1. My Name is Jan Küfner and today I will present a case study analysis of the illegal online marketplace called “silk road”.
2.
    a. I have chosen the United States of America since records from trials in the US are easily available and since the US discloses a lot of content in those files.
    b. I also have chosen the United States since they are one of the leading countries in cyber forensics and since they are internationally well aligned in terms of prosecution.
3. The cybercrime chosen is
    a. Using the Internet to distribute narcotics
    b. Engaging in a continuing criminal enterprise
    c. I have chosen this case due to the remarkably high sentence for the convicted founder of this illegal marketplace, which is life in prison without parole. This sentence peaks interest in the case, since it is interesting to see what negative implications running the website must have had to other people so that a sentence this high is being given to the accused (Hong, 2015) (UN, 2017)
    d. This cybercrime was also chosen, since dark web marketplaces are growing tremendously according to Forbes. This shows that this type of cybercrime is currently not vanishing or declining and that we will see many further trials about darknet marketplaces (Beenu, 2020)(Woolf, 2015)
    e. Lastly, the fact that US law enforcement agencies seized over 1 billion dollars in bitcoins also makes this case very interesting. (Hern, 2020)
4.
    a. When you have a criminal enterprise that uses the internet to distribute drugs, you typically do this with a darknet marketplace. Those darknet marketplaces are like normal web shops. The main difference however is the fact that most items traded on these shops, are illegal goods or services. In the case discussed 70% of the items sold were drugs. The drugs are paid with cryptocurrency and then shipped by standard postal services.
    b. The crime we are discussing is a cyber-enabled crime. It is not a crime that is dependent on the existence of IT technology like ransomware attacks for example are.
    c. It is however largely enabled by modern IT technology, since current software tools offer easy anonymity for parties involved
    d. The first technology essential for the operation of darknet web shops is a way to anonymize the person hosting the website as well as the customers and the vendors of the illegal goods or services. The technology currently used to do this effectively is TOR, which is short for “the onion router”.
    TOR provides anonymity by routing the traffic through a network of servers, that add encryption with each hop, which essentially makes it very hard to trace who send a particular TOR message.
    Providing anonymity unfortunately supports cybercrime, but it is also worth to mention that TOR can circumvent governmental censorship. This is currently being done in Russia by people that want to obtain information from sources that are banned within their own country.
    e. The second technology essential to maintain anonymity is using payment options like Bitcoin and other crypto currency. (Whippman, 2011), (Department of Justice, 2015) (Weiser, 2015), (Hong, 2015), (Mullli, 2015), (UN, 2017), (Beuth, 2022)

5. Now let me talk about how the United States of America deals with cybercrime nationally and internationally
    a. National they do have a plethora of well skilled state as well as nationwide agencies. In this case study the FBI Cyber Division, the DEA`s Organized Crime Drug Enforcement Strike Force, the NSA and the Secret Service as well as many others were involved.
    b. Internationally the US is a member of several multilateral treaties that help to fight cybercrime. The US is for example member of the "Convention on Cybercrime of the Council of Europe" also called "Budapest Convention" and the US is also a member of the "UN Convention against Transnational Organized Crime (UNTOC)" as well as many other treaties.
    c. The US not only has multilateral treaties, but also bilateral treaties. Those treaties typically guarantee mutual legal assistance, which helps to summon witnesses, to collect evidence and finally to prosecute criminals. Some bilateral treaties regulate extradition to and from the US.
    d. The US is also a member of many International Organizations such as the "United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ)", the "Group of Seven (G7)'s 24/7 Cybercrime Network" and the "EUROPOL's Joint Cybercrime Action Taskforce (J-CAT)" (NN, 2016), (Peters and Hindocha, 2020)
    e. There is a lot of legislation available, and it is updated and maintained in the US. One example would be „The Better Cybercrime Metrics Act "which came into force very recently on May 2nd of 2022. It requires the FBI to report statistics on cybercrime, which will enable researchers to investigate the data collected to for example be better prepared for cybercrime in the future. (Tillis, 2022)
6. Typically, the impact of most cybercrimes like ransomware is measured monetary, meaning that you quantify the impact by the amount of money lost due the cybercrime.
   With this case the impact is however different.
    a. Drugs sold on the silk road were linked to six overdose deaths by law enforcement. To establish this link law enforcement agencies had to spend a lot of time and resources. (Department of Justice, 2015), (UN, 2017)
7. On this slide I will talk about issues in the crime investigation and about issues in gathering evidence.
    a. In general, it can be stated that it was very hard to find the identity of the criminals involved since Bitcoin and TOR browser were used.
    b. Additionally, it can be said that many pieces collected from various agents and agencies needed to be interconnected to find a main suspect, which then was put under close surveillance.
    c. Another piece of the puzzle which was also hard to obtain by law agencies and which consumed a lot of resources, was the identify of some of the vendors. The identities were obtained by posing as buyers and by seizing packages with narcotics and by tracing back those packages back to its source and arrest the sellers of the illegal goods. The vendors resided in many different countries, which made this an international attempt.
    d. Infiltrating the administration of silk road by identifying the identify of a forum moderator and by forcing to hand over her credentials to law enforcement, so law enforcement could act as this moderator was another key element that led to the conviction
    e. Additionally, law enforcement tried to build up trust by posing as vendors to obtain information from the accuse, to convict him. This however was not successful.

