ISSN 1734-3801
e-ISSN 2450-081X

MEDIA – KULTURA – KOMUNIKACJA SPOŁECZNA
MEDIA – CULTURE – SOCIAL COMMUNICATION

Nr 20(2024)
85–105

https://czasopisma.uwm.edu.pl/index.php/mkks
DOI: 10.31648/mkks.9347.7442

Zbigniew Osiński
ORCID: 0000-0003-4484-7265
Wydział Filologiczny
Uniwersytet Marii Curie-Skłodowskiej w Lublinie

Specificity of an information and knowledge sharing system in the TOR (The Onion Router) network

Keywords: Dark Web, The Onion Router, information and knowledge sharing system, anonymity in the web, mercantilism

Słowa kluczowe: Dark Web, The Onion Router, system dzielenia się informacją i wiedzą, anonimowość w Sieci, merkantylizm

Introduction

Sharing information and knowledge is a type of information-related behaviour. It is an element of interpersonal communication, with an exchange of information and knowledge, as well as offers, opinions, views, and evaluations between individuals, groups, organisations, and other structures. Its aim is not only to communicate but also to expand knowledge. It is a condition of generating, disseminating and effective use of information and knowledge (Świgoń, 2015). Currently, information and communication technology, including the Internet, is an important intermediary in this communication. This is a system, or rather a set of systems, i.e. objects, methods, procedures and users, interconnected in a specific manner, functioning as a whole. Utility programs and applications, as well as information resources available on hosting servers, together with user activity, are elements of the Internet system of information and knowledge sharing.

A system of Internet resources called Web 2.0 services has been in use for nearly 20 years. The essence of these solutions (e.g. social services, Wiki, social news services, blogs, vlogs) is to provide users with an opportunity to fill the service structure with the content that they prepare. It is estimated that Web 2.0 services brought about fundamental changes in the processes of information and knowledge sharing by Web users. Currently, the information content and the structure of the Web are largely co-created by end users. Internet users became not only consumers of information and knowledge but also its authors, hence the term “prosumer” (producer + consumer). They make virtual communities and networks with various social interactions, including knowledge and information sharing. There is communal information and knowledge processing, i.e. the process that allows for solving problems collectively that go beyond an individual’s capabilities (Cisek, 2009).

The scientific literature mentions the concept of collaborative knowledge, which is generated and shared through the collaboration of individuals or groups. This is a specific type of knowledge generated by people collaborating for a common goal. The emergence of Web 2.0 services has led to community-driven activities, such as Wikipedia (Palermos, 2022). It is believed that knowledge can be built not only in the mind of an individual but also in the conventional, collective mind of a group of people. Therefore, a group and a community can have collective knowledge. A common feature of those who possess such knowledge is that they function within the same social network, they are motivated by filling gaps in knowledge and the will to self-improve, and they believe in the same criteria of the knowledge quality assessment and in the same values (Fazlagić, 2008).

There is a term “collaboration society” in the scientific circulation, which covers the virtual practices carried out on the Web (e.g. culture of gift, partner production, open source and open access, citizen learning, social hacktivism, gamification, prosumer movement, co-production of media and other artistic values) providing a considerable amount of information, which can be studied (Jemielniak and Przegalińska, 2020).

At the same time, the part of the Internet called the Dark Web is being developed. This term describes networks (e.g. TOR – The Onion Router, Freenet, I2P – Invisible Internet Project, Zeronet) in which the network traffic is largely anonymous and hidden cryptographically. The network traffic is based on a computer network (of routers called proxy nodes or servers), owned by volunteers, and on algorithms, which divert the users’ Internet communication through a range of other users’ computers, which basically prevents the association of specific actions with a specific user. Users connect with proxy servers through virtual tunnels instead of through a direct connection, which allows for anonymous activity. The Dark Web resources are not indexed through commonly used search engines (e.g. Google and Bing), so they do not appear in search results (Finklea, 2022; Hatta, 2020; Okyere-Agyei, 2022).

