INFINITY

IMMERSE. INTERACT. INVESTIGATE.

Policy Brief

Cybercrime in Germany

DISSEMINATION LEVEL PUBLIC

PARTNER

BHFOD

AUTHORS

THORSTEN STODIEK

MAX HAUSNER

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883293. The content of this document represents the view of the authors only and is their sole responsibility. The European Commission does not accept any responsibilty for any use that may be made of the information it contains.

Cybercrime Situation in Germany[1]

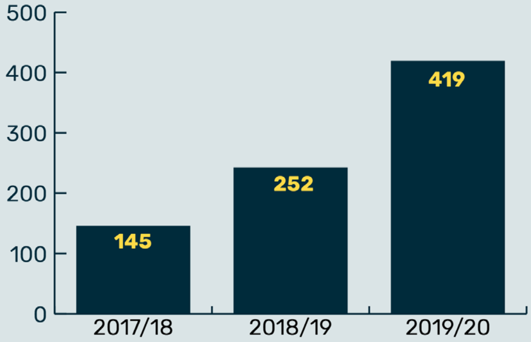
The rate of cybercrime continues to rise in Germany. In 2019, almost 300,000 criminal cases identified the internet as a vector for committing a crime, increasing 8.4% compared to 2018. Examples ranged from distributed denial of service (DDoS) attacks to those connected with online purchases. There were reports of over 150,000 fraud cases, where criminals have failed to deliver goods, offered inferior quality goods, or made no payment for the purchase.[2]

It is not only individual citizens who are targets; in 2019, 75% of German private sector companies were victims of a cyberattack. Often the attack vectors were not the companies' own IT systems but the systems within their supply chains. Recently, cybercriminals have had a change of approach going after high-value targets. While in 2018, cybercriminals were focusing their attacks on small and medium-sized enterprises; by 2019, targets switched to large enterprises and institutions, a phenomenon known as "Big Game Hunting". Those attacks resulted in €102 billion's worth of damage, twice the amount in 2017 and 2018.

Protection of national critical infrastructure from cyberattacks is also of paramount importance. In the year between May 2019 and June 2020, critical infrastructure organisations in Germany reported 419 incidents, while in the previous year it had been only 252. Most incidents were reported by the financial sector, closely followed by the IT and communication sector.[3] Such attacks have the potential to cause devastating impact to a country's operations.

Cybercrime affects all of society: business, critical infrastructure, government, public services and institutions as well as citizens. Developments such as the internet of things (IoT) or Industry 4.0 have a positive impact on ways of living and working; however, they also provide opportunities for cybercriminals by increasing the attack surface. Given these potential threats, cybercrime prevention and investigation must be considered a primary challenge for society. [4]

Number of cybercrime incidents reported by critical infrastructure entities



Source: BSI 2020, p. 36.

Many German citizens already have a perception of the growing threat of cybercrime. A 2019 Eurobarometer survey found 79% of German respondents believed that the risk of becoming a cybercrime victim was increasing. Primary concerns include misuse of personal data (57%), the security of online personal data (41%) and that they might not receive the goods or services that they bought online (25%).[5] Phishing attacks remain high on the agenda, with 21% receiving fraudulent emails or phone calls asking for personal details within the last three years and 10% discovering malicious software on their devices.[6]

This policy brief presents the 2019-2020 cybercrime situation in Germany across different cybercrime phenomena. The thematic areas align with Europol's Internet Organised Crime Threat Assessment (IOCTA) 2020,[7] which distinguishes between cross-cutting cybercrime facilitators; cyber-dependent crime; child sexual exploitation online, payment fraud, and criminal abuse of the dark web.

1. Cross-cutting cybercrime facilitators and challenges

1.1 Social engineering and phishing

Criminals can use the theft of digital identities through social engineering (influencing people into acting against their own interest or the interest of an organisation), the use of phishing attacks, malware distribution or capitalising on data breaches for a plethora of cybercrime activities including the access to streaming services, the illegal agreement of contracts and goods orders, virtual mobbing, stalking or online-money transfers.[8]

In Germany alone, the number of spam emails containing malware increased drastically by 2.8 times in 2019 compared to 2018.[9] Between 2019 and 2020, an average of 35,000 emails containing malware were detected in the German government's networks every month.[10]

In early 2019, the German National Cyberdefence Centre reported a data dump in Germany containing 773 million email addresses and 21 million passwords in cleartext.[11]

