JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2021 Volume 11
https://doi.org/10.47459/jssi.2021.11.7

THE EFFECT OF THE DARK WEB ON THE SECURITY

János Besenyő[1], Attila Gulyas[2]

[1,2]Óbudai University, Doctoral School for Safety and Security Sciences, H-1081 Budapest, Népszínház utca 8., Hungary

E-mail: [1]besenyo.janos@uni-obuda.hu, [2]gulyas.attila@phd.uni-obuda.hu

Received 18 November 2020; accepted 13 March 2021; published 30 March 2021

Abstract. The elementary interest of every country is to maintain its inner security and stability. To achieve this goal the state must restrict within legal frameworks some fundamental rights of its own citizens. One of these fundamental rights is the right to privacy that can be breached only under certain circumstances. It is easy to see that it is unacceptable for a state not to control within the legal frameworks the communication of its own citizens so they can commit crimes, run terrorist rings, or spy rings or establish drug cartels without any consequences. Of course, the control over the communication is not the only means of the successful investigation but undeniably a vital one. That is why the Janus faced nature of the Dark Web is a real security risk nowadays. Although this new medium is the fruit of the last two decades its presence today is stronger than ever before and its popularity is growing day by day. Its most important features are anonymity, hidden geolocation and freedom from censorship. The Dark Web is very useful when it provides anonymity for political dissidents and whistleblowers, but is very harmful when it provides the same features for arm and drug traffickers and terrorists not to mention for pedophiles and so on. This article aims to shed some light on the effects of the Dark Web on the security and economy of the states especially in the aspects of organized crime and the terrorism.

Keywords: security; dark web; terrorism; organized crime; crypto market; cyber-crime; economy

Reference to this paper should be made as follows: Besenyő, J., Gulyas. 2021. The effect of the dark web on the security. *Journal of Security and Sustainability Issues*, 11, 103-121, https://doi.org/10.47459/jssi.2021.11.7

JEL Classifications: F52, K14, K24, H56

1. Introduction

The elementary interest of every state is to maintain its inner security and stability. To achieve this goal the state must restrict some fundamental rights of its own citizens. One of these fundamental rights is the right to the privacy that can be breached only under certain circumstances within legal frameworks. It is easy to see that it is unacceptable for a state not to control the communication of its own citizens within the legal frameworks so they can commit crimes, run terrorist rings, or spy rings or establishes drug cartels without any consequences. That is why the Janus faced nature of the Dark Web is a real security risk nowadays. Although this new medium is the fruit of the last two decades its presence today is stronger than ever before and its popularity is growing day by day. Its most important features are the anonymity, the hidden geolocation, and the freedom from censorship. The Dark Web is very useful when it provides anonymity for political dissidents and whistleblowers, but is very harmful when it provides the same features for arm and drug traffickers and terrorists not to mention for pedophiles and so on… The aim of this article is to shed some light on the effects of the Dark Web for the security of the states especially in the aspects of the organized crime and the terrorism.

In the first part of the study the security and the national security issues are discussed without getting into the deep details. After clarifying this question the Dark Web itself is presented. The third part of the study is about the most typical activities on the Dark Web. The last section presents their effects on the national security.

The study is based on related scholar studies and the author's personal experiences in connection with the usage of the Dark Web.

2. The security and the national security

First of all, the meaning of the word "security" should be clarified. It has many definitions that are slightly different from each other, e.g., "The condition of not being threatened, especially physically, psychologically, emotionally, or financially." (WordSense.eu Dictionary). Another definition: "A feeling of security is a feeling of being safe and free from worry." (Merriam-Webster.com dictionary) According to Fischer and Green (2004, p. 21) "security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of such disturbance or injury." Security itself does not exist it is only an abstract concept like consciousness. The security achieved through conscious defense activities to free someone from threatens for a period of time within a space constrained area, where the main point is the lack of threats. When the word security complemented with another word, e.g. national it gains its real meaning.

The foremost mission and constitutional duty of national security is to protect the people of the state, the way they live and the territory of the nation-state. Governments summarize their security landscape, their commitments to their national interests and threats and challenges and their possible answers in their national security strategies. The threats and the challenges to their security are complex and change rapidly. It is also true for their conditions for protecting their interests and answers for the challenges.

The following list of the national interests and the threats and challenges are arbitrary because there is no universal recipe for the national security strategy since every country has its own security landscape, interests and capabilities.

National interests

- Defending territory, freedom, security and right to self-determination
- Maintaining the fundamental values of democracy, the rule of law, human freedoms and human rights
- Norms and international law
- Ensuring the safety, security and health of the population
- Ensuring supplies and the protection of essential services
- Promoting stability and security in their region
- Maintaining and strengthening cooperation, solidarity and integration with the allies
- Trade
- Civilian and military peace promotion

Threats to security

- Transnational organized crime
- Information and cyber security, digital risks
- Terrorism and violent extremism
- Threats to energy supplies and other critical infrastructures
- Health threats
- Climate change and its effects

Each item of the list above is worth a study, yet in this paper they are discussed in the aspects of the effects of the Dark Web.

3. Dark Web

As it is widely known the Internet or World Wide Web is not a homogeneous medium. It can be partitioned into three different parts. The first part of it the Clear Web or Open Web that is accessible practically for everyone.

There is no need for any special means or authentication but Internet access and a common browser to visit an open webpage. These sites are free for all users. The well-known search engines like Google or Bing (and of course, there are others) are indexing these sites and store them and their metadata to improve the users' search experiences. According to Google the number of Google indexed pages was more than 130 trillion in 2016. (Schwartz 2016)

The second part is the Deep Web. It is still available for everyone but after some authentication in any other aspects it is similar to the Open Web. Sites like online bank accounts, medical records, or email accounts fall into this category. These pages are basically not accessible for the search engines except for some social media sites.

One of the main features of these above-mentioned categories is traceability. The site owners, the visitors and practically everyone who use these two media can be tracked down by their IP addresses.

The third part is the Dark Web (Figure 1). It is a special medium where the anonymity and the hidden geolocation is the most important feature. Access to the Dark Web requires special software solutions and in some cases software dependent IT knowledge. Users on the Dark Web can feel safe. It is theoretically free from the IT giants like Google or Microsoft, free from the watching eyes of the "Big Brother" and free from the censorship, and last but not least free from the Law Enforcement Agencies (LEAs).

Nevertheless, the Dark Web is a double-edged sword. On the one hand it provides a safe haven for dissidents in oppressed countries, the free speech possibility for human rights activists and last but not least the anonymity for the whistleblowers. e.g. The bigger news agencies maintain sites on the Dark Web for whistleblowers. On the other hand, it has a dark side as well. Under the cloak of anonymity pedophiles, drug, arm and human traffickers and other criminals play their filthy games. Besides the above-mentioned two categories there is one more including those who want only privacy. The numbers of those who escape from the Open Web to the Dark Web to hide from the data-hungry giants like Google, Facebook or other commercial organizations is continuously growing. They are not criminals, or freedom fighters they are simply privacy-conscious average people instead

