Bundeskriminalamt

Cybercrime

National Situation Report 2018

Cybercrime - Figures 2018

87,106 cases of cybercrime in the narrower sense (+1,3 %)

271,864 cases of the Internet as an instrument of crime among all offences recorded in the national crime statistic (4.9 % of all offences recorded in the national crime statistic)

723 cases of phishing attacks concerning online banking (-49 %)

EUR 60.7 million losses in the area of computer fraud (2017: EUR 71,4 Mio. million)

13 Organised Crime Groups in the field of cybercrime; 2.4 % of all Organised Crime investigations (2017: 17)

Table of Contents

Gender note:
For reasons of better readability, the generic masculine is used in this situation report.

1 Preliminary Remarks

The statistical part of the National Situation Report on Cybercrime 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 have been changed in the meantime, 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 assumed 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 and 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 quantitatively and qualitatively improved assessment of the situation.

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

2 Presentation and Evaluation of the Crime Situation

2.1 CONDITIONS FOR RECORDING DATA IN THE POLICE CRIME STATISTICS

Cybercrime as a phenomenon distinguishes between cybercrime in the narrower sense and cybercrime in the broader sense. Such a distinction was already made at the Tenth United Nations Congress on the "Prevention of Crime and the Treatment of Offenders" in 2000 and has since been used internationally with individual modifications at judicial and police level in particular.[2]

Cybercrime in the narrower sense refers to all offences that are targeted against the Internet[3], further data networks[4], IT systems[5] or their data. In detail, this includes the following offences defined in the German Penal Code:

- **Computer fraud as cybercrime in the narrower sense** (section 263a of the German Penal Code). As of 01/01/2016, this criminal offence has been broken down into the following types of fraud in the PCS:
  - 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.

[2] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Crimes related to Computer networks, available at: https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf, p. 5.

[3] From a technical point of view, the Internet includes the following services, among others: WWW (webpages, social networks, online shops), e-mail (electronic mail), news (bulletin boards on the Internet), data exchange (FTP, file sharing, etc.), chat (real-time communication via the keyboard), cloud services.

[4] This includes all networks which are not part of the Internet, for instance Intranet, Bluetooth, cross-connects between two end systems.

[5] A self-contained IT device not connected to any network. For instance a stand-alone PC or a USB flash drive.

- **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 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, 202d 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 on digital black markets[6] and 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.

- **Forgery of evidentiary data and/or deception in legal relations** (sections 269, 270 of the German Penal Code) - These offences 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 malware camouflaged as invoices in e-mail attachments.

- **Data manipulation/computer sabotage** (sections 303a, 303b of the German Penal Code) - 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 other persons than the data owner. Sections 303a, 303b of the German Penal Code typically include Denial of Service attacks (DoS/DDoS attacks[7]) as well as the distribution and use of various kinds of malware (Trojans, viruses, worms, etc.).

- **Misuse of telecommunications services** (section 263a of the German Penal Code) - 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 abroad or systematically use premium or value added services.

The 2018 National Situation Report on Cybercrime primarily provides information about the developments in the field of cybercrime in the narrower sense that have come to police notice.

However, the National Situation Report on Cybercrime also contains information on cybercrime in the broader sense, inter alia statistical data on the Internet as an instrument of crime (see chapter 2.5) or the detailed description of the area of digital market places (see chapter 3.8). Cybercrime in the broader sense covers offences in which information and communications technology was used to plan, to prepare or to carry out the offence.

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

[6] Online black markets, frequently on the darknet, used by sellers and buyers to initiate and carry out their criminal transactions throughout the digital world. Also underground economy platforms or darknet markets.

[7] Denial of Service (DoS) attacks target the availability of services, websites, individual systems or 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.

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[8], are, for instance, usually not recorded as cybercrime offences in the PCS but as more serious or specific offences - in this case as extortion.

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 statistical data source in Germany which is based on police investigations. It thus provides a data basis which 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/or 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 when the identity they use in an online shop is stolen) or that the technical devices they use were 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" among 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 vectors or detecting links between offences) but is also the only way to identify and prosecute offenders. The objective must be to identify the originators of cyberattacks and prevent further attacks. The sanctioning of criminal conduct, which is only possible when the facts of the case become known, could also have a deterrent effect on potential offenders.

[8] 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.

2.2 CASE NUMBERS CYBERCRIME

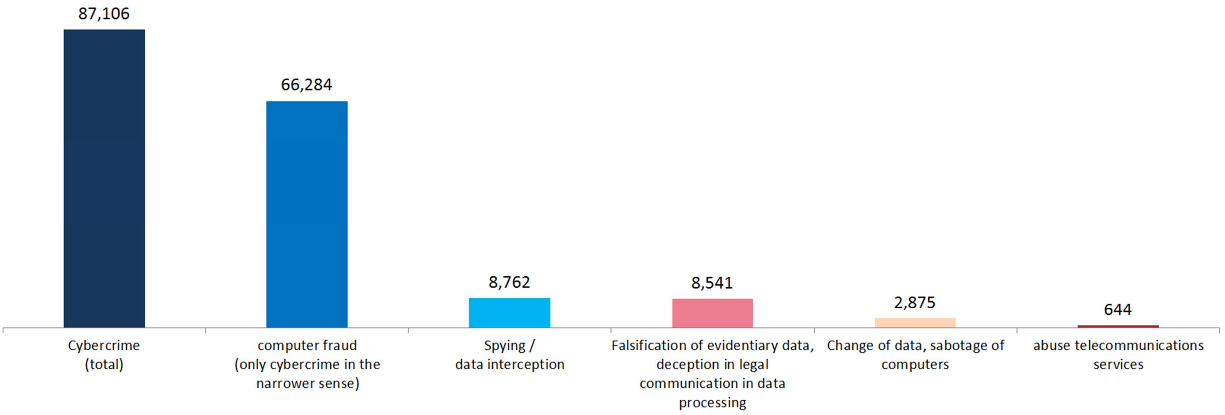
The year 2018 witnessed another increase in the number of offences attributed to cybercrime in the narrower sense. The PCS showed a total of 87,106 offences. This represents a rise of 1.3% compared to the previous year (2017: 85,960 offences). The clear-up rate was 38.9%, which represents a decrease of 1.4% compared to the previous year.

Three quarters of all offences were recorded as computer fraud cases. In 2018, there was an increase of 3.7% in this field of criminal activity. In most of these cases the Internet was merely used as the instrument of crime.[9] These cases are therefore not attributed to cybercrime in the narrower sense. 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 increased by 36.2% to 644 offences in the year under review (2017: 473 offences). The main reason for this is a complex investigation conducted by Oldenburg public prosecutor's office and Osnabrück police station[10] involving numerous (cleared-up) individual cases, which was concluded in Lower Saxony in 2018.

In the field of data manipulation/computer sabotage pursuant to sections 303a, 303b of the German Penal Code, there was a sharp decline of 20.1%. 2,875 cases were recorded (2017: 3,596 cases).

Cases of Cybercrime in the Narrower Sense (2018)



[9] For instance obtaining goods or services by fraud through the following simple method: When attempting to acquire goods or services through the Internet, the fraudsters fail to pay the goods/services purchased.

[10] The suspect gained access to so-called FRITZ! Boxes through the Internet and programmed call forwarding to national and international premium rate numbers. Subsequently, call forwarding was activated automatically so that chargeable connections were made from the router/subscriber's line that had been tampered with. Disguising his real identity, the suspect "rented" the previously programmed national and international premium rate numbers and obtained part of the telephone fees incurred. A loss of approx. EUR 60,330 was identified. The real loss caused is in all probability much higher.

Owing to its high level of development and know-how (in particular with regard to the economy), Germany continues to be an attractive target for cybercriminals:

According to a 2018 study report by the "Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (bitkom)" (German Association for Information Technology, Telecommunications and New Media) on "Espionage, Sabotage and Data Theft - Economic Security in the Industry" (survey of 503 industrial enterprises with at least ten employees, representatively selected according to sector and size), 68% of the industrial enterprises had been victims of data theft, industrial espionage or sabotage during the last two years. A further 19% were probably affected - in these cases, it was not possible to establish beyond doubt if data were actually tapped, or if an attack was not detected.[11]

In a spring 2018 Forsa survey on "Cyber Risks and the German Small and Medium-sized Businesses" (representative survey of 300 decision-makers at small and medium-sized businesses), 30% of the respondents stated they had already suffered economic losses caused by cyberattacks. Approximately three quarters of the respondents reported to have experienced these attacks during the last two years.[12]

For the "Allianz Risk Barometer 2019", more than 2,000 persons from different industrial and economic sectors were surveyed in 86 countries. 37% of the respondents considered "cyber incidents" (cybercrime, IT failures, data breaches[13], etc.) to be the top business risk.[14]

The mentioned 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.

2.3 SUSPECTS

In 2018, a total of 22,051 individuals suspected of cybercrime were recorded. Compared to the previous year, this is a decrease by 1.1% (2017: 22,296 suspects). 67.1% of all suspects were male, 32.9% were female.

What is striking is that female suspects are over-represented in the field of cybercrime in the narrower sense in relation to the total offences (24.87%). The criminal offence of computer fraud, primarily the obtaining of goods by fraud, is the decisive factor for this. This offence type has high case numbers and a high percentage of female suspects (computer fraud pursuant to section 263a of the German Penal Code – female suspects: 34.4%; obtaining goods by fraud pursuant to sections 263, 263a of the German Penal Code – female suspects: 33.6%). With respect to cybercrime offences with lower case numbers, the percentage of female suspects is almost identical with the percentage of the total number of offences (e.g. data espionage, interception of data, handling stolen data pursuant to

[11] Wirtschaftsschutzstudie 2018 (2018 Study on Economic Security), available at: https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf, p. 14.

[12] Cyberrisiken im Mittelstand. Ergebnisse einer Forsa-Befragung Frühjahr 2018 (Cyber Risks in Small and Medium-sized Businesses. Results of a spring 2018 Forsa survey), available at: https://www.gdv.de/resource/blob/32708/d3d1509dbb080d899fbfb7162ae4f9f6/cyberrisiken-im-mittelstand-pdf-data.pdf, p. 3.

[13] A data breach is the intentional or unintentional release of sensitive data to an untrusted environment. Please find more detailed explanations on data breaches from page 14 onwards.

[14] Allianz Risk Barometer. Top Business Risks for 2019, available at: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf, p. 4.

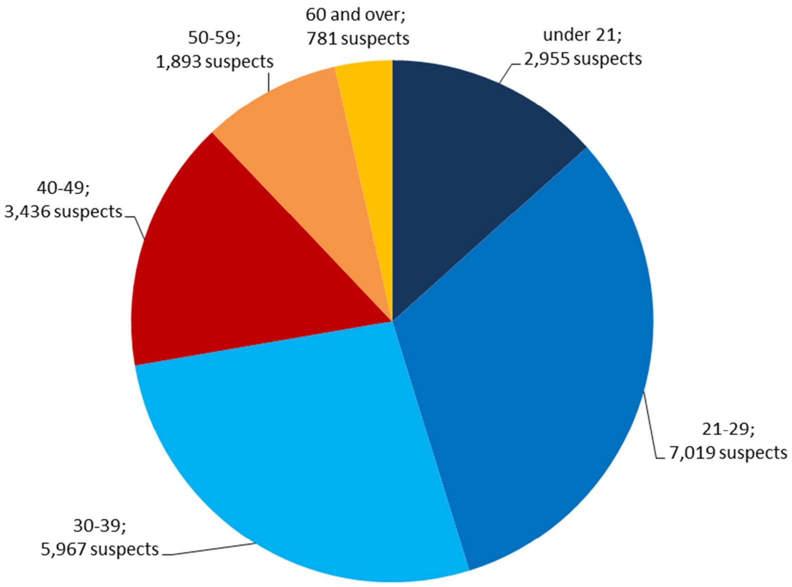
sections 202a-d of the German Penal Code: 25.6%), or is even lower (e.g. data manipulation, computer sabotage pursuant to sections 303a, b of the German Penal Code: 22.3%).

In 2018, 16,832 identified suspects (76.3%) were German nationals. 5,219 suspects were non-German nationals; Turkish (13.5%), Romanian (9.7%) and Nigerian (8.7%) nationals were most heavily represented. While obtaining goods by fraud accounts for the high percentage among Turkish and Romanian nationals, Nigerian nationals are particularly represented in the context of computer fraud using unlawfully obtained other non-cash means of payment.

The private security provider FireEye says in its analysis that only a few states (China, Russia and North Korea) were behind the majority of government-controlled cyberattacks initiated around the world.[15] These states are under-represented with regard to the suspects mentioned in the PCS (Russia: 131 suspects, China: 24 suspects, People's Republic of Korea: 0 suspects).

More than half (58.9%) 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 (2018)



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).

[15] Die Hackergruppen hinter Advanced Persistent Threats (The hacker groups behind Advanced Persistent Threats), available at: https://www.fireeye.de/current-threats/apt-groups.html

2.4 ORGANISED CRIME

Cybercrime is also of importance when it comes to combating organised crime (OC). In 2018, 13 of the altogether 535 registered OC groups were recorded in the area of cybercrime (2017: 17 OC groups).

