CYBERCRIME AND PUNISHMENT
In the shadows of the Internet

University of Tampere
Group “Ray of Light”
Rauli Virtanen

1 Abstract

In the field of crime, It's nothing new that in legislation is continuously trying to keep up with new, unwanted, actions in society. It's like an old cat and mouse -play between police and criminals. Digital development, especially internet and dark net, offers new radical tools to this equation, anonymity and availability – it makes mice bats and forces law enforcement to find wings and learn to fly too.

While changes in the digital world are rapid and somewhat uncontrollable, fundamental legal principles and human rights are considered immutable and unbreakable. Those principles control concrete legislation which on the other hand binds the hands of law enforcement and the court of law. Seems like a cat has some ball chained to in its leg.

Offences are not always new, but the methods to commit them are. Now it is easy to order drugs or attack someone's enterprise from home with a few mouse clicks anonymously. Question is, how much this will this equation of fast, easy and relatively risk-free possibilities to commit crimes and stiff, unfunded and with bloated human rights pressure ridden law enforcement change the field of crime? It is safe to say that a lot of is needed from individuals themselves to be aware of threats and defend their own property and rights.

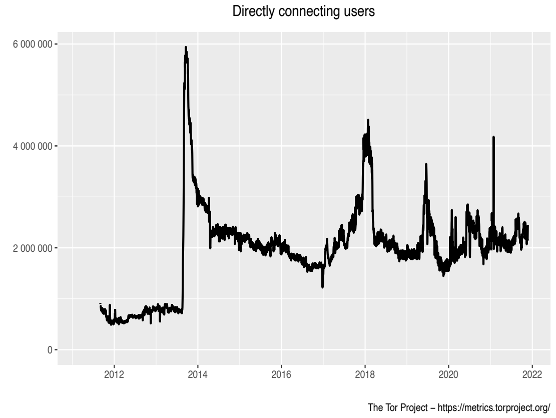
This paper, when dealing with concrete legislation, is written in the Finnish point of view applying the Finnish Criminal Code. It is not possible to analyze differences between different countries in the scope of this paper, nor is it necessary. European Union has been harmonizing legislation also in this field, through the Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems.

"Right or wrong, it's very pleasant to break something from time to time."
— Fyodor Dostoevsky

1.1 The Tor network

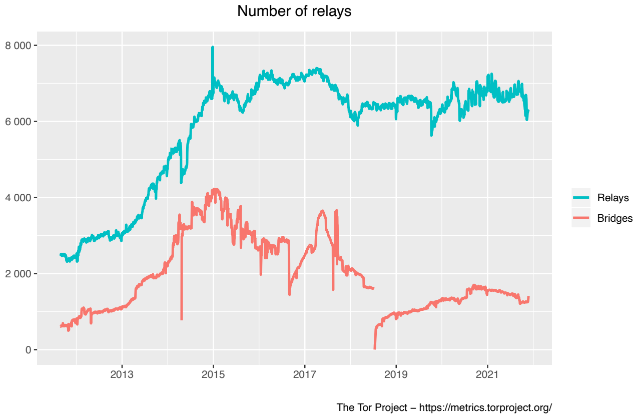
In 2004, Paul Syverson, Robert Dingledine, and Nick Mathewson presented Tor, a circuit-based low-latency anonymous communication service. [1]

Main aspect of the Tor network regarding to this paper and in general is, that Tor provides anonymity and layered encryption to users. As everything, this can be used in good or malicious purposes. As an amount of Tor network users rise, this becomes more and more essential in our world. Today network has over 3 million directly connected users and 6 thousand relays. However, network seems to have reached it's maximum userbase as it is now. [2] (Figures 1 and 2) Large userbase is one important factor in providing anonymity of the network.



The Tor Project – https://metrics.torproject.org/

Figure 1: Tor users



The Tor Project – https://metrics.torproject.org/

Figure 2: Tor relays

In a technical point of view Tor network is circulating the data between source and destination through three random relays and in this way is able to hide users IP -address making it unable to locate them, thus providing anonymity. In addition, Tor Browser prevents websites from "fingerprinting" or identifying you based on your browser configuration. [3]

Relays in the circuit divide their information of the peers. First relay only sees that someone is using Tor network, but can't see what is the content. Middle relay doesn't see who is connect or what is the destination, and the exit relay only sees the destination, but not who is using the service. [1]

1.2 Onion websites

Onion websites are the sites, where (also) illegal marketplaces run. As users, services are hidden too and only accessible from Tor network. Service has a public and a private key. Address is formed by hashing the public key and it is stored in a distributed hash -table. It is protected with a private key by the onion service. With the public key everyone is able to verify that private key only owner has matches it. Onion website addresses end with ".onion".