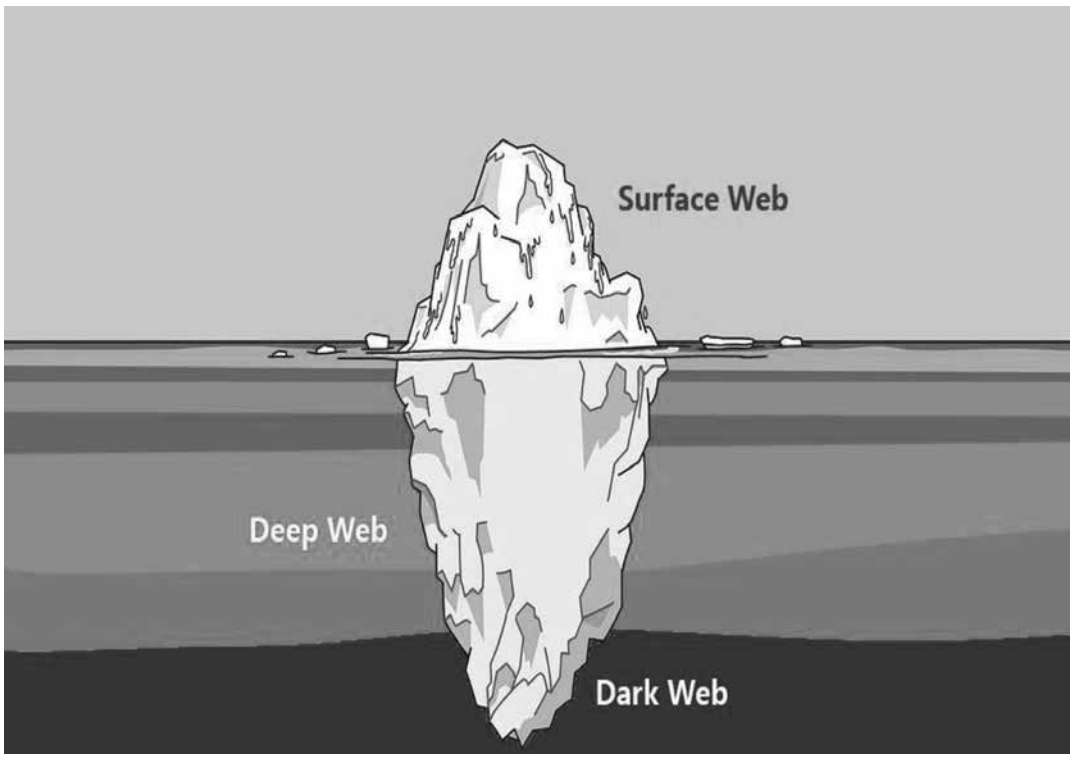

Figure 1. The partitions of the World Wide Web

source: https://hackernoon.com/understanding-the-deep-dark-web-8e4cad356587

At first sight, it seems that the Dark Web is a unitary part of the cyber world but it is far from the truth. It is divided into segments depending on the Dark Web software solutions, because each segment belongs to a software solution. The most popular software packages are "The Onion Router" (TOR), the "Invisible to Internet" (I2P), the "Freenet" and last but not least the "Zeronet". Basically, each provides access to the segment of the Dark Web created by itself. Each has its own hidden webservices and there is no possibility to visit from one segment to other i.e. from Freenet sites to the TOR system or vice - versa (there are solutions for TOR users to visit I2P sites but it is an exception). Among the four solutions, the TOR has a special feature that is provide the accessibility to the Open Net along with the anonymity that is why it is most popular Dark Web software. The Dark Web usage by countries gives some clues to estimate the size of the penetration of this cyber realm. The Table1. shows the numbers of users of the different system by countries. These numbers are based on estimates came from the different system metrics and don't show the real numbers, but the proportions shows the tendencies very well. The systems due to their natures are not suitable for the exact measurement.

The table shows that the most popular application is the TOR that is why in the following part of the study its services will be discussed in more details. The Zeronet users are not in the tables because the system has no metrics site, but it has a catalog of the user's IDs in which are less than 7,000 users. This catalog doesn't show which country the users belong to.

Table 1. Top-10 countries with number of Dark Web users

TOR		**I2P**	**Freenet**
Country	**Users**		
United States	418460	4057	12500
Russia	301518	1661	3500
Germany	184251	809	7800
France	77586	994	5500
Netherlands	74706	499	1400
Indonesia	63838	67	x
United Kingdom	61524	1386	5600
Turkey	50006	119	x
India	46839	286	500
Ukraine	46534	250	x
China	x	996	x

Sources: TOR metrics, https://metrics.torproject.org/ I2P metrics, https://i2p-metrics.np-tokumei.net/ Freenet metrics, https://freenetproject.org/assets/papers/roos-pets2014.pdf

The size of the Dark Web is inestimable, because as it is mentioned before there are no search engines, or domain registrars. Practically anyone who wants can create sites, forums, chats, and webshops (called hidden services in the dark terminology) and can delete them anytime. Here comes into the picture the most important feature of the Dark Web because no one knows the identity of the owner and the physical place of the hidden web service so the censorship at this point gets paralyzed. On top of that even the owner of the hidden service doesn't know the visitors' identity.

These features make the Dark Web be the safe haven for criminals, terrorists and freedom fighters. This paper is about the specific area of the Dark Web that are the organized crime and terrorism and the connection between them. The author grouped the most characteristic crimes into six groups. Although this classification is arbitrary in some way it helps to navigate in this chaotic world, and gives some overview for the readers.

4. Traditional Organized crime related activities

First of all, the organized crime expression should be clarified. According to the FBI: "Transnational organized crime (TOC) groups are self-perpetuating associations of individuals who operate, wholly or in part, by illegal means, and irrespective of geography. They constantly seek to obtain power, influence, and monetary gains. There is no single structure under which TOC group's function—they vary from hierarchies to clans, networks, and cells, and may evolve into other structures. These groups are typically insular and protect their activities through corruption, violence, international commerce, complex communication mechanisms, and an organizational structure exploiting national boundaries "(Federal Bureau of Investigation, n.d.).

It is a general definition of the organized crime groups and their activity, but the evils in the details. Visiting the Dark Web link collections like "Hidden Wiki" the user can find every kind of crime activity typically child porn, drug, arm, counterfeit medicine, counterfeit products, counterfeit notes, stolen credit cards, gift cards and so on… practically everything that a reader can imagine. But there are special services like Red Rooms. In these virtual rooms the viewer can see as human beings (men, women, or children) or animals are tortured and killed according to the viewer's directions. It is a type of quite expensive service. Although this is a horrible thing from the point of view of the study the way is important as they get the victims. The way is the human trafficking, or the kidnapping and the mixture of them. At first sight the human trafficking means that organized crime groups smuggle migrants for money to e.g. Europe. But this type of crime is a lot more complex. It is connected with the illegal human organ trading, the slavery trading, sex slavery trading both in prostitution and pornography (Reid & Fox, 2020).

a, Human trafficking

The concept of human trafficking is not new, it is with us for centuries from the ancient Egyptian or ancient Greek societies. The slaves were separated from their families and were forced to work without pay. This industry works from that time and even in the 21st century it is a highly profitable business. Surprisingly, it works not only in the third world countries but in the Western Hemisphere as well. The victims are from the underprivileged families that are tricked by false promises; often they are drug addicted, in bad living situations. Occasionally the victims are blackmailed with their families or relatives or simply coerced to work for their owner or procurer. Sometimes even their family sold them to the traffickers in the hope of better life expectances. Typical hunting grounds of human traffickers are the refugee camps and internally displaced people camps (IDP camps) among many other places. According to The New Humanitarian newspaper the Libyan Coast Guard intercepted more than 10,000 people in 2020 dragged them to detention centers where thousands disappeared from the plain view into the nowhere thanks to the extortion and abuse. (Reidy, 2020)
The main aims of the human trafficking:

- sexual exploitation
- domestic servitude
- labour exploitation
- forced marriage
- organ harvesting
- forced criminality
- child soldiers

"At any given time in 2016, an estimated 40.3 million people are in modern slavery, including 24.9 million in forced labour and 15.4 million in forced marriage. It means there are 5.4 victims of modern slavery for every 1,000 people in the world. 1 in 4 victims of modern slavery are children. Out of the 24.9 million people trapped in forced labour, 16 million people are exploited in the private sector such as domestic work, construction or agriculture; 4.8 million persons in forced sexual exploitation, and 4 million persons in forced labour imposed by state authorities. Women and girls are disproportionately affected by forced labour, accounting for 99% of victims in the commercial sex industry, and 58% in other sectors" (International Labour Organization, 2017)

The human trafficking is a complex and extensive topic that is why this paper covers only a part of it in detail just for shedding some lite on the way how it works.