Indeed, two police officers that acted as undercover drug vendors were charged stealing bitcoin`s from other vendors on silk road. This shows that it is likely that law enforcement tried several other ways to obtain evidence, that might not be public record, since they did not lead to the conviction. This however got public knowledge due to other reason.

f. FBI specialist identified vulnerabilities on the website leaking the IP of the server and disclosing its location. The Defendant and his lawyers however claim that this is not true and that identifying the location / obtaining the evidence was done unrightfully by the NSA. Once the location of the server was found a copy of it was provided to forensics. Forensics then found an alias of the site admin that later helped to link the accuse with the crime.
g. To provide evidence that holds in court law enforcement agencies finally set a trap for the criminal, where they successfully caught him being locked in as the main administrator of the darknet marketplace silk road.
h. Once they had the laptop, they were able to obtain chat logs as well as personal journals, that provided further evidence of him being the main criminal. This further evidence also shed a light on the extent of his crime and his motivation behind it.

(NN, 2016)(NN, 2015)(Schmeh, 2020)

8. Let me now do a critical examination of public and social perception worldwide as well as in the United States.
    a. Firstly, one can say that there is no difference in comments from the US compared to the rest of the world. We have many people condemning the crime, but also others that do not agree with the verdict.
    Typical comments are that people running the marketplace should get very high sentences.
    Some radical hacktivists however seem to strongly disagree with the justice system by illegally disclosing the social security number and the home address of the judge ruling in that case. This is obviously illegal and an attack of the legal system which is a foundation of the world we live in.
    Complete different but nonetheless noteworthy comments are about the doubt that can be seen in the methods used by law enforcements. Many cannot believe how the FBI found the location of the webserver and see it as proven, that tools from the NSA were used illegally to obtain essential evidence.
    There are also posts, that point out the hypocrisy of the accuse, because the accuse said that he wanted to liberate the people from government oppression with his darknet web shop, which to his believe should lead to peace, whilst himself ordering assassinations of people on his darknet shop, which the opposite of a peaceful behavior. (Gonzales, 2014) (Losbar, 2014)(Pflaum, 2021)(Mullin, 2015),(Calder, 2014),(Gonzalez, 2014),(Mirea, Wang and Jung, 2018)

9.
    a. In conclusion it can be stated that a lot of investigation effort is necessary to convict people committing cyber enabled crimes
    b. It can also be stated that local law is not as important as being well connected internationally with treaties etc., since cybercrimes are hard to solve, when the criminals can act from countries where prosecution is minimal, and extradition is nonexistent. Even in this case, where the accuse acted from within the US, the help from another country was essential to convict the cybercriminal.
    c. Although IT technology like TOR has good intentions, it is nonetheless a strong enabler of cybercrime. However, others say that a darknet market place reduces the

violence, since drugs can be bought from your house, which is a safe environment, compared to real world drug selling placed, where there is typically violence. This disputed argument however is built on the fact that drug consumption would not increase when drugs are sold online instead of in the real world.

d. Darknet shops will continue to boom. Lots of effort from highly skilled personnel is therefore necessary to counter this trend.

10. References

Beenu, A. (2020) *Five Key Reasons Dark Web Markets Are Booming*, *FORBES*. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/04/23/five-key-reasons-dark-web-markets-are-booming/ (Accessed: 10 May 2022).

Beuth, P. (2022) *Ukraine-Krieg: Twitter hilft russischen Nutzern, die Zensur zu umgehen*, *DER SPIEGEL*. Available at: https://www.spiegel.de/netzwelt/apps/twitter-hilft-russischen-nutzern-die-zensur-zu-umgehen-a-97516aee-6d2c-4c2b-bfe9-8431badec933 (Accessed: 10 May 2022).

Calder, R. (2014) *Judge in Silk Road case gets death threats*, *METRO exclusive*. Available at: https://nypost.com/2014/10/24/hackers-threaten-federal-judge-in-silk-road-founder-case/ (Accessed: 11 May 2022).

Department of Justice (2015) *Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced In Manhattan Federal Court To Life In Prison*, *USAO-SDNY*. Available at: https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison (Accessed: 11 May 2022).

Gonzales, P. (2014) *Hackers leak SSN, address of judge in Silk Road case | Washington Examiner*, *Washington Examiner*. Available at: https://www.washingtonexaminer.com/hackers-leak-ssn-address-of-judge-in-silk-road-case (Accessed: 11 May 2022).

