. The Federal Criminal Police Office (BKA) is a member of the ECTEG and has developed three international courses for the ECTEG under the EU-funded ISEC2010 Programme, which have been made available to Europol. CEPOL and Europol (EC3) are also represented in the ECTEG, thus ensuring regular coordination and close cooperation.

The following (non-exhaustive) information was reported with regard to the *Bundesländer*:

Berlin

Over the past 15 years one member of the *Land* Criminal Police Office (LKA) 13 was able to take part in one Europol training course on child pornography. No information is available at this end on the extent to which the content of these courses feeds into the training course at the Federal Criminal Police Office (BKA). Training courses for members of the public prosecutor's office and the courts are conducted in consultation with the department for organised cybercrime via the Senate Administration for Justice and Consumer Protection. No EU organisations have participated so far.

Brandenburg

Basic training of police law enforcement staff for the handling of cybercrime comes within the remit of the Police Academy (FHPol). Further qualifications for specialists, especially in IT forensics, are the responsibility of the *Land* Criminal Police Office. Further training for senior members of the judiciary in the *Länder* of Berlin and Brandenburg has been the responsibility of the Joint Judicial Examination Office of the *Länder* of Berlin and Brandenburg since 1 January 2005. CEPOL further training, which is brought to the attention of the Examination Office by the Federal Ministry of Justice and Consumer Protection for members of the senior judiciary, is regularly advertised for staff. This did not include any training in cybercrime in 2013/2014.

Baden-Württemberg

The Centre for Intercultural Competences and Languages (ZIK) is responsible for designing the content of training in close cooperation with department 5 of the Baden-Württemberg LKA. In addition, successful cooperation with the police in basic training is to be resumed. The Ministry of Justice is responsible for the official administrative management of ZIK training courses as well as for managing budgetary resources. Colleagues working for Europol and Eurojust have acted as speakers in the context of further training.

Mecklenburg-Western Pomerania

Primary responsibility for cybercrime training lies with the Mecklenburg-Western Pomerania University of Public Administration, Police and the Administration of Justice in 18273 Güstrow. Further training programmes are planned at meetings of the members of the Programming Conference. The *Land* Ministry of Justice (Chief Public Prosecutor's Office or the Higher Regional Court) can also offer further training courses, workshops or other kinds of training on topics of particular importance. Tasks relating to further training to combat cybercrime are carried out by the central office in the Chief Public Prosecutor's Office, which is manned by a senior desk officer.

Lower Saxony

The Police Academy is the main body responsible for further training in the *Land* police and, as such, is also responsible for cybercrime training. The Police Academy has developed a modular initial and further training plan together with the police area authorities. The plan is closely aligned with the federal initial and further training plan, and is constantly updated. In addition, cybercrime specialists participate in national further training events and take up training offered by private bodies, including in the context of job shadowing. Cybercrime specialists are currently following a pilot webinar on operating systems and network technology in cooperation with Emden/Leer University of Applied Sciences. None of the European cybercrime training offers have been taken up yet.

Several levels at the public prosecutor's offices are currently working together in designing and carrying out training activities, with the Ministry of Justice ultimately responsible for coordination.

Saarland

LPP 302 and the Police Law Enforcement Services Department of the University of Public Administration.

Saxony-Anhalt

The Police Academy is responsible for central further training. The authorities and institutions of the *Land* police also run their own separate further training courses focusing on the special characteristics of the individual authorities either as decentralised courses or, depending on the available budget, as outsourced courses. The training offered by international training institutes such as CEPOL are available to all police officers and complement the training offered at *Land* or national level. Responsibility for cybercrime training is not centralised. Training is carried out by the Ministry for Justice and Equality (I), the German Judicial Academy (II) or the Judicial Institute for Scotland, the Institute of Judicial Training (Brussels), the Academy of European Law (ERA), the *Centro de Estudos Judiciários* (Portugal), the National Institute of Magistracy or the French National School for the Judiciary (ENM) (III).

Bavaria

Training in judicial matters is organised by the initial and further training department in the Bavarian State Ministry of Justice and is coordinated in close cooperation with the Special Department for Internet Crime in the Criminal Law Department of the Ministry of Justice. CEPOL, ECTEG and Europol/EC3 have not yet been involved in this training.

Bremen

Bremen police are offered police training by the Federal Criminal Police Office (BKA) and the Criminal Police Offices of the *Länder*. Bremen public prosecutor's office benefits from further training events organised by the Judicial Academy or other *Länder*.

Hessen

Hessen Justice Academy and the German Judicial Academy are responsible for organising the training referred to in question 10.B.1. The EU organisations mentioned have not yet been involved.

Hamburg

Hamburg Police Academy is basically responsible for the field of policing, and is the first contact point for training activities. However, there are various further training activities, especially specialised further training, which the Academy is unable to provide. The EU organisations mentioned currently do not have any influence on the training activities, or, if they do, it is minimal.

Training in judicial matters is the responsibility of the Staff Development and Further Training Department of the Justice and Equality Authority. No cooperation currently takes place with CEPOL, ECTEG or Europol/EC3 .

Rhineland-Palatinate

(a) In the police

The LPS/FHöV is responsible for central cybercrime training. Training needs are identified and the aims/content agreed in close contact with police headquarters and the Rhineland-Palatinate LKA. Training offered by CEPOL is advertised internally in Rhineland-Palatinate by the LPS/FHöV coordinating office, and places are filled according to need. However, since there are so few places available (only one or two for Germany as a rule) and they do not come up very often, CEPOL training does not really have any measurable impact on practical work at *Land* level. Training offered by Europol or ECTEG has played no part so far.

(b) In the justice system

The Ministry of Justice and Consumer Protection has primary responsibility for training judges and prosecutors, while the local authorities have secondary responsibility.

Saxony

The organisation of training and recruitment of relevant speakers is the responsibility of the Office of the Chief Public Prosecutor in Dresden and the Saxony State Ministry of Justice. EU-level organisations such as the European Police College (CEPOL), the European Cybercrime Training and Education Group (ECTEG) and Europol/EC3 have so far not been involved in training measures.

Thuringia

The Thuringia Police Training Centre (BZThPol) is responsible for cybercrime training within the Thuringia police force.

However, Thuringia also takes advantage of training provided in the context of security cooperation and the Federal Criminal Police Office (BKA). It was not possible to assess to what extent the European Police College (CEPOL), the European Cybercrime Training and Education Group (ECTEG) and Europol/EC3 contribute to training measures provided, for example, by the BKA. The Federal Criminal Police Office has an annual budget for cybercrime training of approximately EUR 200 000. These costs comprise instructors' fees, travel costs and the purchase of hardware and software.

In 2014, the German Judicial Academy spent EUR 151 844 on instructors' fees alone at its conference site in Trier, while at its Wustrau conference site, instructors' fees amounted to EUR 178 591.

