Bundeskriminalamt

BKA

Cybercrime

National Situation Report 2017

Cybercrime - Figures 2017

85,960 cases of cybercrime in the narrower sense (+4 %)

251,617 cases of the Internet as an instrument of crime among all offences recorded in the national crime statistic (4.4 % of all offences recorded in the national crime statistic)

1,425 cases of phishing attacks concerning online banking (-34.5 %)

EUR 4,000/case average loss from phishing attacks concerning online banking (2016: EUR 4,000/case)

EUR 71.4 million losses in the area of computer fraud (2016: EUR 50.9 million)

Increase in mobile malware (+54 %)

17 OC groups in the field of cybercrime;
3 % of all OC investigations (2016: 22)

Table of Contents

1 Preliminary Remarks

The term cybercrime refers to all offences that are targeted against data networks, IT systems or their data (cybercrime in the narrower sense) or are committed by means of information technology.

The 2017 National Situation Report on Cybercrime provides information about the developments in the field of cybercrime in the narrower sense that have come to police notice. These include:

- **computer fraud as cybercrime in the narrower sense** (section 263a of the German Penal Code; breakdown into different types of fraud, cf. p. 4 f.)
- **other forms of computer fraud** (section 263a subsections 1 and 2 of the German Penal Code and preparatory acts pursuant to section 263a subsection 3 of the German Penal Code)
- **data espionage and interception of data including preparatory acts and handling stolen data** (sections 202a, 202b, 202c, 202d of the German Penal Code)
- **forgery of evidentiary data and/or deception in legal relations** (sections 269, 270 of the German Penal Code)
- **data manipulation/computer sabotage** (sections 303a, 303b of the German Penal Code)
- **misuse of telecommunications services** (section 263a of the German Penal Code)

The statistical part of the situation report is based on data retrieved from the Police Crime Statistics (PCS). The term **"police recorded crime"** refers to all criminal offences including punishable attempts which were handled by the police and handed over to a public prosecutor's office. Since the conditions for recording computer fraud offences had been changed before, the figures gathered from the year 2016 onward are comparable with those from previous years to a limited extent only. In addition, the statements made in the situation report on hand rely on information obtained through the exchange of criminal police information.

In view of the above-average number of cybercrime offences which go unreported and unrecorded (**dark field**), non-police sources of information are also consulted to ensure a profound assessment of the danger potential originating from cybercrime. These include studies conducted by research facilities or governmental bodies, such as the "Bundesamt für Sicherheit in der Informationstechnik" (BSI; Federal Office for Information Security), and by private associations and companies, such as developers of anti-virus software and IT security service providers.

Also, the existing co-operation between the Bundeskriminalamt (BKA) and the "German Competence Centre against Cyber Crime e.V." (G4C)[1] was used even more intensively this year to prepare this situation report. The information obtained in this manner supplements the data available on police recorded crime and thereby facilitates a qualitatively improved assessment of the situation.

[1] members of G4C: Commerzbank, ING-DiBa, Hypo-Vereinsbank, Kreditanstalt für Wiederaufbau, Schufa, Bank-Verlag, R+V, Symantec, Diebold-Nixdorf, Link11, G-Data; co-operation partners of G4C: BKA and BSI.

2 Presentation and Evaluation of the Crime Situation

2.1 CONDITIONS FOR RECORDING DATA IN THE POLICE CRIME STATISTICS (PCS)

When looking at the statistical data gathered by the police, the specific recording and counting conditions in the PCS must be taken into account.

Like the entire area of information technology, the phenomenon of cybercrime is characterised by a highly dynamic development. Therefore, the recording of the pertinent data in the PCS has been refined in the past years. Since 2014, cybercrime offences have only been incorporated in the PCS at national level if there is specific information suggesting that an offence was committed in Germany.

When evaluating case numbers, it must be borne in mind that any illegal act identified in the course of an investigation is recorded as only one case regardless of the number of aggrieved parties. The manipulation of the software of approximately 1.3 million DSL routers of a German internet provider by malware in November 2016, for instance, was only shown as one single case of computer sabotage in the PCS, although the number of aggrieved parties was in the seven-digit range.

Furthermore, when interpreting the statistical data it must be kept in mind that some relevant phenomena, such as acts of extortion committed in connection with targeted DDoS attacks or ransomware, are, for instance, usually not recorded as cybercrime offences in the PCS, but as more serious or specific offences - in this case as extortion - in accordance with the PCS guidelines. Only the special designation "internet as instrument of crime" introduced in the PCS in 2004 may permit to link such offences to cybercrime.

Despite the limited informative value the PCS has with regard to the entirety of cybercrime offences committed in Germany, it must be noted that this is the only collection of statistical data in Germany which is based on police investigations. Thus, it provides a high-quality data basis and at least facilitates trend statements in this area of crime.

Statements about the real level of crime cannot be made on the basis of the PCS alone, because the number of offences actually committed but not known to the police and thus not recorded is believed to be much higher. The reasons for this relate, on the one hand, to the recording conditions described above; on the other hand, the following aspects, some of which are specific to this field of criminal activity, point to a high number of unreported and unrecorded cybercrimes:

- since more and more security devices are installed, many criminal acts committed on the internet do not go beyond the attempt phase and are not noticed by the victims,
- the persons affected do not realize that they fell victim to an act of cybercrime (for instance in the case of identity theft by an online shop) or that the technical devices they use are misused for the commission of cybercrimes (for instance by use of infected PCs or routers as part of a botnet for the commission of DDoS attacks or infection with cryptomining malware),

- victims fail to report offences, particularly when no financial loss has been incurred (such as the mere detection of a virus on the PC) or the loss is adjusted by a third party (insurance company or the like),

- victims, particularly companies, fail to report identified offences in order to ensure, for instance, that they do not lose their reputation as a "safe and reliable partner" vis-à-vis their clients,

- frequently, victims only lodge complaints, e.g. in cases of extortion, if offenders fail to decrypt systems they encrypted before although a ransom has been paid.

The police keeps pointing out that victims should report any act of cybercrime, because this could not only lead to new investigative approaches for a more effective suppression (e.g. by analysing the attack convectors or detecting links between offences), but is also the only way to identify and punish offenders. The objective must be to identify the originators of cyberattacks and prevent further attacks. Sanctioning criminal conduct should also have a deterrent effect on potential offenders.

Cybercrime in the narrower sense comprises the following offences:

- **computer fraud as cybercrime in the narrower sense;** since 01/01/2016, this offence has been broken down into the following types of fraud:

    - fraudulent obtaining of motor vehicles pursuant to section 263a of the German Penal Code,

    - other types of credit fraud pursuant to section 263a of the German Penal Code,

    - fraud using unlawfully obtained payment card data pursuant to section 263a of the German Penal Code,

    - fraud using unlawfully obtained other non-cash means of payment pursuant to section 263a of the German Penal Code,

    - obtaining services by deception pursuant to section 263a of the German Penal Code,

    - accounting fraud in the health care sector pursuant to section 263a of the German Penal Code,

    - transfer fraud pursuant to section 263a of the German Penal Code,

- **other forms of computer fraud** pursuant to section 263a subsections 1 and 2 of the German Penal Code and preparatory acts pursuant to section 263a subsection 3 of the German Penal Code (unless included in the following types of fraud or the "misuse of telecommunications services"),

- **data espionage and interception of data including preparatory acts and handling stolen data** (sections 202a, 202b, 202c, 202 d of the German Penal Code) comprises the theft and handling of digital identities, credit card, e-commerce or account data (e.g. phishing). The stolen data are usually offered for sale as merchandise in the underground economy[2] and

[2] Multiregional black online markets, frequently in the darknet, used by sellers and buyers to initiate and carry out their criminal transactions throughout the digital world.

misused by offenders. Therefore, exploitation is a two-phase process: the sale of the data and the fraudulent use of purchased data. Significant profits are generated at both levels.

- The offences of **forgery of evidentiary data and/or deception in legal relations** (sections 269, 270 of the German Penal Code) include deception (of a person) by forgery of data. Data are forged or altered by their holder and used for deception in legal relations. This is done, for instance, by sending e-mails pretending that their originators are existing persons or companies. A cover identity is used to persuade the victims to disclose their account details or credit card data or to make payments. This category also includes the sending of malicious software camouflaged as invoices in e-mail attachments.

- **Data manipulation/computer sabotage** (sections 303a, 303b of the German Penal Code) is a kind of digital criminal damage. The punishable offence consists of the alteration of data in a data processing system or the alteration of the system by persons other than the data owner. Sections 303a, 303b of the German Penal Code typically include Denial of Service attacks (DoS/DDoS attacks[3]) as well as the distribution and use of various kinds of malware (Trojans, viruses, worms etc.).

The **misuse of telecommunications services** is a special and separately recorded form of computer fraud pursuant to section 263a of the German Penal Code. Offenders exploit vulnerabilities or weak access security features of companies and private homes, e.g. to access routers without authorisation and call expensive telephone numbers or systematically use premium or value added services.

[3] Denial of Service (DoS) attacks target the availability of services, websites, individual systems and entire networks. If such an attack is launched simultaneously by several systems, it is called a distributed DoS or a DDoS attack (DDoS = Distributed Denial of Service). DDoS attacks are frequently performed by a very high number of computers or servers forming a botnet.