There is a multistep process, how client and onion website are making a connection between them through a distributed hash table. Extremely simplified, website is picking three random nodes as introduction points and uses one of them as a rendezvous -point where random nodes between client and this rendezvous -point will be connected. In the end there is five random nodes between client and server, and connection is secured and encrypted with pair of public and private keys.

1.3 Marketplaces

Marketplaces run on onion websites as a hidden services and the host of the service is basicly untraceable. This makes it suitable also to run a basic webshop selling illegal goods.

Count of marketplaces has grown with the grown userbase from the beginning. Onion services V2 are making way to V3, and at the moment there is over 650 thousand V3 onion hidden services. [2] (Figure 3)

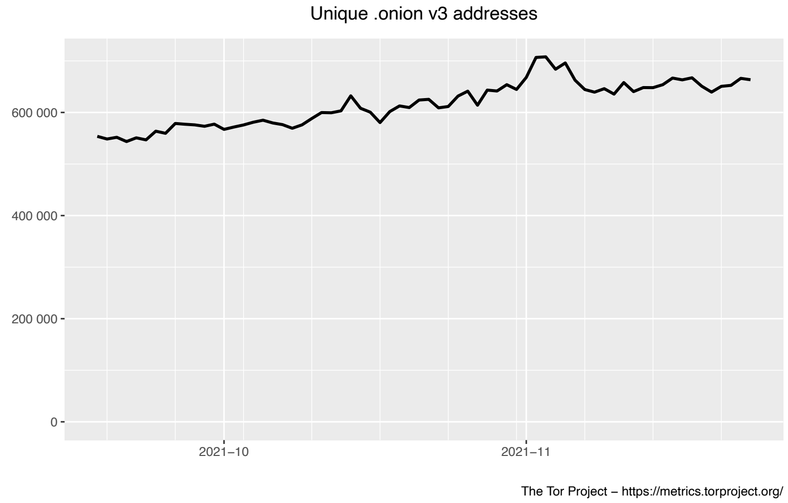


Figure 3: Hidden services

Only a fracture, about 15%, of these addresses are evaluated to be webservices. [4] Marketplace scene and their addresses are somewhat labile with a short lifespan, which makes it hard to estimate the amount of functional web markets at given moment.

There are a large variety of goods to be bought on these marketplaces; physical items, software, malware, information and services. Some of them are illegal to purchase according to Criminal Code of Finland, while others are not.

More about the available purchases in chapter 5.2.

1.4 Cryptocurrencies

Anonymous marketplaces alone wouldn't offer complete anonymity of transactions as a whole. Payment with (legal) credit cards would leave traces which would make it possible to identify both parties. Rise of the cryptocurrencies has provided anonymity also to pay for goods or services making transactions of digital goods hard to trace or untraceable. Physical items need to still be delivered and this makes criminals vulnerable.

Cryptocurrencies are virtual currencies. Bitcoin was the first one, open source software developed by pseudonym called Satoshi Nakamoto 2008-2009. Transactions of this decentralized digital currency are stored in a public blockchain which are verified by cryptography calculated by "miners". Blockchain can't be altered and no central bank supervision is needed. Bitcoin isn't actually anonymous due to the fact of public blockchain.5

After Bitcoin, several other currencies have followed. According to ConMarketCap, world's most-referenced price-tracking website for cryptoassets, there is 14.865 different cryptocurrencies available at the moment. [6]Different currencies have different attributes and perks, and advertise being genuinely anonymous, such as Monero.[7]

1.5 General principles and doctrines of the criminal law

While applying essential elements of criminal acts, the general conditions of criminal liability in criminal code have to be fulfilled as well in cybercrimes. Furthermore complicity (e.g. co-partners, incitement, aiding and abetting in crime) may actually be realized in any type of crime also by taking advantage of the information network. [8]

1.5.1 Legality principle

According to legality principle, “Nullum crimen sine lege”, a person cannot or should not face criminal punishment except for an act that was criminalized by law before he/she performed the act. This idea is also manifested in laws that require criminal acts to be publicized in unambiguous statutory text.[9]

This is a global and generally accepted principle to guarantee a due trial in all civilized countries, and is presented widely in literature, international treaties and also in the Criminal Code of Finland (13.6.2003/515) 3:1 §.

