Crime prevention policy	
EU- priority	Cybercrime; • Child sexual exploitation • Payment card fraud • Cyber-dependent crimes
Country	Germany
Year	2017/2018

1. Overview of the field

Definition of cybercrime

Cyber crime includes offences directed against the Internet, data networks, information technology systems or the data they contain (cyber crime in the narrower sense) as well as offences committed using this information technology.

Assessment of trends and developments

Common forms of cyber crime aim at compromising and manipulating computer systems with malicious software, e.g.

- to tap and exploit the user's personal data and login details (identity theft);
- to encrypt the user's data or files stored in the system using ransomware to blackmail the user into paying a ransom;
- **to "remote-control" the systems, connect them to botnets and use them for further offences.**

Current trends:

Using malware

Malware can be used in many ways: It may be installed on the target system through various channels and is then used to tap data, install other malware or exploit the compromised computer as part of a botnet.
New malware is being developed every second with the aim of circumventing anti-virus software and exploiting vulnerabilities. Malware may spread in the following ways:

- downloading compromised files that are often attached to e-mails sparking the recipient's interest;
- drive-by download: cyber criminals create websites that start an automatic download of malware when visited;

- social networks where compromised attachments and links are shared; or
- spear phishing: cyber criminals send malware or phishing e-mails personally addressing the recipient to obtain data or compromise the victim's computer.

With the exponential worldwide growth in the use of mobile devices, cyber criminals are increasingly spreading malware designed for smartphones, e.g. to circumvent the mobile TAN procedure in online banking.
Like PCs, mobile devices are compromised through malicious e-mail attachments, links and websites or by installing compromised apps.

Digital extortion:

Cyber criminals frequently use ransomware for digital extortion. The software uses cryptography to encrypt files and documents on the compromised computers. To restore access, the offenders ask for a ransom. The malware or criminal "services" needed for such extortion can be bought on dedicated forums of the underground economy. This means that special IT skills are no longer needed for digital extortion.
There are even types of ransomware which encrypt not only local files but also network folders. This ransomware specifically targets companies where such folders are more commonly used. While this type of ransomware initially used payment methods such as Paysafecard or UKash, criminals are now increasingly asking for anonymous digital currencies, primarily Bitcoins.

The victims' computers may be compromised by visiting a compromised website (e.g. by clicking on a malicious link) or by opening malicious attachments in spam e-mails, for example.

Currently, the following types of ransomware are used:

- Locky
- Petya / GoldenEye
- GPCode
- CryptoWall
- CTB-Locker
- WannaCry

Identity theft / phishing:

Digital identity comprises all kinds of user accounts with corresponding personal information such as login details for

- communication services (e-mail and messaging services);
- e-commerce services (online banking, online brokerage, web-based commerce of any kind, e.g. online shops, travel portals);
- work-related information (e.g. online access to a company's internal technical

resources);
- e-government services (e.g. online tax return);
- cloud computing;
- credit card data;
- payment addresses.

Cyber criminals try to access such data, for example through phishing, to sell them for profit or to commit further offences. Phishing means any attempt at obtaining an Internet user's personal data, e.g. through compromised websites, e-mails and text messages, and thus committing identity theft.

Social engineering:

Often, the weakest link in the chain is the Internet user. Cyber criminals know that. Through clever psychological manipulation, they tempt their victims to do things that compromise the security of their data. Criminals exploit human motivations such as curiosity and fear to obtain access to data or to compromise computers. For example, potential victims are selected and then contacted on the basis of what they share on social networks.

Examples of social engineering attacks:

- sending personal e-mails that seem trustworthy and ask the recipient to disclose confidential information for certain reasons (e.g. verifying the online banking account);
- intentionally sending e-mails with malicious attachments to persons identified as appropriate targets based on information gathered on social networks (e.g. staff working in a company's financial department, security advisers);
- offering telephone support to solve a supposed computer issue (if victims do what the offender suggests on their computer or in their network, they may install various malware);
- copying an existing user account on social networks and sending seemingly trustworthy messages to the user's friends, e.g. asking them to communicate via a separate e-mail address or mobile phone number (when clicking on the e-mail address, the victim installs malware on his/her computer; when sending a text message to the phone number, the sender must pay (SMS payment)).

Large-scale remote control of computers (botnets):

The word "botnet" is composed of the words "robot" and "network", i.e. it is a network of robots. A botnet is created when many – thousands or even millions – of computers are compromised with malicious code and connected using a Command & Control Server (C&C server, remote control); criminals then use this network for certain activities.
In particular, botnets are used for Distributed Denial of Service (DDoS) attacks, i.e. targeted attacks that make websites unavailable, or to send spam messages in bulk.
At the same time, the malicious code – mostly installed without the user's knowledge – allows criminals to spy out the compromised systems and obtain the user's personal information (e.g. login details for online banking, social networks and e-mail accounts).
Botnets and their capacities are a regular component of cyber criminals' infrastructures and

are sold as commodities on dedicated forums of the underground economy. Even criminals with few IT skills can rent botnets at low rates to successfully carry out cyber attacks.