1.2 Criminal use of cryptocurrencies

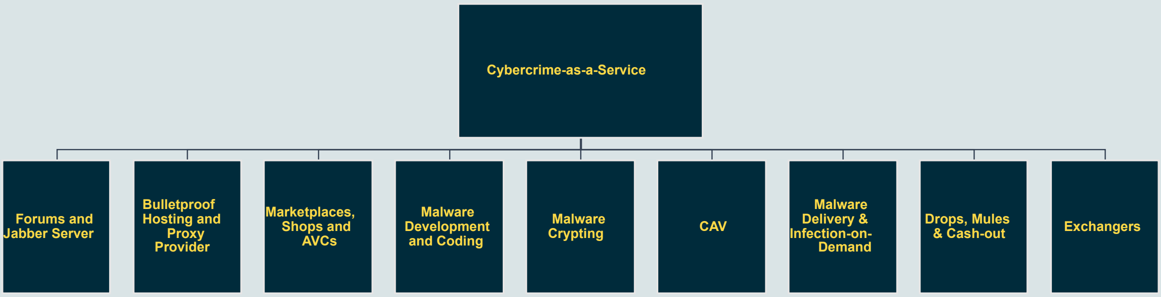
Cybercriminals can use cryptocurrencies for money transfers on the dark web or in requests for ransomware payments. Bitcoin is the most commonly used cryptocurrency for transactions on dark web marketplaces. Some criminals have managed to steal cryptocurrencies from individual and enterprise wallets through so-called 'exit-scams'. In such schemes promoters of a cryptocurrency disappear with investors' money during or after an initial coin offering.[12]

1.3 Cybercrime-as-a-Service

The cybercrime-as-a-Service (CaaS) business model remained a significant threat in 2019, facilitating phishing attacks and the use of malware and ransomware. Cybercriminals who have specialised cyber skills offered their services to other criminals who do not have the technical skills and knowledge to develop specific malware or conduct cyberattacks on their own.[13]

The German Federal Criminal police office (BKA) distinguishes between nine types of CaaS:

- Forums and Jabber servers: offering communication services for vendors and customers of criminal services;
- Bulletproof hosting and proxy provider: offering secure server infrastructures;
- Marketplaces, shops and AVCs (automated vending carts): offering trading platforms;
- Malware development and coding;
- Malware crypting: making malware undetectable by anti-virus programmes
- CAV (counter anti-virus): testing the detection rate of malware by anti-virus programmes;
- Malware delivery and infection on demand;
- Drops, mules and cashing out: facilitating the link between the digital and the real-world in the criminal activity in delivering goods or cashing out money transfers; as well as
- Exchanger: exchanging and mixing digital currencies into/with other digital and state currencies.[14]


Cybercrime-as-a-Service
Forums and Jabber Server
Bulletproof Hosting and Proxy Provider
Marketplaces, Shops and AVCs
Malware Development and Coding
Malware Crypting
CAV
Malware Delivery & Infection-on-Demand
Drops, Mules & Cash-out
Exchangers

Source: BKA 2020a: p. 36. (slightly adapted)

1.4 Criminal opportunism in the context of the Covid-19 pandemic

Due to the physical restrictions enacted to halt the virus's spread, there has been a notable increase in homeworking requiring remote accesses to business resources. The amount of data traffic in Germany increased by 10% compared to the pre-Covid-19 time. VPN servers became lucrative targets for cyberattackers.

During the pandemic, the German Federal Government and the German Federal States' governments introduced huge financial support programmes for companies that suffered from the lockdown in Spring 2020. On government websites, companies could require financial support. Cybercriminals used this opportunity to develop fake websites for phishing purposes that looked virtually identical to the official assistance sites. The police in North-Rhine Westphalia registered more than 1,200 complaints from the public about such fake websites. Applicants had provided sensitive financial data about their companies believing they were applying to the government for financial support. Other Federal States reported similar cases.[15] In many instances, criminals used the sensitive details to apply for payments in the victims' names from the official Covid-19 relief funds. These fake applications often resulted in genuine applicants temporarily being refused their relief payments and caused financial losses for Governmental institutions. In the future, these criminals may also use the data gleaned during these phishing attacks in follow-up attacks on the original victims.[16]

