Mid-Module Assignment 1: Presentation – Principles of Digital Forensics and Cyber Law – Transcript – Michael Geiger

Introduction:

Hello, my name is Michael Geiger. In the following presentation I will discuss the case study of the cybercrime that took place in Germany on the dark web website “Deutschland im Deep Web – Keine Kontrolle, alles Erlaubt”, translated in English "Germany on the Deep Web - No control, everything allowed!" and analyze which technical evidence was collected and what impact the case had on police investigations and legislation.

Background:

In order to understand the scope of this cybercrime, the context must first be created. On the 22 July 2016, a killing spree took place in Munich, Germany, resulting in nine people being killed and 27 injured. According to the German Federal Agency for Civic Education (BpB, 2021), the act of terrorism, classified as racially motivated as a result of the trial, is one of the bloodiest in recent German history. The weapon used by the killer was obtained illegally over the internet from a seller using the pseudonym "rico" (United Nations Office on Drugs and Crime, N.D.a). The contact between the buyer and seller of the illegal weapon was made possible via the German Darknet forum "Germany on the Deep Web", whereby the operator of the website made a significant contribution to contacting the illegal transaction at the time of purchase.

National Importance of the Cybercrime:

According to the Global Study on Homicide of the United Nations Office on Drugs and Crime (2013), Germany has a low murder rate in an international comparison. A lower murder rate can also be determined in comparison with other western European countries. When looking at the murder objects used, it is noticeable that firearms make up a rather small proportion in Europe at 13%.

Criminal offenses involving firearms and killing spree in particular are therefore especially shocking for the population. A detailed review and clarification of how the crime could have happened and how such crimes can be prevented in the future are therefore in the centre of social interest and can lead to demands for stricter laws and more rights for the police.

The cybercrime and the context:

The cybercrime involved the operation of the website "Germany on the Deep Web - No control, everything allowed!“, through which illegal drugs and firearms were traded (United Nations Office on Drugs and Crime, N.D.b). One of the firearms traded through the website was used in the 2016 Munich shooting.

The case study therefore shows the direct consequences that cybercrimes can have in the real world. The case also shows what dangers emanate from misused websites and what responsibility the operator of such a platform bears. In addition, this example can be used to illustrate how police investigations and preservation of evidence can lead to the arrest of the offender.

Since, as a result of the investigations, there were calls for more rights for the police to prosecute and investigate crimes on the Internet, this case also has a significant impact on the legal future of cybercrime in Germany.

International comparison:

When looking at the worldwide distribution of Darknet firearms sellers, it is striking that after the United States of America and Denmark, Germany has the third largest illegal online market in the world. Since the Internet has made it significantly easier to acquire illegal firearms, even across national borders, there is a great need for police action, since preventing illegal arms trade is not only in the national, but also in the international interest and the trade poses great danger to the population of the respective target country.

Cybercrime typology and nature:

The website "Germany on the Deep Web" was primarily a platform created for communication and exchange. The operator of the platform Alexander U. known in the deep web under the pseudonym "lucky" stated that the website was created to be able to communicate anonymously in times of mass surveillance (Tanriverdi, 2018). The website was launched in 2013 under an Onion domain, could be reached via the Tor network and was the largest German-language website on the dark web with over 35,000 registered users and an average of 6 million page views per month (Wilkens, 2017).

The German Federal Office for Information Security (BSI, N.D.a) emphasizes that "moving around the dark web as well as operating a website alone is not illegal, even

if it is a security risk". A person becomes a criminal when they consume or download illegal content, or purchase or sell illegal goods and services. Assisting in such a crime is also prohibited.

In the cybercrime case of the Darknet platform, the operator made himself liable to prosecution for several crimes. On the one hand, illegal drugs were traded via the website. Sellers had to send the operator of the website pictures of the drugs, as well as information and prices about them, whereupon these were activated by the operator in the forum "Offer" (United Nations Office on Drugs and Crime, N.D.b). Only verified sellers were able to independently create drug offers in the "Marketplace - Offer verified" forum.

On the other hand, the "Weapons" forum made it possible to trade illegal weapons. The operator did not play a central role in publishing of offers or their brokerage, but by creating and making this forum available explicitly enabled the potential possibility of illegal arms trading. It must be noted that even if the accused states that he never wanted to support the illegal arms trade, by creating this sub-forum he has accepted that criminal offenses in this context are made possible via the website.

Due to the active role of the operator of the website in trading illegal drugs via the website, he is liable to prosecution for aiding and abetting the illegal advertising of narcotics under paragraph 27 of the German Criminal Law (Gölzer, 2020). Due to the possibility of illegal arms trade being made available via the website, the operator made himself liable to prosecution for aiding and abetting the intentional illegal trade in a firearm and for aiding and abetting the intentional illegal acquisition of a semi-automatic handgun. Thus, the crime of aiding and abetting according to paragraph 27

of the Criminal Law has been realized in both sentences. Furthermore, it was clearly established that the firearm used in the 2016 killing spree in Munich was made possible via the website. As a result, the operator of the website was found guilty of aiding and abetting the intentional illegal trade in a firearm in connection with negligent homicide in 9 counts and in connection with 5 counts of negligent bodily harm.