The Canadian Benjamin Faulkner the owner of the "Child's play" Dark Net site was arrested by the FBI in 2016 after meeting his business partner the American Patrick Falte, the owner of the "The GiftBox Exchange" Dark Net child porn site. Faulkner's site had over one million user profile at the time of his arrest. In parallel with the FBI action, the Interpol was monitoring in Eastern Europe a trafficking ring called "Black Death Group". This organization sold on auctions sex slaves to Saudi Arabia typically virgin girls at age of 15. The adverts included their age, color of hair, and other measurements of their body and the starting price. One of their victims was a 15 year old girl named Laura with the starting price of 575.000 GBP. The abductors gave guarantee that they don't sell terminally ill, or pregnant girls. The most remarkable action of the group was the abduction of Chloe Ayling the famous British top model. She was lured to Milan where Lukasz Herba (Polish criminal) paralyzed her with ketamine and put in a trunk of a car and held as a hostage in a flat. When she arrived to Milan her employer got an email in which the abductor claimed 300.000 GBP for her otherwise, he would auction off her as a sex-slave on the Dark Web. Fortunately, the police found her and arrested her abductor. During her 6-day captivity Herba told her that he had made 15 million GBP by sex-trafficking kidnaped women and selling them via Dark Web. (Murali, 2019) (Rear, 2017)

The Dark web is a heaven for pedophiles. They can connect and share their fantasies in the cloak of anonymity. Hundreds of forums are on Child Porn (CP), but getting in the inner circle is very hard. The owners of the forums and the moderators are very cautious, the novice members are subject to thorough scrutiny and to prove their commitment they are forced to make something child-related illegal action. Some of them are highly skilled IT security amateurs and they teach the others how to keep their anonymity that is why the LEAs face very hard challenges.

b, Drug and arms trafficking

The drug and arms trafficking are in hand in hand with the human trafficking, because they often use the same ways and methods. The drug related crypto markets are far most popular among the illicit goods markets. According to some estimates it takes up 67% of the whole contents of the crypto markets. The most affected countries are United Kingdom, Netherlands and Germany. The Dark Web is not for the "Big Sharks" who export-import tons of drugs, it is for the medium and small category players instead. It is an interesting fact that cannabis and cocaine are sold in retail scale while the MDMA and opiates are sold on larger (medium) scale on the markets. The relatively big profit is affective for these criminals, that is why when LEAs close a bigger crypto market, as it happened i.e. in case of the "Silk Road" or "Alphabay", it is matter of days and a new player emerges from the nowhere. Just for curiosity the Alphabay had 400.000 users (The European Monitoring Centre for Drugs and Drug Addiction, 2017). The crypto markets are very convenient for the "costumers" as well, because they can buy drugs like a phone from a webshop. They don't have to get in touch with criminals personally, on top of that they keep their anonymity so the chance of apprehension is very low. The figure 2. is a screenshot of the drug section of the "World Market" crypto market.

The arms black market is smaller than the drug business, but it still has severe security risk beyond its size. The trade of arms on the Dark Web is smaller in volume than the legal arms trade so it can't be the basis of insurgencies, or wars, but it can be a good alternative for lone-wolf terrorists, criminals, or small gangs. Weapons and ammunition are not produced on the Dark Web, they are (or at least a part of them) circulating between the real world and the hidden markets. The big advantage of the Dark Web arm markets that the weapons are cheaper than on the streets or on the real black markets. Besides the weapons the visitor can buy arm related digital contents. These are typically videos or written guides on printing weapons with 3D printers, or conversion replica guns into live guns, making home-made guns, or special ammunition. One of the most remarkable cases when David Sonboy Iranian - German dual citizen bought a pistol on the Dark Web, and the 18-year-old guy shot down 10 people and other 36 injured in the Olympic Shopping Mall in Munich in 2016 (Deutsche Welle, 2016). The figure 3. is a screenshot of an illegal gun store website on the Dark Web.

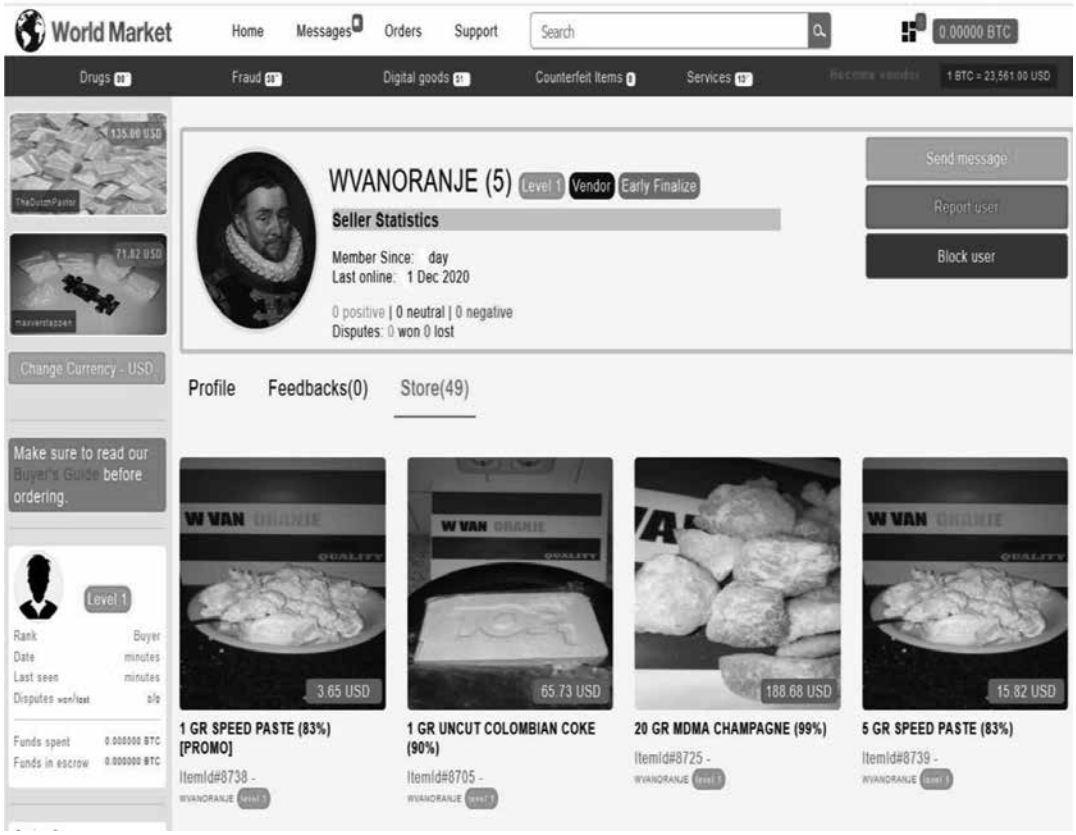

Figure 2. "WorldMarket" crypto market drug section

Source: screenshot by the author (11.12.2020)

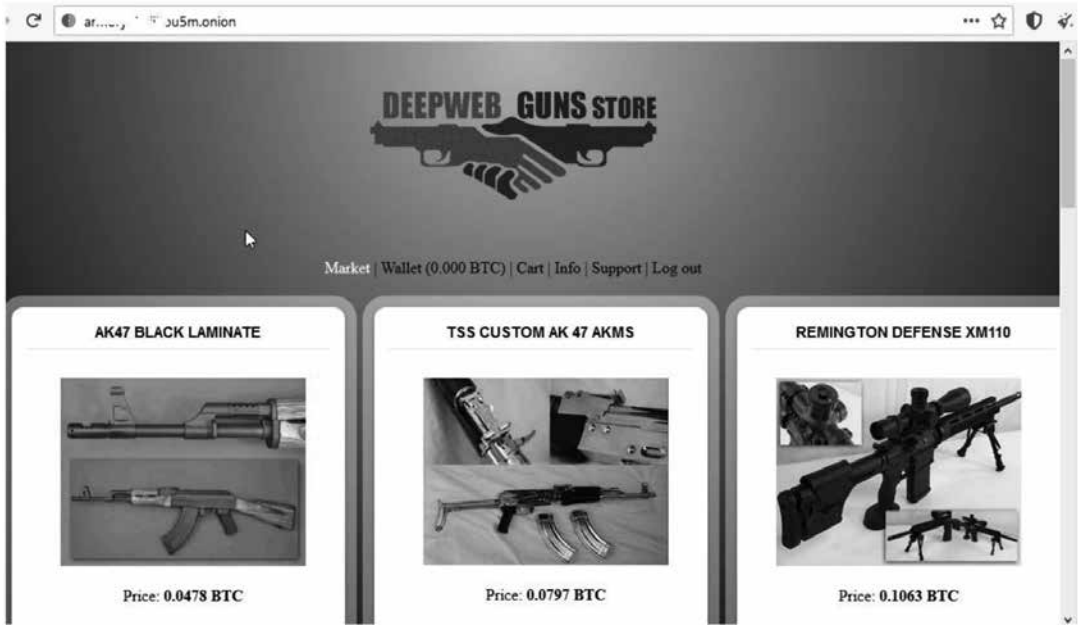

Figure 3. Gun store on the Dark Web

Source: screenshot by Attila Gulyás (11.12.2020)

The biggest source of the illegal weapons of the black markets is the USA (60%), the second bigger source is Europe (25 %) for the rest unspecified regions are responsible (Homeland Security Newswire, 2017).