1.5.2 Intent and negligence

As well as legality principle also intention is related to the fact that citizen must be aware what is illegal and decide nonetheless act against the law. Intent or negligence are prerequisites for criminal liability. Basic rule is, that unless otherwise provided, an act is punishable only as an intentional act.

For example when a perpetrator unlawfully obtains or tries to obtain narcotics and that has been his or her purpose or he or she had considered the consequence as a certain or quite probable result of his or her actions, he or she shall be sentenced for a narcotics offence. (50:1 §)

The conduct of a person is negligent if he or she violates the duty to take care called for in the circumstances and required of him or her, even though he or she could have complied with it. (3:7§) Lines between an accident (not punishable), negligence, gross negligence and intent must be done considering the circumstances of the case.

For example a person who intentionally or through gross negligence imports medicine unlawfully shall be sentenced for a medicine offence (44:5§).

1.5.3 Incitement

A person who intentionally persuades another person to commit an intentional offence or to make a punishable attempt of such an act is punishable for incitement to the offence as if he or she was the perpetrator (3:5§).

Incitement applies to the cases, when a person buys a criminal service such as DDoS attack or a computer break-in (38:8§) from another.

2 Research questions

Laws, criminal laws especially, are the program code of society for humans. It's important to know how the society works and why it doesn't. Difference between the laws and the code is that the bits of society, us, are not reliable. We sometimes act according to law, to (criminal) code and sometimes don't.

It is also interesting to discuss the impact of dark web to obedience of law. In criminology, there is a theory of choice in which individuals balance the benefits and costs of crime. The crime prevention effects of the threat of punishment, the ultimate goal of the criminal law, is called "deterrence". It is clear that anonymity significantly reduces the certainty to get caught or at least makes people think that way, which is the important factor when they are doing the risk analysis – consciously or not. The certainty of being caught is a vastly more powerful deterrent than the punishment.

In this study I am aiming to clarify the actions in the dark web on the criminal point of view focusing on the following research questions:

1) What actions are possible for users and which of them are considered a crime?
2) What crimes could be committed?
3) What could be the consequences?
4) How does the dark web transform the traditional field of criminality?
5) What is the response of the law enforcement?

3 Methodology

3.1 Research design

This paper is not purely quantitative in nature. Marketplaces are studied beyond numbers and explored what kinds of different types of behaviors are possible in sites and at which ones of them and with what qualifications they could be arranged to fit traditional laws.

Crimes could be categorized by the degree they use digital technologies.

1) Aided by them, which includes very large scale of crimes, since even basic communication is nowadays usually done by using the digital media.

2) Crimes where technologies play a significant role, such as

3) Crimes where need of technologies are imperative. Crimes on dark web fall into this category.

To analyze the consequences of the dark web marketplace crimes I have focused on the third point to rule out the crimes that could be done AFK too. I tried to find changes in criminality on the basis of verdicts on these crimes, realizing on the other hand that only a small fracture of them are investigated to the point where they are processed in the court of law.

3.2 Data collection, samples and analysis

To determine possible actions, I have gathered data from the following marketplaces by visiting them in the autumn of 2021 comparing differences and similarities in them. I have visited marketplaces shown in table 1 in a chapter 5.1.

To gather data of the sentences given in Finland I focused in two crimes involving “data system offence device” and to compare number of cases, sentences given in example cases where such “device” is used. This data is collected from the Statistics Finland’s (Tilastokeskus) database: Prosecutions, sentences and punishments. Data consists of number of penalties, has the penalty been fine or imprisonment and how much or long it has been.

Data is presented and analyzed in more detail in chapter 5.

3.3 Limitations

Sentences are only a tip of the iceberg. Only a tiny fracture of crimes is even reported in general depending on a crime and in cybercrimes the proportion is even smaller. This is because of the poor prognose of the crime investigation due anonymity.

On the other hand, if we are able to estimate crime rate from the dark web usage side and polls about it, we can compare these two aspects and get valuable information.

4 User actions on dark web

4.1 Common preliminary actions

Before it is possible to order goods there is some preliminary actions need. Naturally one must download the Tor browser first, since these marketplaces are not viewable with common clearnet browsers. After that user needs to find an url -address of an active and working marketplace and enter the site. Those actions are needed in every case. To be able to browse available goods, some sites require user to register to the site, while others don’t. On a table 1, I have gathered this requirement on some of the largest marketplaces on a dark web.