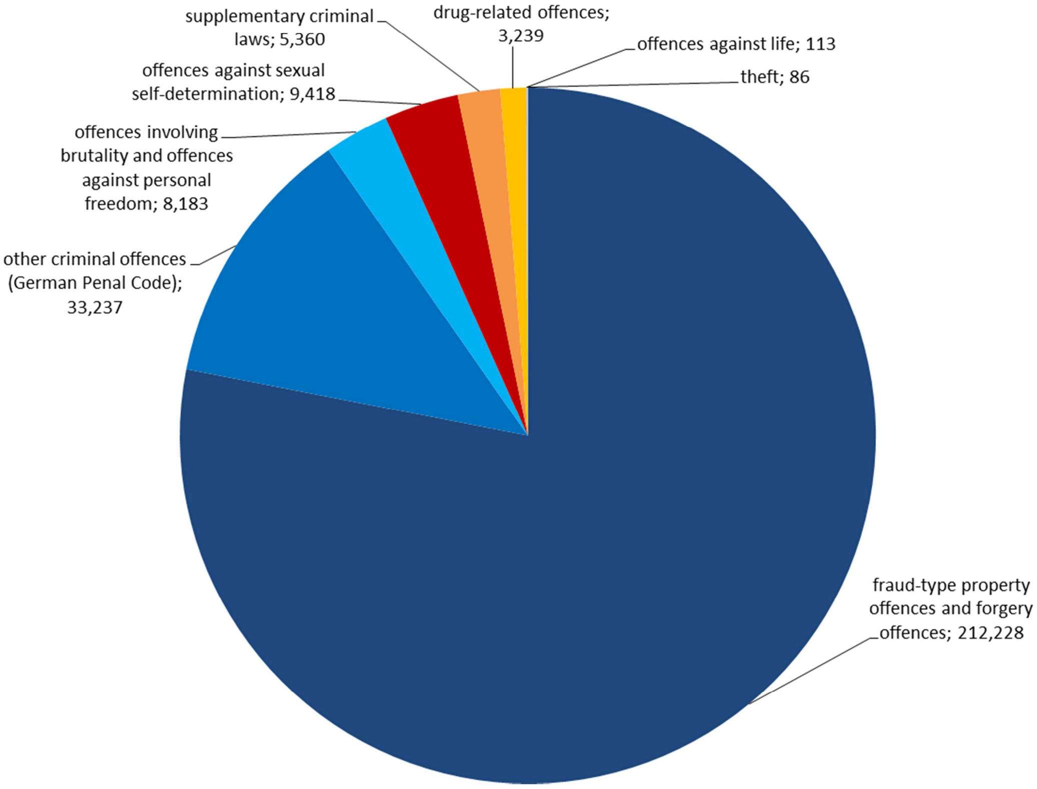
The offences they committed did not differ from those carried out by lone offenders or loose networks. OC groups also committed typical cybercrimes, ranging from computer fraud and attacks on online banking to the distribution of ransomware for digital extortion.

2.5 THE INTERNET AS AN INSTRUMENT OF CRIME

In 2018, a total of 271,864 offences were recorded in the PCS, for which the Internet had been used as an instrument of crime. This represents an increase of 8.1% compared to the previous year (2017: 251,617 cases).

The PCS special designation[16] "Internet as an 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 loose contact between offenders and victims via the Internet prior to the actual offence.

The Internet as an Instrument of Crime - Distribution by Fields of Criminal Activity (2018)



[16] Special designations are characteristics which can additionally be selected in the PCS when recording a crime. Certain PCS-relevant forms of crime are marked with special designations.

In 2018, 75.7% (205,735 cases) of all offences where the Internet was used as an instrument of crime were fraud offences (2017: 74.4%; 183,529 cases). These included 154,773 offences of fraudulent failure to supply goods as agreed and/or obtaining goods by fraud (2017: 134,476 offences), where suspects offered goods for sale on the Internet but provided only inferior-quality items or none at all, or offences, in which suspects ordered goods and did not pay for them.

3 Phenomena in the Field of Cybercrime

The theft of digital identities is a starting point and a „fuel“ of a large number of criminal utilisation models of cybercrime.

The quality and quantity of DDoS attacks has increased.

Cybercrime-as-a-Service enables a wide range of users to commit cybercrime offences without in-depth technical knowledge..

Ransomware was increasingly used to blackmail medium-sized enterprises.

Malware, which downloades further malware, enables the customized misuse of compromised target systems

3.1 THEFT OF DIGITAL IDENTITIES / ID THEFT

The misuse of a natural person's personal data by a third party is still a common and lucrative business model.

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),*
- *job-related information (e.g. for the purpose of online access to a company's internal technical resources),*
- *e-government (e.g. electronic tax return) and*
- *cloud computing (use of storage space, software or computing performance offered as a service).*

All data and/or forms of digital identities that can be used for criminal activities are interesting for cybercriminals. In most cases, the perpetrators have financial motives – e.g. goods are ordered from online shops by using the name and address of the victim (obtaining goods by fraud), paid streaming services are booked by means of stolen identities or mobile phone contracts are unlawfully concluded.

Fraud offences in connection with online banking by the use of stolen data continue to be of great significance in the field of cybercrime – see 3.2 for further details.

The so-called criminal personification aims to steal the victim's identity in order to use it in the future to make false pretences or to damage the victim's reputation by misusing his/her name. Moreover, mobbing and stalking are often related to identity theft.

In many cases, identity theft is the starting point for further cyber offences. According to Link11, a member of G4C (German Competence Center against Cybercrime e. V.), cloud servers have gained in importance with regard to DDos attacks. For instance, "stolen" names and e-mail addresses can be used to create false cloud accounts, which are then used for such attacks. E-mail addresses are used for sending mass spam mails, for example, in order to initiate the dissemination of malware/ransomware.

The perpetrators gain access to the data, e.g. by phishing mails, by using malware (spyware[17], Trojans[18] and keyloggers[19]) or by social engineering where the perpetrators deliberately influence people on an interpersonal level for the purpose of evoking a specific behaviour (particularly in the field of CEO fraud[20]).

Through data leaks in companies, a high number of digital identities enter the "cyber market" and can then be used by the perpetrators. In its report entitled "The State of IT Security in Germany 2018", the Federal Office for Information Security (BSI) states that the use of personal information found in data that has been stolen from large service providers, contacts from e-mail clients in infected systems or researched data is being observed more and more frequently.[21]

Due to the advancing spread of digital technology and the growing use of social networks, "stealing" digital identities is increasingly becoming easier for cybercriminals.

The BSI also states that, in March 2018, criminals sent mass bogus messages in Facebook Messenger, which contained a link to an alleged YouTube video. The link went to a bogus Facebook login page, however. As soon as a user entered his or her login details, the criminals, who were behind the bogus messages, were able to intercept these details and to gain complete access to the victim’s account.

Another method to get into possession of digital identities is the so-called war driving. The perpetrators actively search for unprotected WiFi networks with a view to intercepting the data of all computers connected to the WiFi router.

FORMJACKING

In 2018, the modus operandi of "formjacking" also became increasingly significant. In this context, malicious codes are integrated on websites of online shops. These codes are mostly small but heavily disguised JavaScripts. When customers enter their payment details in an online form to carry out an online purchase, these credit card details are not only passed on to the retailer but also directly to the cybercriminal.

According to the G4C member Symantec, more than 3.7 million formjacking attacks on so-called endpoints were blocked in 2018. Reportedly, known websites, e.g. of ticket shops and airlines, were

[17] This is a neologism created from the words "to spy" and "software". Spyware is a software program designed to secretly gather information about a user and/or the use of a computer and forward it to the creator of the spyware. Spyware is often only found to be annoying; however, it should not be ignored that spyware can also spy out security-relevant information, such as passwords.

[18] 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.

[19] A keylogger is hardware or software designed to record the keystrokes on a 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.

[20] Within the framework of the CEO fraud scheme, perpetrators use false identities to make company employees transfer money to accounts controlled by the perpetrators.

[21] Die Lage der IT-Sicherheit in Deutschland 2018 (The State of IT Security in Germany 2018), available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, p. 46.

also affected.[22] In total, the said IT service provider detected an average of about 4,800 websites compromised by formjacking every month. The majority of these attacks were identified, inter alia, in November/December 2018.[23] Using this modus operandi, the cybercriminals obviously made the targeted attempt to earn illicit profits from the "Black Friday" and/or the Christmas shopping season.

DATA BREACHES

In 2018, various data breaches causing considerable damage were detected.

Data breaches:

The term "data breach" covers both the intentional and unintentional release of sensitive data to an untrustworthy circle of persons. Thus, it includes both "leaks" (technical data leaks) and "intrusions" (active capture, interception or extraction 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.

According to IOCTA 2018 (Internet Organised Crime Threat Assessment) published by Europol, organised crime groups are generally responsible for 50% of the data breaches. Furthermore, a total of 76% of all attacks were financially motivated.[24]

In March 2018, the Spanish police, with the support of EUROPOL, arrested the head of a group of perpetrators who are said to have attacked banks with malware for almost five years since 2013. In this connection, the perpetrators addressed phishing mails with malicious attachment to bank employees. As soon as an employee opened them, the software was automatically installed on the server of the bank so that the perpetrators had access to numerous accounts and cash dispensers. The software had become known under the names Carbanak and Cobalt and caused a loss of up to ten million EUR per attack.

[22] Symantec Internet Security Threat Report (ISTR), Volume 24, February 2019, available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, p. 14.

[23] Ibid., p. 47.

[24] Internet Organised Crime Threat Assessment (IOCTA) 2018, available at: https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf, p. 22.

Also in March 2018, the fitness app „MyFitnessPal“ of the US company Under Armour is said to have been the target of a data breach affecting up to 150 million users. Reportedly, user names, e-mail addresses and passwords were stolen.[25] Similar attacks were made on Facebook accounts in October 2018, with profile information of about 30 million users being intercepted.[26]

The data breach at British Airways in August 2018 illustrates that the travel business is a popular target, too. According to information provided by the airline, the data of about 380,000 credit cards were stolen when passengers were booking tickets via the website and the app of British Airways. Personal and financial details were affected; passport and travel details were not affected.[27]

According to IOCTA 2018, the Yahoo data breach in 2013 has so far been the world's largest attack of this nature. Reportedly, all 3 billion customers were affected by the interception of names, e-mail addresses and passwords.[28]

DOXING/DOXXING

In principle, doxing/doxxing is not a new phenomenon. In the past, this form of data disclosure was used on several occasions in order to influence "persons holding other views". Examples for this are the so-called outing, i.e. the public disclosure of information on the political opponent in the field of politically motivated crime as well as the public disclosure of the names of activists who engage in the fight for human rights and are confronted with malicious campaigns against their person following such disclosures.

Deletion of data once published on the Internet is nearly impossible.

Doxing / Doxxing:

The term "doxing" or "doxxing" refers to the Internet-based collection and subsequent disclosure of personal data, mostly with illegitimate intentions to the detriment of the persons affected. "Doxing" is an abbreviation for "document tracing" or "docs tracing" and was derived from "docs".

Possible motives of the perpetrators are, inter alia, the de-anonymisation or the mere public humiliation and harassment of people.

Based on the data disclosed, further attacks or offences to the detriment of the persons concerned can follow.

[25] Hacker stehlen Daten von 150 Millionen Nutzern (Hackers steal data of 150 million users), available at: https://www.spiegel.de/netzwelt/apps/myfitnesspal-hacker-stehlen-daten-von-150-millionen-nutzern-a-1200644.html, published on 03/03/2018.

[26] Hackerangriff auf Facebook. Detailreiche Informationen ausspioniert (Hacking attack on Facebook. Detailed information spied out), available at: https://www.tagesschau.de/wirtschaft/facebook-datenpanne-103.html, published on 31/10/2018.

[27] Datenpanne bei British Airways (Data breach at British Airways), available at: https://www.tagesschau.de/wirtschaft/datenpanne-british-airways-101.html, published on 10/07/2019.

[28] Internet Organised Crime Threat Assessment (IOCTA) 2018, available at: https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf, p. 22.

As of late 2018, this phenomenon came again into the focus of public attention, when private information on various politicians and other public figures was made available to the general public on the Internet. Complete deletion of data once published on the Internet is difficult or nearly impossible. It is therefore all the more important to protect digital identities, particularly, in order to make it more difficult for cyber criminals to access this kind of "basic material" for subsequent cyber offences.

An example: Doxing/Doxxing

Between 01/12/2018 and 03/01/2019, perpetrators using several online identities published private information on various politicians and other public figures in social networks, mainly via "Twitter". They did so by means of website links leading to various data storage systems, which stored information on the persons concerned in text files (inter alia names, telephone numbers, addresses, e-mail addresses). A large number of these generally accessible text files contained further links for the download of files, such as passport copies, invoices, account statements, contents of social networks used by the persons affected as well as private and business correspondence. This cyberattack affected a total of about 1,000 active and former politicians at EU, Federation, Länder and local level and other public figures (e.g. journalists) directly as well as numerous further persons indirectly (e.g. by published address memories).

On behalf Frankfurt am Main public prosecutor general's office, central office for combating Internet and computer crime (ZIT), the BKA took over the central investigations conducted on suspicion of spying out data, handling stolen data and violation of the Federal Data Protection Act. Within the framework of these investigations, a 20-year-old German suspect was identified and provisionally arrested. During his interview, the suspect made a full confession with regard to the charges preferred against him. According to his statement, the person charged had obtained the personal data via open sources or the affected persons' e-mail and social media accounts to which he had gained access.

Brief assessment:
The modus operandi used by the perpetrator shows how easy it can be to obtain personal data on the Internet and to misuse them. The person charged is not considered to be a fully skilled hacker, who exploited specific technical vulnerabilities or used special techniques/technologies to obtain personal data or take over accounts of the persons affected. Instead, his modus operandi was based on defrauding people by social engineering. He also exploited individual security deficits, which the later victims cannot always be held accountable for. For instance, he used recovery e-mail addresses[29], which had been deleted before and had become available again. The commission of such offences does not require special knowledge but, if at all, thorough research.

This case also illustrates the high importance users should attach to protecting their digital identities. The following measures are considered suitable to render identity theft more difficult: regular updating of the software used, two-factor or multi-factor authentication for accessing accounts and platforms as well as the use of complex passwords or password managers.

[29] Recovery e-mail addresses are indicated by users on various online platforms to restore an account. In case the log-in on a platform is not possible in the usual way for various reasons, the recovery e-mail address can, for instance, be used to reset the password for this platform.

3.2 PHISHING LINKED WITH ONLINE BANKING

Besides the mass theft of digital data, phishing linked with online banking remains a common form of digital identity theft. In a world of a growing spread of digital technology it is common to make everyday business transactions online. This increases the vulnerability to attacks by cybercriminals.