2.2 CYBERCRIME – CASE NUMBERS

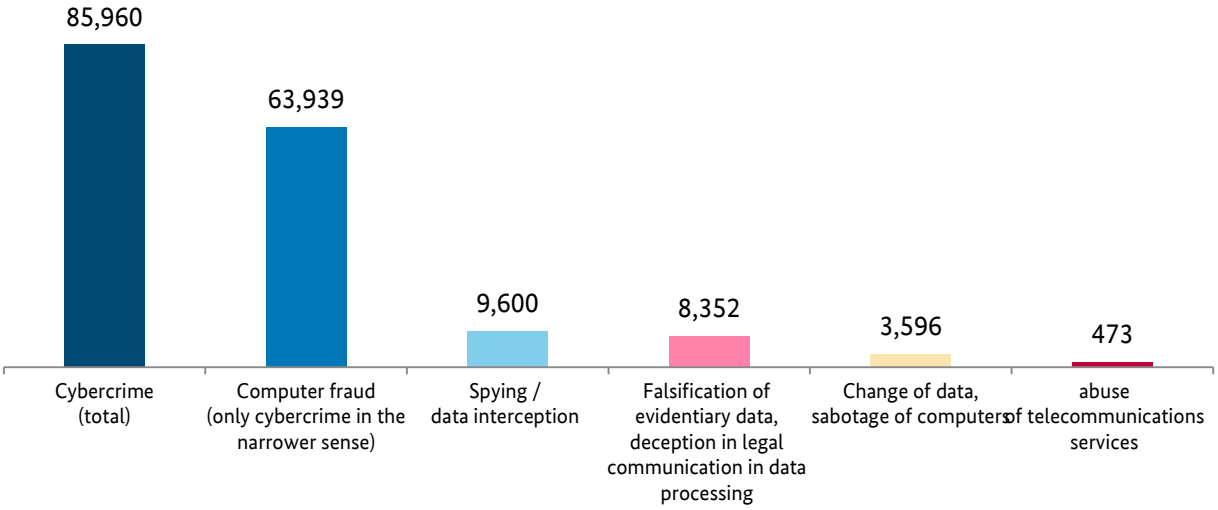
The year 2017 witnessed an increase in the number of offences attributed to cybercrime in the narrower sense. The PCS showed a total of 85,960 offences. This represented an increase of 4.0% compared to the previous year (2016: 82,649). The clear-up rate was 40.3%, which means that there was an increase of 1.6 percentage points compared to the previous year.

Three quarters of all offences were recorded as computer fraud cases.[4] The analysis of the 2016 PCS figures for cases of cybercrime in the narrower sense already showed that the increase in case numbers was accompanied by a relatively sharp increase in the area of computer fraud. In 2017, there was another increase of 9.1% in this field of criminal activity. Inquiries conducted in two major German Länder in 2017 revealed that most of the offences recorded under the relevant key numbers of computer fraud did not constitute cases of "cybercrime in the narrower sense". In most of these cases the internet was merely used as the instrument of crime. This is one of the reasons why the PCS case numbers require differential consideration and evaluation.

The number of cases attributed to the misuse of telecommunications services pursuant to section 263a of the German Penal Code decreased by 41.7%. The 2016 National Situation Report already referred to the modification of the PCS key numbers for recording these offences. The sharp decline in this field of criminal activity continued; only 473 cases in total were statistically recorded. This represents a share of less than one percent of all cybercrime cases.

[4] Since January 2016, the computer fraud types previously recorded as "other forms of computer fraud" pursuant to section 263a of the German Penal Code (PCS key 517500) have been broken down into the following subtypes to ensure a more nuanced representation: Other forms of computer fraud pursuant to section 263 subsections 1 and 2 (PCS key 517510) as well as preparatory acts pursuant to section 263a subsection 3 of the German Penal Code (PCS key 517520), fraudulent obtaining of motor vehicles pursuant to section 263a of the German Penal Code (PCS key 511120), other forms of credit fraud pursuant to section 263a of the German Penal Code (PCS key 512212), fraud using unlawfully obtained payment card data pursuant to section 263a of the German Penal Code (PCS key 516520), fraud using unlawfully obtained other non-cash means of payment pursuant to section 263a of the German Penal Code (PCS key 516920), obtaining services by deception pursuant to section 263a of the German Penal Code (PCS key 517220), accounting fraud in the health care sector pursuant to section 263a of the German Penal Code (PCS key 518112), transfer fraud pursuant to section 263a of the German Penal Code (PCS key 518302).

Number of Cases of Cybercrime in the Narrower Sense (2017)



In a study published in October 2017, the "Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V." (BITKOM, German Association for Information Technology, Telecommunications and New Media) reported that approximately every other internet user in Germany had become a victim of cybercrime. Only 18% of the victims had stated that they had lodged a complaint with the police or a public prosecutor's office.[5] If these figures are extrapolated to the population and the internet users, it becomes clear that the damage actually caused by cybercrime is probably much higher than stated in the PCS.

In 2017, BITKOM published another study dealing with the impact of cybercrime on commercial enterprises. In its report entitled "Protecting the Economy in the Digital World" the digital association explained that more than half of the companies in Germany (53%) had been victims of industrial espionage, sabotage or data theft in the past two years.[6]

Both studies clearly show that the inclusion of dark field information and other external sources is indispensable for a comprehensive assessment of the situation in the area of cybercrime.

[5] **Https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html.**
[6] **https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html.**

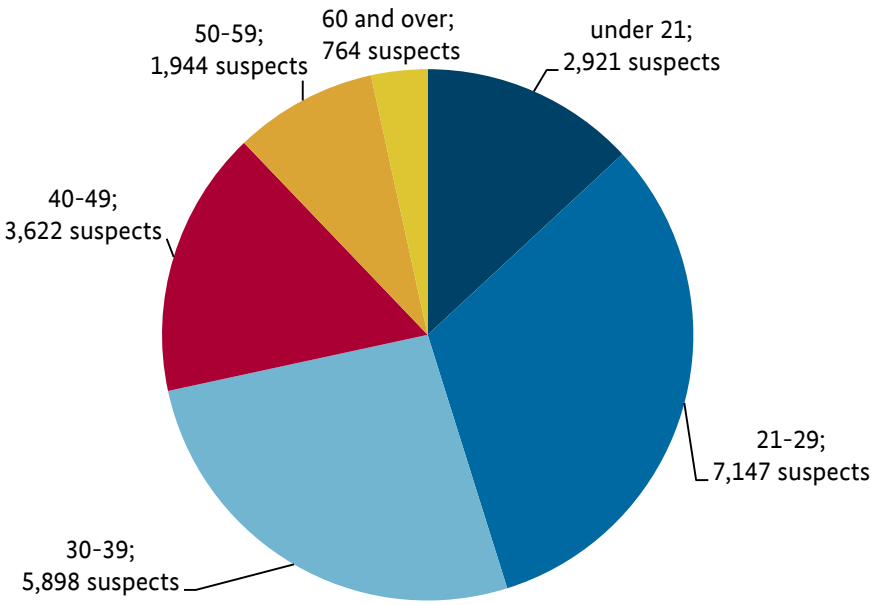
2.3 SUSPECTS

In 2017, a total of 22,296 individuals suspected of cybercrime were recorded (+ 6.6%; 2016: 20,920). 68.3% of all suspects were male, 31.7% were female.

17,131 identified suspects (76.8%) were German nationals. 5,165 suspects were non-German nationals; Turkish (14.0%), Romanian (9.9%) and Polish (6.4%) nationals were most heavily represented.

More than half (58.5%) of the recorded offences assigned to the field of cybercrime in the narrower sense were committed by suspects aged between 21 and 39 years.

Age Structure of Suspects (2017)



The spectrum of perpetrators ranges from lone offenders to internationally organised crime groups. Jointly acting offenders rarely operate in hierarchical structures to commit cybercrimes. Frequently, they do not know each other personally and use the supposed anonymity of the internet even when operating on a division-of-tasks basis.

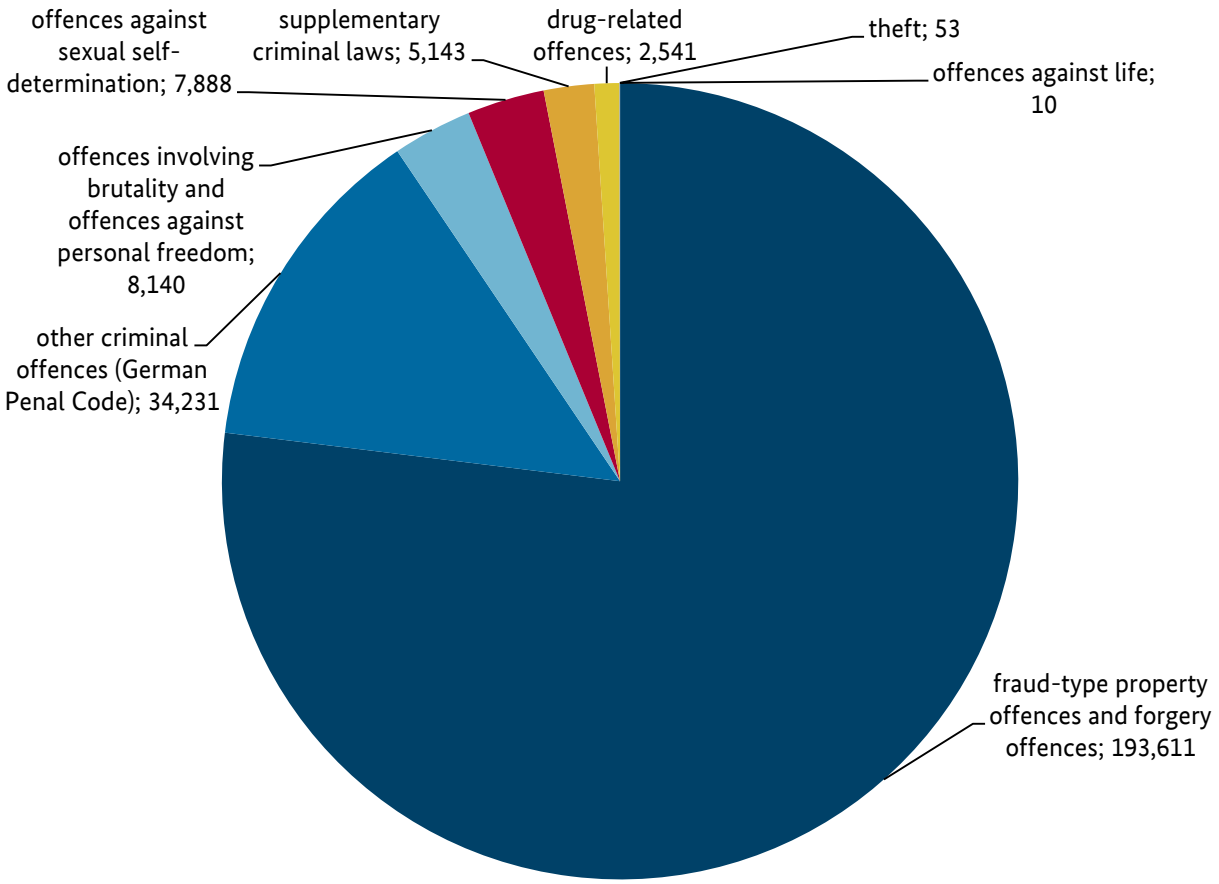
Offenders respond quickly and flexibly to new technical developments and adapt their approaches accordingly. Services they cannot provide are purchased from third parties (Cybercrime-as-a-Service).