The crypto markets today are the second generation virtual markets. The first generation market was born in the dawn of the Internet when the IRC chat rooms were the places where the seller and the buyer met and made deals. It was obviously risky, because there was no protection system, they were easy to trace down by the LEAs. The situation significantly changed as the TOR and other Dark Web system got more popular and widespread. The IRC room markets evolved into serious Amazon like online markets. They introduced the virtual currency payment and for the protection of the sellers and the buyers the escrow system. The crypto markets besides the escrow system employ feedback and purchase review systems.

Silk Road was the first illicit drug devoted crypto market system on the Dark Web. It offered the wide range of the drugs including cannabis, cocaine, Lsd, and prescription medications. The online business went on from 2011 for two years when the FBI sized the market and arrested the owners. Within a few weeks the Silk Road emerged out of the blue, but it had already rivals at that time such as Pandora, Agora, Hydra, Sheep just to name a few. In the history of the new markets were scammers of course, but the introduced feedback systems lowered the risk of the buyers and helped to maintain the confidence in these sites. Today the crypto markets are similar to shopping malls where everything is on sale. The most popular business sites in different languages are dedicated to selling credit cards, pay pal accounts, prepaid gift cards, and counterfeit money and ID cards, passports, and driver licenses. The counterfeit ID cards make possible practically to anyone to hide from the Law Enforcement Agencies (LEAs) or get into countries, and here comes into the picture the above-mentioned human trafficking. The figure 4. is a screenshot of the fake document section of the "World Market" crypto market.

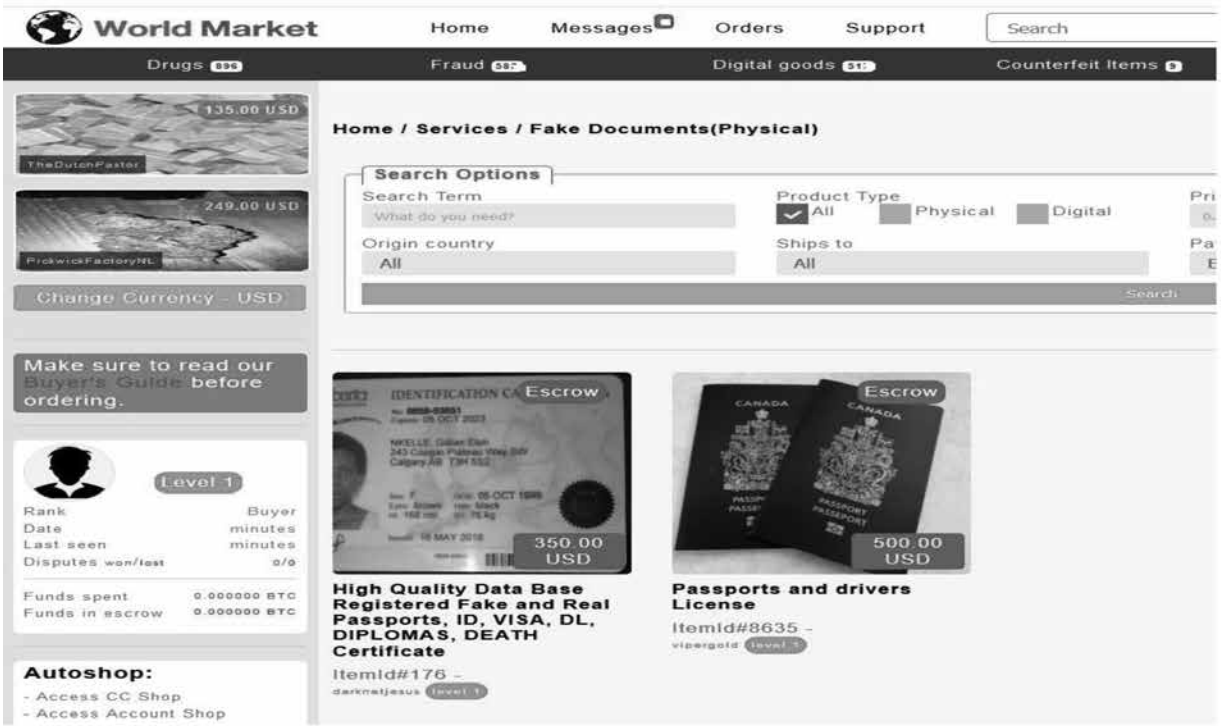

Figure 4. Fake and real passports on the Dark Web cryptomarket

Source: screenshot by Attila Gulyás (11.11.2020)

c, Cyber crime

The cybercrime is a criminal activity in which the cybercriminal targets computer or computer networks using a computer or computer networks. In most cases the cybercriminal or hacker wants to make money. The cybercrime can be committed by individuals or organizations. Usually, the perpetrators are highly skilled professionals but sometimes they are simply script kiddies. Occasionally, for political or personal reasons the perpetrators' aim is to cause damage instead of making money (Kaspersky, n.d.)

The main types of cybercrime that are both on the Open Web and Dark Web:

- Email and internet fraud (phishing)
- Identity fraud (where personal information is stolen and used).
- Theft of financial or card payment data.
- Theft and sale of corporate data.
- Cyberextortion (demanding money to prevent a threatened attack).
- Selling exploits and Zero day vulnerabilities
- Ransomware attacks (a type of cyberextortion).
- Ransomware as service (RAS)
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- Cyberespionage (where hackers access government or company data).
- PUPs

After navigating to one of the hidden services collections on the Dark Web it is easy to find links that lead to sites dedicated to types of cybercrimes listed above. The Dark Web is full with sites and crypto markets where stolen databases (business data, private celebrity data, and list of usernames and passwords) are on sale. The figure 5. and 6. show samples of market places of stolen databases.

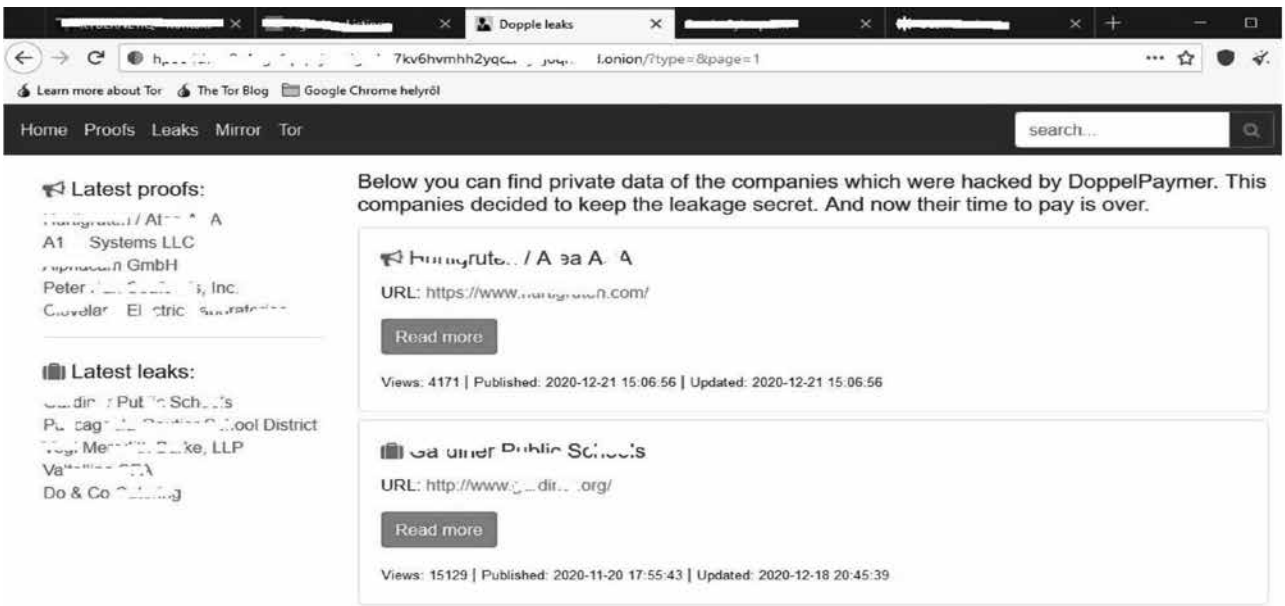

Figure 5. Stolen information on sale on Dark Web (obfuscated for privacy reasons)

Source: screenshot by the author (22.12.2020)

The "REvil" hacker group is one of the classic examples of the very dangerous and unscrupulous cyber-criminal group. They stole data including the customers list, and more than 22,000 files and three more databases, from the Canadian AGROMART group in May 2020. The hacker group put on auction on the Dark Web the stolen information for 50,000 USD and blitz price was 100,000 USD. But not the Canadian corporation was the only victim. They breached e.g. the computer networks of the South African "Telkom" telecommunication provider, and the British "Elexon" energy reporting and accounting company, just to name a few. They use ransomware programs to extort money and steal information from the targets that are usually bigger business corporations, and celebrities. According to some estimation they put on sale 76 corporate related data base on the crypto market, but it seems only the tip of the iceberg. (DarkOwl, 2020) At the time of the writing of this paper they blackmailed the Transform Hospital Group (chain of plastic surgery hospital group) to pay to them otherwise they publish 900 GB intimate photos of their clients including celebrities. They are security savvy so they demand Monero instead of Bitcoin because Bitcoin is relatively easy to trace down.