723 phishing cases were reported in 2018, which represents a decrease by almost 50% compared to the year before. Thus the trend observed in 2017 continued. In that year the number of cases had decreased by 35% compared to 2016.

According to the German Competence Center against Cybercrime e. V. (G4C), the number of such crimes that go unreported can be regarded as rather low because the standard procedures of banks only allow reimbursement in cases where customers filed a criminal complaint. During the first half of 2018, the G4C member Commerzbank observed that malware was hardly used for phishing attacks linked with online banking. Instead, the focus was rather placed on "classical phishing", i.e. the interception of login data for online banking by contacting the victims by e-mail and tricking them into disclosing these data. During the second half of 2018, the number of phishing cases by the use of malware rose again –such activities, for instance in connection with the malware Trickbot, were identified in Germany, too.

A further form of phishing in the context of online banking is the so-called SIM swapping or SIM jacking. This is an "account take over" where the perpetrators have a target's phone number transferred to a SIM card held by the attacker.[30] In order to obtain a SIM card with the victim's phone number from the respective telecommunications provider, the perpetrators often collect the necessary data of the potential victim beforehand by using various methods (e.g. phishing, social engineering)[31]. The SIM card with the victim's phone number then allows the perpetrators to assign new passwords for the victim's accounts held with some providers (e.g. on E-commerce platforms or banking apps).[32]

Phishing linked with online banking remains a lucrative field of activity for cybercriminals.

In early 2019, a group operating throughout Germany was dismantled. Since 2018, the group had illegally obtained online access data of customers of various banks, asked for substitute SIM cards and had these cards activated, thereby replacing the legitimate SIM cards. This also enabled the perpetrators to have the transaction numbers (TAN) required for online transfers send to them and to obtain more than 1.5 million EUR by providing false account details.[33] A similar

[30] SIM Swapping: Wie Hacker Millionen via Mobilfunkanbieter stehlen konnten (SIM swapping: How hackers stole millions worth of crypto via victim's telecoms operator), available at: https://de.cointelegraph.com/news/sim-swapping-how-hackers-stole-millions-worth-of-crypto-via-victims-telecoms-operator, published on 19/08/2018.

[31] E.g. bank and credit card details, SIM card provider of the victim, etc.

[32] Wave of SIM swapping attacks hit US cryptocurrency users, available at: https://www.zdnet.com/article/wave-of-sim-swapping-attacks-hit-us-cryptocurrency-users/, published on 03/06/2019.

[33] Joint press release by Verden public prosecutor's office and Hanover police directorate: Strafverfolgungsbehörden zerschlagen bundesweit operierende Bande von Online-Betrügern (Law enforcement authorities dismantle a gang of online fraudsters operating throughout Germany), available at: https://www.staatsanwaltschaft-verden.niedersachsen.de/startseite/aktuelles/presseinformationen/gemeinsame-presseinformation-der-staatsanwaltschaft-verden-und-der-polizeidirektion-hannover-

modus operandi is the misuse of the so-called pushTAN method, which is used, inter alia, for the mobile online banking service rendered by the German savings banks (Sparkasse).[34] The perpetrator spies out the personal data of the victims and contacts the service centre of the savings bank. Providing the personal details of the respective victim, the perpetrator has the phone number for the TAN process changed so that he receives the pushTAN on his smartphone with the new destination phone number via the savings bank's app. By means of this pushTAN, money transfers can be made without additional devices or contacts.

According to the Federal Office for Information Security (BSI), online banking is no longer confined to PCs but is increasingly done with mobile devices, such as smartphones or tablets.[35] In addition to the apps offered by the large banks, there are also free multibank-capable apps which allow customers to manage accounts held with various banks. These banking apps are often combined with a second application, the so-called TAN app. This app generates a transaction number to secure the transaction made via the banking app.

In Germany, no actually successful technical attacks on mobile banking apps have been identified to date.[36]

As many users underestimate the need for protection of mobile devices, these are increasingly targeted by attackers. The perpetrators try to lure smartphone users to bogus websites with prompts via manipulated apps, e-mails, chats or text messages with a view to intercepting passwords, banking TANs or credit card numbers.

strafverfolgungsbehoerden-zerschlagen-bundesweit-operierende-bande-von-online-betruegern-176733.html, published on 26/04/2019.

[34] TAN-Verfahren. Mit pushTAN, smsTAN und chipTAN Aufträge sicher freigeben (TAN procedure. Make secure transfer orders with pushTAN, smsTAN and chipTAN), available at: https://www.sparkasse.de/service/sicherheit-im-internet/tan-verfahren.html.

[35] Die Lage der IT-Sicherheit in Deutschland 2018 (The State of IT Security in Germany 2018), available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, p. 19.

[36] According to the G4C member Commerzbank.

3.3 MALWARE / MALICIOUS SOFTWARE PROGRAMMES

Malicious software programmes (malware)

Malicious software programmes perform unwanted or harmful functions on information technology systems. The dissemination and use of malware on the victims' systems is the key basis of cybercrime.

The most frequent dissemination channels of malware are attachments in spam mails and infections caused, unnoticed by the users, when they visit prepared websites (drive-by-infection). To an increasing extent, malware is disseminated wormlike. Professionalisation in this field is shown, inter alia, by the fact that malware automatically recognises vulnerabilities.

Cybercrime has become a mass phenomenon, primarily because of widely disseminated malicious software.

According to information provided by the Federal Office for Information Security (BSI), with reference to the findings of the security company AV-Test, the total number of malware variants identified has already more than doubled in the years 2014 - 2017 (concretely: 2014: 326.04 million; 2017: 719.15 million malicious software programmes).
For 2018, a total number of malicious software programmes of more than 800 million and an average increase of about 390,000 new variants per day was expected.

In April 2019, the BSI published the results of the cyber security survey carried out by the "Alliance for Cyber Security". According to these results, 43% of the large enterprises interviewed stated that they had been affected by cyber security incidents in 2018. Regarding small and medium-sized enterprises, this value amounted to 26%. 53% of the attacks reported by the enterprises interviewed were described as infections where malicious software programmes intruded into company IT systems.[37]

CRYPTOMINING

Late in 2017/early in 2018, the private sector (especially antivirus service providers, IT security service providers) reported in various publications on an increasing threat by the dissemination of malicious cryptomining software. 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 the computation of cryptocurrencies[38], especially Bitcoin. This has a negative impact on the performance of the

[37] Cyber-Sicherheits-Umfrage –Cyber-Risiken & Schutzmaßnahmen in Unternehmen (Cyber Security Survey – Cyber Risks & Protective Measures in Enterprises), available at: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2018.pdf?__blob=publicationFile&v=9, p. 11.

[38] Alternative designations: virtual, alternative or digital currencies, money or foreign currencies.

compromised systems, which leads to increased electric power consumption and, eventually, to possibly high electricity costs billed to the victims.[39]

Browser-based cryptomining generates, with or without the knowledge of the victim, cryptocurrency for the period of the visit of certain websites. "Intelligent" terminals of the Internet of Things[40] (IoT) are also misused as cryptominers. Even if these devices usually are not so powerful, the cyber perpetrators benefit from insufficient security checks of these devices and from the large number of systems which can be used over longer periods of time.

However, the data recorded by the police authorities hardly list any cryptomining malware cases. The major reason for this probably is that the victims only rarely notice the damage, or notice it only later on, or that they do not suspect any criminal behaviour.

An inquiry with the local police authorities revealed that only 13 cases of cryptomining were reported in the period January 2017 to June 2018. Consequently, the police database did not support the trend of extremely high rates of increase observed by antivirus service providers in this field.

The issue "exploitation of vulnerabilities" remained relevant in the IT sector in 2018. Early in 2018, security scientists discovered severe vulnerabilities on the processors of billions of computers. Reportedly, the vulnerabilities named "Spectre" and "Meltdown" were found also on AMD, ARM and INTEL processors and enable(d) attackers to read out sensitive storage areas. Shortly after the vulnerabilities had been discovered, manufacturers and software designers offered security updates for operating systems and browsers which were to minimise or exclude the risk of, for instance, data tapping through these loopholes. A possible exploitation of the vulnerabilities "Spectre" and "Meltdown" did not manifest itself in an increasing number of cases to be dealt with by the police in 2018.

EMOTET

Early in December 2018, the BSI warned against dangerous malware named *Emotet* which represents an acute threat to enterprises, authorities and private users and had reportedly caused damage in Germany amounting to millions until that date.[41]

An example: *Emotet* malware

In mid-November 2018, the clinical centre in Fürstenfeldbruck in Bavaria became the victim of Emotet. After an e-mail attachment infected with malware had been opened, the about 450 computers of the clinical centre could no longer be used for days. The clinic even had to be logged out of the system of the integrated rescue co-ordination centre of the local rural district.

[39] Executive Summary - 2018 Internet Security Threat Report (ISTR), Volume 23, available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf, p. 1.

[40] Internet of Things; more detailed explanations are given in chapter 5.2.

[41] Gefährliche Schadsoftware – BSI warnt vor Emotet und empfiehlt Schutzmaßnahmen (Dangerous malware - BSI warns against Emotet and recommends protective measures), available at: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/BSI_warnt_vor_Emotet.html, published on 05/12/2018.

An example: *Emotet* malware

Brief assessment:
The incident illustrates the threat posed by *Emotet* and the far-reaching consequences an infection with *Emotet* may have.

The example of *Emotet* shows how the applications of a certain malware may vary in the course of time. At its origin in 2014, the *Emotet* malware was a mere banking Trojan which manipulated the online banking operations of private customers of German financial institutions to initiate fraudulent transactions. Meanwhile, the Trojan has significantly developed in terms of programming. Now, *Emotet* may rather be called a "downloader" or "dropper", its paramount function consisting in the unnoticed primary infection of the attacked system and the subsequent modular download of further malware. This download function of random malware is offered to other groups on a "Crime-as-a-Service" basis for the purpose of disseminating their malware (such as the banking Trojans *Trickbot* or *Dridex*).

Usually, *Emotet* is disseminated by sending out masses of spam mails. These e-mails usually contain either a Word data file, sent as an attachment, or a link which connect to the Internet when being clicked. This connection is used for an effort to download a data file in Word format. When the document is opened and the macro function is activated, the code embedded in the document causes the execution of a command line code (Powershell) and the download of the actual *Emotet* malware causes the installation on the target system. Thereafter, the computer is under the perpetrators' control. Even as a basic version without any additional modules, the *Emotet* malware can unfold the following, penally relevant activities:

- the capturing of information about the target system and the sending of this information to the perpetrators' control server,
- the registration and storage of keystrokes (keylogging).

In addition, the following *Emotet* malware modules available for subsequent download have been identified over the past months/years:

- the *Emotet* banking module for online banking manipulations,
- capture of passwords stored in e-mail programmes,
- capture of passwords stored in web browsers,
- extraction of names and e-mail addresses of the communication partners in e-mail programmes,
- the *Emotet* DDoS module for DDoS attacks.

Furthermore, it was ascertained that, in addition to its own modules, *Emotet* had downloaded malware of other groups, like:

- the *Dridex* banking Trojan,
  a Trojan active primarily in the USA, Great Britain, Switzerland and Germany to manipulate online banking operations of private and business customers (suspected gainful computer fraud).

- the *Trickbot* banking Trojan,
  a Trojan active primarily in the USA and Great Britain to manipulate the online banking operations of private customers (suspected gainful computer fraud).

- the *UmbreCrypt* ransomware,
  a ransomware which encrypts personal data files of the computer user, especially images and documents, and demands ransom money in Bitcoin for their decryption.

- the *Ryuk* ransomware,
  see item 3.4.

Due to permanent modification, the common antivirus programmes often do not recognise the malware programmes in the first instance. According to the BSI, systems once infected generally have to be regarded as entirely compromised and have to be re-installed.

The extent to which Germany is affected by the *Emotet* Trojan can hardly be quantified since, in cases of possible infections, not *Emotet* itself but the malware downloaded subsequently is often identified on the systems concerned. Usually, the *Emotet* malware and/or the respective modules are not downloaded subsequently from the perpetrators' computers but from compromised systems of other server providers. In this connection, systems also in Germany are regularly compromised for dissemination of the malware.

Attacks on ATMs

Logical/digital attacks on automated teller machines (ATMs) are gaining importance even if in a comparatively small number of cases. Malware is used here again. This field of crime generally differentiates between three modi operandi in this respect:

a. Jackpotting (attacks on the data processor/PC of an ATM by the use of malware)

b. Blackboxing (a variety of jackpotting – attacks on the payment module of the ATM by the use of the perpetrators' hardware)

c. Network attack (malware attacks on the card issuing bank or the processing company to manipulate transaction processes; subsequently, a card-bound "cashout" or malware attack on the bank operating the ATM is carried out to gain direct access to the ATMs connected in the network and to carry out a non-card-bound "cashout").

After the attempted use of a certain malware which is sold via the darknet and is to enable even technically less experienced perpetrators to manipulate ATMs and carry out a "cashout" had been ascertained in November 2017 for the first time, already 20 jackpotting attacks of that kind causing a total loss of about 540,000 EUR became known in 2018.

ATMs are increasingly attacked digitally.

In 2018, there were 43 black box attacks, only four of which proved successful. The loss amounted to about 450,000 EUR.

Furthermore, in 2018, there were network attacks on three Asian banks which resulted in a cashout also in Germany. The worldwide loss amounted to about 39 million EUR. Since 2016, an increasing number of network attacks on ATMs, causing, inter alia, losses in the two-digit million range, have been ascertained all over the world. Due to the high "profit expectations" for the perpetrators, a continuing high threat has to be assumed.

An example: Use of malware for ATM cashouts

Since mid-December 2017, the Bundeskriminalamt has been conducting an investigation initiated by the Zentrale Ansprechstelle Cybercrime (ZAC) [Central Point of Contact Cybercrime - CPoCC] (North Rhine-Westphalia) of the Cologne Public Prosecutor's Office for suspected gang-type and commercial computer fraud to the detriment of a major African bank.