Site name	Requires registration
DarkFox Market	No
TorRRez Market	Yes
CourierMarket	Yes
SilkRoad 4	Yes
Vicecity	Yes
Asap Market:	No
Blackpass	Yes
Monopoly Market	No
Versus Market	Yes
Dark0de	Yes
Archetyp Market	Yes

Incognito Marketplace	Yes
CannaHome	Yes
Tor2door	Yes
Cypher Market	Yes
Cannazon Market	No
Revolution	Yes
Cartel Marketplace	Yes

Table 1: Registering requirements on a different marketplaces

After signing up user must transfer funds to his or her account.

All these actions are necessary but not adequate actions to commit a crime. According to legality principle as described in chapter 2.5.1, the punishment and other sanction under criminal law shall be based on law. There is no law which would unambiguously declare these actions to be crime.

Closest ones one could think of are money laundering and preparing a criminal act, but even if that would be a final intention of the user, at this stage of crime neither of them would alone constitute a crime. These are perquisite acts to many crimes, and could show an intent to commit a criminal act – especially if everything the site has to offer is illegal, but it would be impossible for prosecution to prove which crime user was willing to commit – even if already preparation of such crime would be punishable by law.

4.2 Purchases

There is numerous types of items on the dark net marketplaces like organs for transplant (10.000$), stolen cars (15.000$) and construction sets of a DYI drug lab (400$) , and services like hitman (25.000$/15.000$), kidnapping (500$) and hacking. On the other hand not all of them are illegal. For example buying different kinds of "clicks", followers, retweets and likes is not a crime, although those will probably break user agreements of applications. There are also legitimate software available, and also some tutorial's and ebooks copyright infringements might be on a gray area. In the following chapters I will focus only a few of those items, data and services which deserve some more discussion. In a table 2 I will list some more of acquired goods and which crimes could be committed by acquiring them.

4.2.1 Physical items

Most of the cybercrimes can't be committed by actions taken only on dark web marketplaces, especially when crime would be to acquire or try to acquire illegal physical items. Further information need to be given in private messages – mostly using wickr -message service, which is considered anonymous.

It is notable, that if the buyer chances his/her mind after payment and does not provide additional information, such as delivery address, or by other passivity causes that there is no possible ways to finish the criminal act, his actions are not punishable. An attempt is not punishable if the perpetrator, on his or her own free will, has withdrawn from the completion of the offence, or otherwise prevented the consequence referred to in the statutory definition of the offence. (5:1§)

Therefore, it is paramount to the law enforcement to see the criminal act through before intervening it. Of course, one must bear in mind that the court of law will make the final ruling and consider the degree of the progress of crime and circumstances case by case separately.

Drugs

Drugs are the most common item sold in dark web marketplaces and different variety of them is found in all investigated ones. Some of them sell only drugs and other intoxicating substances as Silk Road 4, Cannazon and Tor Market.

Legally this is pretty straight forward. A person who unlawfully imports or attempts to import or exports or attempts to export a narcotic substance, or transports it or has it transported or attempts to transport or attempts to have it transported or possesses or attempts to obtain a narcotic substance, shall be sentenced for a narcotics offence to a fine or to imprisonment for at most two years.

It would be interesting to know how much anonymity provided by dark web has increased use of narcotics. Even before this possibility acquiring the substances has been relatively easy and hardly a reason for anybody's abstinence from a use of substances. Sadly, this kind of data is not available.

According to an international survey of drug use, Finland was found to be the country with the largest proportion of individuals who acquired drugs on the dark web. Around 45 percent of the nearly 2,200 respondents who had used or bought drugs in Finland over the past year said they had acquired them via the anonymous network.[10]

4.2.2 Digital items

Copyright infringements

Piracy is not a new phenomenon. As long as there has been protected intellectual rights, there has been infringements. Every time, when the media has evolved, the pirates have followed. First on a digital media, then online and finally from peer-to-peer BitTorrent -services to dark web. Finreactor was a Finnish p2p BitTorrent service, online and closed by police 2004. [11] Trial was the first of a kind in Europe. Around the same time was The Pirate Bay, the biggest service in the world, launched and despite several trials it is still running. These services don't provide anonymity to users. These will be punished as a copyright offence.