Cybercrime is also of importance when it comes to combating organised crime. In 2017, 17 OC groups (total number of OC groups recorded in 2017: 572) were linked to the area of cybercrime (2016: 22). The offences they commit do not differ from those carried out by lone offenders or lose networks. OC groups commit typical cybercrimes, ranging from computer fraud and attacks on online banking to the distribution of ransomware for digital extortion.

2.4 THE INTERNET AS INSTRUMENT OF CRIME

In 2017, a total of 251,617 offences were recorded in the PCS, for which the internet had been used. This represents a decrease of 0,7 percent on the previous year (2016: 253,290 cases).

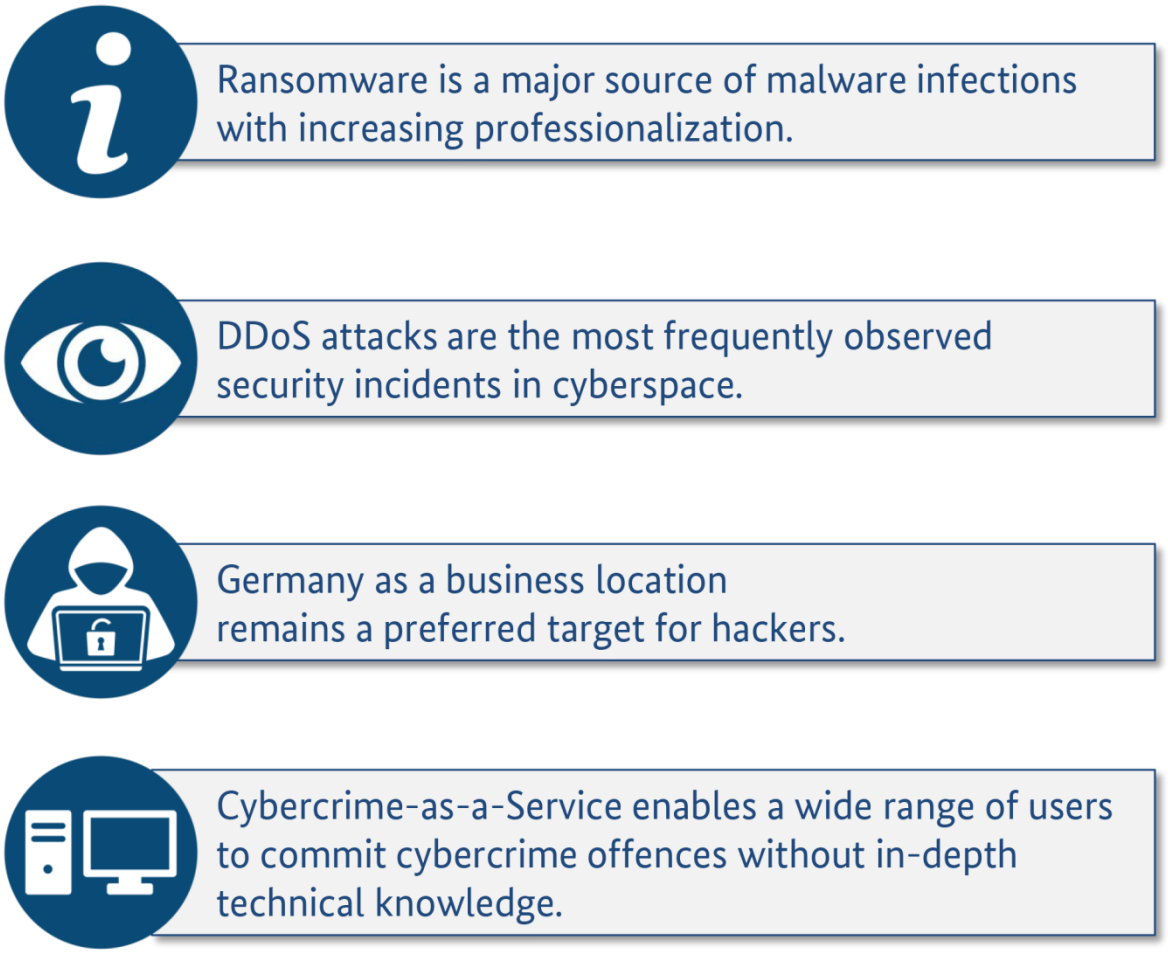
The Internet as Instrument of Crime - Distribution by Fields of Criminal Activity (2017)



The PCS special designation "internet as instrument of crime" is assigned whenever the internet plays an important role for the commission of offences, as in the case of extortions in connection with DDoS attacks or transactions with online mail order shops. The special designation, however, is not used if, for instance, there was only lose contact between offenders and victims prior to the actual offence.

74.4% of all cases recorded in 2017 were fraud offences (183,529 cases). These mainly included offences designated "fraudulent failure to supply goods as agreed", where suspects offered goods for sale on the internet but provided only inferior-quality items or none at all, or offences, in which goods were obtained by fraud (134,476 cases), i.e. ordered and not paid for.

3 Current Phenomena



3.1 RANSOMWARE[7] – DIGITAL EXTORTION

Ransomware usually encrypts the data on a digital system and, in many cases, even blocks other terminal devices accessible through a network (such as an enterprise network).

In most cases, the perpetrators demand ransom money to be paid in digital currency. They promise to send the victim a code that will unlock or decrypt the system once the ransom has been paid, so that the victim will be able to use the system again.

Digital extortion by ransomware is a frequent phenomenon both in Germany and worldwide. Not only enterprises, but also an increasing number of private individuals have experienced ransomware attacks.

[7] Ransomware is malware used by intruders to make individual data or whole computer systems inaccessible or unusable. In most cases it is used to extort ransom money.

From a criminal law perspective, the use of ransomware constitutes a combination of the criminal offences of computer sabotage and extortion, punishable under sections 303 b and 253, respectively, of the German Penal Code.

For 2017, the BKA gathered data explicitly on this phenomenon from the authorities at the federal level and the German Länder in order to get a better overview of the reported ransomware cases. The data collected show that, during that year, a total of 5,191 malware cases including 2,772 ransomware cases had been reported.[8] Eleven of the German Länder could even provide separate figures for the various ransomware families. According to these data, in 2017 the ransomware families most frequently reported to the police were: the "BKA Trojan" (720 cases), CryptXXX (170 cases), Cerber (117 cases) and Locky (55 cases).

What types of ransomware are there?

As a general rule, there are two different kinds of ransomware:

a) *Ransomware that does not encrypt the hard disk, but only blocks user access to the system. The most commonly known type is malware that misuses the names and logos of security agencies[9] in order to make the illicit demand for payment look "official".*

b) *Crypto-ransomware that actually encrypts the data on the compromised terminal systems and, in recent cases, even on systems connected through networks (servers, file storages, etc.). This type is far more dangerous since in a number of cases it is not possible to decrypt and thus restore the data. Furthermore, in many cases paying the ransom demanded does not mean that the compromised system is decrypted afterwards.*

In their report entitled "The State of IT Security in Germany 2017", the BSI found that ransomware has remained the most prominent source of malware infections in 2017 as well.[10]

Frequently, compromised systems are fully encrypted and whole networks suffer significant disruptions. Victims who cannot restore their IT infrastructure based on recent backups experience massive negative impacts on or even total disruption of their business operations. Knowing about the massive potential damage, numerous victims pay the relatively small ransoms demanded.

From the police perspective, such payment should be discouraged since payments support the ransomware "business" and encourage perpetrators to continue committing such criminal offences. A further reason for this stance is that the victims themselves may be able to overcome the infection: In case of a ransomware infection, it may be worthwhile to search for open source decryption tools, for instance through www.nomoreransom.org, a project initiated by Europol and the Dutch cybercrime agency (NHTCU) in co-operation with the private sector.

[8] Data to the collection were contributed by 13 of the German Länder. Hence, the figures cannot be compared to the figures mentioned above and only reflect the current number of ransomware cases reported according to the data gathered by the aforementioned method. At present, it is not possible to identify any trend (increase or decrease of ransomware cases) as a conclusion from these figures.
[9] Famous examples of this type are the "BKA trojan" and the "GVU trojan" (GVU = Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V. [registered association for the prosecution of copyright infringements]).
[10] **Https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html.**

Even in 2017, most of the ransomware used was ransomware involving encryption. For mobile operating systems such as Android, simple lockscreens without encryption of the hard disk have continued to be used as a modus operandi.[11]

In 2017, the major part of the ransomware community professionalized. For one thing, professionally coded and distributed variants such as Locky, CryptXXX, and Cerber continued to dominate the market – an assessment shared by the G4C. For another thing, new variants such as WannaCry proliferated by using alternative distribution channels, in this case the worm-style propagation through IT vulnerabilities. Overall, there were more targeted attacks, some of which involved significantly higher amounts of ransom. As it seems, targets were chosen more carefully than in 2016.[12] However, the major part of ransomware was still distributed by mass propagation waves and involved relatively small amounts of ransom. According to an analysis by the G4C member Symantec, in 2017 the average amount extorted in ransomware cases was about 522 USD (equivalent to about 425 EUR).[13] The year 2016, in contrast, had been characterised by a considerable volume of ransomware attacks. Numerous variants had been developed with the objective to obtain proceeds in the short run; some new versions simply copied older variants. Furthermore, many of the variants observed in 2016 had been coded in an unprofessional way and included design failures.

An example: The encryption software WannaCry

In May 2017, the ransomware WannaCry was used to commit a massive worldwide cyberattack on the computer systems of enterprises, institutions and private individuals. In Germany, the systems of the railway company Deutsche Bahn were compromised. This led to a disruption of service at ticket machines and to messages from the extortionists being displayed on numerous passenger information panels at German railway stations. The attack also compromised numerous private systems.