The following (non-exhaustive) information was reported with regard to the *Länder*:

Baden-Württemberg

Approximately EUR 20 000 annually from the judicial budget for the training of public prosecutors.

Brandenburg

Approximately EUR 7 000 - EUR 10 000.

Saarland

Approximately EUR 20 000.

Saxony-Anhalt

Approximately EUR 40 000.

Bavaria

Approximately EUR 10 000.

Bremen

Approximately EUR 10 000 annually.

Hamburg

Annual external training costs are estimated at approximately EUR 15 000. The total annual budget averages around EUR 180 000.

Hessen

About EUR 15 000 is spent each year on conferences organised by Hessen's Judicial Academy.

Lower Saxony

Approximately EUR 10 000 (public prosecutor training provision).

Rhineland-Palatinate

Approximately EUR 10 000 annually (for police training measures).

Thuringia

About EUR 20 000 in 2013 and about EUR 36 000 in 2014.

In principle, the courses offered by the Federal Criminal Police Office are open to all police officers and employees who need such training. This can include colleagues who are explicitly involved in international cooperation.

The following information was reported with regard to the *Bundesländer*:

Berlin

Three members of staff of the *Land* Criminal Police Office (LKA) 33 attended seminars at EU level. The seminars were held in Ryton, UK and were entitled: 'Advanced network investigators' course'. These one-week courses were funded by the EU.

These seminars always have two primary objectives:

1. Networking (exchange of information at investigator level, establishing contacts, etc.).
2. Technical (content-based) training. The subject of the seminar was 'Internet investigations for advanced users'.

When a specific issue arises, the same members of staff also carry out tasks related to international cooperation. Refresher courses are not currently provided.

Brandenburg

The seminars provided at the *Land* Police Academy (FHPol) are aimed at target groups with different areas of responsibility. No distinction is made between international and national cooperation.

In both 2013 and 2014, the Joint Judicial Examination Office of Berlin and Brandenburg held a one-day training session on 'International legal assistance in criminal matters'. Part of this training session dealt with the cooperation with Europol and OLAF, one of whose tasks is to take action against cross-border computer crime.

Saarland

In Saarland, basic cybercrime training ('first responder training') is provided.

Hamburg

There is no mandatory cybercrime training for members of staff who carry out tasks related to mutual legal assistance in the Hamburg police force. If specific issues arise, experts from the cybercrime unit are available for advice.

The nationwide training courses provided by the German Judicial Academy in the area of international legal assistance are available to the public prosecutor's office in Hamburg. These sessions, usually lasting one week, are available on various topics within the area of international legal assistance (including in relation to cybercrime), and some provide detailed content.

Lower Saxony

Cybercrime training is largely open to participants active in international cooperation. It must be taken into account that the central units organise their mutual legal assistance measures independently, and thus serve a dual function, at least as regards case-related outgoing mutual legal assistance. No specific cybercrime training aimed exclusively at mutual legal assistance specialists was known to be available, and there were no plans to provide any. However, the Central Unit for Crime and Corruption (ZOK) and the EJN also help to organise special training courses for mutual legal assistance units, so if a particular need arises, certain topics can be included.

Saxony

No specific cybercrime training measures are provided for the senior desk officers who carry out tasks related to international cooperation.

Saxony-Anhalt

The conference on 'Manifestations of cybercrime and the fight against it', described above, with its thematic focus on issues such as jurisdiction and international legal assistance, is also aimed at those who carry out tasks related to international cooperation. The same applies to the aforementioned lecture on 'Identification of perpetrators and victims in child pornographic media - including in the context of international cooperation', held as part of the training course 'Current developments in criminalistics and the criminal justice system'. The training course 'Criminal law and the internet' includes the topic 'International investigations in ICT cases', aimed at those who carry out tasks related to international cooperation.

Saarland's point of view is that cooperation with centres of excellence plays an important role in the training of specialist cybercrime and forensic officers. Structured cooperation with these centres is being established as part of the ZAC function within Unit LPP 222 (e.g. with Saarland University, the German Research Centre for Artificial Intelligence (DFKI), and the University of Applied Sciences, Berlin (HTW)).

Universities are playing an increasingly important role in cybercrime education and training. The Federal Criminal Police Office (BKA) works closely with various universities. It is in contact with nine universities altogether, through the network of higher education institutions cooperating in the OpenC³S project. Within the expert training course on forensic ICT, the specialisation level is taught entirely by universities; the specialisation level for Windows, Linux, Macintosh, networks/internet and mobile forensics is taught by the University of Albstadt-Sigmaringen, and the specialisation level for cryptology is taught in close cooperation with the Ruhr University in Bochum.

The current Bachelor's degree course at the Federal University of Applied Administrative Sciences - Departmental Branch of the Federal Criminal Police incorporates a module entitled 'Crime in connection with information and communication media'. It is a four-week module and includes a technical introduction to basic information technology. External lecturers teach the basic concepts and the functioning of the internet. The phenomenon of cybercrime is also assessed from a criminological and criminal justice perspective and students are introduced to criminological and specific legal intervention instruments relating to the phenomenon. A scenario-based exercise at the end of the course allows students to consolidate the taught content with the help of practitioners in a fictitious situation.

The following (non-exhaustive) information has been reported with regard to the *Bundesländer*:

Baden-Württemberg

As part of the police reform, the whole area of education, higher education and further education was centralised under the umbrella of the Police Training College (HfPol). The aim was to provide and coordinate all education services in sufficient quality and quantity from a single source. Given its sole responsibility for all police training in Baden-Württemberg, the HfPol also plays a key role in cybercrime education and training. An individual cybercrime division (IB Cybercrime) was established for this field within the training institute.

In parallel to education and training, a specialist career option in cyber-criminalistics was introduced in 2014, which qualifies career changers from the IT industry to work as senior police officers. The training of these officers for their future deployment at level 3 is organised by the IB Cybercrime.

In addition, lecturers from the HfPol BW were to spend part of a research semester the following summer examining the feasibility of establishing a parallel degree course at their institution with a focus on cybercrime.

Brandenburg

The topic of cybercrime will supplement existing subjects such as criminology, criminalistics (forensics) and criminal law within the training programmes and Bachelor's degree course at the FHPol. The topic is also taught as part of the e-learning application. Students can additionally select the three-week ICT crime module option, which deals with computer crimes and the prosecution of internet crimes, to further familiarise themselves with all the different forms of cybercrime.

Mecklenburg-Western Pomerania:

Unit 45 of the Mecklenburg-Western Pomerania LKA works closely with the University in Wismar on the basis of a cooperation agreement. Two e-learning videos, entitled 'Reading email headers' and 'Investigating in social networks' have already been produced. Students from the University of Wismar, mostly IT students, have completed internships at the Mecklenburg-Western Pomerania LKA. Furthermore, staff at the Mecklenburg-Western Pomerania LKA have helped students to choose a topic for their Bachelor's or Master's thesis and supported them during their work on it.