The background to the proceedings is the simultaneous misuse of 15 credit cards legally issued in an African country in Germany and in the United Arab Emirates in November 2017. The loss caused by several hundred withdrawals amounted to about 550,000 EUR.

In the course of the investigations, cross-connections concerning the modi operandi and personnel overlaps in the perpetrator structures to another investigation conducted in Germany, also under the governance of the CPoC North Rhine-Westphalia, were identified. The subject of these proceedings are 2,176 cases of misuse of 157 credit cards in February 2017. In this connection, a loss of about 3.1 million EUR was caused to the detriment of another major African bank. At that time, the fraudulent withdrawals were carried out coordinately in Germany, Switzerland, Luxemburg and the Netherlands.

As a result of the investigations, it was proven that the perpetrators had infiltrated the IT infrastructure of the African banks on a permanent basis by infecting several processors with malware variants and deactivating the antivirus software at the same time. By means of an available keylogger functionality, the perpetrators had managed to capture the credentials of staff of the banks to finally gain unauthorised access to the databases required for the withdrawal and accounting processes. By manipulating those very databases, the credit card limits and the number of withdrawals per day had been increased so that the above-mentioned abusive withdrawals had become possible.

Within the framework of the investigations, various suspects of African origin were identified in Germany, France and Switzerland.

In close consultation with the French authorities, executive measures against members of the group, including the execution of an arrest warrant against a target person residing in Germany, were carried out.

Brief assessment:
For the first time, the BKA identified a cyber component with a clearly noticeable link to Africa.

The technical modus operandi (network intrusions, persistent infiltration and subsequent manipulations) can clearly be pinpointed in the field of cybercrime in the narrower sense (also according to the court assessment). The components of the offence (recruitment of "runners" on the African continent for the opening of accounts, procurement of a large number of original credit cards, transport of the instruments of crime to the theatres of operations in Europe and in the United Arab Emirates, recruitment of withdrawers and simultaneous activities of disposal, "cashouts") and the considerable criminal profits obtained as a result indicate internationally organised criminal structures.

3.4 RANSOMWARE – DIGITAL EXTORTION

Usually, the use of ransomware leads to the encryption of data of a digital system and in many cases also to the lockdown of other terminals reachable in a network (for instance, in company networks).

Often, infected systems are completely encrypted and entire networks severely disrupted. Victims who cannot restore their IT infrastructure based on recent backups experience massive negative impacts on or even total disruption of their business operations. In view of this massive potential damage, many victims pay the relatively small ransoms demanded.

In most cases, the perpetrators demand ransom money to be paid in a cryptocurrency. They promise to send the victim a release code, once the ransom has been paid, by means of which they will be able to unlock or decrypt and use the blocked system again.

What forms of ransomware exist?

Generally, one can distinguish between two variants of ransomware:

a) Ransomware that does not encrypt the hard disk, but only blocks user access to the system by manipulation. The most commonly known type is malware that misuses well-known names and logos of security agencies[42] 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 has a far more serious threat potential 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.

From the police perspective, such payment should be discouraged since payments support the ransomware "business", encourage perpetrators to continue committing such criminal offences and, in particular, the payment is no guarantee that the encrypted data will be restored.

Parties concerned can possibly take action against the infection themselves: 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. The BKA expressly supports the strategic goal of this project and has been an official "Supporting Partner" since 29/09/2017.

[42] 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]).

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.

Digital extortion by ransomware has been a frequent phenomenon, both in Germany and worldwide, for some time. After the year 2017 had been dominated by the ransomware waves *WannaCry* and *Petya* (see National Situation Report on Cybercrime 2017), ransomware waves of this dimension were not identified in 2018. Nevertheless, there were targeted ransomware attacks in the year under review which were primarily aimed at enterprises.

In their report entitled "The State of IT Security in Germany in 2018", the Federal Office for Information Security (BSI) found that the threat posed by ransomware continued in 2018 but in smaller dimensions than before. The reasons given for this are the shift and/or supplementation by cryptomining and the perpetrators' concentration on more targeted attacks, circumstances which, however, cause high pressure, above all on enterprises - also in the field of "critical infrastructures" - to avert or confine attacks and to minimise potential damage.[43]

Ransomware attacks are increasingly directed against enterprises.

The G4C member Symantec ascertained a decrease in the whole area of ransomware by 20% for the year 2018 compared to the previous year – but the number of ransomware variants carrying out targeted attacks on enterprises reportedly increased by 12% in the same period. These developments prove an increasing threat to the economy and indicate more targeted and professional action by the cybercriminals who shift their activities to more "profitable" business sectors.[44]

The ransomware community is characterised by increasing professionalism.

The ENISA[45] Threat Landscape Report 2018 still classifies the area of ransomware as a threat, even if the report points out, with reference to several cybersecurity enterprises, that a decrease in the number of ransomware incidents can generally be noticed. According to the report, different or specific sectors have come to the fore as a result of the cybercriminals' specialisation. According to the ENISA report, 85% of the malware attacks on medical devices were ransomware attacks.[46]

GandCrab was first identified in January 2018 as a new malware campaign which remained active over the whole year and posed a worldwide threat even thereafter. The dissemination took place classically via e-mails containing infected attachments, but also via cracked software through to

[43] Die Lage der IT-Sicherheit in Deutschland 2018 (The State of IT Security in Germany 2018), available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, p. 13.

[44] Symantec Internet Security Threat Report (ISTR), Volume 24, February 2019, available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, p. 9.

[45] European Network and Information Security Agency / Europäische Agentur für Netz- und Informationssicherheit.

[46] ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport, p. 100.

exploit kits[47]. In Germany, it was one of the most active ransomware families. The e-mails known so far were addressed primarily to enterprises of which the perpetrators expected higher amounts of ransom money than of private individuals.

However, by reference to the results of examinations of the *GandCrab* ransomware, the IT security service provider Check Point states in its Security Report for 2018 that, owing to the business model "Ransomware-as-a-Service", even "amateurs" profited from this extortion business. According to the report, the actual cybercriminals and the developers of the malware act on the basis of a division of tasks and share the ransom money obtained at a ratio of 60 to 40. Furthermore, Check Point assumes that *GandCrab* infected more than 50,000 networks within a period of two months in 2018 and that the perpetrators demanded ransom money between 300,000 and 600,000 dollars.[48]

The *GandCrab* malware is sent in spam mails containing malicious attachments. These spam mails are camouflaged as application e-mails and contain - packed in a .zip file - a curriculum vitae, an application photo and a cover letter. When the file is clicked, the document pretends "to have been created with an older version of Microsoft Word" and tries to induce the victim to activate active contents of the document via the compatibility mode. As soon as this happens, the malware contained in the .zip file is activated. The Trojan can access the system and encrypt important data.

GandCrab obtains a large quantity of data about the PC of a user, for instance, the user name, the name of the PC, the domain, the keyboard layout and the operating system. Furthermore, the public IP address is stored. For each user, a distinct address under which the amount of ransom demanded by the extortionist and the payment instructions can be seen is generated on a Tor hidden service (a network for the anonymisation of connection data). The amount is adjusted to the respective victim. The criminals use malware versions which are slightly altered every day to render their recognition by antiviral programmes difficult. The application e-mails are, for example, sent under different names and show subject headings which are adjusted in different ways.

The online magazine ZDNet also reported on *GandCrab*. According to their report, the masterminds of this ransomware announced that they were going to abandon their business model "Ransomware-as-a-Service" within one month. Allegedly, the announcement comes from a source from the malware community and seems to be confirmed by a contribution of the actors in a hacking forum. According to its own statements, the group reportedly obtained and already laundered ("legalised") more than 2 billion dollars of ransom money.

In October 2018, it became known that the Romanian police, in co-operation with other states, EUROPOL and the Internet security company Bitdefender, had found the way of decryption for various versions of the ransomware variety of *GandCrab*. The perpetrators responded to this by using a new variety of the malware.

Ransomware finds its way onto the victims' affected processors also through the malware described in chapter 3.3. The *Emotet* malware, for instance, was used to download the *Ryuk* ransomware onto infected computers. In May 2018, the Federal Bureau of Investigation (FBI) published a report according to which *Ryuk* had reportedly been used by unknown cybercriminals since August 2018 to blackmail more than 100 international companies. Within this context, individual Bitcoin

[47] Malicious software programmes exploiting vulnerabilities of programmes installed on the target systems for execution

[48] The GandCrab Ransomware Mindset, available at: https://research.checkpoint.com/gandcrab-ransomware-mindset, published on 13/03/2018.

ransom demands in amounts equivalent to up to 5 million USD were reportedly identified. The victims were reportedly promised a decryption programme in return.

The ransomware encrypts data on network drives and infected file systems, primarily the data classified as sensitive or important by *Emotet* beforehand. The particular aspect of *Ryuk* is that, in addition to the encryption of the important data, all existing backup copies of these data are deleted at the same stroke. Thus, their restoration is rendered much more difficult. The targets chosen by *Ryuk* are different but the attacks concentrate on enterprises with high annual turnovers, in the hope that higher amounts of money can be obtained.

3.5 BOTNETS – MASS REMOTE CONTROL OF COMPUTERS

Even if major botnet architectures like *Avalanche*[49] and *Andromeda*[50] were dismantled in the recent past, botnets play a central role for cybercriminals also in 2018. In addition to computers, an increased number of mobile and "intelligent" terminals[51] of the Internet of Things (IoT) were "pooled together". Especially the IoT offers manifold possibilities for the expansion of botnets.

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/users of the networks receive messages with infected 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.

Further distribution channels are Usenet[52] *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. The numerous devices infected by malicious code are controlled remotely through "command & control" servers without their owners knowing.

Due to the manifold possible uses of botnets (identity theft, DDoS attacks, dissemination of malware/spam mails), the threat posed by them as a central attack resource has not lost its significance.

In its annual report for 2018, the BSI informs that up to 10,000 botnet infections of German systems are registered by security scientists and reported to the German Internet providers through the BSI per day. 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. Reportedly,

[49] Avalanche was dismantled in 2016 by the Verden Public Prosecutor's Office in co-operation with the Zentrale Kriminalinspektion Lüneburg (Central criminal police inspectorate Lüneburg) and international partners.

[50] Intelligent terminals are Internet-enabled everyday devices by which the user or further devices can communicate via the Internet. Intelligent terminals are Internet-enabled everyday devices by which the user or further devices can communicate via the Internet.

[51] Intelligent terminals are Internet-enabled everyday devices by which the user or further devices can communicate via the Internet.

[52] A separate, independent service of the Internet which exists alongside the common World Wide Web.

Microsoft Windows systems are predominantly affected but other operating systems and Android devices are gaining importance for the botnet phenomenon.[53]

The BSI reports further that the infections reported spread over 130 different botnet families in the period under review[54] and that a detailed study of these botnets revealed that the following botnet applications were in the foreground:

- Online banking fraud
- Droppers used for downloads of further malware
- Klick fraud
- Bitcoin mining
- Spam dispatch
- DDoS attacks

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

In 2018, the BKA supported investigations of the US American FBI *against* the masterminds of the *Necurs* botnet. According to the results of these investigations, important parts of the criminal infrastructure are presumably hosted in Germany.

An example: *Necurs* botnet

In August 2018, the *Necurs* botnet was linked to an attack against enterprises of the financial sector. On that occasion, RATs (remote access Trojans) were disseminated. The security company Confense reported that masses of spam mails had been sent purposefully to about 2,700 banks in the course of that attack. The messages were kept very short and simple with a subject line formulated in a general manner. According to Confense, this spam campaign ceased abruptly after it had been detected.

Brief assessment:
Due to its size and its manifold application possibilities (incl. spam mail dispatch, ransomware dissemination, initiation of DDoS attacks), the *Necurs* botnet is assessed as one of the "most dangerous" botnets worldwide. The "Crime-as-a-Service" idea plays an important role also in this field of cybercrime.

According to the US American IT company International Business Machines Corporation (IBM), the *Necurs* botnet consists of up to 6 million bots. It has existed for several years, but becomes active

[53] Die Lage der IT-Sicherheit in Deutschland 2018 (The State of IT Security in Germany 2018), available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, p. 28

[54] Ibid., p. 30.

only occasionally in the course of a year for targeted attacks. To date, millions of spam mails have been dispatched with the use of the *Necurs* botnet. In addition to this primary purpose of use, this botnet is also used to infect processors with ransomware and malware, to initiate DDoS attacks and to capture access data.[55] Firstly, the *Necurs* botnet became known by the dissemination of Trojans like *Dridex* or *Trickbot*, but, secondly, also by the dissemination of ransomware like *Locky* or *Scarab*.

A further example of the multifunctionality of botnets and of the cybercriminals' increasing professionalism in this field is the phenomenon "click fraud" by which the perpetrators have already obtained considerable criminal profits by the use of a large IT infrastructure in Germany:

An example: Botnet – "click fraud"

The BKA was requested for assistance within the framework of investigations conducted by the US American authorities into unknown perpetrators who had committed computer fraud offences to the detriment of the (digital) web industry and its customers by means of click fraud for years.
Acting in accordance with the modus operandi named "Metan fraud scheme" by the US authorities, the perpetrators had offered themselves as an advertising medium for Internet advertisements. After conclusion of an agreement according to which the advertising medium is paid by the number of clicks on adverts posted, the perpetrators rented thousands of servers from a German hosting provider. While a few servers were used for steering and control purposes, the perpetrators installed "browser bots" on most of the other servers which caused countless clicks on the third-party advertisements hosted by the perpetrators.

To conceal that the clicks had been caused by bots, the perpetrators additionally relayed data traffic from malware-infected computers of ordinary users in the USA so that it would appear to the advertising companies that normal end users from the USA had clicked their advertisements.

According to estimates by the US authorities, the total loss amounted to more than 36 million USD in the years 2014 to 2018. The costs of the botnet "set up" by the perpetrators in Germany amounted to approx. 250,000 EUR per month.