The European cybersecurity agency ENISA (European Union Agency for Network and Information Security) estimated that over 230,000 systems in more than 150 countries of the world had been affected by the attack. In the United Kingdom, for instance, the attack had major negative impacts on the health service. Further known infections compromised systems in Russia, China, Ukraine, the USA, Spain, France, Hong Kong, Japan and other countries.

The ransomware WannaCry propagated largely without user interaction, very much like a worm, and exploited a vulnerability in the Windows SMB protocol commonly known as "ETERNALBLUE". Its spread was provisionally stopped by an IT security expert by means of a kill switch domain.

Brief assessment:
The ransomware WannaCry was characterised by its largely automatic, worm-style propagation that exploited IT vulnerabilities. The damage caused is enormous and highlights the damage potential that ransomware had in 2017.

[11] **Https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html**.
[12] This assessment is also shared by the German Competence Centre against Cyber Crime (G4C e.V.).
[13] Cf. Symantec ISTR 2018; **https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf**.

3.2 FURTHER TYPES OF MALWARE

Malware

Malware runs undesired or malicious operations on information technology systems. The distribution and use of malware on the victims' systems is essential as a basis for cybercrime. The most common malware distribution channels are attachments in spam e-mails and infections that occur – without the users noticing – when they visit webpages with malicious content (drive-by downloads). There is an increasing trend for malware to spread like worms by exploiting vulnerabilities automatically detected.

The BSI report entitled "The State of IT Security in Germany 2017" estimates the total number of malware variants for computer systems to be more than 600 million (560 million in 2016).

In addition to ransomware, numerous other types of malware were detected in 2017 as well. This included, above all, banking Trojans, keyloggers, adware and spyware. Furthermore, incidents also included malware attacks on cash dispensers.[14]

According to a survey by the BSI, 70 per cent of the German enterprises surveyed had been targeted in cyberattacks in 2017. Malware had been involved in the major part of these attacks (57 per cent).[15]

Data collected by the BKA (cf. p. 10) on malware incidents reported to the police included a total of 924 cases of banking Trojans. This is equivalent to about 16 per cent of the total number of malware cases reported.

According to the G4C, there was an increase in cryptomining malware, in particular towards the end of the year 2017. The objective of this type of malware is to infiltrate private and business systems in order to use the computing power of these systems for calculating cryptocurrency – in particular Bitcoin – transactions. This has a negative impact on the performance of the compromised systems, and can also lead to excessive electric power consumption and thus excessive electricity costs billed to the victims.[16] However, the data recorded by the police authorities hardly list any cryptomining malware cases in 2017 at all. The major reason for this probably is that the victims do not notice the damage at all, or only notice it later on, and that they do not suspect any criminal behaviour.

[14] Cf. BKA, Angriffe auf Geldautomaten [Attacks on Cash Dispensers], Bundeslagebild [National Situation Report] 2017, p. 11.
[15] **Https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Allianz_digitalundsicher_15022018.html**.
[16] Cf. also **https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf**.

An example: The malware NotPetya

June 2017 saw the massive destructive impact of a malware program on enterprise IT systems worldwide.

In Germany, targets included enterprises, mainly in the logistics, finance and health sectors.

The malware "NotPetya" infected several enterprises, mainly in Ukraine, through a vulnerability in an accounting software application. The malware then spread itself like a worm targeting numerous further enterprises that also used this software. In addition to enterprises in Ukraine, enterprises in numerous further countries were infected by "NotPetya".

"NotPetya" caused enormous damage. Decisive parts of the compromised systems became unusable, some of them permanently. Even weeks after the attack, some enterprises had not been able to fully restore their IT infrastructure. Both the Danish shipping company MAERSK and the freight forwarder TNT Express stated that they had suffered damages amounting to more than 300 million USD each. The total damage caused in Europe alone has been estimated to amount to more than 1 billion EUR.

Brief assessment:
Contrary to the frequently heard initial assessment that "NotPetya" was a variant of the ransomware Petya, it turned out that it had not been distributed with the "classic" intention to extort ransom money. The malware was rather distributed in order to destroy data and block/sabotage business processes. Hence, the distribution of "NotPetya" is primarily an act of cybersabotage.

The example illustrates the enormous damage potential of malware. "NotPetya" is characterised by its particularly clever distribution method. Following the initial infection, the malware spread itself to further vulnerable systems, even beyond the systems of already compromised enter-prises. This is proof of the development that malware increasingly uses advanced technologies.

3.3 BOTNETS – MASS REMOTE CONTROL OF COMPUTERS/DDOS ATTACKS

3.3.1 Botnets

As a key resource for attacks, botnets have continued to be a prominent threat even in 2017. Botnets are numerous systems compromised by malicious code that are controlled remotely through "command & control" (C&C) servers without their owners knowing. The systems compromised include not only computers, but an increasing number of mobile and "intelligent" Internet of Things (IoT)[17] terminal devices.

How are botnets created?

Botnets are created by installing malware on victim PCs, usually without their owners noticing.

The malware is installed in a variety of ways, for instance, by opening an infectious e-mail attachment or by a "drive-by infection".

A further way is the distribution of malware through social networks (such as Facebook). Members of the networks receive messages with infectious attachments from senders they believe to be friends or acquaintances. When they open such an attachment or click a link included in the message, their computer is infected.

Distribution channels furthermore include the Usenet and filesharing/peer-to-peer networks where the malware is available for download – usually camouflaged as a video or audio file.

Once the malware has been installed, the perpetrator has almost full access to the compromised system of the victim.

As botnets can be used for a wide variety of purposes, they continue to be profitable goods traded worldwide in the underground economy. However, it is nearly impossible to provide reliable figures for the total number of computers in Germany or worldwide that have been pooled together in botnets.

The operators of botnets rent out bots that can be used, for instance, for targeted DDoS attacks on enterprise servers, for sending mass spam e-mail, or for targeted data thefts.

Some of the botnets have been created with a multifunctional approach and can thus be flexibly used for a wide variety of purposes.

[17] For more information on the Internet of Things, cf. chapter 5.2.

An example for a botnet: "Andromeda"

In November 2016, a coordinated international operation dismantled the botnet structure "Avalanche". This infrastructure was found to include the malware "Andromeda", which was distributed through yet another botnet. During extensive international investigations involving, in Germany, the public prosecutor's office in Verden and the criminal investigation department in Lüneburg, Lower Saxony, the botnet was analysed and the command-and-control servers decisive for the botnet structure were identified. In November 2017, this international botnet structure was taken down during an "action day".

The presumed main perpetrator was arrested in Belarus during the "action day". Not only was extensive evidence recovered, but the 7 command-and-control servers in 6 different countries that had been used to distribute the malware were confiscated and taken down as well. Furthermore, 1,500 malware domains were sinkholed[18]. As a result, on 30/11/2017 alone, 1.35 million IT systems worldwide were identified that had been infected by "Andromeda".

The victim systems were infected by e-mail containing a malicious link, or by drive-by exploits on compromised banner ads or websites, mainly with dubious content (pornography, illegal sales, copyright violations due to video streaming, etc.). The malware spied out the infected systems and included a feature that could download a banking Trojan tailored to the victim's data that had been spied out before. The perpetrators managed to infect several million PC systems over the last few years. Focuses were North America, Asia, and Europe, where most of the compromised systems were located in Romania, Italy, Germany, and Poland.

The police measures involved forces not only in Germany, but also in Finland, France, Poland, Italy, Russia, the Netherlands, Belarus, and the USA. A total of 27 countries worldwide were involved in the action.

The action was supported by the BSI, the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), the Shadowserver Foundation, and the Registrar of Last Resort (RoLR). Furthermore, EUROPOL and EUROJUST played a significant role in the coordination of the measures.

Brief assessment:
The fact that until early in 2018, and in spite of all the measures taken, 39 per cent of the computer systems originally compromised by Avalanche in Germany – even 55 per cent worldwide – still continued to be infected highlights the need for further efforts, in particular, efforts to clean up systems that have been identified to be running bots.

[18] Redirecting requests from botnet-infected systems to other computer systems generally run by computer security experts.

3.3.2 DDoS attacks

DDoS attacks are closely linked to botnets since the victim systems merged into a botnet are used to commit such attacks. DDoS attacks are among the most frequent security incidents observed in cyberspace. Criminals have developed business models on this basis and rent out botnets in various sizes.

Police data on the number and duration of DDoS attacks in Germany are not available to the BKA. According to a study by the G4C member Link11, both the number of attacks and their duration as well as the average bandwidth have increased in 2017.[19]

When sales portals (such as online shops, service providers, cryptocurrency trading platforms) are unavailable due to a DDoS attack, this can lead to considerable economic losses in the highly competitive internet market segment.

The motives of the perpetrators vary between purely monetary interests (ransom DDoS), gaining competitive advantage, revenge, and political or ideological motives.

It is not possible to definitely quantify the losses that DDoS attacks cause to victims since it is generally hard to provide figures estimating the impacts of such attacks, such as

- system outage/disruption of work processes,
- temporary and long-term sales shortfall (customer churn and damage to the reputation of the business), and
- costly and laborious protective and preventive measures to fend off future attacks.

DDoS attacks are characterised by a tremendously fast increase in bandwidth. New dimensions are reached as IoT devices are exploited for the attacks.

The issues that are important in connection with the services available on the internet and used in such attacks include: Product packages vary by duration of the attack and number of days that the attack is to be active (30 or 90 days). They also vary in terms of throughput/intensity of the attack (usually 15 to 20 gigabits per second). Several different methods of attack of various intensities are available. Payment methods are Bitcoin and PayPal. Only a username, an e-mail address and a password of one's own choice are necessary for registration.

[19] Cf. Link11 DDoS Report for Germany, Austria and Switzerland; **https://www.link11.com/de/ddos-report/**.

An example: DDoS attacks

In 2017, the police in Bielefeld investigated a 24-year-old German national for several cases of suspected computer sabotage and extortion.