In the winter term 2014, the University of Wismar introduced a part-time forensic engineering degree course, which includes modules on cybercrime.

Lower Saxony

A framework cooperation agreement between the Lower Saxony *Land* police headquarters and the University of Emden/Leer is soon to be signed, providing for cooperation in the areas of cybersecurity and the fight against cybercrime through specific training, research and teaching projects. In addition to reciprocal work shadowing, common research projects and participation in each other's training activities, the introduction of special part-time degree courses for police officers on cybercrime and cybersecurity at the University of Emden/Leer is under consideration.

Saarland

The German Police University (DHPol) provides such training for senior police officers. Saarland University has established a new cybersecurity degree course.

Saxony-Anhalt

The degree programme at the Police Academy includes 20 hours of instruction on cybercrime as a compulsory subject at the end of the course. The students learn:

- to describe the current situation and manifestations of crime in connection with ICT;
- to apply the relevant punishable offences (in particular Section 148 of the Telecommunications Act and Sections 202a et seq. of the Criminal Code);
- how to carry out the necessary police measures as a first responder at a crime scene and when filing a report in connection with the above-mentioned forms of crime.

Furthermore, cybercrime is also offered as a module at the end of the course. This involves four hours of instruction and covers current forms of internet crime and relevant cross-border cooperation. Of note in this respect are: the European Convention on Cybercrime, botnets used in DoS/DDoS attacks, and Trojans. The topics mentioned are part of the optional module entitled 'International crime control'.

Hamburg

The University of Applied Sciences within the Hamburg Police Academy is responsible for the initial training of police officers in Hamburg in the area of cybercrime. Forms of computer crime and related basic principles have been an integral part of the curriculum of the University of Applied Sciences (or its predecessor, the Hamburg Police University) since 2007.
In the module 'Introduction to information and communication technology', taught in the foundation year of the course, students learn the following:
• the architecture of computer systems and computer networks;
• technologies and the most important internet protocols;
• basic principles of IT security and security risks;
• data systems used by the Hamburg police and the federal government.

Building on this knowledge, the module 'Computer crime' in the main study phase provides students with the following skills:

• evaluation of crimes in connection with electronic data processing;

• evaluation of electronic data as evidence;

• knowledge of the principles of backups and the handling of backed-up data as well as of the relevant supporting services within the Hamburg police.

The module essentially comprises the following topics:

• offences pertaining to ICT and the use of the internet;

• law enforcement on the internet: basic technical principles;

• back-up and analysis of data carriers, network data and network traces;

• the computer as an instrument of law enforcement.

Both modules have a teaching time of 165 hours. These key skills are taught on an interdisciplinary basis by the Faculties of Applied Computer Science and Law. In addition, there is a high level of cooperation with the Hamburg LKA, in order to document new forms of computer crime and include them in the teaching and research programmes.

In 2013, in cooperation with the Hamburg Police Academy (previously University) and the Justice and Equality Authority, Hamburg University organised a symposium on cybercrime at which topics discussed by experts and students included aspects of this area of crime, the relevant criminal offences in the German Criminal Code and the investigative methods of the law enforcement authorities.

Saxony

The University of Applied Sciences Mittweida in Saxony is the only one in Germany to offer a degree in General and Digital Forensics. It provides IT experts with specific training in computer forensics. The degree course equips them with forensic knowledge for practical use in both public authorities and private companies. The focus is on computer forensics and the related specialised fields, which range from cryptology to criminology. The knowledge and skills that students acquire can also be put to use in combating cybercrime.

Thuringia

A number of German universities offer training in the field of IT forensics. The national expert training programme is developing specialised modules in partnership with universities (Bochum, Albstadt-Sigmaringen). In 2006, on the initiative of Unit 43 of the Thuringia Criminal Police Office (LKA), a foundation course in cryptography was developed in collaboration with Ilmenau Technical University. In the past the course was run several times at the Thuringia Police Training Centre in Meiningen with numerous participants from different *Länder*.

Unit 64 of the Thuringia Criminal Police Office held a seminar at the University of Public Administration - Police on combating child and youth pornography.

Cybercrime within the competence of the Thuringia Ministry for Education, Science and Culture is defined as follows: a wide range of criminal activities where computers and information systems are either the main instrument or the main target, comprising traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. online distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).

Broadly speaking, the universities in Thuringia do not offer special courses on cybercrime as defined above. The subject is nonetheless well covered in a wide range of courses, in particular the topics of IT and network security, e.g. fundamental principles, risks, attack mechanisms and cryptographic procedures for securing interconnected IT systems.
At the Bauhaus University in Weimar, for example, researchers are focusing on media security and on content management and web technologies.

8.2. Awareness-raising

On account of Germany's federal structure, nationwide police prevention work is not developed and implemented by a national central authority, but in ongoing collaboration between national and *Länder* police. In this context it is worth mentioning the *Länder* and Federal Police Crime Prevention (ProPK) programme, whose prevention activities in the field of cybercrime are described below.

The programme seeks to give the general public, multipliers, the media and other prevention bodies information on the forms of crime and on ways to prevent it. It achieves this inter alia through press and public relations work on crime prevention, and by developing and publishing media, initiatives and policies to back up the prevention activities carried out by local police departments and other institutions such as schools.

On the subject of cybercrime/media security, the ProPK has launched the following initiatives, and has produced/published and distributed throughout Germany the following media:

- Guide – 'In the network of new media':
  This is a comprehensive guide to media literacy among children and young people.
  It conveys a basic knowledge of the subject, and also deals with cyber-bullying. In addition, it provides references to selected materials and information sources for further reading. The guide is aimed at multipliers, and has recently been revised and updated.

- Leaflet series – 'Click moments':
  This pack contains seven leaflets, each dealing with a specific aspect of modern electronic media security, as well as internet risks. Each leaflet begins with a concise explanation of the topic. It then gives tips, which even less advanced users can follow. Extracts from legislation have also been included to highlight the link between some of the contents and criminal law. The individual topics covered are: social networks, identity theft and phishing, personality rights and copyright on the internet, internet fraud, malware and botnets, banned contents on the internet, smartphones and tablets.
- Short film – 'Chat, but keep it safe!':
  This video gives children rules for safe online chatting. The professional footballer Bastian Schweinsteiger features in the film with rules for safe chatting. See www.kinder-sicher-im-netz.de.
- Short film – 'Surf, but keep it safe!'
  This video is another element of the 'Children safe on the net' campaign. The TV presenter Rudi Cerne gives parents tips on how to protect their children from the dangers of the internet. Both films are available on DVD for use on-the-spot and also as internet content.
- 'Internet shopping - the sensible way!' website (www.kaufenmitverstand.de):
  This website is the virtual platform of the 'Internet shopping - the sensible way!' campaign. The campaign is jointly sponsored by ProPK, the online marketplace eBay and the Federal Association of German Mail Order Traders. The aim of the campaign is to protect people from fraudulent internet purchases by providing them with simple rules and information. It puts forward 'seven golden rules' and explains them in detail. An information card on 'Internet shopping - the sensible way!' (called a 'safety card') with the seven golden rules can be downloaded from the website. In addition, the website features a quiz, campaigns and novelties, as well as a press section on this topic.