Apart from this, there is a term “Dark Net” with a narrower meaning, which covers the anonymous nodes, such as computers, servers, and routers, connected into a technical network, which enables the functioning of Dark Web resources, tools and services (Finklea, 2022; Hatta, 2020). The Internet resources of the Dark Web are available only through special software, e.g. the most popular TOR network uses the Tor Browser (or Onion Browser for the iOS system). The TOR network architecture ensures both anonymous resource sharing and anonymous browsing. According to data from the Tor Metrics analytic tool (https://metrics.torproject.org/), this network is used every day by 2 to 2.5 million users, mainly in the USA, Germany, India, Indonesia, Russia, France, Finland, the Netherlands, the UK and Egypt.

The studies conducted so far show that the activity of the TOR network users can be divided into three main categories: 1) social (e.g. ecological) activism, journalism and reporting any irregularities; 2) criminal activity on virtual markets; 3) sharing tools for creating cybersecurity threats, including botnets and malicious software, e.g. ransomware (Wang et al., 2019). Active users share mainly the following thematic groups of content: pornography, cryptocurrency, Bitcoin, drugs, hacking, harmful software, gambling, and political and religious issues (Faizan and Khan, 2019).

The dominant trend in Dark Web studies focuses on how anonymity favours criminal activity and on the technical aspects of the functioning of "dark webs" (Management Association…, 2018; Okyere-Agyei, 2022). It is noteworthy that the University of Arizona AI Lab Dark Web project involves accumulating the Internet content generated by international terrorist groups, including websites, forums, chats, blogs, social services, and films. Different techniques of data, text and website exploration were developed, which made it easier to explore and understand international terrorism through computational and data-oriented approaches (Chen, 2012).

Dark Web research can be divided with respect to the roles that the authors attribute to the web resources. Gupta, Maynard and Ahmad (2019) identified the following roles: drug markets, malicious software markets, trading in stolen documents and identities (credit cards, ID documents, personal data), trade in child pornography, arms trade, platforms for anonymous financial transactions with Bitcoin, communication platforms (discussion forums, chats), the area of activities of special services combating cybercrime, the market of hosting servers for hidden services and resources, tools for bypassing censorship blockades and protection against persecution by the authorities. It was also established that the following issues dominate in the research conducted so far: technical and technological solutions (27% of publications), Dark Web network analysis (24.5%), cyber-attacks on users (15%), illicit trade (12.5%), theoretical analyses of privacy and security (10%) and evaluation of illegal activities on the Dark Web (9%). The papers that analysed the content shared by users on "dark webs" account for 8.5% of publications found during the preparation of the literature review on the Dark Web in 2022 (Tazi et al., 2022).

The literature review shows that not all the aspects of the Dark Web functioning have been examined comprehensively. According to Wang, Mirea and Jung (2019), insufficient attention has been given to the issues related to non-criminal users enjoying the freedom of speech typical of the Dark Web, ensured by anonymity, in order to report various irregularities, political or ecological activism, bypassing the limitations imposed on the Internet by authoritarian regimes or sharing information and knowledge for any other reasons. This seems to be not entirely reasonable, given the information provided in the book "Cyberpolityka. Internet jako przestrzeń aktywności politycznej [Cyberpolitics. The Internet as a space of political activity]" (Majorek et al., 2018). Those authors mention the role of the Dark Web in disseminating information during the Arab Spring, in spreading information blocked by totalitarian regimes, in various actions of objection against oppressive authorities of non-democratic countries and as part of the unhindered self-organisation of activists and revolutionaries. They referred to two publications which reported study findings (Klimburg, 2014; Yetter, 2015).

According to the findings of other studies, social interactions on the Dark Web involve tools known from the first-generation Internet: chats, thematic discussion forums and e-mails. Obviously, each of these tools functions in a form that is characteristic of anonymous networks (Xyan i., 2020). Pete et al. (2020) identified patterns of interactions, the features of communities that took part in discussions on Dark Web forums, and the structure and nodes of the discussion participant network. Robert Gehl (2016) presented actions taken by administrators of the Dark Web Social Network service aimed at introducing the same standards as those followed on Facebook and Twitter. The aim was to create a secure and moderated environment for productive information exchange by individuals who value anonymity. However, it must be stressed that a large majority of science publications on the Dark Web operation (at least those indexed in the Scopus database or shown in the Google Scholar search results) focus on illegal user activities and also on security in the network, as well as ethical and IT-related aspects. The Dark Web is not only used by criminals but also by non-criminal users for information and knowledge sharing, and this phenomenon needs to be studied comprehensively.