DDoS attacks (Distributed Denial of Service):

In DDoS attacks, IT systems forming a network (frequently botnets; see above) send a huge number of requests to selected servers until these servers reach their maximum capacity and "crash" under the load of requests. Offenders use a Command & Control Server to make the connected devices (bots) attack the selected server, unnoticed by the user. IT systems integrated into such a botnet can also be used to execute other commands, distribute files or anonymize data. Offenders can also exploit the computing power of a botnet to gain (mine) cryptocurrencies such as Bitcoin.

Challenges

Offenders seem to become more *service-oriented* (selling or renting out malware or infrastructure that is easy to use also for people without special IT skills → Crime-as-a-Service). Many different products allow even non-specialists to enter the criminal cyber scene and to commit offences quite easily. The *Cybercrime-as-a-Service* business model continues to grow. Providers have even started to offer *customer support* as known from legal software products. For example, such support includes updates for malware, advisory services, anti-detection mechanisms and assistance with technical problems.

The darknet plays an important role because it gives users maximum anonymity. In addition, there are many forums and marketplaces for illegal weapons and services and other illicit goods. For criminals, it is an attractive means to commit offences, which can be concluded from their increasing activity on the darknet.

Moreover, the number of anonymization and encryption tools for transmitting and storing data has significantly increased. These often free or pre-installed software products offer such a high level of security that even law enforcement authorities are sometimes no longer able to de-anonymize or decrypt the data.
Cyber criminals increasingly use anonymization and encryption tools to reduce the risk of being detected.
Due to highly dynamic innovation processes, the number of IT systems and the amount of information stored on them is increasing. Collecting, processing and analysing digital data and traces therefore place ever growing demands on the technical equipment and infrastructure needed by the police to combat cyber crime.

The quality of *connected devices* is improving as well. Appliances such as refrigerators, TVs and radiators as well as production and maintenance processes are increasingly controlled online. Terms such as Internet of Things (IoT) and Industry 4.0 describe this rise in digital interconnectedness in both the private and professional context. The more society inhabits the digital world, the more opportunities are created for cyber criminals to commit offences.

Recent overview of statistics and research
Current figures on cyber crime (2017): • Cyber crime (total): 85,960 criminal offences • Computer fraud (cyber crime in the narrower sense): 63,939 criminal offences • Data espionage/interception: 9,600 criminal offences • Falsification of legally relevant data; deception in legal transactions in connection with data processing: 8,352 criminal offences • Alteration of data, computer sabotage: 3,596 criminal offences • Fraudulent use of telecommunications services: 473 criminal offences The Federal Criminal Police Office (BKA) is currently involved in research projects on cyber crime in the following fields: virtual currencies; darknet marketplaces and other aspects of criminal activity on the darknet; use of artificial intelligence to support the fight against child sexual exploitation; and assessment of damage caused by cyber crime.

Other national priorities besides child sexual exploitation, payment card fraud and cyber-dependent crimes?
High-tech crime

2. Crime strategy and coordination

Objectives of the crime strategy
Combating cyber crime is a top priority of all federal and state police forces in Germany. The corresponding strategy informs political, strategic and operational decision-makers about current developments and trends in cyber crime. Based on a situation assessment, the strategy identifies relevant fields of police action, defines strategic goals and specifies requirements and recommendations for flexible and comprehensive measures to combat cyber crime at national and international level.

Role of prevention in the crime strategy on state/regional/local level
Prevention is one of the eleven fields of action identified in the strategy.

Implementation of the policy (which level is responsible for the implementation and how is the implementation coordinated?)
The strategy was developed following a decision of the Standing Conference of the Interior Ministers of the *Länder* in the Federal Republic of Germany (IMK). At the request of the internal security working group (AK II) and the criminal police working group (AK Kripo), the Crime Fighting Commission (KKB) created a joint federal/state project group to draw up a revised police strategy for combating cyber crime. The project group

headed by the BKA is composed of representatives of federal and state police forces and of judicial authorities.
The strategy became effective after adoption by the IMK.
Developing and revising the strategy is an ongoing process.

Stakeholders (working groups, specialised agencies, partners, etc)
Several expert bodies from the fields of prevention, research and basic and advanced training assist and advise the aforementioned project group. It can also draw on cyber security expertise.

Participation in European/ international networks, working groups, etc.
Experience gained through international cooperation continuously feeds into the national strategic process.

3. Good practices

Overview of recent good practices, prevention programs, etc.
The BKA does not have an overview. However, one example of a successful practice is cooperation between cyber crime offices in the framework of the central cyber crime contact points of the federal and state police for businesses (ZAC). For example, a flyer giving businesses recommendations for dealing with cyber crime was drawn up in the network. (https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsbereiche/InternetKriminalitaet/handlungsempfehlungenWirtschaft.html, in German) Another successful practice is cooperation under the federal and state police crime prevention programme (ProPK). The programme is intended to inform the public, multipliers, the media and other stakeholders about different types of crimes and ways to prevent them (https://www.polizei-beratung.de).