- Security compass for a secure PC (http://www.polizei-beratung.de/themen-undtipps/gefahren-im-internet/sicherheitskompass.html):
  This website lists the top ten rules for increasing internet security. It uses the image of a compass to convey the message. Depending on where they place the needle of the compass, users can choose between ten different topics with the corresponding security tips. These are: 1. secure passwords; 2. co-users; 3. software updates; 4. firewall; 5. emails and attachments; 6. browser security; 7. downloads; 8. radio networks; 9. personal data; and 10. hardware.
- Leaflet – 'All about the law':
  This leaflet, published jointly by the ProPK, eBay and the Federal Association of German Mail Order Traders, has tips for buyers who have ordered items over the internet, but have either not received them, or have received items which do not meet the terms of the contract. It sets out possible courses of action and explains the buyer's rights in three different situations: (a) if the item was paid for but not delivered; (b) if the item has gone missing or been damaged during dispatch; (c) if the delivered item is faulty. Besides providing information on individual legal matters, the leaflet also lists internet addresses for further information.
- Comic-style booklet – 'Hey - that's enough'
  This booklet depicts children's day-to-day experiences in a child-friendly way, dealing especially with violence, bullying, blackmail, property damage and online chatting, and gives them rules on how to behave in these situations. It is aimed at primary schools.
- Leaflet – '...and you're the one talking about respect and dignity':
  This comic is an initiative in collaboration with handysektor.de to enhance media literacy. It provides a vivid depiction of the damage that can be caused by circulating offensive contents about people by internet, mobile phone or social networks. It is aimed at children and young people.

- Leaflet – 'The internet never forgets':
  This flyer also forms part of the collaboration with handysektor.de. A comic story explains why people should disclose an absolute minimum of personal information about themselves and others on the internet. It is aimed at children and young people.
- Leaflet aimed at victims – 'Victim, slut, son of a bitch - against bullying':
  This comic, also published in collaboration with handysektor.de, tells a story about cyber-bullying. It explains the functions of smartphones and shows how mobile connections with the social networks can be used as cyber-bullying tools. It also - and this is the main message - urges victims not to give in to bullying. Victims of cyber-bullying can and should seek the help of others. It is aimed at children and young people.
- Leaflet – 'Apps to go':
  This leaflet, which was developed in collaboration with handysektor.de, contains tips on how to use apps on smartphones and tablets securely. It sets out the basic rules on using apps in an age-appropriate way. The leaflet provides information on hidden costs, advertising, protective software, access rights and operating system settings.
- Media pack – 'Net attack':
  This media pack consists of a DVD and an accompanying booklet. It was developed for use in schools. It also has materials for downloading (workshop module). The film, taken from the krimi.de series, deals explicitly with cyber-bullying. It shows that cyber-bullying is not only morally reprehensible, but also illegal, as it may qualify as libel, slander or defamation, with corresponding consequences under criminal law. The media pack is out of stock. The film is available on the video platform YouTube, and the accompanying booklet can be downloaded (source: http://www.youtube.com/watch?v=aHMgcmYuz2M.). It is aimed at children and young people.

- Media pack – 'Misclicked!':

  The 'Misclicked!' media pack was published in March 2014. It comprises a film approximately 50 minutes in length which is aimed at children and young persons aged 12 years and up and seeks to raise their security awareness in their everyday digital world. The educational booklet that goes with the film allows teachers, or any other education professionals, to take an in-depth look through discussions and project work at the various issues arising from the use of digital media, which are presented in the three-part film. The contents of the booklet are based on the events depicted in the film. The topics covered are: cyber-bullying, illegal downloads, hidden costs, personality rights and copyright. Further topics include conduct on social networks, contents that are harmful to minors and password security.

- Information sheet – 'Violent videos on schoolchildren's mobile phones':

  This information sheet deals with illegal content on schoolchildren's mobile phones. In particular, the offences include the use of an integrated digital camera to take pictures or make videos, possession of illegal visual material such as pornographic images/films or violence, and distribution of stored illegal content. In addition, the information sheet gives advice to parents whose children use mobile phones on what to look out for and what line to take with their children. The leaflet also provides advice for schools and teachers, and lists websites with further information.

- Information sheet – 'Facilitators are abusing online carpooling agencies':

  The information sheet entitled 'Facilitators are abusing online carpooling agencies' describes how facilitators are using these agencies to transport people in circumvention of the laws on entry into the European Union. If unsuspecting drivers transport facilitated individuals, they will, if subjected to checks, quickly be suspected of belonging to smuggling rings. This could lead to their being arrested and questioned, and to lengthy criminal proceedings.

- Information sheet on hardware security:
  This information sheet provides tips on protecting high-quality hardware (laptops, computer parts and accessories) used by authorities, institutions and companies from theft and unauthorised use. In addition to advice on prevention, there are also recommendations on what to do in the event of theft.
- Internet portal – 'time4teen' (www.time4teen.de):
  This site is specifically targeted at young people. It contains information about a wide range of criminal acts, including child abuse, bullying and sexual violence. Under the heading 'Rules for the game of life', the site provides information about legal and illegal conduct with regard to such things as weapons, extremism, computers/internet and mobile phones. There is also legal information on the consequences of a criminal act, information about the police, details of the help that is available to young people, and games and quizzes. In the 'kids' world' section, younger children can learn about security in a fun way. There is an interactive educational game, which deals with everyday risks and tests children's knowledge of them. There is also a section on news and events and a section containing services and further information.
- www.polizei-beratung.de

In addition, ProPK provides comprehensive information and tips on its central website under http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet.html. For many years, ProPK's website content has been a cornerstone of public crime prevention. It provides the general public with information on the forms of crime as well as tips on protection. The content is regularly updated. Information was recently added on new forms of crime, such as 'romance scamming', a variant of the so-called Nigeria Connection advance payment fraud, which uses online dating pages and social networks, and on financial agents.

The information was completely revised in 2010 and made available at the beginning of 2011. A clear structure and user-friendly navigation menu now provide a rapid overview of the range of topics. There is also extensive information on the safe use of 'new media' and on internet crime. The information, which is intended to educate the general public and raise awareness, deals with content-related risks (extremism, pornography/child pornography, violence, fraud, etc.), communication risks (cyber-grooming, cyber-bullying, identify theft) and technical risks (hardware security, viruses, worms, trojans, etc.).