The German national who used the pseudonym "zzb00t" during his offences was suspected of having crashed the websites of victim enterprises by creating an overload (i.e. by DDoS attacks) by using cybercrime services available on the internet. During or after the DDoS attacks, the enterprises received demands for ransom in Bitcoins in return for the cyberattacks to be terminated by the perpetrators. When the searches ordered in May 2017 were carried out, the perpetrator was logged into several internet services that sell "IP stress tests". The webpages displayed on the perpetrator's computer showed active (DDoS) attacks by these providers targeting various IP addresses. Obviously, the perpetrator was using several of these service providers in order to flood websites of his choice with mass requests, thus crashing them. The investigation revealed that the perpetrator/the internet services had shut down the websites of several well-known German enterprises by using a botnet, i.e. numerous hijacked computers merged into a network. The information available so far suggests that the perpetrator's motives were purely financial – he wanted to obtain Bitcoins by extorting the enterprises.

The perpetrator furthermore used the services of a provider of "disposable" e-mail addresses ("byom.de"). Using an ID of one's own choice, one can have a proper e-mail address assigned, which can be used in public. It is not possible to check any e-mail messages sent to the address generated. According to the default settings, the service provider deletes the e-mail messages after one hour.

In the meantime, the perpetrator has been sentenced by Bielefeld local court to a prison term of 1 year and 10 months.

Brief assessment:
With the help of services available from several service providers on the internet, even individuals without any in-depth specialist knowledge of their own are able to carry out DDoS attacks. The internet not only makes it possible to rent the tools for such attacks, it also provides instruments that help to camouflage the identity of the perpetrators.

DDoS attacks are characterised by a tremendously fast increase in bandwidth. They reach unprecedented highs by exploiting IoT devices. Due to the fact that the security standards of many IoT devices are deficient, it is usually very easy to merge them into botnets. It may well be assumed that this trend will continue and that we will see an increase in quantity and quality of DDoS attacks committed by means of botnets, for instance.

3.4 MOBILE MALWARE

According to the 2017 JIM study (yearly study conducted by the "Media Education Research Association Southwest" on youth, information and multimedia), almost 100 % of all households are meanwhile in possession of media devices (smartphones, PCs, internet access, televisions).[20] The market development from conventional computers to mobile terminal devices such as smartphones and tablets continues.

In contrast to traditional PCs, mobile terminal devices are usually online all the time. Nowadays, users carry out a major part of their digital activities via these devices. Due to online banking transactions, the access to e-mail accounts and social networks or activities in the field of E-commerce – often enabled by corresponding apps –, smartphones and tablet computers are attractive attack targets for criminals.

On account of the prevailing update cycles, recognised vulnerabilities in the device software frequently remain unclosed for quite some time or are never closed as a result of ever shorter product cycles because the support period has expired.

In most cases, it is the users' own behaviour that enables malware to gain access to mobile devices. The lack of awareness of the risks connected to the use of mobile terminal devices such as, for instance, installing apps from untrustworthy sources, renders technical security measures ineffective and allows attackers to penetrate secure networks.

Users of mobile terminal devices and smart home devices need to be further sensitized.

The growing importance of mobile terminal devices for cybercriminals is particularly reflected in the increase in malware developments in the field of mobile operating systems. A report of the IT security company Kaspersky states that known malware mainly aims at Android systems.[21] The G4C member Symantec reports a rise in mobile malware by 54 % in 2017 compared to the previous year and a total number of 27,000 different variants.[22]

The 2017 situation report by the BSI confirms these tendencies, as well, and indicates, inter alia, the following vulnerabilities: insufficient encryption when using personal data, security-critical software versions regarding mobile devices and actual user behaviour. Moreover, the BSI perceives a risk of misuse of devices (for example, the integration into a bot net) and a high risk of malware in the mobile context, if security updates are lacking.[23]

At present, reliable figures on the volume of mobile malware in Germany can hardly be derived from police databases. The major reason for this is probably the low extent to which cybercrime is reported and – as a result – the large number of unreported and unrecorded crimes.[24]

---

[20] **Https://www.mpfs.de/fileadmin/files/Studien/JIM/2017/JIM_2017.pdf**.
[21] **Http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/KL_Mobile-Report_GER_FINAL.pdf.**
[22] Cf. Symantec ISTR: **https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf.**
[23] **Https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.**
[24] Cf. also **https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html.**

In 2017, the BKA carried out a Federation-Länder survey on mobile malware. According to this survey, 330 cases were reported to the police. This represents a share of 6.4 % of all cases of malware infections reported to the police in 2017.

3.5 THEFT OF DIGITAL IDENTITIES/PHISHING IN THE CONTEXT OF ONLINE BANKING

The misuse of a natural person's personal data by a third party is still a common and lucrative business model. All data and/or forms of digital identities that can be used for criminal activities are interesting for perpetrators. This includes, for example, access data for communication services, banking portals, booking systems and online shops. Subsequently, the digital identities obtained are misused for criminal purposes (frequently fraud offences) or sold – often via illegal sales platforms of the underground economy.

What is a digital identity?

The term "digital identity" refers to the sum of all possibilities and rights of the individual users as well as their personal data and activities within the overall structure of the internet. Specifically, this also includes all kinds of user accounts, i.e. also access data in the following areas:

- *communication (e-mail and messenger services),*
- *E-commerce (online banking, online stock trading, all kinds of internet-based sales portals),*
- *professional information (e.g. for the purpose of accessing internal technical company resources online),*
- *e-government (e.g. electronic tax return) and*
- *cloud computing.*

To gain possession of personal data, perpetrators use different types of malware (spyware[25], Trojans[26] and keyloggers[27]) but quite often also phishing e-mails.

[25] This is a neologism created from the words "to spy" and "software". Spyware is defined as software that is designed to surreptitiously gather information about a user and/or the use of a computer and forward it to the creator of the spyware. Spyware is frequently only regarded as annoying; however, it should not be ignored that spyware can also spy out security-relevant information such as passwords.
[26] A Trojan is a program with a covert, undocumented function or effect. Trojans do not spread on their own but trick users into installing them by promoting the alleged usefulness of the host program. Users have no influence on the execution of this function; a Trojan could, for instance, enable attackers to gain backdoor access to the users' computers.
[27] A keylogger is hardware or software designed to record keys struck on a computer keyboard. It records all keyboard entries with a view to forwarding them to the attacker, if possible without being noticed. Subsequently, the attacker is able to filter data important to him from this information, such as registration data or credit card numbers.

To this end, the stolen identities are transferred – by means of the malware deployed – to specific storage locations on the internet (commonly referred to as drop zones) that are accessible by the perpetrators and/or the person(s) giving instructions. In case of phishing attacks, the victims are induced to enter relevant information on servers controlled by the perpetrators.

In the course of open source research on a platform of the underground economy carried out in 2017, the BKA found an aggregation of approximately 500 million e-mail addresses/password combinations in a structured form that probably originate from different time frames and sources and had most probably been compiled by an unknown "collector". In the underground economy, this data collection is called "Anti Public Combo List" and offered for download free of charge. The access data are believed to originate from a large number of website hacks committed over a longer period of time. The latest access data spied out that are indicated on this list date from December 2016. The BKA submitted the data to the appropriate security authority (BSI) and the Hasso-Plattner-Institut (HPI) that runs a web service called "Identity Leak Checker" where 3.7 billion compromised access data had already been stored at that time. This service can be used by everyone to check whether he or she might be affected.[28]

In its 2017 situation report, the BSI states that the use of personal data tapped from large service providers is currently observed increasingly frequently.[29] This is confirmed by ENISA (European Union Agency for Network and Information Security) in the "Threat Landscape Report" indicating that the number of "data breach" incidents rose by 25 % in 2017 compared to the previous year and that further incidents keep coming to light.[30]

[28] **Https://sec.hpi.uni-potsdam.de.**
[29] Die Lage der IT-Sicherheit in Deutschland 2017, BSI (The State of IT Security in Germany 2017, BSI).
[30] **Https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport**

Data breaches:

The term "data breach" covers both the intentional and unintentional release of sensitive data to an untrusted environment. Thus, it includes both "leaks" (technical data leaks) and "intrusions" (active capture, interception or transfer of data by third parties).

The individuals affected often do not know that their data had been "lost" or stolen. In many cases, this only comes to light months or years later, when the consequences of the data misuse become apparent; these could be economic disadvantages, because criminals exhausted the limit of the credit card account, or personal disadvantages, such as image damage, because the individual's personal data were misused to insult or even sexually harass another person via a social network.

The causes for such data losses are manifold. One of the reasons is that companies do not handle data in a sufficiently secured form. In most cases, technically adept perpetrators, commonly known as hackers, are responsible for the attacks.

The website **www.breachlevelindex.com** that is quoted within the framework of the iOCTA (Internet Organised Crime Threat Assessment) indicates that a total number of approximately 1.9 billion data records were stolen in the first half of 2017. Almost half of the data breach incidents were recorded in Europe (49 %).[31]

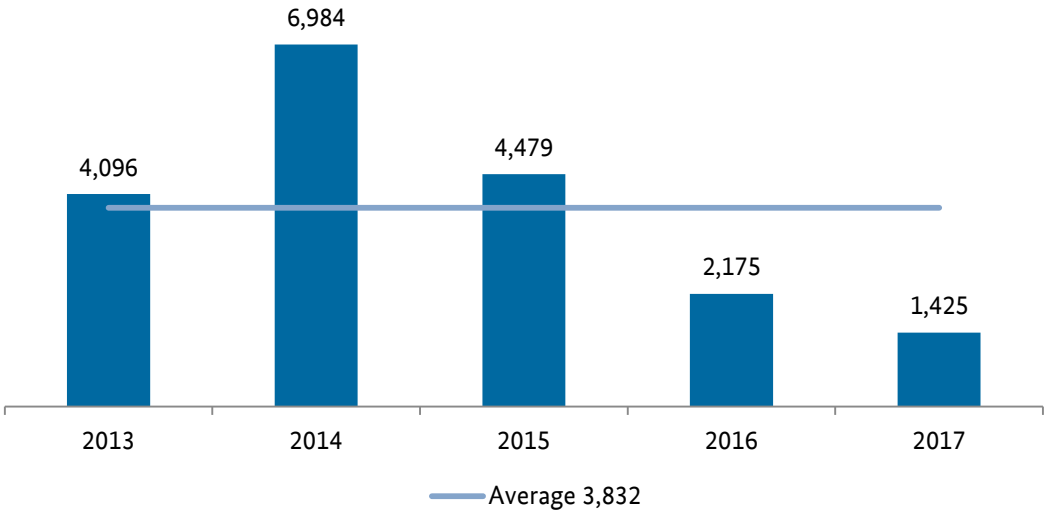
In 2017, media coverage focussed on the loss of data records of 148 million US citizens that had been stolen from a private-law information database. The said breach that happened between May and July 2017 led to the loss of especially names, birth dates, addresses, loan and credit card information as well as driving licence and social security numbers.[32] In the USA, these incidents led to a public discussion about tightened cyber security laws that is still ongoing.