Since the dominant offenses was aiding and abetting a crime in a total of five different contexts, this crime must be examined in more detail. According to Wullbrandt (2015), a distinction must be made between a simple and a particularly serious case of the crime of aiding and abetting. In a simple case, imprisonment of up to 5 years or fines can be possible. In a particularly serious case, the prison sentence is six to ten years.

Due to the large number of cases in which the operator was guilty and the fact that a killing spree took place as a result of the trafficking of illegal firearms via the website, the accused Alexander U. was sentenced to six years in prison for particularly serious aiding and abetting.

Legislative and national efforts:

The website "Germany on the Deep Web" was already known to the police since 2014 and, like the seller of the weapon, was monitored by the authorities. However, it was not until the killing spree in July 2016 in Munich that police investigations intensified (Hostettler, 2017).

On the 23 August 2016, the website was infiltrated by an undercover agent using the pseudonym "Gazza". The investigator took an active part in the participation on the

platform and thus gained the trust of the operator. Attempts to determine the operator’s place of residence using Internet signatures failed, as it turned out that a randomly generated block of text was loaded with each visit to the website, so that it could not be unmasked by the Tor network (Tanriverdi, 2018). However, the suspect called for donations on his website, which according to the United Nations Office on Drugs and Crime (N.D.b) amounted to 9,850 Euro. Investigators were able to trace the money's path and led them to the currency marketplace operator, bitcoin.de. The police were able to use the marketplace operator to determine the residential address and real name of the suspect (Tanriverdi, 2018).

Knowing the suspect's technical skills, investigators wanted to ensure that the primary evidence, the suspect's computer, was on and accessible to the police at the time of arrest. To ensure this, the undercover investigator "Gazza" contacted the suspect via the website immediately before the suspect's house was searched on June 8, 2017 and stated that the website had vulnerabilities. At the same time, the agents launched an SQL attack so that the operator focuses on the computer (United Nations Office on Drugs and Crime (N.D.b). The plan worked and the suspect, as well as all evidence, was successfully confiscated (Mey, 2018).

Cost of the crime and identified issues concerning the crime:

While the crimes did not result in any quantifiable costs, the main reason for the effective investigation was the suspicion of arms trafficking, which resulted in the killing spree in Munich 2016. It can be assumed that, in addition to drug trafficking, other weapons were also traded, which poses a serious risk to the population.

Due to the professionalism of the operator, tracing the operated website was difficult. The operator has not made traceable signatures possible for investigators by loading random blocks of text. The determination of the residential address of the operator could only be determined via Bitcoin transactions.

Due to the operator's actions, the police feared that they would not be able to access the computer if they did not arrest the suspect while the devise was switched on, and that key evidence for the criminal hearings could have been lost.

Examination of public and social perception:

The presented case study shows that the dark web represents a potential space for criminal offenses. In particular, website operators are therefore responsible for only allowing legal actions and actively combating illegal processes. The potential danger posed by the disguised activities of the dark web should not be underestimated, as this can have a serious impact on the security of the population, as the case study has shown.

The dark web and actions that are carried out in this area, as well as the potential for danger, are evaluated differently by population groups. Odendal et al. (2019) find in their studies that older people statistically have little knowledge and skills in relation to the dark web and are rather biased. Younger people, on the other hand, perceive the dark web more positively, but may not act in a sufficiently reflective manner.

The Centre for International Governance Innovation (2019) finds that 66% of respondents think the dark web should be shut down. The German population confirms the international average. However, it must also be highlighted that only 24% of Germans in the survey said they do not use Tor or other dark web

technologies, as they think these technologies are used by criminals. The international average is even only 13%. Few see the benefits that the dark web has in terms of anonymity and freedom of expression.

As a result of the legal investigation of the killing spree and the illegal actions of the criminal Darknet platform "Germany on the Deep Web", political and social demands were made in Germany to change the law and give the police more powers in criminal investigations. Since the legal situation regarding illegal forums on the Darknet and Deep Web has not been sufficiently clarified and there is a question about the complicity of operators, the Federal Council launched a legislative initiative in March 2019 for the criminal record of operators of illegal trading platforms on the Internet (Tremmel, 2019).

The IT Security Act 2.0 of 2021 gave the investigating authorities the authorization to receive more information from the German postal service. The law is listed in the Criminal Law under paragraph 126a and allows a prison sentence of up to three years to be imposed on the operator (BSI, N.D.b). Paragraph 99 of the Law of Criminal Procedure was also changed in such a way that it enables the investigators to obtain information about the mail items received and sent by suspects.

Furthermore, the Federal Office for Information Security is calling for a revised version of the IT Security Act, which should enable the authorities to adopt virtual identities without authorization, to receive more information from service providers and to penetrate systems without authorization.