Aims, object and methodology of study

The purpose of this research is to create a model that represents the information and knowledge-sharing system that exists on the Dark Web in early 2023. The model aims to capture not only the structure of the system but also the way it is perceived by its users, who are individuals that share information and knowledge.

The uncertainty concerning the moment of the system's existence arises from the fact that the nodes operated on the Dark Web are owned by private individuals – volunteers. They are not always on, and there is frequent rotation – some end their activity, and others are started. Therefore, the system is evolving.

It should be emphasized that users of the Dark Web networks remain anonymous, making it difficult to examine the information and knowledge--sharing system. The networks can be used to bypass the mechanisms of content filtering, censorship and other communication restrictions. This should translate into developing solutions and resources that do not have any restrictions, even into anarchism, breaking the law, and a much higher level of freedom of speech than is commonly used on the visible Internet. Therefore, a question presents itself: how does anonymity affect the information-related behaviours whose consequence is the existence of an information and knowledge-sharing system? It seems important not only to determine the elements and features of the system but also to demonstrate potential differences between the methods of information and knowledge sharing followed by users of the Dark Web and the visible Internet. It should also be established whether users of the system under study act as prosumers or create virtual communities and whether their activities result in generating collaborative knowledge.

The current study analysed solutions supporting the information and knowledge sharing process as well as the active (in early 2023) resources generated in this process, existing in one of the Dark Web networks – the popular TOR network. It is a virtual computer network which uses onion tracing (a technique of communication anonymisation on the Internet). Data packages in the TOR network are sent through several network nodes called onion routers, and the encryption/decryption technique, similar to taking off onion layers, ensures relative anonymity for both the Internet resource developer and all its users. Each proxy node knows the location of only the preceding and the following router. This prevents network traffic analysis, which is the basis for anonymity. TOR servers and services are available in the .onion pseudo-domain rather than in the DNS system. The services and resources in the TOR network are not indexed by Google or Bing search engine bots. One has to know the direct address in the .onion pseudo-domain and use a specialist Tor Browser. TOR enables concealing the identity (location) of both the content consumer (i.e. an ordinary user) and its provider (Hatta, 2020; Okyere-Agyei, 2022).

The study was empirical and consisted of the acquisition of quality data directly from the study object. To this end, collections of links to resources in the .onion pseudo-domain were used, as well as two types of tools that allow for identifying Dark Web resources and reaching them – search engines that can be used in the TOR network and resource catalogues available on the network. The first stage of the study involved service catalogues prepared by TOR network users (in the “dark web” and in the visible Internet) with a view to identifying resources whose authors share information and knowledge (or tools and auxiliary services) on the Dark Web. The second stage involved searching for further “dark web” resources with Ahmia and Torch search engines. Search words associated with information and knowledge sharing, identified at the first stage of the study, were used. The following words were used: blog, e-book, forum, library, freedom of information, freedom of speech, and wiki. The experiment was repeated several times. The collected empirical material was analysed using the content analysis method, which allows for a systematic and objective content description. Qualitative data processing (qualification) was performed, which resulted in identifying resources in which users share information and knowledge, and the resources were divided into relatively homogeneous groups comprising the model of an information and knowledge-sharing system. Subsequently, the TOR-specific system features were identified.

Various techniques and tools are used to acquire data when studying dark web resources. IT tools – crawlers (searching bots) and scripts in the Python language (e.g. Dark Web OSINT Tools https://github.com/apurvsinghgautam/dark-web-osint-tools), which allow for automatic data downloading, are becoming increasingly popular (Chen, 2012; Ferry et al., 2019). However, the author decided to employ the technique described above, based on catalogues and search engines, because it is used by the dominant group of Dark Web users who are not researchers. This move is related to the main study objective – to develop a model of the information and knowledge sharing system in the shape it is constructed but also perceived by its users – individuals who share information and knowledge and not by Dark Web researchers.