Besides the mass theft of digital data, "phishing in connection with online banking" remains a common form of digital identity theft.

In 2017, the police authorities of the Länder reported 1,425 cases linked to the phenomenon of phishing to the BKA. In comparison to 2016 (2,175), case numbers thus decreased by 34.5 % to their lowest level in five years, which confirms the declining trend of this phenomenon that was also observed by Europol.

[31] **Http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf.**
[32] **Https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?utm_term=.846d59ae8dde.**

Phishing cases in connection with online banking



Since banks, as a rule, only reimburse customers for damage resulting from a phishing incident in connection with online banking if the incident is reported to the police, it is likely that the number of unreported and unrecorded phishing offences is very low.[33]

With regard to phishing attacks, perpetrators do not rely on technical solutions alone but attempt to obtain necessary customer information through social engineering[34]. Thus, the perpetrators try to circumvent the authorisation mechanisms used for online banking in Germany that require an active action of the person authorised to draw on the account (by using a second communication channel[35]).

Since 2014, there has been a downward trend in the number of phishing cases in connection with online banking. The consistent further development and fine-tuning of mechanisms enabling banks to detect such attacks, including the possibility to detect malware-based skimming in connection with online banking, can be regarded as an explanatory approach.

Furthermore, the G4C sees a declining trend in 2017 for the malware-based approach concerning online banking fraud, inter alia, as the malware-based approach for phishing in connection with online banking involves much greater technical effort for the perpetrators than the skimming of account information by means of phishing e-mails.

The transfer of assets from compromised accounts via virtual wallets (e.g. Bitcoin wallets) can be cited here as an example of how perpetrators adjust e-mail-based phishing. According to information provided by the G4C member Commerzbank, identity verification information needed

[33] As of 2019/2020, banks will be obliged to report such cases to the European Banking Authority (EBA) with the consequence that a comprehensive phishing situation report should then be available there.
[34] Social manipulation – to induce an individual to disclose confidential information. When criminals use social engineering to commit cyberattacks, they attempt to dupe victims into disclosing data voluntarily, circumventing security measures or installing malicious codes on their systems independently. Both in the fields of cybercrime and espionage the perpetrators act cleverly to exploit alleged human weaknesses such as curiosity or fear and to thus gain access to sensitive data and information.
[35] Commonly known as two-factor authentication.

for transactions from cash accounts to wallets (usually the rightful account holder's photographed identity card) is also skimmed during the phishing attack.

Despite the declining development in terms of quantity, phishing remains a lucrative and thus attractive field of activity for perpetrators as regards the possibilities available and the criminal proceeds that can be generated. The average loss incurred in the field of "phishing in connection with online banking" in 2017 was around 4,000 EUR per case. This corresponds to a total loss of 5.7 million EUR, which, however, is significantly lower than the average loss incurred in the past five years (average 2013-2017: 15.3 million EUR).

3.6 CYBERCRIME-AS-A-SERVICE

"Cybercrime-as-a-Service" (CaaS), illegal forums and illicit trading platforms of the underground economy promote dynamic developments in almost all fields of crime and are now established as successful business models. Digital market places also play an ever growing role for the commission of offences in the area of cybercrime. On the one hand, criminal services are offered and/or searched for there; on the other hand, cybercriminals exchange information about their criminal know-how (e.g. about how to take advantage of vulnerabilities) in relevant forums.

In the underground economy, products and services are offered for the following cybercrime phenomena:

- ransomware,
- bot nets for criminal activities,
- DDoS attacks,
- malware production and distribution,
- data theft,
- sale/offer of sensitive data (access or payment data),
- anonymization and hosting services to conceal one's identity,
- portals to test if the malware purchased or produced is detectable and
- drop zones to store illegally obtained information and/or goods.

A recent trend is the professionalization of perpetrators in the field of CaaS. The criminal services offered make it possible to delegate the entire process – from consulting "customers", through selecting a vulnerability, adjusting the malware and introducing it into the target system to organising the illicit money flows, – to specialised service providers in the form of contract work. The "customers", which means the criminals, who, for instance, use such tools for cyberattacks, hardly need to have any technical skills themselves any more. As a result, the phenomenon of cybercrime becomes open to a wide spectrum of users without profound technical knowledge.

Figures on the CaaS phenomenon are not available. In our estimation, however, it is assumed that the number of market places (both in the clear/visible web and the darknet) and the related range of products and services remains large.

3.7 UNDERGROUND ECONOMY – DIGITAL BLACK MARKETS

Illegal forums or market places in the clearnet, deepweb[36] and darknet play an ever increasing role in the commission of cybercrime.

The services listed under "CaaS" continue to be offered. However, the forums are still also used for the communication between cybercriminals, the transfer of criminal know-how and the exchange of information on how to take advantage of vulnerabilities and therefore for the preparation of cyberoffences.

Apart from these cases that are to be classified as CaaS, there is still an increasing shift of the other, classic types of crime to the virtual world. In the clearweb but particularly also in the darknet, illegal goods such as drugs, weapons, counterfeit money, forged identity documents, stolen credit card details or counterfeit branded goods are offered. The supposed anonymity, a presumed lower risk of detection and the possibility to reach customers worldwide via the market places might be explanatory approaches in this context. Even the forums and market places in the darknet are available to every internet user. In this case, as well, profound technical expertise is not required.

Whereas there are no specific platforms for the above-mentioned offences, the trafficking in child pornography is usually carried out via platforms created for this specific purpose.

The administrators of the forums frequently have a share in the proceeds from the sale of the illegal goods via a trusteeship system.

As regards the payment of the goods traded, only digital cryptocurrencies[37] enabling customers to pay anonymously or under a pseudonym are accepted.

An example: Digital black markets – underground economy

Since January 2017, the BKA – under the governance of the Public Prosecutor General's Office in Frankfurt/M. and in close co-operation with the High Tech Crime Unit of the Dutch police – had been conducting police investigations into the responsible operators of the darknet trading/sales platform "HANSA market" that could be accessed via the Tor network and had finally become the second largest platform.

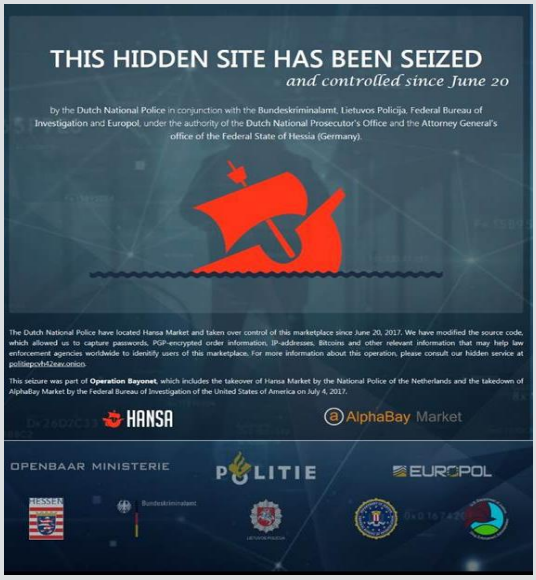
The investigations particularly targeted two 30- and 31-year-old administrators, who were suspected of having violated the Narcotic Drugs Act. The aim of the investigations conducted by the Dutch police was the technical take-over of the market place with a view to identifying so-called power sellers.

[36] The deepweb is that part of the internet which cannot be found by general search engines. The contents include databases, intranets or specialised websites.
[37] Alternative terms: virtual, alternative or digital currencies, money or foreign currency.

An example: Digital black markets – underground economy

In June 2017, several premises were searched and the subjects were arrested. At the same time, the market place was taken over by the Dutch police and subsequently shut down.

The measures taken became visible to the underground economy scene through the "seizure banner" placed on the website:



The police measures taken against this platform in the underground economy again confirm the trafficking in narcotic drugs on the internet.

Moreover, the police investigations proved that the subjects acted extremely professionally and on the basis of a division of tasks and led to the dismantlement of the perpetrator network.

In addition to HANSA market, the largest German-speaking forum "Deutschland im Deep Web" (DiDW, Germany in the deepweb) that could be accessed via the Tor network was shut down by security authorities in 2017.

DiDW had been administered and operated by a 30-year-old German national who was placed in pre-trial detention in June 2017. In the course of the investigations, full access to the productive system of the forum was gained, the related database was seized and subsequently the platform was de-activated in June. At the time of de-activation of this darknet platform, more than 20,000 users were registered there. Narcotic drugs/pharmaceuticals, firearms/war weapons requiring permits, counterfeit money and forged identity documents were traded on "DiDW".

The forum "DiDW" became widely known through the media coverage of a killing spree at Munich's Olympia shopping centre in July 2016, because the 18-year-old gunman had bought the crime weapon, a Glock 17 pistol, via this platform. He killed nine persons and himself on his rampage.

An example: Digital black markets – underground economy

Within the framework of the further analysis of the leading members of the forum "DiDW", investigations into two moderators and one power seller were initiated. All three users were, apart from their role in the forum, active sellers of illegal narcotic drugs, prescription-only pharmaceuticals and other illicit goods and/or services.

3.8 ATTACKS ON ENTERPRISES/ CYBERESPIONAGE

Enterprises continue to be targets of cybercriminals. A study carried out by KPMG AG in 2017 also proves that enterprises are largely affected by computer crime.[38]

The above-mentioned phenomena such as ransomware, malware, DDoS attacks and bot net activities also pose a threat with a high destructive potential to enterprises at the business location Germany, as well. In fact, Germany-based enterprises are worthwhile attack targets of cyber-espionage.

According to the BSI, the number of cyberespionage attacks on enterprises is currently on the rise again after a decrease in 2015/2016.[39] In particular, enterprises that are extensively active abroad are the subjects of attacks committed by governmental or governmentally controlled players.