Vaccines for Covid-19 appeared almost immediately for sale on the dark web

Between January and April 2020, the registration of new domain names related to Covid-19 peaked at 116,357. Almost 2% of these new domains were considered malicious, and more than a third as highly risky. Of the 2,022 malicious domains, approximately 16% hosted phishing sites and the remaining 84% for various malware.[17] Between January and July 2020, more than 95,000 cyberattacks had been conducted in Germany using a Covid-19 narrative.[18]

In the clearnet and dark web, there was also a spread of fake offers of face masks, remedies for strengthening the immune system or antibody tests.[19] Even before Pfizer/BioNTech had delivered the first Covid-19 vaccine to the UK in December 2020, alleged vaccines by Pfizer/BioNTech were offered on the dark web.[20] By Mid-January 2021, the number of Covid-19 vaccine adverts on the dark web had increased by 400%.[21]

2. Cyber-dependent crime

2.1 Malware

Malware is widely present in cybercrime. Criminals are using malware for spying on and forwarding account data such as usernames and passwords; manipulating or destroying data, illegally utilising computing power for crypto-mining, encrypting data, constructing botnets for DDoS attacks or remotely controlling IT systems.[22]

In 2019, Emotet was one of the most harmful malware available. Given its versatile use, Emotet acted as a banking Trojan that served as a loader/dripper to deliver additional malware payloads such as Ryuk ransomware and TrickBot. TrickBot extracts sensitive data from IT systems and transfers them to an external command and control server. Ryuk encrypts data and requests ransom.[23]

Other malware that has been delivered subsequently to Emotet included software for manipulating online banking, spying out passwords in web-browsers and email; conducting DDoS attacks; and extracting information from email address lists.[24]

Common malware present in Germany

- **Emotet** loader software
- **AZORult** identity theft software
- **GrandCab** ransomware which encrypts IT systems and requests ransom for de-encryption
- **Sodinokibi**, 2019 successor to GrandCab
- **njRAT** remote access tool used for keylogging as well as third-party access to microphones and webcams of PCs

2.2 Ransomware

In 2019, ransomware attacks further increased. Common ransomware includes:

- Software that does not encrypt data on a hard drive but blocks the user's access to the system.
- Crypto-ransomware that encrypts data in the IT systems of PCs or network servers
- So-called 'Wipers' that do not intend to de-encrypt the data after the ransom has been paid but destroy the infected data.

In 2019, ransomware attacks focused primarily on state institutions and private sector companies. However, universities and hospitals have increasingly become targets.[25] The typical modus operandi of ransomware attacks has been modified by including 'double extortion' attacks, where criminals threaten to encrypt the data and publish sensitive data before it is encrypted if the ransom is not paid. The ransomware Maze, Nemty and Sodinokibi were used for such attacks, and criminals posted the data on 'public-shaming'-websites. The BKA expects that these types of attacks will further increase. In the Ransomeware-as-a-Service business model, one criminal group develops the ransomware, while the so-called operators load the ransomware onto the target system.[26]

2.3 Distributed Denial of Service (DDoS)

The number and intensity of DDoS attacks have further increased in 2019. With DDoS attacks, criminals aim to disrupt and block websites, servers, or networks of public or private sector institutions to make their services unavailable. For DDoS attacks, a botnet infects vast numbers of PCs allowing them to be remotely controlled.[27] Between 2019 and 2020, up to 20,000 Bot-Infections of German IT systems were registered every day, and the longest attack lasted for 107 hours.[28]

In addition to high-volume attacks, some DDoS also focused on attacking the victims' IT systems' internet protocols to make their systems inaccessible. In contrast, others focused on attacking specific applications of a website to disrupt their services.

DDoS attacks are now also increasingly using connected devices, such as TVs, cameras, routers, and other Internet of Things (IoT) devices.[29] Furthermore, cloud servers have also become the target of attacks in 2019. Already 45% of attacks targeted cloud-server systems.[30]

3. Child Sexual Exploitation Online

In 2019, the German police recorded 14,360 cases of online Child Sexual Abuse Material (CSAM) uploaded to the internet by users with IP addresses in Germany, an increase of almost 65% compared to 2018.[31] In June 2020, police seized CSAM of 700 terabytes in just one case alone.[32]

4. Payment fraud

Attacks on ATMs occurred primarily by jackpotting the PC of an ATM with malware. Jackpotting also happened through the use of external black boxes to manipulate the cashing module of the ATM and through network attacks on the ATM-related banking or processing company to manipulate money transfers and prepare a card-bound cash-out at the ATMs. Following a significant increase of jackpotting attacks in 2018, cases remained at a high level in 2019 (21 jackpotting cases with malware/47 jackpotting cases with black boxes), causing financial damage of €1.65 million.[33]