Brief assessment:
Click frauds committed by malware-based botnets are no innovation. However, a new aspect of this modus operandi is that the perpetrators used an own botnet, based on rented servers, to generate clicks and that they used the user-PC botnet just as a disguise.

The case illustrates that the existing protective mechanisms of the advertising industry are insufficient. The "Metan fraud scheme" botnet, for instance, has already been active since 2014 and generates enormous profits, despite immense expenses incurred by the perpetrators to set up the botnet in Germany (approx. 250,000 EUR per month).

[55] Necurs Spammers Go All In to Find a Valentine’s Day Victim, available at: https://securityintelligence.com/necurs-spammers-go-all-in-to-find-a-valentines-day-victim, published on 12/12/2018.

3.6 DDOS ATTACKS

DDoS attacks are designed to overload web sites, servers and networks of individuals or organisations of any kind, thus causing a non-availability of services. As hundreds to thousands of systems are required to carry out such an attack, criminals or those who act on their behalf primarily use botnets.

DDoS attacks

When carrying out so-called "Distributed Denial of Service" (DDoS) attacks, bot nets request huge amounts of data from selected servers until the maximum capacity of the attacked systems is exceeded so that they "break down".

The motivation to carry out such attacks vary (monetary interests[56], afflict damage to business competitors, political reasons, etc.). Even though the specific objectives of the criminals vary, their primary intention when carrying out DDoS attacks is to afflict maximum damage to the individuals or organisations that own the attacked systems.

Non-availability of web sites not only results in a loss of business processes and a drastic decrease in sales leading to significant financial losses, but also in a damage to reputation and a loss of trust of business partners and customers. That is why DDoS attacks often cause businesses financial distress: The IT company and G4C member Link11 which specialises on the prevention of DDoS attacks says the loss incurred by a successful DDoS attack might amount to as much as 45,000 EUR. [57]

According to information provided by Link11, DDoS attacks strongly increased in quantity and quality in 2018. Compared to 2017, the number of DDoS attacks carried out in 2018 reportedly increased by 34% and so did the average bandwidth of such attacks from 1.7 Gbit/s[58] to 4.9 Gbit/s which resulted in the fact that attacked services collapsed faster.[59] In 2018, the Link11 Security Operation Centre registered more than 54,000 DDoS attacks on targets in Germany, Austria and Switzerland alone.[60]

DDoS attacks continue to increase in quantity and quality.

In future, DDoS attacks are expected to be carried out against industries and companies in a more target-oriented manner.

The focus of DDoS attacks, too, has changed. Cloud storage providers (such as Amazon) have come into the focus of criminals, be it as a target or as a platform to launch attacks. In 2018, one out of three DDoS attacks was carried out making unauthorised use of cloud servers - that is approximately 80% more than in the year before. The cloud servers were either hacked or, for example, rented under a

[56] So-called "ransom DDoS": Threatening with a DDoS attack to extort the victim

[57] G4C Workshop held on 12 March 2019

[58] Gigabits per second is a unit of measurement that can be used to depict data transfer rates.

[59] G4C Workshops held on 12 March 2019

[60] LINK11 DDoS-Report für die DACH-Region (LINK11 DDoS report covering Germany, Austria and Switzerland), available at: https://www.link11.com/de/ddos-report/

false name with stolen credit card information.

The focus also shifted in respect of intensity and objectives of the criminals. In 2018, DDoS attacks increased by up to 70% on calendar days crucial for online vendors and web marketplaces (e.g., Amazon's CyberMonday or Black Friday).[61] On such days, not only providers (mostly online vendors or trade exchanges) were affected, but also payment providers, such as PayPal, or logistics companies were targets of DDoS attacks. Critical infrastructures and mid-sized businesses were targets of that sort of criminal activities as well. It is to be assumed that, in the future, DDoS attacks will be carried out against specific industries and companies in an even more target-oriented manner.

In 2018, DDoS attacks were mostly carried out in connection with so-called multi-vector attacks. The potential danger results from the fact that not only one attack, but different kinds of several synchronous attacks have to be prevented. In 2018, 59% of all DDoS attacks were multi-vector attacks.

An equally threatening trend in this area is the so-called layer 7 attack. The name refers to the structure of the so-called OSI model[62], a reference model for network protocols consisting of seven layers or levels. The seventh layer of the OSI model is the so-called application layer. This layer provides services for direct user interaction, is often similar to an application programming interface (API) and manages entry, output and validation of data, for example, when a user logs on to an email account.

While conventional DDoS attacks often target a network or system as a whole, a layer 7 attack merely overloads the application programming interface of a web site or service, thus causing a "collapse" of such web site or service. This type of attacks attracts cybercriminals, as fewer resources (and thus fewer systems within a bot network) are required to overload the system under attack. Moreover, this kind of attacks is hardly identified as "bot attacks", as their behaviour (use of legitimate network queries) appears unsuspicious.[63]

[61] LINK11 DDoS-Report für die DACH-Region (LINK11 DDoS report covering Germany, Austria and Switzerland), available at: https://www.link11.com/de/ddos-report/

[62] Open Systems Interconnection model

[63] Defending against Layer 7 DDoS Attacks, available at: https://blog.verisign.com/security/defending-against-layer-7-ddos-attacks/, published on 29/09/ 2016

An example: Webstresser

In April 2018, the biggest marketplace for DDoS attacks called "Webstresser" was decommissioned following a coordinated operation of law enforcement/prosecution authorities in the Netherlands, UK, Serbia, Croatia, Spain, Italy, Germany, Australia, Hong Kong, Canada, and the USA in cooperation with EUROPOL. In such a "DDoS-for-hire" market place customers can rent a botnet and launch DDoS attacks on web sites without having any technical computer knowledge, since the target can be selected in a web interface.[64] The infrastructure of the service was hosted in Germany, in the Netherlands and in the USA.

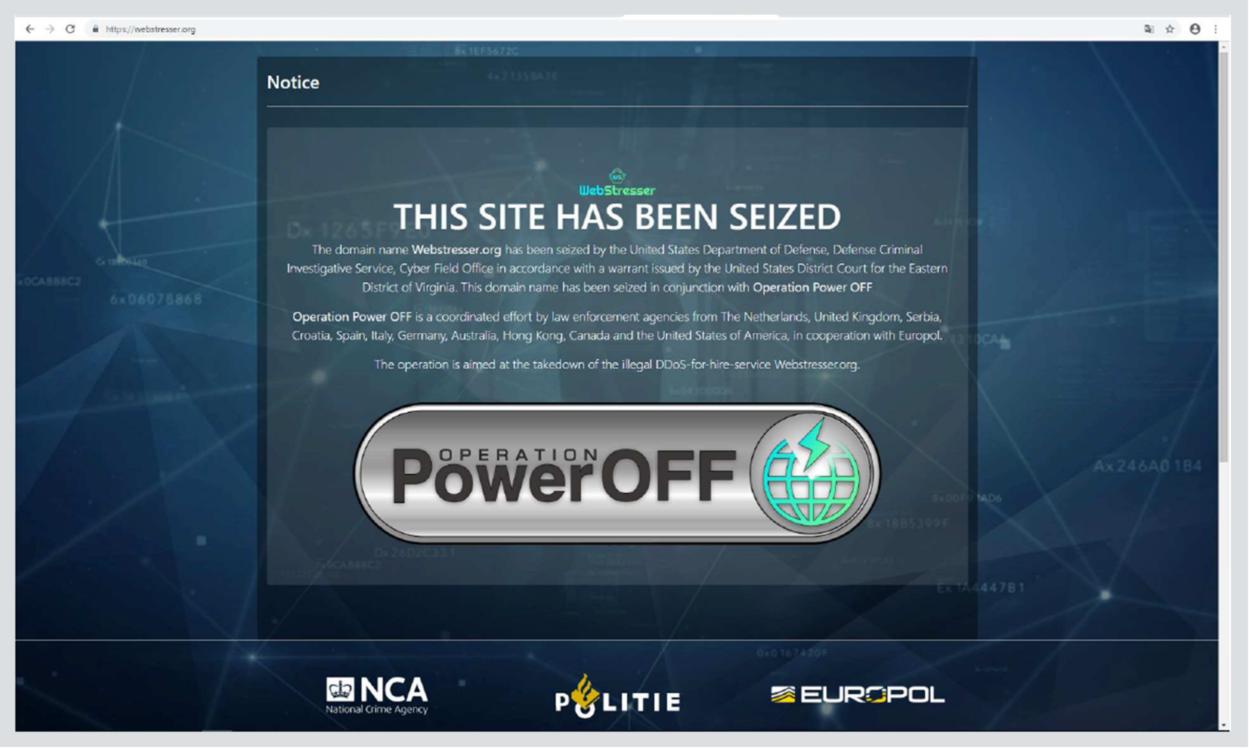
The "Webstresser" server was hosted by a known German data centre in Frankfurt. As part of operational measures the server was seized and the administrators of "Webstresser.org" were arrested on 24 April 2018. In addition, more than 250 users of this DDoS attack platform will now have to stand trial.

Launched in 2015, "Webstresser.org" originally was a minor service which evolved over the years to become the biggest "DDoS-for-hire" marketplace worldwide. There were approximately 151,000 registered "Webstresser" users. By April 2018, four million attacks were reportedly launched via this platform, aimed mostly at government bodies, banks, police authorities and the games industry. Attacks could already be launched for a fee of 15 EUR.

Brief assessment:
Due to the fact that administrators, users, victims and the infrastructure were located in different countries, good international police cooperation was of the essence for a successful criminal procedure against the persons charged.

After the portal had been decommissioned there was a significant decrease in DDoS attacks throughout Europe. Nevertheless, the "DDoS-for-hire" problem, which can be subsumed under the term "Crime-as-a-Service", generally still prevails.

[64] A web interface may be a graphical user interface allowing the user to interact with the system via a web browser, or a web service enabling the system to provide other systems with various functionalities and data.



THIS SITE HAS BEEN SEIZED

The domain name **Webstresser.org** has been seized by the United States Department of Defense, Defense Criminal Investigative Service, Cyber Field Office in accordance with a warrant issued by the United States District Court for the Eastern District of Virginia. This domain name has been seized in conjunction with **Operation Power OFF**

Operation Power OFF is a coordinated effort by law enforcement agencies from The Netherlands, United Kingdom, Serbia, Croatia, Spain, Italy, Germany, Australia, Hong Kong, Canada and the United States of America, in cooperation with Europol.

The operation is aimed at the takedown of the illegal DDoS-for-hire-service Webstresser.org.

In late September 2018, the German Federal Office for Information Security (BSI) reported a DDoS attack on the Internet presence of the energy utility company RWE.[65] Prior to the attack, unidentified individuals had published a YouTube video threatening to carry out an attack on RWE servers, if the deforestation of the Hambacher Forst would be continued. Hackers attacked the RWE web site by generating a flood of enquiries which the server that operated the web site was no longer able to process. As a result, the web site was temporarily not available. That shows that "political conflicts" are dealt with in cyberspace as well.

3.7 MOBILE MALWARE

Especially in private households, PCs are being increasingly replaced by mobile terminals, such as smartphones and tablets. According to a "bitkom" survey, eight out of ten people in Germany use a smartphone.[66]

That explains why the use of "mobile malware", which is specifically tailored to mobile terminals, has been continually increasing for years[67]. This trend is also reflected by a variety of offences and types of attack on users: Phishing, social engineering, drive-by-infection, download of infected apps, or exploitation of security gaps in relevant operating systems. Often bank and payment data are stolen and SIM card data are illegitimately captured using different kinds of malware. Moreover,

[65] Cyber-Angriff auf RWE, (Cyberattack on RWE), available at: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber-Angriff_RWE_25092018.html, published on 25/09/2018.

[66] Smartphone-Markt wächst um 3 Prozent auf 34 Milliarden Euro (Smartphone market grows by 3% to 34 billion EUR), available at: https://www.bitkom.org/Presse/Presseinformation/Smartphone-Markt-waechst-um-3-Prozent-auf-34-Milliarden-Euro, published on 20/022019.

[67] ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018, p. 27

smartphones are frequently used as a door-opener for malware to infect company systems and business networks.

Attractiveness of "mobile malware" has been increasing for years.

Another risk of infecting mobile terminals with malware is incurred by surfing in open WLAN networks or by downloading apps from unknown sources instead of using official stores. But even official Google or Apple stores cannot guarantee protection against malware. Over and again, perpetrators manage to smuggle infected apps onto the platforms of official stores. According to Symantec 17% of all Android apps are camouflaged malware.[68] In 2018 alone, Symantec researchers found 38 malware-infected apps in the Google Play Store that conceal their existence on user devices after installation.[69] In its report "Mobile Threat Predictions", software company "Avast" emphasised that in 2018, the use of Trojans on mobile devices in the online banking area increased by 150% compared to the year before.[70] In addition, fake apps reportedly increased by 24% and ad-based malware by 49%.

McAfee, too, points out that the use of malware on mobile terminals has increased in 2018. Fake apps were one of the most effective methods to deceive users and install malware without attracting attention.[71] They say that Android users are especially affected: On average, G-Data identified 11,700 new "mobile malware" for Android per day, i.e., one new malware every eight seconds.[72] But also IOS terminals are increasingly damaged by all sorts of malware[73].

G-Data estimated the number of malware variants infecting Android devices alone at approximately 4.1 million in 2018 - which is commensurate with an increase of approximately 27% compared to the year before. All in all, so McAfee, the number of existing "mobile malware" variants exceeded the 30 million mark for the very first time.[74]

A lack of security precautions and updates make mobile terminals especially vulnerable.