As mentioned in connection with the individual initiatives, the private sector is involved. No national or international funds were used. The *Länder* organise some prevention activities in addition to those coordinated by the ProPK at national level.

In order to prevent the various forms of cybercrime and risks associated with the internet and digital media, a large number of wide-ranging projects and initiatives are run by various bodies at local, regional, *Land* and national level. Additional players at national level include: the Federal Office for Information Security (www.bsi.bund.de); the Federal Ministry of the Interior and its 'A secure Germany on the net' initiative (www.sicher-im-netz.de/); the Federal Ministry for Family Affairs, Senior Citizens and Youth and its various initiatives, including jugendschutz.net(www.jugendschutz.net); the Centre for Child Protection on the Internet (www.i-kiz.de/) and its initiative entitled 'Look what your child's doing with media!' (www.bmfsfj.de/BMFSFJ/kinder-und-jugend,did=6212.html); the Commission for the Protection of Minors in the Media (KJM) of the *Land* media authorities (www.kjmonline.de/); Klicksafe (based at the *Land* Authority for Media and Communication of Rhineland-Palatinate; http://www.klicksafe.de/); the Digital Opportunities Foundation; and the aforementioned Police Crime Prevention Programme (ProPK; www.polizei-beratung.de) at *Land* and federal level.

A large number of awareness-raising initiatives are also carried out in schools, as the teaching environment is the best place in which to systematically reach out to children and young people. The materials used are in part those produced by the ProPK. Generally speaking, most of the materials developed by the ProPK (see 10.C.1) are also suitable for use in school or are designed for that purpose, one example being the 'Misclicked!' media pack.

The following information was reported with regard to the *Länder*:

Lower Saxony

In cooperation with the Lower Saxony school authority and external partners, two specific programmes were run to increase media literacy in schools. They were initiated and supported by the *Land* police. The 'comPass - I know my way round the net' programme and the 'cyber-licence - media driving licence' programme allow schools to support the further development of media literacy. In these programmes, teachers play the part of mediators/multipliers. The 'comPass' programme is also targeted at adults working in adult education. In addition, some regional police puppet theatre groups dealing with prevention have staged puppet shows on media security for third- and fourth-year pupils at primary schools within their areas of responsibility.

Schleswig-Holstein

In collaboration with the Schleswig-Holstein Institute for Quality Assurance in Schools, the Independent Centre for Data Protection of the *Land* of Schleswig-Holstein and the Consumer Centres, the *Land* police organise a 'media day' in schools on request, which is entitled 'Media are catching on'. Specially trained prevention officials are responsible for giving classes on crime prevention. Complementing the work done in class, the police can run sessions at the request of schools for all seven primary classes to raise children's awareness of the rules and to give advice on safe behaviour for witnesses and victims of crime.

8.3. Prevention

8.3.1. National legislation/policy and other measures

In accordance with its mandate, the Criminological Institute (*Kriminalistisches Institut*; KI Department) of the BKA deals in particular with the criminal and criminological aspects of cybercrime offences; however, for reasons relating to competence it does not have the leading role in strategic issues relating to cybercrime prevention in Germany.

This is the responsibility of the *Länder*. According to the information supplied by the *Länder*, this does not give rise to specific rules for prevention in the field of cybercrime. There is a national cybersecurity strategy and national organisations to prevent cybercrime.

The Federal Office for Information Security (BSI) is responsible for formulating standards to protect federal authorities.

The following information – not intended to be exhaustive – was received from the *Länder*:

Baden-Württemberg

Participation in events by police personnel working in the field of crime prevention is organised in a targeted way so as to reach the widest possible range of people, to raise awareness about cybercrime by means of presentations and the provision of advice and information, thereby preventing crime.

Brandenburg

In 2013, the police's preventive efforts in connection with cybercrime/new media referred to under 5.A.5 were aimed in particular at children and young people in primary and lower secondary education. The aim is to enable them to develop appropriate and prudent media use by providing them with information on the potential risks posed by internet and new media use and the legal framework in terms of administrative and criminal law (e.g. copyright), as well as making them aware of appropriate behaviour to avoid becoming a victim.

Events focused on the same subject are also held for adults, parents and teachers to familiarise them with the subject, enable them to develop a security-aware and responsible approach to the internet and new media, and enlist their help as multipliers. In addition, parents and teachers are made aware of how to manage children's and young people's media use, what action is recommended to enhance children's and young people's media literacy, and how to give the appropriate support. Supporting material such as brochures and media supplied by the *Länder* and the Federal Police Crime Prevention Programme (*Programm Polizeiliche Kriminalprävention der Länder und des Bundes*, ProPK), for example the content of 'Preventing abuse', are used within the framework of these prevention events. Reference is also made to internet sites such as 'www.fragfinn.de' ('ask Finn') and 'www.bsi-fuer-buerger.de' (the BSI for citizens) as sources of further information. The University of Applied Sciences of the Brandenburg Police (*Fachhochschule der Polizei des Landes Brandenburg*, FHPol) focuses as much as it can on aspects of teaching media literacy, providing information about crime and its risks, and on the importance of police work and police presence on social media. Apart from contributing a large number of specialist presentations at conferences, for other police authorities and directly in schools and youth facilities, the focus of activities is in particular on academic research into the criminological significance of the risks posed by interaction and communication in the digital environment. The FHPol is also currently involved in two research projects in this field. The international research project 'Hate Communities: A Cross-National Comparison' is aimed at collecting empirical data on the structures, motives and phenomenology of hate crime on the internet. The use of social media by the police is the main focus of the EU research project 'Solving Crime through Social Media' (SOMEP).

Saarland

The *Land* police headquarters, and specifically Unit LPP 246 – police crime prevention and victim protection – is responsible primarily for increasing media literacy. The unit is also responsible for giving technical advice concerning storage and the sealing of hardware such as laptops, desktop computers, components and accessories.

Increasing media literacy is based on three pillars:

- the approaches and media of the *Länder* and Federal Police Crime Prevention Programme (ProPK)
- media literacy working group
- advice given by Unit LPP 246.

(Unit LPP 246 gives advice on this subject to citizens, schools and other institutions on a case-by-case basis on request, distributes ProPK media and is available to give interviews to the press, radio and television broadcasters. The unit also give its own ad hoc presentations on the issue of 'the dangers of the internet/media literacy', especially following incidents in schools.)

Thuringia

Since 2009 the Thuringian police have been participating in the multiplier training that takes place across Thuringia entitled 'Media protection for young people on the internet', which is aimed at teachers and youth workers. This targeted preventive measure aimed at combating violence on the internet is divided into basic and advanced training and has been attended by police officers from the various regions of Thuringia, who act as multipliers.