5. Criminal abuse of the dark web

Market places on the dark web often facilitate the trade of illegal goods such as illicit narcotics; licensed chemicals; weapons and explosives; CSAM; counterfeit money and forged documents, stolen goods and counterfeit branded items; stolen user credentials and credit card data; malware, guidance for committing crimes; as well as information about and services for money laundering. In 2019, illicit drugs remained the main commodity traded on the dark web.[34]

Dark web forums provide a platform for discussions, sharing of information and experience, announcements between vendors and customers, and ratings of the reliability and quality of vendors and their goods. Other major discussion topics are operational security issues, such as the concealment of user identities, safe communication methods, and the latest investigation techniques by LEAs.[35] Linklist updates provide an overview of the URLs of hidden services.[36] Other services offered in the dark web include server hosting or VPNs, Bitcoin mixers, and crypto exchanges.[37]

6. Conclusions: Future challenges and opportunities

Cybercrime continues to rise in Germany. Due to underreporting, cybercrime case numbers are probably much higher than reported in official police statistics.

Cybercriminals have become more sophisticated in their attacks. Attacks are growing in technical complexity by dividing labour among cyber experts within the cybercrime-as-a-service business model, where several specialists conduct different steps during a cyber-attack.[38]

As cybercrime affects all of society, it is vital to raise awareness of the threat of cybercrime and potential mitigating measures among internet users, public institutions and private enterprises alike. This education must include essential elements such as handling email or the need to create frequent data back-ups. The adoption of IT security concepts is indispensable for public and private enterprises and institutions.[39]

6.1 LEA capacity building for the fight against cybercrime

To counter the rising threat of cybercrime in Germany has required increasing the capacity of specialised cybercrime units at the federal and state police levels. At the federal level, the BKA set up a new cybercrime department in April 2020. The aim is to pool the competencies within the BKA to combat cybercrime and advance the necessary specialisation of staff in this area. The new cybercrime department succeeds the "Group Cybercrime", created in 2013 and integrated with its 100 staff into the Department of Serious and Organised Crime. The new cybercrime department will gradually grow over the next few years to around 280 staff, including forensic officers, analysts and IT experts with a wide range of specialisations.[40]

The cybercrime department has the following responsibilities:

- to conduct investigations against criminals active in cyberspace and dismantles criminal networks and structures responsible for cyber-attacks on high-ranking targets in Germany;
- to ensure the collection, preparation and analysis of relevant information as a basis for investigations into highly complex cyber technologies by the federal and state police;
- to prevent cyberattacks on federal facilities and critical infrastructure in Germany;
- to advise the Senior Management of the BKA on criminal policy issues related to cybercrime; and
- to actively participate in the further development of relevant legal provisions.

The National Cybercrime Cooperation Centre (NKC), located in the cybercrime department, is responsible for cooperation with public authorities and private sector companies in this area of criminal phenomena. Additionally, the NKC is responsible for coordinating and liaising with the National Cyber Defence Centre, which comprises representatives of the Federal Office for Security in Information Technology, the Federal Office for the Protection of the Constitution, the Federal Office for Civil Protection and Disaster Relief, the Federal Police, the Bundeswehr, the Military Counterintelligence Service and the Customs Criminal Office. In this circle, security-relevant cyber incidents are collected and evaluated together on a working day basis.

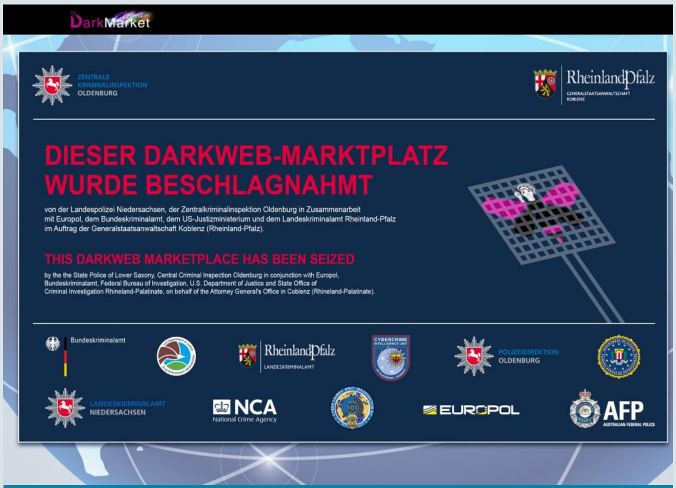
Furthermore, the cybercrime department performs administrative management in the federal-state network of the Central Focal Points Cybercrime (ZAC). The ZAC network was set up to provide companies affected by cybercrime with direct contact with the federal and state police services' relevant cybercrime units.