Study findings

The TOR network is explored with the Tor Browser – the first element of the information and knowledge-sharing system in the network under study with which a user comes into contact. The "New to Tor Browser" button leads the user to the basic explanations of the rules of the TOR network and the browser operation. The "Check our Tor Browser Manual" link takes one to more comprehensive explanations of these issues. It also refers to the TOR project website (https://www.torproject.org/). One may thus reach elements of the visible Internet, but one also acquires knowledge necessary to use the Dark Web efficiently (see App. 1). These resources are a manifestation of information and knowledge sharing by "dark web" users. Therefore, both the project website and similar resources are regarded as part of the system under study. The resources described above allow for reaching further visible Internet services in which TOR users share information and knowledge (see App. 2).

The main elements of the system in question are parts of the TOR network (in the .onion pseudo-domain). The Tor Status service showed 6,170 TOR routers (called proxy nodes and servers) operative in January 2023, approx. 83% of which were described as stable, 49% as operating nearly without interruptions, and 25% as outward ones (allowing for communication with the visible Internet). A majority of the routers were running on Linux (approx. 5760) and FreeBSD (approx. 300). They were located mainly in Germany (1660), the USA (1350), The Netherlands (435), France (325), Serbia (180), the UK (165), Finland (160), Switzerland (160) and Canada (155). This service and other data sources do not allow for determining how many devices (computers) which work as routers run the software, which makes them WWW servers with services and resources, which can be classified as an information and knowledge-sharing system. The scale of this phenomenon can only be estimated by searching and browsing services in the .onion pseudo-domain. At the end of January 2023, Tor Metrics showed that – depending on the day – there were 650 thousand to 800 thousand unique .onion addresses.

These resources can be browsed with the Tor Browser, which offers an essential tool for searching the TOR network – the DuckDuckGo search engine. It can not only search through a domain from outside the DNS system (and .onion is such a domain), but it also does not collect information about the users. There are many search engines on the TOR network because their usability in the world of .onion addresses is much greater than that of similar tools in the world of DNS domains. There were 37 active search engines in January 2023 (apart from DucDuckGo): Ahmia, Amnesia, Bobby, Deep Search, Excavator, Find Tor, GDark, GoDeep, Grams, Haystak, Hologram (Amnesia group), Hoodle, Kraken, MetaGer, Ondex, OnionLand Search, OnionSearch, Onion Search Engine, Onion Search Serwer, Our realm, Phobos, Search Demon, Sentor, Stealth (Amnesia group), Submarine, Tor66, TorBook, Torch, TorDex, Torgle, TOR Google, TorLanD, Tornet Global Search, Tor Search, Tor Search Engine, TorTorGo and Venus Search Engine. The multitude of search engines is a consequence not only of the fact that website addresses in the TOR network are complicated and random strings of characters. A large majority of the above-mentioned search engines display advertising banners of markets and shops on the Dark Web, and their owners are undoubtedly paid for this.

Another essential tool, without which the information and knowledge-sharing system on the TOR network would be deficient, are catalogues of websites in the .onion pseudo-domain (Table 1).

Table 1 shows that an element of the information system which is disappearing from the visible Internet – website catalogues – is growing in the Dark Web. The reasons are similar to the quantitative growth of search engines – complicated .onion addresses and earning money on advertising banners.