In particular, mobile ransomware becomes increasingly popular with criminals: According to Symantec, Germany ranks third behind the USA and China as the frequency of infections by

[68] Executive Summary - 2018 Internet Security Threat Report (ISTR), Volume 23, available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf

[69] Hidden App Malware Found on Google Play, available at: https://www.symantec.com/blogs/threat-intelligence/hidden-app-malware-google-play, 09/05/2018

[70] 2019 Predictions, Part 2: Mobile Threats, available at: https://blog.avast.com/avast-mobile-threat-predictions,published on 09/01/2019

[71] McAfee Mobile Threat Report Q1, 2019, available at: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf, p. 2

[72] Cyberangriffe auf Android-Geräte nehmen stark zu (Cyberattacks on Android devices increase significantly), available at: https://www.gdata.de/blog/2018/11/31254-cyberangriffe-auf-android-gerate-nehmen-stark-zu, published on 07/11/2018

[73] Sophoslabs 2019 Threat Report, available at: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf, p. 20

[74] G DATA Internet Security. Android erreicht Höchstwertung bei AV-Comparatives und AV-TEST (G DATA Internet Security. Android achieves highest rating in AV-Comparatives and AV-TEST, available at: https://www.gdata.de/news/2019/04/31641-g-data-internet-security-android-erreicht-hochstwertung-bei-av-comparatives-und-av-test, published on 10/04/2019

mobile ransomware is concerned.[75] It is mostly a lack of security precautions and security updates as well as inadequate decryption of personal data that make mobile terminals an easy target for malware.

According to Symantec, one out of 36 mobile terminals is infected with malicious apps.[76] The total number of malicious apps blocked by Symantec totals to approximately 10,500 per day.

According to the German Federal Office for Information Security (BSI) more than one third of smartphone users are not aware that a smartphone requires the same security precautions and protective measures as a PC.[77] In this respect, further smartphone-specific attack vectors could be identified: In addition to email, especially instant messaging services such as Telegram or WhatsApp and SMS, can be used for phishing. Social media apps, such as Twitter or Instagram, can be misused for social engineering as well to feign trust and authenticity - two key aspects of social media.[78] The so-called URL padding[79], too, uses a peculiar feature of the smartphone, i.e., its small display: Because of the limited size of the smartphone display the user cannot fully view a fake URL extension. This URL, which is manipulated to conceal the true domain, leads the user to a compromised web site. The malware is downloaded from the destination web site itself.

A special example of "mobile malware" is Gustuff, a Trojan specifically programmed for the Android operating system. The programmers upgraded and extended Gustuff by various functionalities several times already. Today, Gustuff is capable of stealing logon data from approximately 100 banking and 32 crypto currency apps.[80] Preferred targets are banking apps; but Gustuff can also read out data from payment and messaging apps, such as PayPal, Skype and WhatsApp.

Other than Gustuff, TimpDoor is disseminated via text messages. Using phishing methods, the victim is misled to download a fake voice message app. The installation of the app enables criminals to circumvent device security and access internal networks and data. Moreover, the device, as a component of a botnet, can be misused to send further phishing messages or carry out DDoS attacks.[81]

As is the case with most phenomena in the cybercrime area an over-average number of undetected cases are to be assumed. This is primarily due to a low reporting rate on the one hand and the ignorance of actually having fallen victim to a crime on the other. Especially the latter turns out to

[75] Symantec Internet Security Threat Report (ISTR), Volume 24, February 2019, available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, p. 41

[76] Ibid.

[77] Die Lage der IT-Sicherheit in Deutschland 2018 (The State of IT Security in Germany 2018), available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6.

[78] ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport, p. 41

[79] The Mobile Phishing Threat You'll See Very Soon: URL Padding, available at: https://info.phishlabs.com/blog/the-mobile-phishing-threat-youll-see-very-soon-url-padding, published on 15/06/2017

[80] Gustuff: Android-Trojaner nimmt mehr als 120 Banking- und Messaging-Apps ins Visier (Gustuff: Android Trojan aims at more than 120 banking and messaging apps), available at: https://www.zdnet.de/88357205/gustuff-android-trojaner-nimmt-mehr-als-120-banking-und-messaging-apps-ins-visier, published on 29/03/2019

[81] McAfee Labs Threats Report, December 2018, available at https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf, p. 12

be an increasingly frequent problem: Cryptojacking and other malware keep evolving in respect to spoofing and concealment on the target system.

3.8 UNDERGROUND ECONOMY – DIGITAL BLACK MARKETS

Illegal forums or marketplaces on the clearnet, deep web and darknet continue to play an increasingly important role in cybercrime.

Definitions

Clearnet: *(also called visible web, surface web, open web). The generally "known" Internet that can be accessed by anybody, operated with regular browser programs and supported, for example, by simple handling with search engines. The clearnet, too, contains many illegal contents, such as politically motivated criminal offences, dissemination of child pornography, "underground economy" sites (criminal offences mostly committed in the cybercrime area in the narrower sense), etc.*

Deep web: *(also called hidden web, invisible web). Part of the Internet the contents of which cannot be found by search engines, for example, because web sites were not indexed or linked to search engines or because they are not intended for common use. Deep web contents may be databases, intranets or specialised web sites and can be accessed by "regular" browsers, if and insofar as the URL is known and the user is authorised to access the site.*

Darknet: *Darknet contents can only be viewed when using a special anonymisation software. The darknet consists of forums, blogs/wikis, etc. with highly diverse - even legal - contents. However, the majority of darknet contents are to be considered illegal. A significant part consists of darknet markets where (mostly incriminated) merchandise is traded anonymously. There are also various Crime-as-a-Service offerings (offers to commit crimes on a contractual basis) or darknet sites containing child pornography. The structure and use of other darknet segments do not differ from the clearnet. In darknet forums, too, opinions are expressed and topics are discussed, and wikis contain explanations. In the darknet, however, these mostly refer to illegal activities and contents (e.g., narcotic drugs).*

Below we list the offences that are typically committed in the abovementioned marketplaces:

- Trafficking in narcotic drugs on a repetitive and gainful basis
- Trafficking in weapons, war weapons and explosives on a repetitive and gainful basis without holding the required licence

- Counterfeiting and putting false money in circulation on a repetitive and gainful basis
- Dissemination, acquisition and possession of child pornography
- Forgery of documents and trading such on a repetitive and gainful basis
- Data espionage and handling stolen data
- Computer fraud on a repetitive and gainful basis
- Violation of the provisions of the Medicinal Products Act

Illegal narcotic drugs are the by far biggest merchandise group in almost all darknet markets. In the meantime, the dimension of these offerings is to be considered a mass crime. National and international investigations into platform operators and providers (so-called vendors) revealed that a wide range of almost all kinds of narcotic drugs, incl. new psychoactive substances (NPS), is offered on both the clearnet and the darknet.

Narcotic drugs are the biggest merchandise group on the darknet.

The share of weapon offerings is significantly lower than that of other incriminated merchandise offered on the darknet. With a view to the inherently existing potential danger of weapons the activities carried out by the police on the darknet to identify real weapon offerings and potential buyers in Germany are of particular importance. In the meantime, trading in firearms for which a licence is required is prohibited on most platforms. Users/vendors who violate this prohibition and sell or buy these "forbidden goods" are excluded from the marketplaces. Similar applies to material containing child pornography – which often is also categorised as "forbidden goods".

Making profits is the primary objective in darknet marketplaces. The administrators of forums and marketplaces often participate in the profits generated by selling illegal merchandise through a trust system. Only digital crypto currencies providing for anonymous or pseudonymous payment are accepted. Sites frequented by paedophiles, for example, are mostly used to exchange materials containing child pornography, whereas sites dealing with politically motivated crime are used to exchange information between like-minded people or promote political objectives.

Cryptocurrencies are a popular means of payment on the darknet.

Given the rising number of digital offerings and the trend towards a stronger use of the Internet and the darknet it is to be assumed that these media will be increasingly used as an instrument of crime. In the light of technical development it is just as likely that these media will be used with increasing proficiency.

After having abolished the digital black markets Alpha Bay and Hansa Market in 2017, the competent law enforcement and prosecution authorities conducted intense investigations in Germany that revealed that users and vendors have been looking for alternatives. In the past, the decommissioning of marketplaces was followed by the establishment of new, smaller marketplaces, but not so in 2018. The sales and purchasing activities were moved to a few bigger and allegedly "secure" platforms. One of these platforms was a digital black market called Wall Street Market.

An example: Wall Street Market

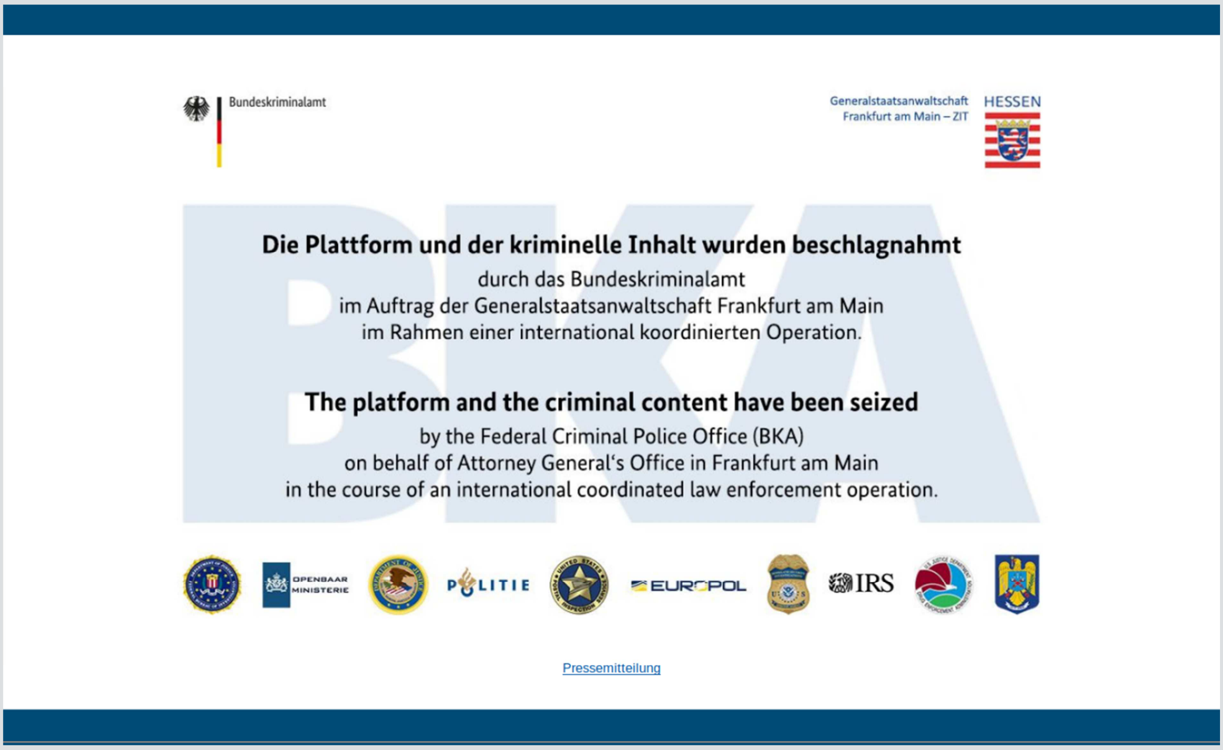
Since November 2017 the German Federal Criminal Police Office (BKA), under the direction of the Public Prosecutor General's Office Frankfurt/Main ZIT, has been investigating into the operators and administrators of the digital black market Wall Street Market (WSM). These investigations were conducted in strong collaboration with the law enforcement and prosecution authorities on a national and international level, including but not limited to the Netherlands, the USA and EUROPOL.

During the period in which the investigations were conducted, WSM was one of the biggest darknet platforms for illegally trading various merchandise, especially narcotic drugs. The trading platform and the associated forum were available on the TOR network only.

The majority of goods, especially narcotic drugs, were dispatched from Germany. During the investigations, more than 400,000 sales were registered that were successfully effected on this platform. In 250,000 cases deals with illegal narcotic drugs were made most of which were dispatched from Germany. On average, there were approximately 1,250 transactions per day. For each transaction the operators/administrators received a sales commission of two to six percent of the sales price. The users of the online marketplace paid with the Bitcoin and Monero cryptocurrencies.

When the suspects allegedly responsible for the illegal online marketplace (three German nationals) started to transfer money the customers had already transferred to the marketplace to their own accounts (so-called "exit scam"), extensive search measures were carried out. In the homes of the suspects the police seized more than 550,000 EUR in cash as well as tens of millions of Euros in Bitcoin and Monero cryptocurrencies, several expensive cars, and many other pieces of evidence (primarily computers and data carriers).

The WSM infrastructure ran on servers in Germany, the Netherlands and Romania. Until 02/05/2019 further legal and technical requirements were defined for a coordinated decommissioning/takeover of the technical WSM infrastructure which was publicly documented per seizure banner.



Bundeskriminalamt

Generalstaatsanwaltschaft
Frankfurt am Main – ZIT

HESSEN

Die Plattform und der kriminelle Inhalt wurden beschlagnahmt
durch das Bundeskriminalamt
im Auftrag der Generalstaatsanwaltschaft Frankfurt am Main
im Rahmen einer international koordinierten Operation.

The platform and the criminal content have been seized
by the Federal Criminal Police Office (BKA)
on behalf of Attorney General's Office in Frankfurt am Main
in the course of an international coordinated law enforcement operation.

Pressemitteilung

Brief assessment:
Due to intensive investigations, one of the biggest and internationally most significant darknet marketplaces could be decommissioned, despite of the fact that the modus operandi was highly anonymised and conspiratorial and the technical WSM infrastructure was complex and distributed across several countries. The intensive and trusting cooperation of many national and international law enforcement/prosecution and security authorities significantly contributed to the success of the investigations.

Apart from WSM, altogether six digital marketplaces/forums and news web sites have been decommissioned since 2017 with the help of German law enforcement and prosecution authorities:

- Deutschland im Deep Web – officially commissioned: March 2013, decommissioned: June 2017
- AlphaBay – officially commissioned: December 2014, decommissioned: July 2017
- Hansa Market – officially commissioned: July 2015, decommissioned: July 2017
- Silkkitie / Valhalla Market – officially commissioned: October 2013, decommissioned: April 2019
- deepdotweb.com – officially commissioned: October 2013, decommissioned: May 2019

In four cases, the investigations were conducted by the German Federal Criminal Police Office (BKA). The number of registered users per platform ranged from approximately 23,000 to approximately 1.8 million. The profits generated in the illegal marketplaces varied accordingly. In the AlphaBay marketplace, the profit amounted to approximately 628 million EUR.