Malware and username/password -bundles

A person won't commit data and communications offences (chapter 38) such as message interception (38:3§), interference with communications (38:5§), interference in an information system (38:7a§), computer break-in (38:8§) or offence involving a system for accessing protected services(38:8b§) by buying tools to commit these crimes.

There are however two separate statues concerning bundles and malwares. 34:9a§ which is harmonized according to the European union directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems, passed 2013[12] about importing and procurement for use of these tools and older one, 34:9b§, including possession of the tool.

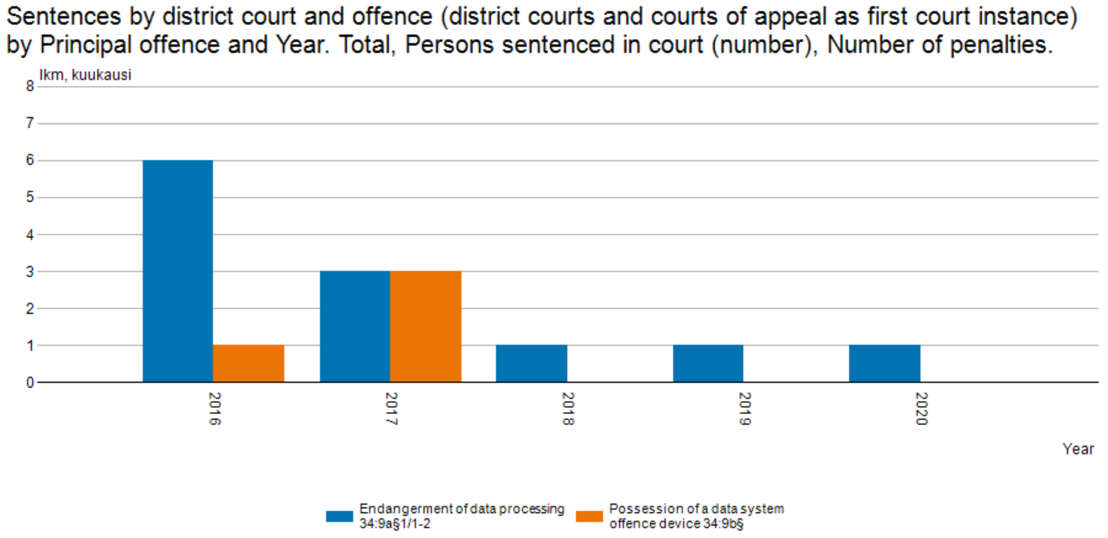
As “tools” are considered to be 1) a device or computer program or set of programming instructions designed or altered to endanger or damage data processing or the functioning of an information system or telecommunications system or to break or disable the technical security of electronic communications or the security of an information system, or 2) an information system password, access code or other corresponding information belonging to another.

According to the directive and 34:9a§ it is also considered a endangerment of data processing, if one disseminates or makes available instructions for the production of a computer program or set of programming instructions of such program. There are two things to point out in this. Firstly, acquiring such instructions is not criminalized, only selling and secondly it is hard to draw a line in which programming tutorials can be used also to malicious purposes.

It is also important to notice, that not every kind of importing, obtaining or possessing is punishable. That has to be made in order to impede or damage data processing or the functioning or security of an information system or telecommunications system.

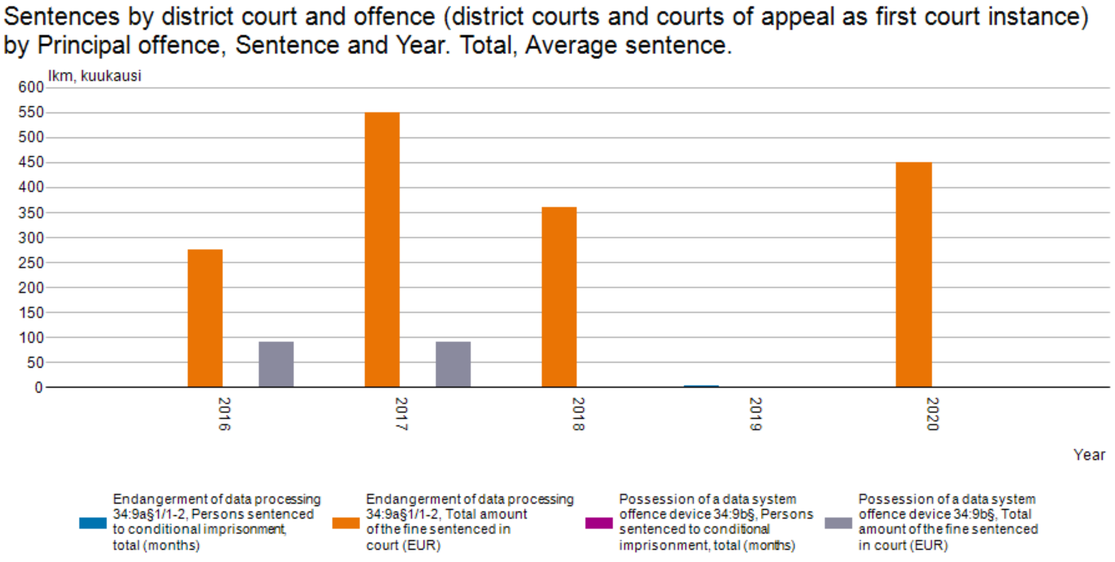
These crimes a rarely in the court of law. In 5 year period, from 2016 to 2020 there has only been 16 persons in total who has been sentenced for acquiring or possessing tools with an intent to commit a cybercrime. These cases are presented in figure 2.