Gonzalez, P. (2014) *Hackers leak SSN, address of judge in Silk Road case*, *Washington Examiner*. Available at: https://www.washingtonexaminer.com/hackers-leak-ssn-address-of-judge-in-silk-road-case (Accessed: 11 May 2022).

Hern, A. (2020) *US seizes $1bn in bitcoin linked to Silk Road site | Bitcoin |*, *The Guardian*. Available at: https://www.theguardian.com/technology/2020/nov/06/us-seizes-1bn-in-bitcoin-linked-to-silk-road-site (Accessed: 11 May 2022).

Hong, N. (2015) *Silk Road Creator Found Guilty of Cybercrimes - WSJ*, *THE WALL STREET JOURNAL*. Available at: https://www.wsj.com/articles/silk-road-creator-found-guilty-of-cybercrimes-1423083107?mod=WSJ_hp_RightTopStories (Accessed: 10 May 2022).

Losbar, Y. (2014) *Ross Ulbricht Silk Road Trial Judge Facing Death Threats on Dark Net*, *CCN.com*. Available at: https://www.ccn.com/ross-ulbricht-silk-road-trial-judge-facing-death-threats-dark-net/ (Accessed: 11 May 2022).

Mirea, M., Wang, V. and Jung, J. (2018) 'The not so dark side of the darknet: a qualitative study', *Security Journal 2018 32:2*, 32(2), pp. 102–118. doi: 10.1057/S41284-018-0150-5.

Mullin, J. (2015) *Ulbricht guilty in Silk Road online drug-trafficking trial*, *Ars Technica*. Available at: https://arstechnica.com/tech-policy/2015/02/ulbricht-guilty-in-silk-road-online-drug-trafficking-trial/ (Accessed: 11 May 2022).

Mullli, J. (2015) *Ulbricht guilty in Silk Road online drug-trafficking trial*, *Ars Technica*. Available at: https://arstechnica.com/tech-policy/2015/02/ulbricht-guilty-in-silk-road-online-drug-trafficking-trial/ (Accessed: 11 May 2022).

NN (2015) *United States of America v.- Ross William Ulbricht*.

NN (2016) *ROSS WILLIAM ULBRICHT, a/k/a DREAD PIRATE ROBERTS, a/k/a SILK ROAD, a/k/a SEALED DEFENDANT 1, a/k/a DPR, Defendant-Appellant. Before: NEWMAN, LYNCH, and DRONEY, Circuit Judges.* doi: 10.54648/aila1979007.

Peters, A. and Hindocha, A. (2020) *US Global Cybercrime Cooperation: A Brief Explainer – Third Way*. Available at: https://www.thirdway.org/memo/us-global-cybercrime-cooperation-a-brief-explainer (Accessed: 11 May 2022).

Pflaum, A. (2021) *Cyberbunker: Knapp sechs Jahre Haft für Betreiber von Darknet-Rechenzentrum*, *DER SPIEGEL*. Available at: https://www.spiegel.de/netzwelt/web/cyberbunker-knapp-sechs-jahre-haft-fuer-betreiber-von-darknet-rechenzentrum-a-88b75402-24d0-494f-91f9-82d57d74d2d1#kommentare (Accessed: 11 May 2022).

Schmeh, K. (2020) *Illegale Handelsplattform Silk Road: Wie das Amazon des Darknet aufflog*, *heise online*. Available at: https://www.heise.de/hintergrund/Illegale-Handelsplattform-Silk-Road-Wie-das-Amazon-des-Darknet-aufflog-4954604.html (Accessed: 11 May 2022).

Tillis, T. (2022) *Tillis Legislation to Help Fight Cybercrime Signed Into Law*, *US Senator for North Carolina*. Available at: https://www.tillis.senate.gov/2022/5/tillis-legislation-to-help-fight-cybercrime-signed-into-law (Accessed: 11 May 2022).

UN (2017) *United States of America v. Ross William Ulbricht, No. 15-1815-cr (2d Cir. May 31, 2017)*, *UNODC.org*. Available at: https://sherloc.unodc.org/cld//case-law-doc/cybercrimecrimetype/usa/2017/united_states_of_america_v._ross_william_ulbricht_no._15-1815-cr_2d_cir._may_31_2017.html?lng=en&tmpl=sherloc (Accessed: 10 May 2022).

Weiser, B. (2015) *Ross Ulbricht, Creator of Silk Road Website, Is Sentenced to Life in Prison*, *The New York Times*. Available at: https://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentenced-to-life-in-prison.html (Accessed: 11 May 2022).

Whippman, R. (2011) *Bitcoin: the hacker currency that's taking over the web | Technology*, *The Guardian*. Available at: https://www.theguardian.com/technology/2011/jun/12/bitcoin-online-currency-us-government (Accessed: 11 May 2022).

Woolf, N. (2015) *How to Cite Pictures in PowerPoint*, *The Guardian*. Available at: https://www.howtogeek.com/664876/how-to-cite-pictures-in-powerpoint/ (Accessed: 11 May 2022).