Table 1

Catalogues of websites in the .onion subdomain

No.	Name	Website categories
1	2	3
1.	BlackButterfly666's Link Collection	links to websites about cryptocurrencies and Bitcoin stock exchanges
2.	Blood Moon Wiki	Search Engines, Market Places, Wiki, Press/News, Cryptocurrency, Drugs, Adults, Carding/Financials, Email Provider, Communities, Ransomware/Hackers
3.	DarkDir	Blog, Catalogue, News, Search, Social, Shop/Store/Market, Other
4.	Dark Eye	catalogue of websites associated with illicit trade
5.	Darknet Home	Bitcoin, Blogs, Cards, Catalogues, Drugs, E-Books, E-Mail, Escrow, Forums, Gambling, Hacking, Hosting, Markets, Money, News, Other, PayPal, Search, Weapons, Wikis
6.	Darknet Hub	links to markets and shops
7.	Darkzone onions	Search Engines, Link Lists, Marketplace – Commercial, Weapons – Commercial, Counterfeits – Commercial, Cryptocurrency – Commercial, Gift Cards – Commercial, PayPal – Commercial, Drugs – Commercial, Hacking – Commercial, Bitcoin, Web/Image Hosting, Secure Email Provider, News
8.	Deep Links Dump	Search Engines, Link Lists, Carding, Market Place, Hacking, Cryptocurrency, Gift Cards, News, Pay Pal, Hosting, Drugs, Weapons, Counterfeits, Email Provider, Misc.-Other

cont. Table 1

1	2	3
9.	DeepLink Onion Directory	Market, Hacking, Hosting, Forum, Blog, Link List/Wiki, Communication, Social, Financial Services, Adult, Search Engines, Private Sites
10.	Directory Satanic Goat Onion Link	Adult, Services, Shop/Market, Social Media, News/Blog, Link Lists, Search Engine, Book
11.	Fresh Onions	Search engines, Link lists, Carding, Marketplace, Counterfeits, Cryptocurrency, Gift cards, PayPal, Hacking, Gambling, Electronics
12.	General Tor Links	Search Engines, Catalogues and Wikis, Shops and Markets, Anonymous Services, Bay Crypto, E-mail Services, Social, Forums, Hosting, Scam List
13.	Global Tor Links	Search Engines, Marketplace/Shop/Exchange, Forums/Boards/Chans, Wallet/Escrow/Financial Services, Email/Messaging, Hacking/Ransomware/Virus, Share/Upload, Hosting/Domain Services, Library/Books, Strange, Chat, Social networks, Pastebin, VPN/Security/Privacy, Press, Blog, Torrent, Music, Scam
14.	HD Wiki	Search on the deep web, Premium financial services, Darknet markets, Other financial services, Safe email providers, Hosting, Blogs and Forums and IRC, Illuminati
15.	Hidden Bitcoin Wiki	links to websites about cryptocurrencies, including Bitcoin stock exchanges
16.	Hidden Reviews	Blog, Catalogue, Chat, E-mail, Forum, News, Other, Search Engine, Shops/Stores/Markets
17.	Hidden Wiki Fresh 2022	Search engines, Where to get bitcoin, Best VPN Services, E-mail services, Certified scam places, Marketplaces, Carding, Money Counterfeits, Crypto services, Porn, Electronics, Betting, Escrow, Imageboard, Forums, Books, Social Networks, Non-English
18.	King Wiki	Email providers, Press/News, Communities, Adults, Cryptocurrency, Search engines, drugs, carding, marketplace, ransomware/hackers, wiki
19.	Link Directory Pro	Useful (chat, email providers, forum, search engine), Carding, Catalogue (wiki, link list), counterfeits, Crypto, Drugs, Electronics, Escrow, Gambling, Guns, Hacking, Marketplace, XXX
20.	Nexus	Marketplaces, Directories, Drugs, Hacking, Cryptocurrency, Search Engines, Email, Forums, Social Media, Hosting, Operating Systems
21.	Not Evil	Adult, Crypto Investments, Forums, Hacking, Links Directories, Markets, Scam List,
22.	OnionDir	Shops/Markets, Libraries/Wikis, Escrow, Forums, Mail services, Hacking/Security, Search Engines
23.	Onion Scanner	links to shops and markets
24.	Paul Onion Links	Last added, Adult/Porn, Commercial/Market/Shop/Store, Communication, Crypto/Digital, Hacking, Hosting, Libraries/Wiki, Link lists, Search, Security
25.	ShopsDir	links to shops and markets
26.	Snow Bin	a collection of uncategorised links