Furthermore, sentences have been really mild. Only in one case sentence has been conditional imprisonment month, others were fines in average 260 – 550 euros per year. This is shown in figure 6.



Source: Prosecutions, sentences and punishments, Statistics Finland

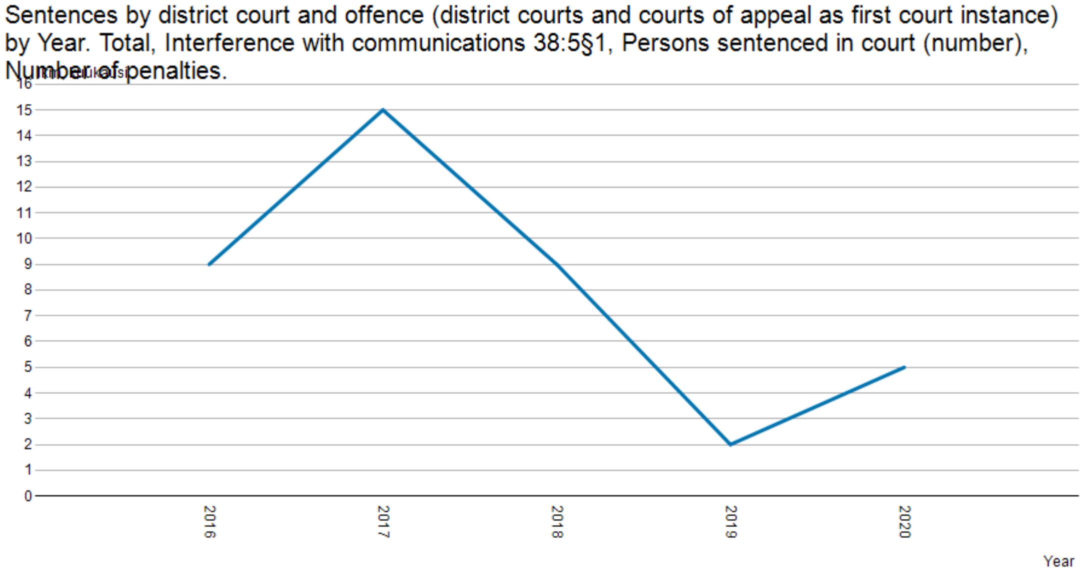
Figure 4: Persons sentenced in court for endangerment of data processing or possession of a data system offence 2016-2020



Source: Prosecutions, sentences and punishments, Statistics Finland

Figure 5: Sentences in court for endangerment of data processing or possession of a data system offence 2016-2020

It is notable though that using above mentioned tools would be processed under different paragraphs, such as illegal data interference (40 cases) as shown in figure 6. Here I am only focusing of buying and possessing id bundles or tools from dark web, not about using them outside the market.



Source: Prosecutions, sentences and punishments, Statistics Finland

Figure 6: Cases of illegal data interference in years 2016-2020

4.2.3 Services

There's a lot of services on the different marketplaces to order. Here I define service as a bought unique work performance which is performed as ordered. Customer is here passive and does nothing after order. Many items sold under the service option are variety of money transfers, a type of money laundering, but since customer needs actively participate to crime, those do not fall in this category on this paper.