Figure 6. Philippine voter database 70 million voters on sale on the Dark Web

Source: screenshot by Attila Gulyás (21.12.2020)

d, Extremist and anarchist content

There are corners on the Dark Web where different extremist right and anarchist movements spread their ideology and the members communicate with each – other. As it is widely known the extremist movements are getting stronger in the western hemisphere in the last two decades. Far-right violent extremism has become increasingly evident with attacks on mosques, synagogues, public gatherings and politicians, emerging from anti-immigration activism and conspiracy theories. Their communication is filtered on the social media. Twitter, Facebook, Instagram and other social sites keep on filtering their contents that is why they turned to Dark Web. The social media censorship is very useful, but it has a big disadvantage. Persecuting these movements to the Dark Web the LEAs lost the control over their communication, they lose sight of the extremist activists and it is very dangerous. Similarly, to other illegal hidden services it is easy to find forums and chat rooms where extremist or anarchist contents are published. The figure 7. is a screenshot of a neo- Nazi Dark Web forum where the visitor can read and download illegal contents. However, it is very hard to get into the inner circle of the extremist forums or chat rooms, because there are different membership levels with strict authentication. Besides the forums and chat rooms there are blogs and sites dedicated to these contents where the visitors can find different dangerous textbooks such as "Anarchist cookbook"-s, or "Anarchist poison book"-s with detailed instructions on how to make and use bombs, and different poisonous materials.

New dimensions to violent extremism are becoming increasingly evident, witnessed by the presence of Incel (involuntary celibate) themes in recent attacks, the radicalization of hate crime, the pervasive impact of conspiracy theories, together with new vocabularies of extremism. Violent extremism is changing as the boundaries between different expressions of radicalization become more plastic, and the older opposition between 'organized' and 'lone actor' terrorism are no longer reality. The internet and emerging forms of digital sociability are fundamental to this reconfiguration, and as such, online radicalization and its implications for offline violence are increasingly obvious.

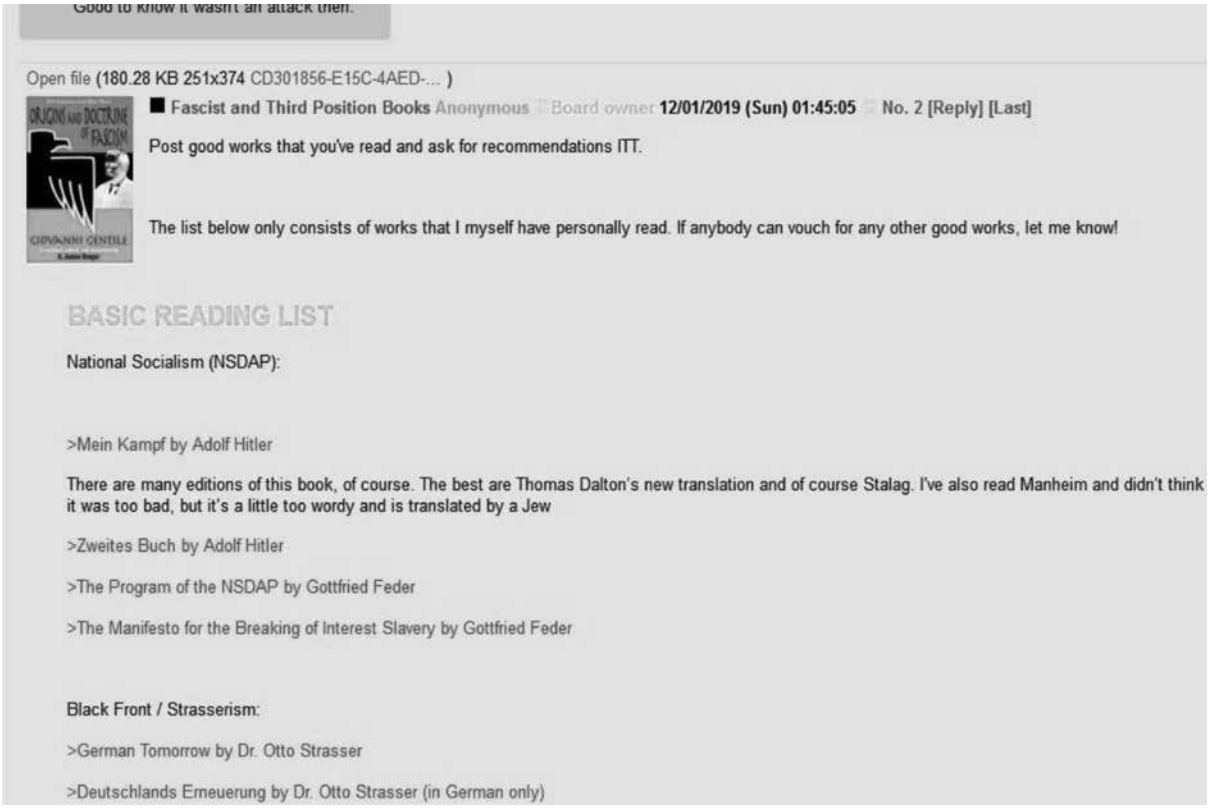

Figure 7. Post on a neo-Nazi Dark Web forum

Source: screenshot by Attila Gulyás (21.12.2020)

e, Terrorist activity

Terrorists have been active on the Internet since the dawn of the Internet. Their sites were monitored by the counter terrorist agencies, when a site got closed, they moved on to another they played cat and mouse game. The situation totally changed after the attacks in Paris in November 2015. The terrorist sites got into the focus of the public and the different social media sites started employ serious censorship against their content and volunteer hacker groups started attack their sites. Hundreds of ISIS related websites were taken down in the course of "Operation Paris" (OpParis) campaign launched by the Anonymous hacker group. They got under a never experienced pressure by counter terrorist agencies, the LEAs and the social media censorship, not to mention the volunteer hacker groups. That was the point where the terrorist groups turned to the Dark Web. This new realm provided them with the anonymity and the censor free communication. The Al-Hayat media outlet posted a link that led to an ISIS related Dark Web forum. The post included detailed instructions on how to get to the Dark Web. A new post with the same content appeared on the Telegram channel of the ISIS. The Telegram is one of the favorite applications of the terrorist organizations. This is an end to end encrypted messenger application that works on Windows, Linux, MacOS, Android, and IOS operating systems. The user can send messages to his partners and can create channels as well. This application provides the terrorists with the privacy they are looking for. The owner of the Telegram is a private person who allegedly denied any cooperation with LEAs. All in all, it is an ideal tool for those who seek anonymity.

Unfortunately, the chasing of the terrorists on the Open Web had a contra-productive effect on the security. The counter terrorist agencies lost the control or at least a part of it over the illegal communication.

Terrorists do the same on the Dark Web what they do on the Open Web, but more securely. They provide information and propaganda for their sympathizers, recruit and radicalize, coordinate their actions and raise funds. The Dark Web introduced a new opportunity for the fund raising by the use of crypto currency. The transactions with this virtual currency are very hard to trace down. That is why it is such a popular currency on the Dark

Web. The figure 8 is a good example of a Dark Web fund raising webpage where the sympathizer gets detailed instructions on sending virtual currency to the organization.