The cybercrime department's Quick Reaction Force (QRF) is a 24/7 "first assault" call unit in law enforcement. The QRF initiates the first non-deferred criminal procedural measures in the event of cyberattacks on critical infrastructure or federal facilities.[41]

Given the transnational nature of cybercrime, there is a need for practical international law enforcement cooperation in the fight against cybercrime. The cybercrime department coordinates the international exchange of information.

6.2 Recent LEA cyber operations

A major success of such cooperation was the takedown of the world's largest illegal marketplace on the dark web, the DarkMarket, by German LEAs on 11 January 2021. The seizure of the DarkMarket and the arrest of the suspected operator by German police resulted from an international law enforcement operation, including agencies from Australia, Denmark, Moldova, Ukraine, the UK and the USA, and Europol. More than 20 servers were seized in Moldova and Ukraine. Almost 500,000 users and more than 2,400 sellers had been active on the DarkMarket, conducting over 320,000 transactions, with a money transfer of more than 140 million EUR. The vendors on the DarkMarket had mainly traded all kinds of drugs and sold counterfeit money, stolen or fake credit card details, anonymous SIM cards and malware.[42]


DarkMarket
ZENTRALE KRIMINALINSPEKTION OLDENBURG
RheinlandPfalz GENERALSTAATSANWALTSCHAFT KOBLENZ
Bundeskriminalamt
RheinlandPfalz LANDESKRIMINALAMT
CYBERCRIME INTELLIGENCE UNIT
POLIZEIDIREKTION OLDENBURG
LANDESKRIMINALAMT NIEDERSACHSEN
NCA National Crime Agency
EUROPOL
AFP AUSTRALIAN FEDERAL POLICE

DIESER DARKWEB-MARKTPLATZ WURDE BESCHLAGNAHMT

von der Landespolizei Niedersachsen, der Zentralkriminalinspektion Oldenburg in Zusammenarbeit mit Europol, dem Bundeskriminalamt, dem US-Justizministerium und dem Landeskriminalamt Rheinland-Pfalz im Auftrag der Generalstaatsanwaltschaft Koblenz (Rheinland-Pfalz).

THIS DARKWEB MARKETPLACE HAS BEEN SEIZED

by the the State Police of Lower Saxony, Central Criminal Inspection Oldenburg in conjunction with Europol, Bundeskriminalamt, Federal Bureau of Investigation, U.S. Department of Justice and State Office of Criminal Investigation Rhineland-Palatinate, on behalf of the Attorney General's Office in Coblenz (Rhineland-Palatinate).

Seizure of the DarkMarket by the BKA and other international LEAs.

In another major international law enforcement operation in January 2021, law enforcement and judicial authorities from Canada, France, Germany, Lithuania, the Netherlands, the UK, the USA and Ukraine countries with coordination support from Europol and Eurojust disrupted the "world's most dangerous malware" Emotet.43 LEAs gained control of the Emotet infrastructure, including several hundreds of servers located across the world. They took the infrastructure down from the inside by redirecting the victim's infected machines towards law enforcement controlled infrastructure.[44]

References

[1] This Policy Brief was prepared by the University of Applied Sciences for Public Service in Bavaria (BHFOD), Department for Policing, as part of T10.5

[2] See Bundeskriminalamt (BKA), 2020a, Cybercrime. Bundeslagebild 2019, Wiesbaden 2020 [Federal Criminal Police Office: Cybercrime. Federal Situation Picture 2019], p. 50, retrieved from: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html;jsessionid=84ADE59C8966B97AB919A84BE5E55CBA.live0612.

[3] See Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020, Die Lage der IT-Sicherheit in Deutschland 2020, Bonn 2020 [Federal Office for Information Security: The State of IT Security in Germany in 2020], p. 36, retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2; and BKA 2020a, p. 42.

[4] See BKA 2020a, p. 54.

[5] See European Commission 2019, Eurobarometer Cybercrime 2019. Factsheet Germany, October 2019, p.1, retrieved from: file:///D:/Eurobarometer%20Cybercrime%202019%20ebs_499_fact_de_en.pdf.