8.3.2. Public-private partnership (PPP)

In 2013, representatives of a number of banks (ING-DiBa, Commerzbank and Hypovereinsbank) set up the German Competence Centre against Cybercrime (G4C) association. The BKA has entered into an agreement with this association concerning cooperation in the field of cybercrime. The cooperation is focused on optimising protection from cybercrime. The association is a new type of operational centre in which representatives from the private sector work together with the BKA to develop measures to protect against cybercrime and to devise solutions to current and future issues in the field of cybercrime.

Baden-Württemberg

Cooperation between the private sector, academia and the public sector has now been considerably intensified. Below are some examples of cooperation in which Baden-Württemberg LKA is involved:

- Cybercrime Security Cooperation (involving Baden-Württemberg LKA, North Rhine-Westphalia LKA, Saxony LKA and Lower Saxony LKA, as well as the Bitkom Association);
- the Alliance for Cybersecurity in Baden-Württemberg (involving the Baden-Württemberg Ministry for Internal Affairs, the Baden-Württemberg LKA, the Baden-Württemberg Office for the Protection of the Constitution, the IT Centre of Baden-Württemberg *Land* Administration, the Ministry for Science, Research and the Arts, and the Ministry for Finance and Economics);
- the Alliance for Cybersecurity in Germany (involving the Federal Office for Information Security (BSI), the Bitkom Association, and the Baden-Württemberg LKA), the cross-border cybercrime cooperation involving Baden-Württemberg, Bavaria, Austria and Switzerland;
- the German Competence Forum for Cybersecurity (involving Microsoft, HAS, the Bitkom Association, the Bavarian LKA, the Federal Police and the Baden-Württemberg LKA), among others.

Lower Saxony

Following the example of North-Rhine Westphalia LKA and Baden-Württemberg LKA, on 11 March 2014 Lower Saxony LKA became a member of the Cybercrime Security Cooperation with the Bitkom Association. The areas of cooperation include joint activities concerning exchange of information and knowledge transfer, mutual work shadowing, research into hidden areas of crime, development and implementation of preventive measures and helping to find the appropriate expert in individual cases.

Once a year a joint event is held at which the cooperation activities are presented, and workshops can be organised where there is a need. With a view to the adhesion of further partners, the Security Cooperation partnership is currently focusing its attention on drawing up rules of procedure. On 27 September 2009, the White IT Alliance was established by the Lower Saxony Minister for Internal Affairs and Sport with the aim of combating child pornography on the internet. Since then, 60 partners from industry, academia, trade associations and victim protection associations, as well as representatives of the healthcare professions, have joined the alliance to jointly promote activities aimed at combating child sexual abuse, with a particular focus on preventive aspects and the development of strategies and approaches to this end. In this context, White IT supports the 'Global Alliance against Child Sexual Abuse Online' initiated by the European Commission. Other initiatives relating to child pornography include regular symposiums in Lower Saxony, which are attended by both public law enforcement authorities and private enterprises.

8.4. Conclusions

- **The BKA has developed various initial and further training courses on cybercrime, including in the field of ICT forensics and nationwide multiplier training courses (training for trainers in the *Länder*).**

- **The German Judicial Academy offers seven conferences and training courses to judges and prosecutors on an annual basis.**

- **At *Land* level, there are different initiatives in the field of training. For example, North Rhine-Westphalia and Lower Saxony organise a joint training programme for specialists for both the police force, public prosecutors and judges. Although the level of participation of judges in these trainings is not particularly high (only 10%), this is considered by the evaluation team to be a very good practice.**

- **Awareness-raising efforts are also very well organised. A large variety of guides, leaflet, films, websites and information sheets have been made available to disseminate useful information to the public.**

- **The police has put together a booklet containing recommendations for the industry on how companies can protect themselves against cybercrime, what kind of information companies should register in view of possible cyber-attacks, etc. The booklet was disseminated in hard copy, for example at the annual BKA conference, and is also available to download from the internet.**

- **Basic courses are provided for any police officer in Germany (internet basics) and intermediate and advanced/specialised cybercrime training for cybercrime police officers are also provided. Training for court experts is also available.**

- **Furthermore, German police officers are involved in various training courses together with EUROPOL, INTERPOL, ECTEG, CEPOL, OLAF and Academia (network of nine German universities).**

- **Specialised cybercrime training is provided to prosecutors at *Land* level. Prosecutors are used to attending national and international training courses.**

- **There is no obligation for judges to attend training in cybercrime. However, training courses are available for judges. It is left to them to decide whether they wish to sign up for training courses.**

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Germany

Germany would propose the following improvements to help in fighting the cybercrime phenomenon:

• comprehensive initial training and further training for law enforcement authorities and the judiciary;
• recruitment of IT staff in the police;
• implementation of technical systems for handling big data.

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 Germany was able to satisfactorily review the system in Germany.

Germany should conduct a follow-up on the recommendations given in this report 18 months after the evaluation and report on the 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 German authorities. Furthermore, based on the various good practices, related recommendations to the EU, its institutions and agencies, particularly Europol, are also put forward.

9.2.1. Recommendations to Germany

8. Consider implementing additional and easy-to-use ways for transmitting information between police and prosecutors in the 16 *Länder* in a secure way (using encryption);

9. Consider further improving the exchange of best practices in the field of training of practitioners between the 16 *Länder*;

10. Consider ensuring that police and other law enforcement authorities participate in cyber-exercises organised by national institutions, such as BSI, in order to identify any possibilities for improvement of their working procedures;

11. Continue the promotion of the use of JITs, e.g. by further making information available to practitioners, notably prosecutors, about the possibilities and advantages of JITs;

12. Consider allowing comparisons of the hash-values of child sexual abuse material with material available in open sources;

6. Consider introducing specific instructions (guidelines) for assisting the online reporting of cyber-criminality, especially for small and medium enterprises.

7. Continue efforts to allow e-evidence to be presented in court proceedings in digital form;

8. Consider the possibility of aligning the format of statistics from the police and the prosecution services to allow them to be compared[9].

[9] Germany recalls that Article 14(2) of Directive 2013/40/EU specifically does not oblige Member States to expand their collection and evaluation of statistics.

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

9. Member States should ensure that information can be transmitted in a secure way (using encryption) between practitioners in the Member States, such as prosecutors and other law enforcement authorities, and the relevant European agencies;

10. Following the CJEU's judgement of 21 December 2016 (joined cases C-203/15 Tele2 Sverige AB v Post-ochtelestyrelsen and C-698/15 Secretary of State for Home Department v Tom Watson and Others), the European Union institutions should analyze the implications of the ruling and reflect on the most appropriate way to remedy problems regarding cooperation among member states in the context of electronics traffic data retention;

11. Consider replacing in future legislation the term 'child pornography' with 'child abuse material' or another appropriate term;

12. The European Commission should further explore the possibility of identifying solutions to legal challenges for cross-border data access.