The hidden world is a perfect realm for purchasing illicit goods. According to legal sources the weapons used in the Paris attack are thought to be purchased on the Dark Web from a German Dark Web vendor under the pseudo name "DW guns" who converted start pistols into live weapons following Dark Web tutorials and sold them on the black market for extra money. (Fox News, 2015)

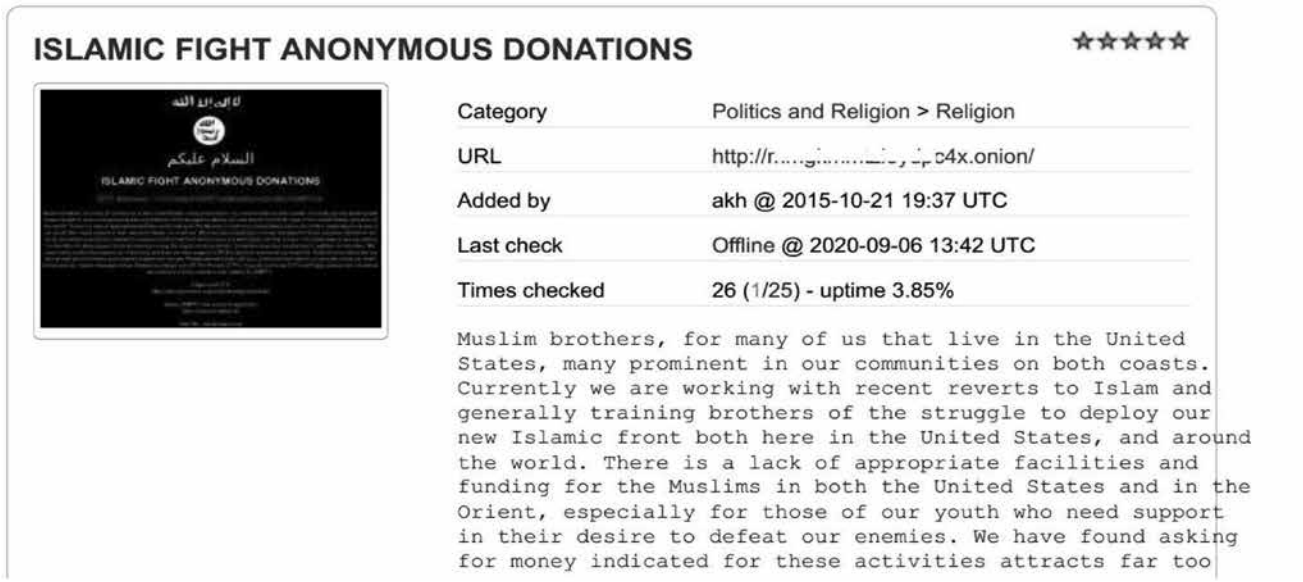

Figure 8. Call for donation on the Dark Web

source: screenshot by Attila Gulyás (21.12.2020)

f, Information market.

The information has been power and money for centuries. This statement never was so much true than in present.

We live in the era of the information technology with its every benefit and drawback. Today the amount of the private, and especially the business information is growing by geometric sequence in the world. The importance of the intelligence and the information protection is vital and it is one of the most burning questions in the industrial world. The business and the state actors alike are hungry for the information on their counterparts or enemies while they try to keep their own secrets. That is why the information trade is a fruitful business both on the Open and the Dark Web.

On the one hand hackers and hacker groups including the organized crime criminals steal information from private or business entities and sell it on the Dark Web. This type of crime is in tight connection with the cybercrime that was discussed above. The way as they do it is various but the presentation of their methods is out of the scope of this paper. Typically, the information is sold on crypto markets, the price depends on the business value of the data e.g., a worth of 1000 USD PayPal account for 40 USD, or a 70 million Philippine voter database for 10 USD. The size of the information market is nearly inestimable, in all likelihood, it is over millions of dollars per year. The information trade is a "one man's loss is another man's gain" game.

On the other hand this new phenomenon fostered new possibilities: a new industry emerged that is the Dark Web monitoring businesses. Today it is a standard practice that an entity either private or business who is worried about his own data hires an OSINT professional IT company to monitor both the Open and the Dark Web looking for his leaked data or looking for data of his interest. Today it is a flourish business sector and its importance is showing growing tendency.

5.The Dark Web currency and its effect

The most accepted currency on the Dark Web is the Bitcoin. Bitcoin eliminates the physical boundaries, the currency exchange issues and provides a basic anonymity which is vital for the Dark Web sellers and buyers.

With the growing popularity of the Bitcoin it has effect on the economy and the national security as well. That is why it is inevitable to look at closer the cryptocurrency system especially the Bitcoin.

a, Bitcoin

The Bitcoin is the first and most well-known cryptocurrency created by an unknown computer programmer or programmer group under the pseudo name "Satoshi Nakamoto" in 2009. It is an electronic payment system where the transactions are validated by the users of decentralized networks and cryptographic method that is why there is no need intermediary contributors (such as banks). The cryptocurrency systems use public ledgers. The users can establish an account with an alias name (or an address that is actually his public key) that can be seen for the entire network. The user also has a private key (must kept secure) which is paired with the public key.

When a user would like to pay for some service or goods, he needs the seller address (public key). The buyer unlocks the cryptocurrency with his private key and allows to the seller to lock it with his private key. The user can create a "wallet" at service providers or third party cryptocurrency exchanges to make more user-friendly the access to the cryptocurrency system. It is generally a website or a special application with username and password authentication. At first sight the transaction itself is very similar to a traditional money wiring.

The transaction is not over with locking the cryptocurrency. These systems use a blockchain technology to validate the transaction. It means that the special members of the network validate the transaction by solving a complex cryptographic problem. Who is the first solver validates the transaction by linking the transaction to the end of the blockchain that is actually the ledger. The solver in exchange gets some cryptocurrency for his work. Those who validate the transactions are the miners. The integrity of the ledger is secured by a very complex cryptographical method. Any modification in the previous transactions will corrupt the chain and visible for all members.

The amount of the cryptocurrency is limited in the system and the reward for the mining is decrease with the growing amount of the cryptocurrency to retain the value.

People can buy cryptocurrency on certain exchanges using official currencies or can mine cryptocurrency, but in some countries, there are cryptocurrency ATMs as well.

b, Importance of the Bitcoin

The judgment of cryptocurrencies including the Bitcoin is controversy in different countries. Some countries accept as legal currency others tolerate while there are countries where their use is forbidden.

The transactions per day is a good indicator of the prevalence of the Bitcoin. One industry data show that the number of transactions averaged about 328,000 per day globally in contrast with the Visa transactions that reached the 378 million per day in 2019. (David W. Perkins, 2020)

Although it seems that the significance of the cryptocurrencies is quite small nowadays according to observers their importance is growing because in the next decades more and more people will realize their benefits.

One of the benefits of the cryptocurrency systems is the lower cost than the traditional electronic payments systems. These systems maintain infrastructures, networks, servers, databases and employ thousands of people.

The costs of these systems are charged on the costumers. The proponents of the new currency argue that the

spread of these systems will lower these costs significantly. Another advantage of these systems that they don't depend on governments, so people who can't trust their governments or financial system of their country can turn to decentralized systems.

Besides its growing popularity the cryptocurrency is facing challenges in the widespread adoption. One of the challenges is the acceptance. Today still consumers and businesses are hesitating to accept a decentralized computer network where the users are covered by alias names and the work of the system is not clearly understandable for them. Another challenge is the volatility, although the cryptocurrencies are not affected by monetary policy, inflation rates or economy performance the exchange rate is changing driven by the following factors: (Coincache, n.d.)

- The price is mainly influenced by the supply and demand of the given cryptocurrency
- The amount of rewards after mining, if the given coin can be mined, as this is actually the inflation rate of the coin, which is regulated through the rate of issue.
- Awareness of the given coin, number of users and areas of use
- The growth potential of a given cryptocurrency
- The number of cryptocurrencies competing for investors 'money
- The number of exchanges on which the cryptocurrency is traded and the liquidity available there
- Regulations and laws governing the operation, trading and distribution of a given coin

c, Technological challenges

Today with 328,000 transactions per day the validation of the blocks in the network takes about 10 minutes due to the complex cryptographical system in contrast with the traditional systems where it is practically a matter of seconds. It seems that the cryptocurrency system would not be able to handle millions of transactions within reasonable time. When the price of the cryptocurrency is raising the reward for the mining is relatively high that is why more people want to be miners. Unfortunately, it generates a race for being first to publish the validated block chain. The miners buy new stronger computers to increase their chance. These computers take much more energy because the solution of the complex cryptographical problem takes huge amount of computational resources. When the value of the currency deflated many miners give up the mining. The validation of the transaction slows down. The energy consumption at first sight seems moderate because of the relatively low number of transactions, but according to estimations the electric consumption of the Bitcoin system is comparable to Ireland. (David W. Perkins, 2020) This is only the Bitcoin system, but there are hundreds of cryptocurrency systems in different size around. With the growing popularity of these systems the energy consumption may increase by an order of magnitude. Unfortunately, the higher electric consumption is associated with greater pollution.