Cybercrime-as-a-Service

The underground economy provides a broad range of illegal offerings and/or services enabling or facilitating all sorts of cybercrime. The offerings include

- Digital data theft
- Provision of botnets for various criminal activities
- DDoS attacks
- Programming and dissemination of malware
- Sale/offer of compromised sensitive data, such as access or payment data
- Provision of financial or goods agents to conceal the origin and protection of funds or goods obtained by criminal activities
- Communication platforms for the exchange of criminal knowledge, such as forums
- Anonymisation and hosting services to conceal the identities of criminals, and
- Password-protected "dropzones" (digital storage locations) for storing illegally obtained data and/or information, such as passwords and account data

Furthermore, the users are often also offered additional support services on these platforms, such as

- Malware updates
- Consulting services
- Advanced anti-detection mechanisms
- Technical support

The list shows that potential, even technically unskilled offenders can easily gain access to sophisticated and dangerous tools enabling them to carry out various cybercrime attacks and conceal the identity of the initiator.

Anybody can acquire criminal knowledge on the net.

The malware/ransomware, botnets and DDoS phenomena are proof of the extensive realisation of the "Cybercrime-as-a-Service" idea and/or this business model.

3.9 DIGITAL CURRENCIES

Cryptocurrencies, such as Bitcoins (BTC), Tether (USDT) or Monero (XMR), are digital or virtual means of payment the genesis and use of which are based on mathematical calculations, cryptographic procedures and digital signatures. All that is required for private use is the installation of a specific software to set up a digital account (a so-called "wallet"). On many platforms, such as Coinbase, Gemini or BitPanda, various types of crypto currencies can be legally bought and sold. Technically, most crypto currencies are based on the "blockchain" principle which can be described as a public or private, decentrally managed digital accounting system for the ongoing recording of transactions (distributed ledger technology).

Cryptocurrencies as such and their generation and use are mainly legal. On countless platforms crypto currencies can be legally sold or used as a means of payment. Because of the decentralised accounting, lack of a regulated supervision by government or banks, fast global availability, possibility of being used in international trading, and pseudo-anonymity within a network, cryptocurrencies have proven a popular means of payment for criminals. By using cryptocurrencies it is basically possible to conceal identities: You can see that transactions have been made and view the addresses of their respective senders and recipients, but you cannot see the names of the wallet owners involved.

Thus, cryptocurrencies are in the focus of criminal activities not only as a means to an end, but also as something worth stealing. Attempted fraud (scams), theft of digital wallets, cryptojacking, and misuse of technical infrastructures for criminal purposes are only some of the offences that have established themselves in the cryptocurrency environment. The laundering of digital money, too, is an increasing phenomenon[82] which is additionally facilitated by unregulated trading platforms, inadequate security precautions for wallets and cryptocurrency exchange platforms, or non-implementation of anti-money laundering legislation on the Internet (e.g., inadequate ID verification or other Know-Your-Customer procedures).

It is to be assumed that the increasing acceptance of digital currencies in the free market and evolving new cryptocurrencies which are based on yet more anonymity create additional incentives to use cryptocurrencies in a criminal context.

3.10 TECHNICAL SUPPORT SCAMS / SEXTORTION

In 2018, the cybercrime units were not only confronted with handling cybercrime phenomena in the narrower sense. Phenomena such as the "technical support scam" or the handling of a large number of "sextortion" cases posed further challenges to law enforcement/prosecution authorities.

"Technical support scams" are a type of fraud: Scammers call the victim on the phone pretending to be members of the support staff of a software company (e. g. Microsoft) and to have found a severe problem with the victim's computer. Scammers ask the victim to install a remote access tool,[83] allegedly to carry out remote maintenance and to fix the problem. Instead, however, they manipulate or read out the victim's data or install malware remotely.[84] In some cases, the following modus operandi is used in preparation of this type of fraud: Fake warnings and error messages are displayed to the victim on a compromised website. At the same time, the fake message indicates a purported support hotline, actually run by scammers, and instructs the victim to call this hotline. At the end of the process, the victim receives a demand for payment, be it in the form of a fake invoice or by way of a ransomware infection.

[82] Geldwäscheverdacht bei Kryptowährungen (Suspicion of money laundering regarding cryptocurrencies), available at: https://www.bundestag.de/hib#url=L3ByZXNzZS9oaWIvNjQ4OTA2LTY0ODkwNg==&mod=mod454590, published on 21/06/2019.

[83] Remote access tools enable the user to access a computer remotely from another computer. All entries can be made remotely (keyboard, mouse).

[84] Protect yourself from tech support scams, available at: https://support.microsoft.com/en-us/help/4013405/windows-protect-from-tech-support-scams.

"Sextortion", by contrast, is a form of extortion which is based on the pretext that perpetrators supposedly hacked the computer or webcam of their victim and filmed the victim when visiting pornographic websites and/or masturbating. They threaten to e-mail the supposedly available material to the victim's contacts or to publish it in social networks.[85] In particular, the perpetrators pretend that the only way for the victim to prevent this is to transfer money to the blackmailers.

3.11 "LIVING OFF THE LAND" / "SUPPLY CHAIN ATTACKS"

"Living off the land" methods (LotL) and "supply chain attacks" – methods already known in the field of cybercrime – saw a significant rise in 2018 and might increasingly be used by cybercriminals in future due to inherent specific characteristics.

"LotL" methods, also known as "fileless attack" or "fileless malware", differ from "traditional" types of attack insofar as primarily no external malware is installed on the target system. Instead, attackers use administration or system tools, scripts or software macros, such as Powershell or MS-Office, they find on the target system, to launch an attack. The aim of these attacks often is to commit data theft or espionage or to distribute further malware.

Since no malware is installed at first but common tools and software are misused maliciously, such attacks leave behind only slightly modified system files. Therefore, it is difficult to detect and trace back such attacks. For that reason, this type of attack is very popular among criminals: According to Symantec, the number of malicious Powershell scripts, an administration script of Windows systems, blocked in 2018, rose by 1,000% compared to the previous year. Moreover, an increase in the number of attacks on MS Office documents was identified.[86]

"Supply chain attacks" pursue a different, more indirect approach: At first, third-party subsystems, information and communication chains, clouds or software are infected. Subsequently, they are used to distribute malware and infect the actual target system, frequently the systems of companies. In this respect, the victim who is attacked first can be seen as the bridge to the actual target. In September 2017, the software CCleaner was infected by unknown hackers and exploited as such an entry point. The infected software was then downloaded by approximately 2.3 million users.[87] The malware contained in the infected software read out the users' data and information and decided which users would become the actual target. Subsequently, these were to be infected with further malware. The attack actually aimed at spying out the data of high-ranking employees of various companies.

"Supply chain attacks" choose the least protected parts of the "supply chain". If one part of the "supply chain" is infected, the attackers can reach their actual target. This type of attack, as well, is not easy to detect because of its indirect nature and sometimes international network chains

[85] Sextortion Bitcoin scam makes unwelcome return, available at: https://blog.malwarebytes.com/cybercrime/2019/02/sextortion-bitcoin-scam-makes-unwelcome-return, published on 11/02/2019.

[86] Symantec Internet Security Threat Report (ISTR), Volume 24, February 2019, available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, p. 11.

[87] Do not become a link in a supply chain attack, available at: https://www.kaspersky.com/blog/ccleaner-supply-chain/21785, published on 26/03/2018.

between systems. Moreover, the types of initial infection take many forms and can be based on malware, spear phishing[88] or social engineering.

An example of a "supply chain attack" coupled with "LotL" methods was Petya, a ransomware that mainly spread across Ukraine. Although Petya targeted the systems of local multinational companies, the attack started at MEDoc. This is a tax and accounting software package popular in Ukraine that is also used by international companies targeted by the criminals. Exploiting resources available on the systems, such as Windows Management Instrumentation Command-Line or Windows Server Message Block, Petya spread from MEDoc to its actual target systems.[89]

3.12 CLOUD COMPUTING / INCREASED NETWORKING THROUGH THE "INTERNET OF THINGS"

Cloud computing will become an increasingly relevant subject both for law enforcement/prosecution authorities and criminals due to further developments. In 2018, there was again a growth in the number of attacks on cloud instances. For example, an increased number of attacks were identified for Amazons' cloud service AWS S3 bucket, with a total of approximately 70 million data records being stolen.[90]

Poorly secured cloud instances still carry a high risk for companies. Especially for the German economy, such attacks result in business process failures and a loss of reputation among customers.

Cloud computing continues to gain importance.

The "Internet of Things (IoT)" should also be considered a very high uncertainty factor - mainly due to the substantial rise in the use of corresponding devices. On average, every German household has more than six IoT devices that are exposed to fundamental risks due to exploits or simple passwords. Scan lists and specific search engines such as Shodan simplify the perpetrators' preparatory activities by listing devices connected to the Internet, including webcams or even traffic lights.

In addition, the constantly growing number of IoT malware poses a particular threat to IoT devices. In the third quarter of 2018 alone, approximately 45,000 new pieces of malware targeting IoT devices were identified.[91] Moreover, the increased use of IoT devices directly at the workplace (language assistants, security cameras, etc.), further heightens the threat posed to corporate networks and company systems.

On average, every German household has six IoT devices.

[88] "Spear phishing" is a type of attack in which criminals send fraudulent e-mails to deliberately selected organisations. These e-mails contain, for example, an Internet link. If an employee clicks on this link, malware will be installed on the computer concerned.

[89] Petya ransomware outbreak: Here's what you need to know, available at: https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper, published on 24/10/2017.

[90] Symantec Internet Security Threat Report (ISTR), Volume 24, February 2019, available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, p. 19.

[91] McAfee Labs Threats Report, December 2018, available at: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf, p. 28.

3.13 MACHINE LEARNING

The use of artificial intelligence and/or machine learning remains an important phenomenon in the digital world. This field offers opportunities but also involves risks. With a view to countering cybercrime, artificial intelligence (AI) and machine learning can be used to detect anomalies in networks and systems at an early stage or to detect and remove malware. In particular for companies, this would be a positive development in terms of data security.

Artificial intelligence presents both opportunities and risks.

For law enforcement/prosecution authorities this should also offer new opportunities. With their project "Cyberguide", Lower Saxony police are developing an interactive business process application. It promises to facilitate the automation of business processes and case management by machine learning. In future "Cyberguide" is intended to be used, for example, to record cybercrime complaints. Initially, "Cyberguide" is expected to learn to properly classify cases through question-answer processes in order to deliver information on responsibilities and measures to be taken on the basis of various knowledge sources to which it will have access.[92]

However, criminals, too, will exploit machine learning - for illegal purposes. There is reason to fear, inter alia, that AI will be used for communicating with malware. Moreover, AI might be used as a monitoring application for malware and control it dynamically, for instance, by making decisions about which files and/or file paths on the compromised system should be targeted. Furthermore, it cannot be ruled out that AI is able to create and/or forge pseudo-authentic certificates for the purpose of deceiving security systems.[93] Criminals might also use AI for phishing and/or social engineering attacks and, in this context, for searching the Internet for information about the target and collecting it, writing automated e-mails or even imitating chatbots.

[92] proPOLIZEI. Informationen für Niedersachsens Polizei, Heft Mai/Juni 2016, (proPOLIZEI. Information for Lower Saxony police, May/June 2016 edition), available at: https://www.polizei-nds.de/download/72565/proPOLIZEI_Mai_Juni_2016.pdf, p. 5 ff.

[93] Under the Radar – The Future of Undetected Malware, available at: https://resources.malwarebytes.com/files/2018/12/Malwarebytes-Labs-Under-The-Radar-APAC-1.pdf, p. 10.

4 Attacks on Business Enterprises / Attacks on Critical Infrastructures

Cyberattacks do not only target authorities but also enterprises: To this end, data are spied out, modified or destroyed. Moreover, webservers are impaired in terms of accessibility and/or infected with malware and contents stored on servers are manipulated.

In this context, novel threats and effects arise from cyberattacks on the "central nervous systems" of our society, the so-called critical infrastructures. This includes the sectors energy, water, food, information technology and telecommunications, finance and insurance, transport and traffic, health, media and culture as well as government and administration.

Smooth operation of critical infrastructures ensures the functioning and fundamental processes of modern societies; an up-to-date IT infrastructure enhances their efficiency and sustainability. Therefore, it is of outstanding significance that the police are capable of intervening promptly and effectively when taking measures with a view to warding off danger and criminal prosecution.

The German authorities already recorded various cyberattacks affecting enterprises from critical infrastructure sectors, such as health, transport and traffic as well as energy. In the period between 01/10/2017 and 25/10/2018, a total of 21 cyberattacks committed on enterprises with critical infrastructures[94] were reported to the central points of contact for cybercrime at the Land Criminal Police Offices and the BKA.

Enterprises with critical infrastructures are obliged to report disruptions to the Federal Office for Information Security (BSI) pursuant to the BSI Act. In its 2018 situation report, the BSI states that a total of 145 incidents were reported between 01/06/2017 and 31/05/2018. As in the previous year, the focus was on the information technology and telecommunications sectors.[95]

We have to assume that the number of such attempted attacks on critical infrastructures and related threat-relevant effects will rise even further.

Attacks committed by governmental players primarily take the form of Advanced Persistent Threats (APT). Such attacks represent a serious and ever increasing threat to the economy as well as to public and non-public bodies and institutions. This is particularly true when enterprises with critical infrastructures are involved.

[94] Critical infrastructures are defined as organisations and facilities that are vital to the community and whose failure or impairment would result in long-term supply shortfalls or major disruptions of public safety or would have other dramatic consequences.