Conclusion:

The case study presented and the causal connection with the shooting spree in Munich show the drastic consequences that illegal crimes on the Internet can have. The Internet and actions in this space must therefore not be regarded as closed off and detached from the real world, since harmful and illegal online actions can lead to damage for the victims, which can cause not only financial losses, but also psychological and physical damage. In the context of the illegal activities on the "Germany on the Deep Web" website, there is also an imminent threat to the population, since traded weapons are still in circulation and can be used for crimes. As consequence, the responsibility of website operators can be determined, which was included in the German law as a result of the presented cybercrime and makes negligent behaviour a punishable offence.

Possible procedures and investigation methods were presented. It should be noted that criminal investigations into cyber crimes always require the cooperation between investigations on the Internet and analogue investigations. In order to be able to prosecute criminals legally, they must be arrested physically, which is where police operations on the Internet can be of great benefit. Finally, the case shows that police authorities, but also legislation, are confronted with new challenges due to technical advances in the digital space. Legal adjustments may therefore be necessary in order to be able to counteract the new potential criminal offences. In addition, the rights and powers of the investigating authorities must be checked in order to give them sufficient authorization to take effective action against criminal activities.

Thank you for your attention.

References:

BpB (2021) Vor 5 Jahren: Rechtsextremer Anschlag in München. Available from: https://www.bpb.de/kurz-knapp/hintergrund-aktuell/336826/vor-5-jahren-rechtsextremer-anschlag-in-muenchen/ [Accessed 06 September 2022].

BSI (N.D.a) Darknet und Deep Web – wir bringen Licht ins Dunkle. Available from: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Darknet-und-Deep-Web/darknet-und-deep-web_node.html [Accessed 09 September 2022].

BSI (N.D.b) Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). Available from: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html [Accessed 12 September 2022].

Centre for International Governance Innovation (2019) CIGI-Ipsos Global Surver on Internet Security and Trust. Available from: https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/ [Accessed 12 September 2022].

Gölzer, V. (2020) Beihilfe zum Betäubungsmittelhandel – Vermittlung von Rauschgift an Abnehmer muss konkret festgestellt werden. Available from: https://rechtsanwaeltin-goelzer.de/strafrechtsblog/rechtsmittel/beihilfe-zum-betaeubungsmittelhandel-vermittlung-von-rauschgift-an-abnehmer-muss-konkret-festgestellt-werden/ [Accessed 10 September 2022].

Hostettler, O. (2017) Hilflose Ermittler – Warum Kriminelle im Darknet wenig zu befürchten haben. *Bundeszentrale für politische Bildung*. Available from: https://www.bpb.de/shop/zeitschriften/apuz/259137/hilflose-ermittler/ [Accessed 11 September 2022].

Mey, S. (2018) Darknet: Waffen, Drogen, Whistelblower. *CH Beck*.

Tanriverdi, H. (2018) Wie “Lucky” demaskiert wurde. *Sueddeutsche Zeitung*. Available from: https://www.golem.de/news/deutsche-darknet-groesse-wie-lucky-demaskiert-wurde-1811-137709.html [Accessed 06 September 2022].

Tremmel, M. (2019) Neuer Straftatbestand Handelsplattform – Betreiber im Darknet. *Golem*. Available from: https://www.golem.de/news/gesetzesinitiative-des-bundesrates-neuer-straftatbestand-handelsplattform-betreiber-im-darknet-1903-140105.html [Accessed 12 September 2022].

United Nations Office on Drugs and Crime (2013) Global study on homicide: trends, contexts, data. Available from: https://www.unodc.org/documents/gsh/pdfs/2014_GLOBAL_HOMICIDE_BOOK_web.pdf [Accessed 09 September 2022].

United Nations Office on Drugs and Crime (N.D.a) LG München I, Urteil vom 19.01.2018, 12 KLs 111 Js 239798/16. Available from: https://sherloc.unodc.org/cld/case-law-doc/illicitfirearmscrimetype/deu/2018/lg_munchen_i_urteil_vom_19.01.2018_12_kls_111_js_23979816.html?lng=en&tmpl=sherloc [Accessed 08 September 2022].

United Nations Office on Drugs and Crime (N.D.b) BGH, Beschluss vom 06.08.2019, 1 StR 188/19. Available from: https://sherloc.unodc.org/cld//case-law-doc/drugcrimetype/deu/2019/bgh_beschluss_vom_06.08.2019_1_str_18819_.html?lng=en&tmpl=sherloc [Accessed 06 September 2022].

Wilkens, A. (2017) Betreiber eines Darknet-Froums in Karlsruhe festgenommen. Heise. Available from: https://www.heise.de/newsticker/meldung/Betreiber-eines-Darknet-Forums-in-Karlsruhe-festgenommen-3740829.html [Accessed 07 September 2022].

Wullbrandt, T. (2015) BGH: Wann liegt Beihilfe im besonders schweren Fall vor? BGH, Beschluss vom 27.01.2015 – 1 STR 142/14. Available from: https://www.wullbrandt-rechtsanwaelte.de/bgh-wann-liegt-beihilfe-im-besonders-schweren-fall-vor-bgh-beschluss-vom-27-01-2015-1-str-14214/ [Accessed 13 September 2022].