The evaluation team considered it necessary to highlight certain of Germany's good practices observed during the evaluation visit, which could serve as a basis for other Member States:

- the existence of prosecutors and units specialised in the fight against cybercrime in many *Länder*;
- the possibility of establishing temporary task forces between police and prosecutors to fight cybercrime, which makes it possible for the same people to work on cases;
- experts' meetings on international cooperation at both federal and *Land* level;

- the involvement of various ministries in the fight against cybercrime, and the coordination of their efforts at an inter-ministerial cybercrime 'jour fixe', when all the relevant actors in the field of preventing and combating cybercrime gather to share and discuss issues of common interest in the matter;
- the existence of a central investigations register designed to identify overlapping investigations at an early stage;
- the existence of hotlines to denounce child pornography;
- the organisation by North Rhine-Westphalia of joint training sessions on cybercrime for prosecutors and judges, which can lead to common understanding and other benefits.
- the fact that very good care is taken of staff involved in the fight against child pornography, such as by offering psychological assistance;
- the extensive attention paid and support provided by the authorities to the protection of SMEs in the context of the fight against cybercrime;
- the establishment of the iPPP project;
- the good practice of taking down child pornography websites and, if that is not possible, placing the URLs on a blacklist which is communicated to interested persons and organisations, such as libraries;
- the possibility for private industry to report cybercrime online (and the existence of guidelines and points of contact in this respect);
- Germany's active participation at international level, such as through J-CAT, of which Germany holds the chairmanship since January 2016, Empact and the deployment of liaison officers to many countries;
- the increased allocation of resources to the fight against cybercrime;
- the extensive involvement of Eurojust by German judicial authorities in complex cross-border cases.

9.2.3. Recommendations to Eurojust/Europol/ENISA

1. The European Cybercrime Training and Education Group (ECTEG) should continue to offer and promote training on cybercrime for law enforcement authorities in the Member States.

2. Both Eurojust and Europol should consider ways to make JITs easier to set up, including by facilitating access to available funding to ensure their effectiveness for the Member States.

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT

Monday, 23 May 2016 **Arrival**	
During the day	Arrival of GENVAL Experts at Airport Berlin Tegel/ Berlin Schönefeld Hotel Titanic Comfort/ Arcotel John F.
Tuesday, 24 May 2016 **Federal Ministry of Justice and Consumer Protection (BMJV), Berlin** Room: Gustav-Radbruch-Saal (5.001)	
8:45 a.m. 9:15 a.m.	**<u>Federal Ministry of Justice and Consumer Protection</u>** • **Introductory remarks** • **Welcoming** of the Evaluation Team *by:* **Hans Georg Baumann**, Director General of the Criminal Law Directorate General in the Federal Ministry of Justice and Consumer Protection **Photo opportunity** with the Evaluation Team

9:30 a.m.	**Legal Aspects** 1. Criminalisation – 2.A. 2. Statistics (Justice) – 1 Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office
10:45 a.m.	**Coffee break**
11:00 a.m.	**Legal Aspects (continued)** 1. Procedural issues – 2.B. 2. Jurisdiction – 2.C Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office
12:45 a.m.	**Lunch** on invitation of the Federal Ministry of Justice and Consumer Protection
2:00 p.m.	**International cooperation** **- Tools:** • Mutual legal assistance – 7.A. • Mutual recognition – 7.B. Surrender/Extradition – 7.C. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Public Prosecutor's Office, Federal Office of Justice, Eurojust, Federal Criminal Police Office, Federal Office for Information Security (BSI)

	<u>International cooperation</u> **- partners** • Cooperation with EU Agencies – 8.A. • Participation in JITs/cyber-patrols – 8.B. Cooperation with third countries – 8.C. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Public Prosecutor's Office, Eurojust, Federal Criminal Police Office, Federal Office for Information Security
4:00 p.m.	**<u>Coffee Break</u>**
4:30 p.m.	**<u>Cooperation with the private sector</u>** – 9. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Ministry of Economic Affairs and Energy, Federal Criminal Police Office, Federal Office for Information Security, German Competence Center against Cyber Crime (G4C), Bitkom (digital industry association)
6:30 p.m.	**<u>Guided tour through the Federal Ministry of Justice and Consumer Protection</u>**
7:00 p.m.	**<u>Working Dinner on invitation of the Federal Ministry of Justice and Consumer Protection</u>** Restaurant Mark Brandenburg, Mohrenstr. 30

Wednesday, 25 May 2016 **Federal Ministry of Interior (BMI), Berlin** Federal Office for Information Security (BSI) Federal Criminal Police Office (BKA) Room: C.0.435 at the Conference Center (+ Lobby)	
9:00 a.m.	**Welcoming** of the Evaluation Team by Dr. Stefan Grosse, Head of Division, General issues concerning cybercrime, cyber espionage and cyber terrorism
9:15 a.m.	**National structures** • General Matters, Cyber Security Strategies, Statistics (police) – 1 • Judiciary (prosecution and court) – 3.A • Law enforcement authorities – 3.B. • Other authorities – 3.C. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office
10:30 a.m.	**Coffee break**
10:45 a.m.	**Offences related to child sexual abuse online and child pornography** • Specific questions related to the act/victim – 5.A. • Filtering/Blocking of access to/Removal of content/Take down of web pages containing or disseminating child pornography – 5.B. • International cooperation – 5.C. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Ministry for Family Affairs, Senior Citizens, Women and Youth, Federal Criminal Police Office

12:45 a.m.	**Lunch** on invitation of the Federal Ministry of the Interior Room: Conference Center, Lobby
2:00 p.m.	**Cyber attacks – 4.** • presentation of the BSI-situation report • regulations under the new IT Security Act, reporting obligations • CERT structures in Germany Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office, Federal Office for Information Security (BSI)
3:00 p.m.	**Online Card Fraud –** 6. Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office
4:00 p.m.	**Coffee Break**
4:15 p.m.	**Prevention of cybercrime, training and awareness raising activities** • Prevention – 10.A. • Training – 10.B. • Awareness Raising – 10.C Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Federal Criminal Police Office, Federal Office for Information Security

5:30 p.m.	**Visit of the Tränenpalast ("Palace of the Tears" - former border crossing between "East und West" at Berlin Friedrichstraße train station)** • Guided Tour
7:00 p.m.	**Dinner on invitation of the Federal Ministry of Interior** Restaurant Zollpackhof
Thursday, 26 May 2016, Berlin **General Public Prosecution Office, Celle** Central Office Organised Crime and Corruption (ZOK)	
08:00 a.m.	**Transfer to Celle** Meeting point: in front of the hotel Titanic Comfort
11:30 a.m.	**Visit of the Central Office Organised Crime and Corruption** (Zentrale Stelle Organisierte Kriminalität und Korruption – ZOK) Participants: Federal Ministry of Justice and Consumer Protection, Federal Ministry of the Interior, Public Prosecutor's Central Offices for the Prosecution of Cybercrime of Celle, Verden, Berlin, Cologne and Bamberg, Police Officer of Lüneburg
4:00 p.m.	**Transfer to Berlin**
6:00 p.m.	Evening at free disposal