[95] Die Lage der IT-Sicherheit in Deutschland 2018 (The State of IT Security in Germany 2018), available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=6, p. 10.

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 characterised by a very high deployment of resources and significant technology skills on the part of the attackers and are usually difficult to detect.

Characteristic of APT attacks is that they are used both for espionage, i.e. spying out data, and for sabotage, i.e. disturbing processes.

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, dynamic server infrastructures and highly professional malware components, subject to permanent sophistication, are used for cyberespionage attacks throughout the world.
- The main attack vector is the sending of "spear phishing e-mails"[96], including both malicious links and malicious attachments, which are used to infect the victims' systems. Prior to launching cyberespionage attacks, criminals usually check the targeted persons in a professional manner. To this end, they do not only carry out classical checks on the Internet and in the social media but also apply classical methods of espionage, such as gathering communications intelligence and using agents.
- Publications of numerous private IT security providers regularly point out that Germany is one of the targets of cyberespionage attacks. However, a concrete and actually reliable attribution of such intelligence service/government-controlled attacks, is hardly possible.
- The percentage of unreported crimes is likely to be high as a result of undetected and/or unreported attacks.

It is taken for granted that – due to the comparatively high level of competitiveness and technological expertise of the companies located in Germany – the domestic business hub will remain an interesting target for cyberespionage and/or hackers committing offences of a general nature.

[96] Sophisticated phishing based on a more targeted personal approach ("spear").

5 Damage Resulting from Cybercrime

Cybercrime causes severe material and immaterial damage to citizens, authorities and economic enterprises that might even threaten the very existence of the targets.[97] Thefts of millions of data, manipulations of numerous technical devices and related media reports have a highly negative impact on the public's sense of security. According to a survey of the BSI and the Law Enforcement Crime Prevention Programme (ProPK)[98], approximately one third of the persons interviewed (29%) considered the risk of themselves falling victim to cybercrime as high or very high[99].

Even people who do not actively use the Internet depend on the smooth running of data networks, in particular the Internet. For instance, major providers purchase electricity and gas through digital channels for subsequent distribution via networks. Conventional retail businesses also store more and more customers' details in databases that can serve as targets for criminal hackers and are vulnerable to misuse, as well. In short: "Analogous" life, too, strongly depends on smoothly running processes of IT and communication structures, service companies, the industrial sector or wholesale and retail enterprises; sometimes they even guarantee a continued existence.

According to an online study carried out by the German TV stations ARD/ZDF in 2018, more than 90% of the German population (about 63.3 million people) are Internet users. Compared to the previous year, this represents an increase of 1.4 percent or 0.9 million people. The study states further that there was also a rise in the frequency of use regarding online media: In 2018, the average user was online for about 3:16 hours; this is 47 minutes longer than in 2017.[100]

The Police Crime Statistics do not provide a basis for valid statements on the actual overall financial loss arising from cybercrime since they solely indicate losses resulting from computer fraud and the misuse of telecommunications services. The total loss in these fields reported for 2018 amounted to 61.4 million EUR (compared to 71.8 million EUR in 2017). Approximately 60.7 million EUR (2017: 71.4 million EUR) of the total loss were attributable to computer fraud, and almost 0.7 million EUR (2017: 0.4 million EUR) to the misuse of communication services.

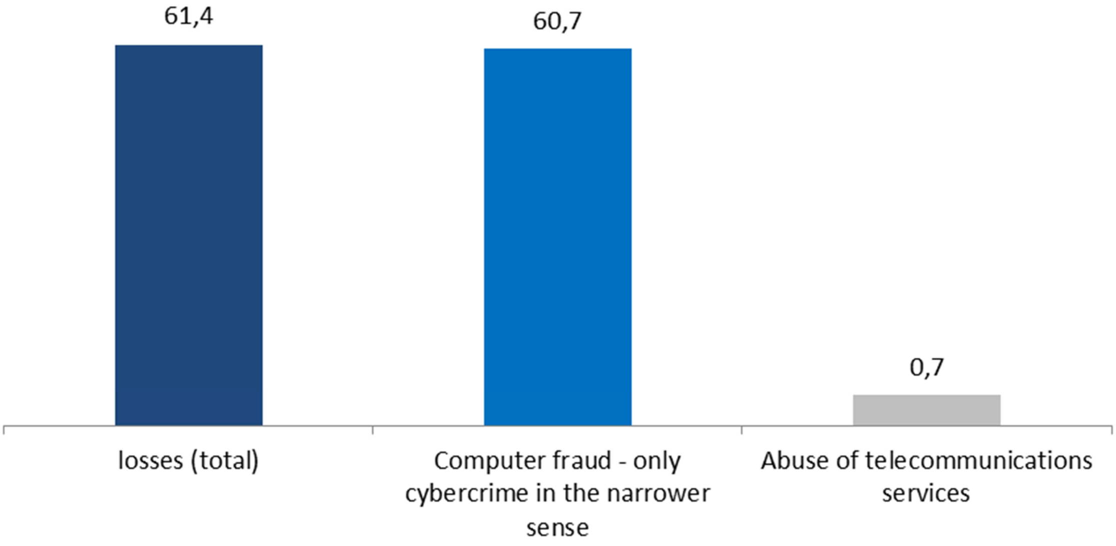
[97] Wirtschaftsschutzstudie 2018 (2018 Study on Economic Security), available at: https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf, p. 25.

[98] Law Enforcement Crime Prevention Programme of the Federation and the Länder (federal states)

[99] Digitalbarometer 2019: Bürgerbefragung zur Cyber-Sicherheit (Digital Barometer 2019: Public-opinion survey on cyber security), available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2019.pdf?__blob=publicationFile&v=3

[100] ARD/ZDF-Onlinestudie 2018 (ARD/ZDF online study 2018), available at: http://www.ard-zdf-onlinestudie.de/ardzdf-onlinestudie-2018.

Losses Resulting from Cybercrime, in Million EUR (2018)[101]



It should be borne in mind that there are not only statistical limitations but that financial losses resulting from a successful cyberattack often are not fully known or non-quantifiable. Moreover, reputational or image losses are difficult to describe in financial terms. Furthermore, 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 impairs entire networks and supply chains linked to them.

Some studies illustrate the real extent of the damage. For example, the Center for Strategic and International Studies (CSIS) and the security company McAfee ascertained that global economic losses caused by cybercrime rose to 600 billion USD. This study attributes about one quarter of the overall loss to the theft of intellectual property.[102]

There are major discrepancies between losses recorded in the Police Crime Statistics and findings made by the private sector.

According to information provided by the G4C member R+V, its insurance division CyberRisk estimates that the costs per claim range between 10,000 and 25,000 EUR for small and medium-sized enterprises with a turnover of up to 10 million EUR. This largely depends on the "quality" of the attack, on whether or not data are secured and on the number of computers affected. CyberRisk calculates approximately 1,000 EUR for restoring one computer. If a system, i.e. a network or several interconnected computers, is affected, the sum amounts to 5,000 EUR on average. Extorted money is not included in the calculation for lack of insurance cover.

[101] In cases where the financial loss is not known, a loss of 1 EUR is assigned as a symbolic value.

[102] Economic Impact of Cybercrime, available at: https://www.csis.org/analysis/economic-impact-cybercrime, published on 21/02/2018.

In the context of another study carried out by the German association "bitkom", interviews of Internet users revealed that financial losses had actually been incurred in 54% of all cases reported. [103]

A "bitkom" study estimates that cybercrime caused financial damage of 43.4 billion EUR to the German economy in the past two years.[104] This figure is reportedly based on information obtained from affected companies in the context of the study. It remains a problem to determine what types of losses should be considered when it comes to identifying the financial losses resulting from cyberattacks. There is no uniform system for dealing with this question. Neither has it been possible to determine the losses for private individuals.

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

[103] Cybercrime: Jeder zweite Internetnutzer wurde Opfer (Cybercrime: Every second Internet user fell victim), available at: https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html, published on 10/10/2017.

[104] Cyberattacken auf deutsche Industrie nehmen stark zu (Strong rise in the number of cyberattacks on the German industry), available at: https://www.bitkom.org/Presse/Presseinformation/Cyberattacken-auf-deutsche-Industrie-nehmen-stark-zu.html, published on 11/10/2018.

6 Overall Assessment and Outlook

The use of digital information and communication technologies is an essential basis of modern social and economic life. The Internet and Internet-based services are moving closer to the people: For example, body measuring data and personal location data are permanently recorded and processed by means of wearables (e.g. smartwatches, fitness trackers, clothes). Data stored by Internet service providers facilitate the creation of comprehensive personality and activity profiles.

Progressive developments, such as the Internet of Things (IoT), Industry 4.0, "Smart Home" or Automotive IT (AIT), and a substantial rise in the number of "addressable" objects on the Internet offer cybercriminals a broader spectrum of potential targets. Insufficient security features and outdated technologies enhance the opportunities for crime.

The increasing spread of digital technology goes along with more opportunities for cybercriminals.

Highly dynamic developments in the field of artificial intelligence (AI) offer considerable potential for economic value creation. However, they also provide criminals with a multitude of opportunities (such as "learning malware"). In short: The more a society moves about in the digital world and the more possibilities it offers, the greater are the opportunities for cybercriminals.

This is not only reflected by a rise in case numbers compared to the previous year coinciding with a lower clear-up rate but also, for instance, by a massively increased range of malicious software programmes available: In the first half of 2018, the G4C member G DATA identified an average of about 13,000 completely newly programmed types of malicious software[105]. Many of these were specifically programmed for mobile terminal devices, are almost invisible (e.g. cryptojacking malware) or are able to adjust themselves through updates and to develop dangerous features. The quality of such attacks improved considerably due to technological progress and a growing professionalisation of attack vectors. We must counteract these dynamics continuously with adequate security updates and measures.

However, there are also positive developments in the fight against and prevention of cybercrime. For example, the decrease in the number of phishing cases linked with online banking can be explained by the fact that TAN procedures are being improved in terms of security and that recognised vulnerabilities are closed effectively.

Not only are the opportunities offered by the digital world expanding but managing technological know-how is also experiencing an increasingly worrying trend: On the one hand, the Internet in general and the darknet in particular facilitate the exchange of expertise regarding the use of criminal malware. On the other hand, this knowledge is no longer necessary due to the availability of Cybercrime-as-a-Service. Every part/detail needed for an attack, be it with regard to the software or the knowledge of how to use it, can be purchased on digital black markets and can thus also be used by "technological laymen" having criminal intentions.

[105] G DATA-Blog; Malwarezahlen erstes Halbjahr 2018: Die Gefahr lauert im Web (G DATA blog; Malware figures for the first half of 2018: The danger is on the web), available at: https://www.gdata.de/blog/2018/08/31027-malwarezahlen-erste-halbjahr-2018-die-gefahr-lauert-im-web

Owing to its high level of development and know-how (particularly in economic circles), Germany continues to be an attractive target for cybercriminals: Attacks on corporate processes and IT systems of enterprises with critical infrastructures pose an abstract high threat to public order. Small and medium-sized enterprises have also increasingly become a favoured target of criminal activities (mainly through ransomware attacks).

The perpetrators act in a highly professional way, for example when attacking small and medium-sized enterprises: In the run-up to an attack, perpetrators often gather information about the respective enterprise. They hope to obtain data and facts about the enterprise which they can exploit for their extortionate activities later. Criminals especially use turnover figures to adjust their ransom demands accordingly.

But protecting IT systems is not enough; it is also necessary to sensitize company personnel for phenomena, such as social engineering or phishing.

In view of rapid developments taking place and since many attacks and/or offences remain unreported or unrecorded, it is difficult to assess the whole dimension of the threat posed by cybercrime. It can be assumed that both the case numbers and the losses as well as the number of victims are far higher than indicated in the police statistics. To make reasonably valid statements on the actual dimension of cybercrime and to be able to combat cybercrime effectively, law enforcement/prosecution and security authorities are required to initiate various measures taking into account personnel, financial and, above all, technological aspects, such as the teaching of basic skills, additional basic and advanced training and the provision of appropriate hardware and software. Enhanced co-operation with research institutes and the private sector may also contribute to clearing up (at least some) undetected cases of cybercrime.

The users themselves are also encouraged to ensure the security of their technical devices and to avoid careless disclosure of information on the Internet. In this context, it is imperative that users obtain relevant information and become acquainted with instruments and measures that will help them to protect themselves from attacks of various kinds.

Cybercrime knows no national boundaries.

Cybercrime is a specific crime phenomenon that is getting more and more important in terms of quantity and quality and for which national borders are of no relevance/importance. It is all the more necessary to further expand both national and international co-operation between security authorities and partners from research, industry and trade.

In November 2010, the Council of the European Union established the EU Policy Cycle for the fight against organised and serious international crime.
The aim of this multi-annual policy cycle is to coherently and systematically address the most important threats posed to the EU by organised and serious crime through optimising co-operation between the competent services of the Member States, the institutions and agencies of the EU as well as third countries and organisations, also involving the private sector. This co-operation is implemented via the EMPACT platform (European Multidisciplinary Platform Against Criminal Threats) set up for that purpose.
Cybercrime is one of the prioritised phenomena that have to be combated jointly in this context at European level.

The activities in the field of cybercrime control in 2019 are focussed on implementing a joint suppression strategy elaborated by all participating states. This strategy includes operational measures, such as developing new analysis tools, co-ordinating joint investigations with a stronger operational orientation, co-operating with third counties and expanding co-operation with private partners. In view of the huge amount of data to be handled in this connection, measures are required to facilitate data collection and analysis methods for law enforcement/prosecution authorities at both national and international level. These developments also require adequate advanced training for police officers. This is the only way to keep abreast of the developments in the area of cybercrime outlined before.

The response to growing cybercrime is to expand and improve national and international co-operation.

Publishing information

Published by
Bundeskriminalamt, 65173 Wiesbaden

Last updated in
October 2019

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

This report is published by the Bundeskriminalamt as part of its public relations work.
It is made available free of charge and is not destined for sale.