Typical examples of governmentally controlled cyberattacks are what is referred to as APT attacks (Advanced Persistent Threat).

APT attacks (Advanced Persistent Threat)

Advanced Persistent Threats (APT) are targeted cyberattacks on selected institutions and facilities, with an attacker gaining permanent access to a network and subsequently extending this access to further systems. Such attacks are characterized by a very high deployment of resources and significant technical skills on the part of the attackers and are usually difficult to detect.

[38] **Https://home.kpmg.com/de/de/home/themen/2017/04/ecrime-studie.html.**
[39] **Https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.**

The BKA has made the following findings in the field of cyberespionage:

- Cyberattacks against Germany have become an important method for foreign intelligence services to collect information.
- Again and again, the same server infrastructures and malware components are used for cyberespionage attacks throughout the world.
- In many cases, the main attack vector is the sending of spear phishing e-mails[40], including both malicious links and malicious attachments, which are used to infect victims or rather their systems. Prior to the cyberespionage attacks, perpetrators usually check the victims professionally by means of social engineering but also carry out classical checks on-site.
- In various publications, numerous private IT security providers regularly point out that Germany is one of the targets of cyberespionage attacks. A concrete and actually identifiable and reliable attribution regarding such attacks, however, is not or hardly possible.

Also as regards the field of cyberespionage, it is assumed that the number of unreported crimes is high as a result of undetected and/or unreported attacks.

3.9 ATTACKS ON CRITICAL INFRASTRUCTURES

Critical infrastructures are organisations and institutions that are of significant importance to the community. A failure or impairment of such critical infrastructures may result in long-term supply shortfalls and/or major disruptions of public security.[41]

In principle, the operators of critical infrastructures are exposed to the same dangers as all other enterprises. The destructive potential, however, is considerably higher. Therefore, this field is not only considered a target of financially motivated perpetrators but potentially also for politically motivated perpetrators. The field of government and administration falls per se within the target spectrum of such perpetrators.

Enterprises with critical infrastructures are obliged to report incidents to the BSI pursuant to the IT Security Act. In its 2017 situation report[42], the BSI states that a total of 34 incidents were reported between the date this act had come into force (July 2015) and 30/06/2017. The focus was on the information technology and telecommunications sectors.

Recent examples of the general vulnerability of enterprises with critical infrastructures were the cyberattacks committed on the Deutsche Telekom AG (Mirai) and the Deutsche Bahn AG (WannaCry).

[40] Sophisticated phishing using a more targeted personal approach ("spear").
[41] **Http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS_Flyer.pdf**.
[42] **Https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.**

It is a fact that the business location Germany – due to its comparatively high level of competitiveness and technological expertise – represents an interesting target for cyberespionage or hackers committing general criminal offences. Consequently, cyberattacks also focus on operators of critical infrastructures. Cyberattacks on the energy sector identified worldwide in 2017, hacker attacks on the network of the Federal administration and ransomware attacks targeting enterprises with critical infrastructures reveal the threat potential for Germany, as well.

4 Damage Resulting from Cybercrime

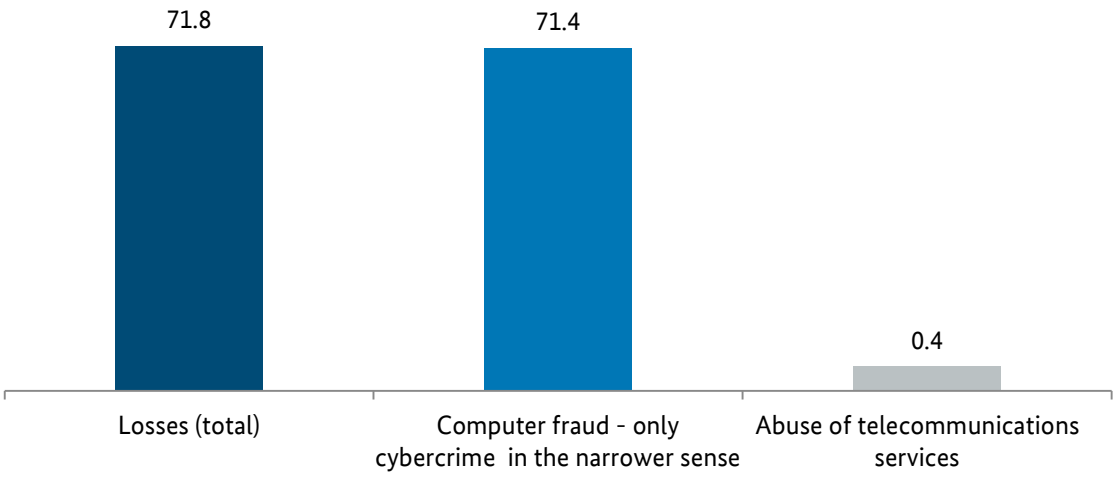
Cybercrime causes considerable material and immaterial damage to citizens, authorities and businesses. Media reports on thefts of millions of data or manipulations of numerous technical devices have a highly negative impact on the public's sense of security.

Even people who do not actively use the internet depend on the smooth running of data networks, in particular the internet. For instance, electricity and gas are purchased through digital channels by major providers and then distributed via networks. Conventional retail businesses also increasingly store their customers' data in databases which, in turn, serve as targets for criminal hackers and are open to misuse. According to an online study carried out by German TV stations ARD/ZDF, the number of internet users rose to a total of 62.4 million in 2017. This represents a share of 89.8 per cent of the German-speaking population from the age of 14 onwards and an increase of 4.4 million people compared to 2016[43].

Police statistics on cybercrime, however, exclusively indicate losses resulting from computer fraud as cybercrime in the narrower sense and the misuse of telecommunications services. The total losses reported for 2017 amounted to 71.8 million EUR (2016: 51.6 million EUR). Approximately 71.4 million EUR (2016: 50.9 million EUR) of the total loss recorded were attributable to computer fraud, and more than 0.4 million EUR (2016: 0.7 million EUR) to the misuse of communication services.

Since losses are statistically recorded only in the aforementioned fields of criminal activity, the Police Crime Statistics do not provide a basis for qualified statements regarding the actual overall financial loss arising from cybercrime.

Losses resulting from cybercrime, in million EUR (2017)[44]



[43] Http://www.ard-zdf-onlinestudie.de/ardzdf-onlinestudie-2017/.
[44] In cases where the financial loss is not known, a loss of 1 EUR is assigned as a symbolic value.

Financial losses brought about by a successful cyberattack are often not fully known or non-quantifiable. Moreover, reputational or image losses are difficult to define in financial terms. In addition, an attack - depending on how it is carried out - often not only crashes an individual system for a certain period of time but sometimes even paralyses entire networks. To illustrate the real extent of the damage, several factors must therefore be taken into consideration. Studies on this topic undertaken by private companies are available: For example, the Center for Strategic and International Studies (CSIS) and the security company McAfee have ascertained that global economic losses caused by cybercrime have risen to 600 billion USD. According to the study, about one quarter of the overall loss can be attributed to the theft of intellectual property.[45]

In the context of the study carried out by Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM, German Association for Information Technology, Telecommunications and New Media), interviews of internet users revealed that financial loss had been incurred in 54 per cent of all cases[46]

Great discrepancy between losses documented in police statistics and findings of the private sector.

A BITKOM study assesses that cybercrime caused financial damage of 55 billion EUR to the German economy in 2017.[47] This figure is based on information provided by affected companies in the context of a survey. It remains a problem to determine what types of losses should be included when it comes to assessing the financial losses resulting from cyberattacks. There is no uniform system for dealing with this question.

It can be concluded that the relatively small losses listed in the Police Crime Statistics probably do not reflect the real dimensions at all.

An example: Damage resulting from cybercrime

In July 2017, Cologne Regional Court sentenced the person who had crashed the routers of a telecommunications provider to imprisonment of one year and eight months. When considering the costs, the affected company reported damage in the amount of two million EUR, about 50 per cent of which were actually accepted by the court (as costs incurred as a result of the cyberattack). For example, additional expenses for personnel deployed to resolve the incident were not included.[48]

Brief assessment:
The sometimes enormous cybercrime-related damage amounts listed in studies undertaken by security service providers must also be evaluated against the background of the aforementioned court decision.

[45] **Https://www.csis.org/analysis/economic-impact-cybercrime.**
[46] **Https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html.**
[47] **Https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html.**
[48] **Https://www.justiz.nrw.de/nrwe/lgs/koeln/lg_koeln/j2017/118_KLs_4_17_Urteil_20170728.html.**

5 Trends and Outlook

Besides the developments in the aforementioned fields of crime, the following elements are likely to have an impact on the development of the cross-cutting phenomenon of cybercrime, even across national borders. The law enforcement agencies will have to focus their attention on these issues as well.

5.1 DIGITAL CURRENCIES

Digital currencies, such as Bitcoin (BTC), Litecoin (LTC) or Ethereum (ETH), are virtual monetary units produced and used on the basis of mathematical calculations and cryptographic processes. The installation of a "wallet" software usually suffices to make use of them.

It is not illegal to use digital currencies. For example, it is possible to purchase and sell them (conversion from legal tender into legal tender) through various online exchange platforms. At present, BTC is the most widely used digital currency. It is already possible to pay with BTC in numerous online stores and several shops and cafés.

Virtual currencies are traded by means of cryptographically secured protocols directly between users, without any involvement of central banks or credit institutions. Hence, they are largely unaffected by state intervention. Transactions are processed anonymously as long as source and destination addresses cannot be linked to their possessors.

Consequently, cryptocurrencies are an attractive digital means of payment for criminal offenders. They are used in almost all the fields of cybercrime described in this report. There is particular danger that digital currencies might be misused especially for money laundering activities and financing terrorism.