Another problem comes from the most unique feature of the cryptocurrency systems. As mentioned above the transactions are linked to the blockchain, but this can't be undone. If the seller doesn't post the goods to the buyer, or if the buyer posts the goods without receiving the price, it is almost impossible to get it back so the money is gone. In most cases the partners even don't know each other. That is why the escrow service as intermediary is introduced and it is very common even on the crypto markets. Typically, the escrow company holds the buyers' cryptocurrency until delivery is confirmed. After the confirmation, the company passes the virtual money onto the seller.

d, Criminality of cryptocurrencies

Criminals and terrorists prefer cash, but due to the international efforts against money laundering and financing of terrorist activities their playground is narrowed. That is reason why they turned to the relatively anonymous cryptocurrency systems. Although the ledgers are public, they only show the public keys of the business partners. Some of the systems such as "Monero" obfuscate the public keys in the transactions to hide the users' identity however it is not a perfect solution, yet.

As it mentioned above the Bitcoin is the most popular currency on the Dark Web. The ledger of the Bitcoin is public so the transactions are can be followed but the identification of the users is far from easy. The analysis

of the public transactions can yield patterns that help identify the suspicious activities and the identification of the alias names with real -life persons. For example, the public key of a transaction can be linked to a costumer of an exchange. In other cases, it is cumbersome work or impossible to identify the users.

The law enforcement agencies have the right to ask information from exchanges, and they are subject to regulations to report suspicious activities.

Besides financing illegal activities on the Dark Web, the other harmful effect of the cryptocurrency is that creates opportunity for TAX evasion. These two functions are hand in hand, one comes from another. Just to name one of the TAX evasion is the VAT (Value Added Tax). The trade on the Dark Web is free from taxes; these tax revenues are missing from the budgets of countries so in this aspect the cryptocurrencies weaken the economy. The size of the Dark Web cryptocurrency traffic is inestimable but it is sure that its importance is increasing and the demand for elaborating some solution against the tax evasion is inevitable. Different countries have different solutions against the cryptocurrency tax evasion but the Dark Web is still a dark spot in this context.

6. The effect of the Dark Web on the national security

The security landscape of a country is subject to always changing. Threats eliminate and new challenges come up suddenly so this is an ever changing process. The Dark Web is a new phenomenon with series of threats and threat actors that national security professionals should be aware of.

This paper in the previous sections presented the main activities on the Dark Web that may have security implications for the national security. The following section presents the effects of the illegal Dark Web activities on the components of the national security highlighting the main challenges and risks. Because of its complexity, the elements of the national security depend on each other to a certain extent so one harmful activity can have effect on more components. The drug problem is one of the complex challenges just to name one of them.

a, Economy

The problem is very complex because some kinds of crimes overlap more areas of national security. The drug trafficking and trading has effect on economy, public security and the healthcare system. Beyond the earlier discussed Tax related crimes, the crypto markets strengthen the grey and black economy. The trade of counterfeit goods cause harm to the companies by lowering their incomes, and ruin the reputation of their brands and the consumer confidence. The trade of counterfeit money-related services like gift cards, credit cards, and other services including the forged or stolen bank accounts ruin the financial system. These kinds of crimes not only cause damage but they shake the public confidence in these systems.

b, State secrets, espionage

In order to secure the sovereignty of the countries and to protect their constitutional order they must kept secure their military and state secrets against malignant efforts to acquire, disclose or change them. It is usually the responsibility of the national security services. They have to detect and prevent efforts and activities threatening political, economic defense and other interest of the countries. This is a very complex and responsible assignment even without the Dark Web. This new realm makes their task more complex and harder. The hidden geolocation and anonimity poses new challenges to these services. Today there is no real effective solution for the eavesdropping of the communication on the Dark Web, and the de-anonymization, or the localization of the perpetrators is a real question. The new challenges require new answers.

The hidden communication can substitute in certain cases the personal contact that is why there is no need to establish dead drops or personal letter boxes in the real world, because the clandestine sources can forward their messages to the intelligence officer via the Dark Web. It also facilitates the disclosure of state secrets. Unfortunately, it is hard or in some cases impossible to find the sources of disclosure state or business secrets.

A good example of the damage caused by hackers is when the "ShadowBrokers" hacker group released in 2016 the NSA special software kits that were used to collect information on enemies. Nearly one year later the WikiLeaks published the Vault 7 and Vault 8 CIA projects that are complex clandestine information collection systems. The projects with their source codes and user manuals are available on the Dark Web. On one hand these leaks caused a huge damage for the US on the other hand they helped countries with less resource build their own cyber capabilities because they could use the source codes to develop their own cyber weapons. Unfortunately, these source codes and manuals are available for black hat hackers as well and they can use it to develop malwares. These incidents have been dramatically changed the security landscape, the damages and consequences caused by leakers are inestimable in both short and long term.

c, Public safety and security

Most of the aforementioned crimes endanger the public safety and security in some way. The Dark Web is an ideal environment for the criminals because it provides the anonymity and the hidden geolocation for the illicit activities. The popularity of the crypto markets is growing day by day due to these features and in parallel with it the task of the LEAs is harder. In spite of the relatively low social penetration its danger much higher than it seems at first sight. There are unforeseen capabilities and potential risks in the spread of this new medium.

The sense of public safety and security for the people depends on the feeling that not only the bigger crime perpetrators but the petty criminals are persecuted and apprehended by the LEAs as well. But on the Dark Web there is no real chance to it because the efforts put in the identifying the petty crime perpetrators are out of proportion to the profit. The most of the petty criminals get away with buying drug, or counterfeit goods and other misdemeanors. It has a very harmful and degradative social morality message for the society. That is one of the fuel factors of the growing popularity of the Dark Web. On top of that these hidden systems are more secure with more users. That is a typical catch twenty-two situation.

d, Critical Infrastructure protection

The protection of critical infrastructures is the basic interest of every country, because these systems keep a society and country alive. (Besenyő & Fehér, 2020) The critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to a country. Their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. (Critical Infrastructure Sectors | CISA, n.d.) Today common news, that hospitals and other critical infrastructures are attacked by ransomware programs. The attackers try to extort money, typically some kind of cryptocurrency, from the victim. On the course of the action the attackers lock and encrypt the victims' files so they paralyze them. Sometimes even after paying the ransom the hackers steal and upload the databases and files from the victim to the Dark Web where they try to sell the stolen data. The attacks besides the material damage cause life-threatening situations by paralyzing the hospitals and lower the confidence of the people in the systems. A sad example from Germany is when a woman who attempted suicide died at Düsseldorf University Hospital in September 2020, because she could not be transported to another hospital on time because the hospital's IT system was attacked by a ransomware attack (Tidy, 2020).

Usually, the ransomware program origin is some Dark Web site, or the command control server is on the Dark Web. Widespread business model is the Ransomware as Service (RaS) solution as well.

The Dark Web is ideal for procuring, developing, testing and using exploits and ZeroDay (0day) vulnerabilities. The exploit procuring is very easy because there are a lot of dedicated sites for these kinds of programs, and the anonymity is favorable for testing and using the newly developed malwares.

e, Public health

The public health is a very important component of a society. First of all to maintain a flourishing economy and a sound society without healthy people is impossible. According to the World Health Organization today the most popular drug is the cannabis followed by opioids, amphetamine-type stimulants and the cocaine. Besides

the traditional substances it has been an unprecedented increase in the use of synthetic psychoactive drugs such as synthetic cannabionids and cathinones. (World Health Organization, n.d.) Due to the fight against illegal drug consumption the chemists in the drug labs every day come up with new formulas to circumvent the designer drug lists.