Services would be the most probable way to commit a crime on a whim. There's no delivery, hence no physical address needed and for example DDoS attack could be carried only by knowing the target url -address. Order could be carried out by a simple message included to the web order. There not much additional information to be given in different messaging -services.

On the sites studied for this paper, same services occur almost in every marketplace. Most typical illegal ones are hacking, cracking and DDoS-attacks. Some cases physical violence, framing for crimes (ruin life, swatting), kidnapping, killing are also available, but they are not so common.

Also, different kind of boosts for numerous different social media platforms are available, but as long as these services don't use illegal methods to perform the task, those are not criminal acts. They might be violations of the end-user license agreement though.

By ordering services, it is possible to commit a large scale of crimes. Ordering illegal service, a crime, is a criminal act as incitement and will be punished as the client would have committed the crime him- or herself. So, for example ordering a DDoS attack on a target is considered illegal interception.

5 Results

Answers to the research questions:

1) What actions are possible for users and which of them are considered a crime?

Possible and needed actions are downloading a tor browser, creating an account, and transferring funds to own account. Those actions are not considered criminal according to the Finnish criminal code. After that it is possible to buy physical items, digital software and data, and different kind of services. If it's criminalized to acquire an item and user has carried out actions to the stage, where it's possible for him or her concretely to gain possess to it, it is considered a crime. When an illegal service is ordered and seller has enough information to fulfill the order, it is considered a crime.

2) What crimes could be committed?

Most of the items are only tools to commit crimes. Only buying items that are criminalized to acquire, physical or digital, is illegal. Bought services shall be punished as incitement like user would have done the criminal act by him- or herself.

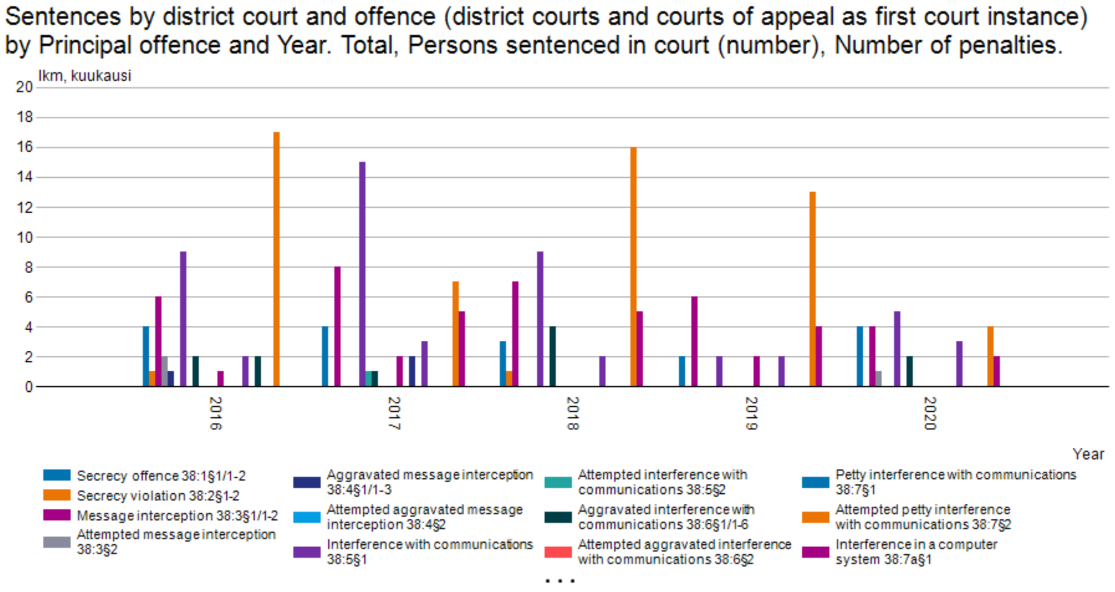
I have collected a summary of most common items that are offered on different dark web marketplaces in a table 2.