Offenders might also seek to steal such currencies and to incriminate the blockchain[49]. This happened, for example, when offenders gained access to a so-called seed generator for Bitcoin wallets, which enables users to create a "master key" for their wallets. By accessing the master key, the offenders were able to steal, for example, cryptocurrency worth about four million USD. It also surfaced that virtual currencies in the amount of 430 million EUR had been stolen from another platform.[50]

Early in 2018, researchers of RWTH Aachen University and Goethe University in Frankfurt am Main discovered several illegal contents in the blockchain of a digital currency which had been rendered non-erasable by this technology. Such contents were information fragments which did not directly belong to the transaction; they had been placed in the blockchain by the perpetrators. Altogether, the researchers found more than 1,600 data files, including two lists of links referring to child abuse material. No specific cases of dissemination, possession or procurement of child abuse material for

[49] The blockchain forms the technological basis for cryptocurrencies, such as Bitcoin. It is a public or private, decentrally managed digital accounting system (Distributed Ledger Technology) for continuous recording of transactions. Transactions are closely linked in blocks by means of cryptography, which guarantees pseudonymity and security against counterfeiting.

[50] **Https://iota-deutschland.de/timeline/iotas-im-wert-von-mehreren-millionen-durch-seed-scam-gestohlen/.**

third parties have so far come to notice. The mere technical possibility to programme illegal contents into the blockchain poses major challenges to security agencies.

5.2 INTERNET OF THINGS

The term "Internet of Things" (IOT) describes the trend that not only commonly used devices (computers, smartphones, tablets), but more and more "intelligent" terminal devices are connected to the internet that are permanently online. These include household appliances such as refrigerators, TV sets or routers, but also sensors controlling other devices by smartphone or tablet via the internet. These devices usually have their own computing capacity and are equipped with corresponding operating systems, which the manufacturer often develops specifically for them on the basis of open source codes.

Network technology is an essential aspect when it comes to the security of the Internet of Things. IoT connections are not only based on Wi-Fi but also on e.g. Bluetooth, Near Field Communication (NFC) and Radio Frequency Identification (RFID[51]). Network security therefore requires consideration of many different connection types and interfaces.

Smart home offers countless new opportunities for committing crimes.

Numerous IoT devices can be easily attacked: Open ports without authentication, pre-set standard login data or missing security updates are among the many vulnerabilities. Many manufacturers who intend to make their products internet-compatible have no experience in developing secure software. They are pressed for time, not willing to accept delays in the market launch and reluctant to bear additional costs required to build up or purchase the necessary know-how. Instead, manufacturers should continuously update their firmware to ensure protection of the users.

Owing to the large number of additional IoT devices being used, DDoS attacks are characterised by a tremendously fast increase in bandwidth. The maximum bandwidths now reach dimensions which could not be achieved in the past by infecting, in particular, desk-top PCs. This raises the danger potential also for major internet service providers whose infrastructures formerly used to withstand attacks. An example of this are the attacks staged by means of the Mirai botnet in 2016. Since then, numerous Mirai successors and variants have emerged.

For instance, researchers warn that "IoTroop/IoT_reaper" might develop into one of the largest botnets of the past years.[52] It is believed to grow considerably faster than the Mirai botnet. At present, IoTroop/IoT_reaper reportedly controls nearly two million webcams, security cameras and digital video recorders. While Mirai was especially aimed at creating web traffic for DDoS attacks, the function of IoTroop/IoT_reaper is still unclear.

[51]"Identification by means of electromagnetic waves".
[52] **Https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/iot_reaper/**.

The "Satori" botnet, on the other hand, particularly targets home routers and IoT devices for the purpose of mining cryptocurrencies. To this end, the botnet exploits a vulnerability of a mining software called Claymore. The malicious code replaces the victim's wallet address with one of its own addresses. As a consequence, the devices carry out the mining for the masterminds behind the botnet without the victim noticing.[53]

In contrast, the "Hide'n Seek" (HNS) botnet primarily focuses on IP cameras. Latest results of research into the "Hide'n Seek" bot show that it is more complex and has new capabilities. The HNS bot makes it possible to steal information and is potentially suitable for purposes of espionage or extortion.[54]

It has also been revealed that perpetrators capture IoT devices by use of another Mirai successor ("OMG" botnet) and subsequently misuse them as proxies. The persons behind the scenes intend to disguise the data traffic of their illegal activities, e.g. attempts to hack networks or theft of data.[55]

As there is an ever-growing trend towards the so-called smart home, i.e. the interconnection of home technology and household appliances (e.g. blinds, heating, garage door etc.) and the specific remote control of functions via the home network and the internet, countless new opportunities are created for the commission of crimes (e.g. deactivation of home alarm systems to prepare burglaries, manipulation of motor vehicles).

The danger potential is constantly growing: According to the market research company Gartner, 8.3 billion networked devices were in use in 2017 - 31 per cent more compared with the previous year. It is estimated that this number will have risen to 25 billion devices in the year 2020 (machines, vehicles etc.). This figure does not include smartphones, tablets and computers. According to Gartner, 5.2 billion networked devices were used by consumers and 3.1 billion by enterprises.[56]

With regard to the end consumer segment, Gartner expects the largest growth in the field of networked vehicles (also in connection with autonomous driving) - in addition to smart TVs and digital set-top boxes. The related possibilities are manifold, ranging from automatic damage reports and internet-based navigation up to data interchange with third parties like insurance companies. With regard to enterprises, Gartner expects the largest growths in the field of smart electricity meters and surveillance cameras.

Gartner expects that a five billion EUR black market for forged sensors and video data, which might be used by perpetrators, will develop until 2020. The IoT makes available information on geo location, temperature, air pressure, light conditions, presence or absence of persons, identities of persons, changes in the surroundings etc.

[53] **Https://www.heise.de/security/meldung/Satori-Botnetz-hat-es-auf-Ethereum-Miner-abgesehen-3946840.html.**
[54] **Https://www.heise.de/security/meldung/Hide-n-Seek-IoT-Botnetz-mit-Spionage-Skills-3950938.html**.
[55] **Https://www.heise.de/security/meldung/OMG-Botnet-macht-aus-IoT-Geraeten-Proxys-3982037.html.**
[56] **Https://www.gartner.com/newsroom/id/3598917.**

5.3 INDUSTRY 4.0

The growing interconnectivity of machines and devices and the increasing tendency towards electronic and web-based command-and-control processes result in a higher threat potential in this area. Companies become more dependent on a well-functioning information technology and are therefore likely to remain in the focus of cybercriminals.

Since attacks on IT infrastructures of companies meanwhile not only disrupt communications but rather involve the risk of a total production standstill, the losses incurred as a result of such cyberattacks are likely to increase as well. In the light of the developments described above, it may well be assumed that the number of malware attacks on companies will rise even further.

5.4 ARTIFICIAL INTELLIGENCE

Automation of intelligent behaviour and machine learning as well as their commercial use continue to gain importance. These developments are also observed by cybercriminals. The worm-style propagation of malware is an indication that malware-based cyberattacks are committed in an increasingly professional manner. The integration of intelligent and self-learning vulnerability scanners additionally promotes the independent, worm-style propagation of malware.

From the police perspective, forecasts concerning technical innovations and their potential for misuse should, in principle, be subject to cautious appraisal. Nevertheless, concrete experience gained in previous years suggests that the above-described trend towards a growing professionalization of cyberattacks will continue in 2018.

This is reinforced by the fact that artificial intelligence offers more opportunities for cyberattacks than for cyberdefence - a view also shared by the G4C.

6 Overall Assessment and Outlook

In 2017, the case figures in the field of cybercrime have risen at a moderate rate. Estimates regarding unreported and unrecorded crime and recent research results underline the high threat and damage potential emanating from cybercrime. The growing importance of information technology for companies, authorities and the private sector boosts possibilities for manipulation and attacks. Current technology trends open up new opportunities for crime and are likely to aggravate the threat situation even further.

Continuous increase in quantity and quality of cyberattacks.

Police investigative results also suggest that cybercriminals are becoming more and more professional by reacting flexibly to current technical framework conditions. Today, cybercriminals no longer confine themselves to committing offences in the digital space but also offer malware to facilitate the commission of crimes, or even entire technical infrastructures, through the underground economy on the internet. Due to their easy handling, these tools also make it possible for perpetrators without specialised and sound IT knowledge to commit offences via the internet. Consequently, more and more perpetrators without specific expertise are enabled to acquire the know-how required to commit such offences and to buy relevant tools. The spectrum of potential perpetrators is broadening accordingly. For this reason, the quantity and quality of cyberattacks are generally expected to increase.

The supposed anonymity offered by the darknet makes this part of the internet especially attractive for perpetrators. This also applies to organised crime groups. In general, cybercriminals have been found to act on the basis of a division of tasks. For a successful fight against cybercrime, law enforcement authorities should therefore pay special attention to the fact that crimes might be committed in an organised way.

There is an imbalance between the extent of damage and the potential punishment.

In the context of cybercrime, there are fields of criminal activity in which the extent of the damage and the potential punishment appear to be marked by an imbalance. This concerns, for example, the operation of illegal sales platforms of the underground economy or the creation and operation of botnets, e.g. for the purpose of staging DDoS attacks to the detriment of companies or critical infrastructures. At international level there is a need to take action, e.g. to establish a co-ordinated legal framework for collecting electronic evidence from internet service providers, which are often based abroad and store data in other countries. As the location of data can change any time due to cloud algorithms, legal assistance measures to collect data of use as evidence cannot always be carried out effectively.

The close, even institutional, co-operation between security authorities and the business community – another core element of a successful fight against cybercrime – is of particular significance. A holistic approach to prevention and suppression of cybercrime in a national (e.g. Joint Cyber Defence Centre) and international context (e.g. Europol, Interpol) is indispensable, not least because the vast majority of cybercrime cases fall within the scope of transnational crime.

Repeated large-scale thefts of data and the fact that every single user is affected on a daily basis, e.g. by spam e-mails, involve the risk that users become less aware of the imperative need to take their own preventive measures to protect themselves. In this regard, mobile terminal devices are an especially important issue since users often neglect their protection. The current developments in the synthetic creation of voices or personal identities are suggestive of a high misuse potential of such technologies, for example, in connection with online identity verification or voice-controlled manipulation of smart home systems. For the aforementioned reasons, users of smartphones, tablets and smart home technologies need to be further sensitized.

Publishing information

Published by
Bundeskriminalamt, 65173 Wiesbaden
Last updated in
July 2018
Designed by
Bundeskriminalamt, 65173 Wiesbaden
Picture credits
Bundeskriminalamt
Please visit our website if you wish to download further publications of the Bundeskriminalamt:
www.bka.de/Lagebilder