The drug addiction beyond the harmful effect on the user and his relatives burdens the social security system as well. People with drug use disorders often experience difficulties at work and in relationships with family and friends. Drug use disorder is a risk factor for multiple health conditions such as infections, road traffic injuries and suicide. On top of that it is the origin of the criminal career and tightly related to prostitution as well. Today it is a serious challenge in most countries because the drug addiction associated with its side effects takes significant amount of resources both in money and human resources and the trend is emerging year by year.

The drug trading is not the only source of danger on the Dark Web, the aforementioned human and the organ trafficking also poses health challenges to countries. People of all ages and genders are affected and it is a major source of child labor globally. Both physical and behavioral health implications of the human trafficking are boundless. The most typical diseases such as tuberculosis, malnutrition are in connection with the living conditions. Injuries are also significant issues resulting from torture, physical violence, and accidents during the forced labor. The other factor is the lack of protective cloth and other safety appliances. Mental health problems, which come from the emotional and physical insult, include the full spectrum of traumas anxiety, depression, post trauma stress syndrome, and phobias. These problems are also typical for the victims of child abuse. Because of the traumas and the hopeless live situations victims often turn to alcohol and drugs and the outcome is substance abuse problems or engaging in risky sexual behavior. The unplanned pregnancies and the forced unsafe abortion or the selling of babies is also a common phenomenon. Victims of the trafficking often don't have health insurance or they are even not registered at all in the social security systems. That is why they not vaccinated and the preventive health screening is missing. Their chronic diseases, such as diabetes or high blood pressure, are not treated that may lead their early death. Likewise, the forced or deceived organ donors without proper health care can lost their life after the surgery.

These problems pose challenges to countries and the fight against the human trafficking and its consequences takes enormous resources from the whole society.

Conclusions

This paper shed some lite on the context of the dark web and national security issues. As it presented in the previous sections the crimes in the new digital world have negative effects on practically every factor of the national interests. The Dark Web penetration in countries today is still relatively low, but it has bigger effect on societies than it is expected by its size. Due to its structure and its features this part of the cyber-world blurs the boundaries both physically and morally, and it poses a significant and growing threat to national security with implications for economy, public safety, public health, and democratic institutions.

The European Union realized that the only cure for the new disease is the coordination between the Law Enforcement Agencies. The Europol has established a dedicated Dark Web Team to work together EU partners to decrease the number of illegal crypto markets. The team will elaborate a coordinated approach with sharing information, providing operational support and expertise in different crime types and development of tools, tactics and techniques to help investigators identify threats and targets. The good example of the cooperation is e.g., the shutdown of the "Alphabay" and "Hansa" crypto markets. The two markets were responsible for more than 350,000 illicit goods such as drugs, firearms and cybercriminal tools. (Europol, 2018)

The Dark Web applications are developed by enthusiast volunteers and their aim is not to support the criminals, but their intention is to provide the digital freedom for people who consider it very important, instead. There are dedicated sites for whistleblowers and for journalists' informants, not to mention the human right activists and revolutionists, free thinkers in oppressed countries. The possibility of the free speech without censorship

or restraint is undoubtedly vital.

It would be unfair to blame the Dark Web for everything. It is only a mirror, it reflects only a small sample of our societies, the roots of the problems are somewhere else.

References

WordSense.eu "security" in WordSense.eu Online Dictionary (10th December, 2020)

Besenyo, J., & Feher, A. (2020). Critical infrastructure protection (CIP) as new soft targets: private security vs. common security. Journal of Security and Sustainability Issues, 10(1), 5-18. Doi: 10.9770/jssi.2020.10.1(1)

Cisa.gov. n.d. Critical Infrastructure Sectors | CISA. [online] Available at: https://www.cisa.gov/critical-infrastructure-sectors [Accessed 6 January 2021].

CoinCash. n.d. Bitcoin Exchange Rate. [online] Available at: https://hu.coincash.eu/arfolyam/btc/usd/1y [Accessed 30 December 2020].

D.W. Perkins, 2020. Cryptocurrency: The Economics Of Money And Selected Policy Issues. [ebook] Washington: Congressional Research Service, Available at: https://crsreports.congress.gov/product/pdf/R/R45427 [Accessed 1 January 2021].

Dark Web, illegal arms, criminals, terrorists | Homeland Security Newswire. (2017). Retrieved 18 December 2020, from http://www.homelandsecuritynewswire.com/dr20170726-u-s-weapons-main-source-of-trade-in-illegal-arms-on-the-dark-web

Drugs and the darknet: perspectives for enforcement, research and policy | www.emcdda.europa.eu. (2017). Retrieved 18 December 2020, from https://www.emcdda.europa.eu/publications/joint-publications/drugs-and-the-darknet_it

Europol. 2018. Crime on The Dark Web: Law Enforcement Coordination Is The Only Cure. [online] Available at: https://www.europol.europa.eu/newsroom/news/crime-dark-web-law-enforcement-coordination-only-cure [Accessed 9 January 2021].

Federal Bureau of Investigation. n.d. Organized Crime | Federal Bureau Of Investigation. [online] Available at: https://www.fbi.gov/investigate/organized-crime [Accessed 15 December 2020].

Fischer, R.J. and Green, G. (2004) Introduction to Security, 7th ed. Boston, MA: Butterworth Heinemann

International Labour Organization, (2017). Forced labour, modern slavery and human trafficking. Retrieved 20 December 2020, from https://www.ilo.org/global/topics/forced-labour/lang--en/index.htm

Kaspersky. (n.d) Tips on how to protect yourself against cybercrime. Retrieved 16 December 2020, from https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Merriam-Webster. (n.d.). Security. In Merriam-Webster.com dictionary. Retrieved December 10, 2020, from https://www.merriam-webster.com/dictionary/security

MURALI, J. (2019). Human-trafficking on the dark-web. Retrieved 20 December 2020, from https://www.deccanchronicle.com/nation/in-other-news/020919/human-trafficking-on-the-dark-web.html

Organized Crime | Federal Bureau of Investigation. Retrieved 15 December 2020, from https://www.fbi.gov/investigate/organized-crime

Rear, J. (2017). Kidnapped British model: what is the dark web and who are Black Death? - Verdict. Retrieved 20 December 2020, from https://www.verdict.co.uk/kidnapped-british-model-dark-web-black-death-group/

Reid J., Masys A. (eds) Science Informed Policing. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-41287-6_5

Reid, J., & Fox, B. (2020). Human Trafficking and the Darknet: Technology, Innovation, and Evolving Criminal Justice Strategies. In Advanced Sciences and Technologies for Security Applications (pp. 77–96). Springer International Publishing. https://doi.org/10.1007/978-3-030-41287-6_5

Reidy, E., 2020. How Did COVID-19 Affect Migration In 2020?. [online] The New Humanitarian. Available at: https://www.thenewhumanitarian.org/news-feature/2020/12/22/Migration-forced-displacement [Accessed 23 December 2020].

REvil hackers continue to wrack up high-profile targets with ransomware attacks — DarkOwl | Dark Web Search Engine. (2020). Retrieved 27 December 2020, from https://www.darkowl.com/blog-content/revil-hackers-continue-to-wrack-up-high-profile-targets-with-

ransomware-attacks

Rivera, J., & Archy, W. (2019). The Role of the Dark Web in Future Cyber Wars to Come | Small Wars Journal. Retrieved 6 January 2021, from https://smallwarsjournal.com/jrnl/art/role-dark-web-future-cyber-wars-come

Schwartz, B. (2016). Google's search knows about over 130 trillion pages. Retrieved 12 November 2020, from https://searchengineland.com/googles-search-indexes-hits-130-trillion-pages-documents-263378

Tidy, J. (2020). Police launch homicide inquiry after German hospital hack. Retrieved 12 December 2020, from https://www.bbc.com/news/technology-54204356

United Nations. (n.d.). What is Human Trafficking?. Retrieved 20 December 2020, from https://www.unodc.org/unodc/en/humantrafficking/what-is-human-trafficking.html#What_is_Human_Trafficking

World Health Organization. Expanding Public Health Approaches to the world Drug Problem. Retrieved 6 January 2021, from https://www.who.int/substance_abuse/ungass-leaflet.pdf?ua=1

János BESENYŐ
ORCID ID: http://orcid.org/0000-0001-7198-9328

Attila GULYAS
ORCID ID: http://orcid.org/0000-0001-5645-144X