Act	Punishable	Criminal Code	Offence
Create an account	No	-	-
Transfer funds to account	No	-	-
Acquire and/or import without a license:			
Narcotics	Yes	50:1§	Narcotics offence
Tools/substances to produce narcotics	Yes	50:3§	Preparation of narcotics offence
Medicine	Yes	44:5§	Medicine offence
Other psychoactive substances	Yes	55:5a§	Violation of a ban of psychoactive substances in consumer trade
Weapons or ammunitions	Yes	41:1§	Firearm offence
Money	Yes	37:1§	Counterfeiting
Passports, drivers licenses etc. ids	Yes	33:4§	Possession of forgery materials
Download data or software			
To alter bank, paypal etc. accounts	Yes	37:11§	Preparation of means of payment fraud
Ebooks, applications etc.	Usually	49:1§	Copyright offence
Id/passport bundles	Yes	34:9a§	Endangerment of data processing
Orders services			
DDoS attack	Yes	38:5§	Interference with communications
Hack an email	Yes	38:3§	Message interception
Hack other accounts or computers	Yes	38:8§	Computer break-in
Clicks, likes, followers in social media	No	-	-

Table 2: Summary of potential criminal offences

3) What could be the consequences?

When getting caught, the most usual punishment is fine. There can also be, depending on the offence, damages to pay and confiscation of the tools and benefits gotten out of criminal acts. Damages can be sometimes high. In a figure 7 is presented data and communication offence cases in the court of law 2016-2020. Cases are really rare and certainly do not correlate with the number of crimes committed.



Source: Prosecutions, sentences and punishments, Statistics Finland

Figure 7: Cybercrimes in the court of law 2016-2020

4) How does the dark web transform the traditional field of criminality?

This is an interesting question and unfortunately there is no simple answer available to give on a basis of collected data. One can only present some hypothesis. As presented earlier, deterrence is the most efficient factor to prevent crimes and anonymity significantly reduces the risk of getting caught. We can try to imagine a worst-case scenario in this point of view, more like philosophical question, how much would people commit criminal acts if there was no law trying to prevent that. What is the role of consciousness of the people and social contract. Would most of the society remain the same or would it be war of everyone against everyone, is it "not wisdom but Authority that makes a law".

5) What is the response of the law enforcement?

As we can see by comparing the general userbase and traffic of tor network, which we can honestly assume that most of it happens for illegal reasons, to a number of cases in the court of law, it is clear that law enforcement needs more means to keep up with the criminals. With insufficient funds and under the pressure of human rights the task is not easy.

Despite well-formulated declarations and criminal policies it seems that neither national nor international law enforcement and judicial mechanisms have been able to address cybercrime effectively in the meaning of stopping crimes, dismantling criminal organizations and bringing the culprits to justice. [13] Actions seem to be more defencive, reactive, than proactive.

6 Conclusions

Criminal intents and thoughts are not punishable. Only actions that are unabigiously criminalized by law. Therefore actions prior transactions on the dark net marketplaces are not punishable. Even transactions are not punishable if that is enough to constitute the crime without further actions of the user.

On the other hand, after ordering an item, data or service has reached the state that users actions are no more required, almost everything seems to be criminalized. Some items are as drugs and weapons are naturally illegal to purchase without a license.

Interesting is that also tools to commit cybercrimes are too, if a client has malicious intent to do so. These are not punishable as data and communication crimes, because – again – mere intention is not punished, but acquiring these kinds of tools is after European union directive implementation 2015, punishable as *endangerment* of the data processing.

Buying services on the other hand can be considered as a cybercrime as an incitement to do so.

However, even if the massive traffic, userbase and nature of offered goods in the dark web marketplaces would indicate grown cybercrime rates globally and therefore in Finland too, number of the cybercrime cases in the court of law doesn't. One can only come to one conclusion: anonymity works and is hard to preach in concrete law enforcement.

References

[1] R. Dingledine, N. Mathewson and P. F. Syverson. Tor: The Second-Generation Onion Router. (2004)
[2] https://metrics.torproject.org/
[3] https://tb-manual.torproject.org/about/

[4] J. Nurmi: Understanding the Usage of Anonymous Onion Services. University of Tampere, 2018. p. 39
[5] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. (2008) p. 1-3. https://bitcoin.org/bitcoin.pdf
[6] https://coinmarketcap.com
[7] https://www.getmonero.org/resources/about/
[8] M.Tolvanen: Cybercrimes in finnish criminal law. Cybercrime, law and technology in Finland and beyond, 2019 p. 13-51.
[9] K.Nuotio: Perusoikeuksien merkityksestä rikosoikeudessa 1998 s. 148-149,
[10] https://www.globaldrugsurvey.com/gds-2019/
[11] http://www.kolumbus.fi/sidewinder/Turun_HO_R_07-176.txt
[12] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040
[13] P.Sund: Global and European Responses to Cybercrime. Cybercrime, law and technology in Finland and beyond, 2019 p. 67-123.