[6] See European Commission 2019, p. 3.

[7] See Europol, 2020, Internet Organised Crime threat Assessment 2020, retrieved from: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020. The topics of this report are used as a template for the policy briefs on the cybercrime situation in the six INFINITY LEA partner countries Belgium, Germany, Greece, Spain, Portugal and UK to facilitate coherence of the topics and structure of the various country reports.

[8] See BKA 2020a, p. 7.

[9] See BKA 2020a, p. 7 and BSI 2020, p. 6.

[10] See BSI 2020, p. 37.

[11] See BKA 2020a, p. 7.

[12] See BKA 2020a, p. 31.

[13] See Europol 2020, p. 27 + 31; and BKA 2020a, p. 35.

[14] See BKA 2020a, pp. 36-40.

[15] See BKA 2020b, Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie, Wiesbaden 2020 [Federal Criminal Police Office: Special Analysis Cybercrime in Times of Corona Pandemic], p. 5, retrieved from: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeSonderauswertungCorona2019.html?nn=28110.

[16] See BSI 2020, p. 34.

[17] See BKA 2020b, p. 6.

[18] See BKA 2020b, p. 10

[19] See BKA 2020b, p. 13.

[20] See Vice World News, 2020, Darknet Drug Dealers Are Now Selling 'Pfizer COVID Vaccines', retrieved from: https://www.vice.com/en/article/akdkkg/darknet-drug-dealers-are-now-selling-pfizer-covid-vaccines.

[21] See Check Point, 2021, Covid-19 'Vaccines' Touted for Just $250 on Darknet, retrieved from: https://blog.checkpoint.com/2020/12/11/covid-19-vaccines-touted-for-just-250-on-darknet/

[22] See BKA 2020a, p. 12.

[23] See BKA 2020a, pp. 16f.

[24] See BKA 2020a, p. 17.

[25] See BKA 2020a, p. 21 and BSI 2020, p. 13.

[26] See BKA 2020a, pp. 21f.

[27] See BKA 2020a, p. 25.

[28] See BSI 2020, p. 16.

[29] See BKA 2020a, pp. 25ff.

[30] See BKA 2020a, p. 27.

[31] See Bundeskriminalamt (BKA), 2020c, Zahlen & Fakten 2019 [Federal Criminal Police Office: Figures & Facts 2019], p. 1, retrieved from: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Kinderpornografie/ Zahlen_und_Fakten/ zahlen_und_fakten_node.html.

[32] See Polizei NRW, 2020, Hightech-Täter: Die Kinderschänder aus dem Schrebergarten haben versteckt im Digitalen gewirkt [Police North-Rhine Westphalia: The child molesters from the allotment garden acted in the digital environment], retrieved from: https://polizei.nrw/artikel/hightech-taeter-die-kinderschaender-aus-dem-schrebergarten-haben-versteckt-im-digitalen-gewirkt.

[33] See BKA: 2020a, p. 18.

[34] See BKA 2020a, p. 30.

[35] See BKA 2020a, p. 32.

[36] See BKA 2020b, p. 33.

[37] See BKA 2020a, p. 34.

[38] See BKA 2020a, p. 53.

[39] See BKA 2020a, p. 54.

[40] BKA 2020d, Bundeskriminalamt stärkt die Cybercrimebekämpfung [Federal Criminal Police Office: BKA strengthens the fight against cybercrime], press release on 01.04.2020, retrieved from: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2020/Presse2020/200401_pmAbteilungCC.html.

[41] BKA 2021, Abteilung Cybercrime [Federal Criminal Police Office: Cybercrime Department], retrieved at: https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/cybercrime_node.html;jsessionid=73107A46EAF34AA9803778993841D0EB.live0601

[42] See Europol, 2021a, DarkMarket: World's largest illegal dark web marketplace taken down, Europol press release of 12 January 2021, retrieved from: https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down.

[43] See Europol 2021b, Word's most dangerous malware Emotet disrupted through global action, Europol Press release of 27 January 2021, retrieved from: https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action.

[44] See Europol 2021b.

Image Credits

p. 1 - Image from https://pixabay.com/illustrations/eu-stars-privacy-shield-symbol-5837837/

p. 4 - Image from https://www.pexels.com/photo/a-close-up-view-of-a-covid-19-vaccine-vial-on-blue-background-5878503/

p. 7 - Image from: https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down