Friday, 27 May 2016 **Federal Ministry of Justice and Consumer Protection (BMJV), Berlin** **Gustav-Radbruch-Saal (5.001)**	
9:00 a.m.	**Wrap-up-session** • General observations • final remarks
12:00 am	Close of the meeting

ANNEX B: PERSONS INTERVIEWED/MET

Venue: Federal Ministry of Justice and Consumer Protection

Person interviewed/met	**Organisation represented**
OStA beim BGH Markus Busch	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
RD Dr. Garonne Bezjak	Federal Ministry of Justice and Consumer Protection
OStA Dr. Michael Sommerfeld	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of the Interior
N.N.	Federal Ministry of the Interior
N.N.	Federal Criminal Police Office

Venue: Federal Ministry of Justice and Consumer Protection

Person interviewed/met	**Organisation represented**
OStA beim BGH Markus Busch	Federal Ministry of Justice and Consumer Protection
MR Dr. Katrin Brahms	Federal Ministry of Justice and Consumer Protection
OStA beim BGH Oliver Sabel	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
RiAG Michael Rothärmel	Federal Ministry of Justice and Consumer Protection
StA Christoph-Severin Haase	Federal Ministry of Justice and Consumer Protection

Frau Johanna Sprenger	Federal Ministry of Justice and Consumer Protection
Frau Kirsten Jakobs	Federal Ministry of Economic Affairs and Energy
N.N.	Federal Ministry of the Interior
N.N.	Federal Ministry of the Interior
N.N.	Federal Criminal Police Office

Meetings on

Venue: Federal Ministry of Justice and Consumer Protection

Person interviewed/met	**Organisation represented**
OStA beim BGH Markus Busch	Federal Ministry of Justice and Consumer Protection
MR Dr. Katrin Brahms	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
RiAG Michael Rothärmel	Federal Ministry of Justice and Consumer Protection
MDgt Klaus Meyer-Cabri	Eurojust
RD Dr. Holger Karitzky	Federal Office of Justice
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security
StA Christoph Lecher	General State Prosecutor

Venue: Federal Ministry of Justice and Consumer Protection

Person interviewed/met	Organisation represented
OStA beim BGH Markus Busch	Federal Ministry of Justice and Consumer Protection
RD Harald Schoen	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security
Frau Kirsten Jakobs	Federal Ministry of Economic Affairs and Energy
Rechtsanwalt Dr. Mark Ennulat	BITKOM e. V. (digital industry association)

Venue: Federal Ministry of Interior

Person interviewed/met	Organisation represented
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security

Meetings on

Venue: Federal Ministry of Interior

Person interviewed/met	Organisation represented
MR Dr. Eberhard Schollmeyer	Federal Ministry of Justice and Consumer Protection
Frau Karla Brambati	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Criminal Police Office
N.N.	Federal Criminal Police Office
N.N.	Federal Ministry for Family Affairs, Senior Citizens, Women and Youth
N.N.	Federal Ministry of Economic Affairs and Energy
N.N.	Federal Review Board for Media Harmful to Minors
N.N.	jugendschutz.net (NGO)

Venue: *Federal Ministry of Interior*

Person interviewed/met	Organisation represented
MR Dr. Eberhard Schollmeyer	Federal Ministry of Justice and Consumer Protection
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security

Venue: *Federal Ministry of Interior*

Person interviewed/met	Organisation represented
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security

Venue: *Federal Ministry of Interior*

Person interviewed/met	Organisation represented
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection
N.N.	Federal Ministry of Interior
N.N.	Federal Ministry of Interior
N.N.	Federal Criminal Police Office
N.N.	Federal Office for Information Security

Venue: *Central Office for Organised Crime and Corruption in Celle*

Person interviewed/met	**Organisation represented**
OStA Carsten Rosengarten	Central Office for Organised Crime and Corruption Crime in Celle
OStA Frank Lange	Public Prosecutor's Office in Verden
StA Markus Hartmann	Central Office for Cybercrime, Public Prosecutor's Office Cologne
StA Marcus Hartmann	Central Office for Cybercrime, Public Prosecutor's Office Berlin
OStA Lukas Knorr	Bavarian Central Office for the Prosecution of Cybercrime
KHK Jörn Bisping	Lüneburg Police Station
RiAG Nicole Fleischer	Federal Ministry of Justice and Consumer Protection

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	GERMANY OR ACRONYM IN ORIGINAL LANGUAGE	GERMANY OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
	BBK		Federal Office of Civil Protection and Disaster assistance
	BfJ		Federal Office of Justice
	BKA		Federal Criminal Police Office
	BMFSFJ		Federal Ministry for Family affairs, Senior Citizens, Women and Youth
	BMI		Federal Ministry of Interior
	BMJV		Federal Ministry of Justice and Consumer Protection
	BMWI		Federal Ministry of Economic Affairs and Energy
	BPjM		Federal review Board for Media Harmful to Minors
	BPol		Federal Police
	BSI		Federal Office for Information Security
CEPOL			European Police College
	CERT-Bund		Federal Computer Emergency Response Team
CSAM			Child Sexual Abuse Material

	Cyber-AZ		National Cyberdefense Centre
	DRV		German Travel Association
EC3			European Cybercrime Centre
ECTEG			European Cubercrime Training and Education Group
EJTN			European Judicial Training Network
ENISA			European Network and Information Security Agency
EWPITC			Interpol European Working Party on IT-Crime
	FHPol		Police Academy
	G4C		German Competence Centre against Cybercrime e.V.
	GenStA		General State Prosecutor
	GMLZ		Joint Information and Situation Centre
	iPPP		Institutionalised Public-Private Partnership
ISF			Internal Security Funds
	IT-KRZ		National IT Crises response Centre

J-CAT			Joint Cybercrime Action Task
	KKB		Fight against Cyber Crime Committee
	LKAs		Criminal Police Offices of the Länder
	PCS		Police Crime Statistics
	ProPK		Federal Police Crime Prevention
	RBE		Regional Evidence Collection Unit
	RiStBV		Guidelines for criminal and monetary fine proceedings
	SN4C		Cybercrime Competence Centre
	StPO		Code of Criminal Procedure
	ZAC, StA Koln		Central Office for Cybercrime, Public Prosecutor's Office Cologne
	ZCB		Bavarian Central Office for the Prosecution of Cybercrime
	ZKA		Customs Criminal Investigation Office
	ZKI		Police Station
	ZOK		Central Office for Organised Crime and Corruption Crime