cont. Table 1

1	2	3
27.	Tasty Onions	Search Engines, Link Lists, Carding – Commercial, Marketplace – Commercial, Counterfeits – Commercial, Cryptocurrency – Commercial, Gift Cards – Commercial, PayPal – Commercial, Drugs – Commercial, Weapons – Commercial, Hacking – Commercial, Bitcoin, Web & Image Hosting, Secure Email Provider, News, Misc./ Other
28.	The Dark Stream	Search Engines, Active Hidden Markets, Mail Services, Forums, Hacking, News/Whistleblowing, Files
29.	The Hidden Links	Accounts, Blog, Carding, Catalogue, Chat, Counterfeits, Cryptocurrency, Drugs, Electronics, Email Providers, Escrow, Forum, Fun, Gambling, Gift Cards, Guides, Guns, Hacking, Hitman, Marketplace, Money Transfers, Multi Shop, News, Other, PayPal, Search Engine, Social, Wiki, XXX
30.	The Hidden Wiki	Search Engines, Drugs, Fraud/Carding, Counterfeit, Cryptocurrency, Hacking, Firearms, Gift Cards, Gambling, Airdrop, Hosting, Escrow,
31.	The Hidden Wiki (new)	Introduction Points, Financial Services, Commercial Services, Anonymity/Security, Darknet versions of popular sites, Blogs/ Essays/Wikis, Email/Messaging, Social Networks, Forums/Boards/ Chats, Whistleblowing, Hack/Phreak, Anarchy, Hosting, Website developing, File uploaders, Audio-Music/Streams, Video-Movies/TV, Books, Drugs, Erotica, Non-English, Chat centric services
32.	The Safe Onion Links	Adult, Market, Hacking, Cryptocurrency/Investments, Forums, Scam List
33.	Tor Link List	Top onion sites, Markets, Carding, Transfer, Escrow, Links, Email, Hosting, Hacking, Search, Scam
34.	Top Onions	several most frequently visited sites
35.	Topic Links	links to several dozen categories of porn websites
36.	Tor.Fish	catalogue of websites associated with illicit trade
37.	Tor Links 2023	Bitcoin, Blogs, Cards, Catalogues, Drugs, E-books, E-mail, Escrow, Forums, Gambling, Hacking, Hosting, Markets, Money, News, Other, PayPal, Search, Weapons, Wikis
38.	Tornode	Cryptocurrency, Lists, Email, Forums, Government, Hacking, Hosting, Marketplaces, Music/Video, News/Blogs, Porn, Scam, Search Engine, Security, Software, Whistleblowing
39.	TOR Scam List	a catalogue of websites operated by fraudsters and swindlers
40.	Truly Wiki	Search Engines, Marketplaces/Shops, Gambling, Hacking, Electronics, Wiki Link List/Catalogue
41.	Trusted Links	Wiki/Links, Search Engines, Email Providers, Marketplaces/Shops, Communities/Forums, Press/News, Adults/Erotic, VPN/Privacy, Personal/Blog, Ransomware/Hackers, Hosting/Upload, Library/Books
42.	TrustWiki	Search Engines, Marketplaces, Anonymous Services, Buy Cryptocurrency, E-mail Services, Forums, Hosting, Scam List
43.	VCS Onion Links	Search Engines, Link Lists, Carding, Marketplace, Ransomware, Cryptocurrency, Adults, Press/News, Privacy/VPN, PayPal, Hosting, Escrow, Drugs, Email Provider
44.	Verified Links	Markets, Search Engines, Forums, Email, Blogs, Hosting

Discussion forums enjoy a similarly intensive growth. In spring 2023, the Torch search engine showed 992 websites in response to the word "Forum", while Ahmia – 285 (both search engines were chosen because of a relatively large number of items in the search results; DuckDuckGo was left out because it also shows results from the visible Internet). However, a large majority of them are only channels for communication between criminals (hackers, thieves, drug dealers, political extremists, etc.) and potential clients. Some of the forums have had no active users for months. The number of results is increased by the fact that both search engines showed clones of some forums as unique .onion addresses. Both lists contain relatively many (even over 80%) services which are not discussion forums. Catalogues of TOR network resources are more effective in providing information on discussion forums. Relatively regular information and knowledge sharing takes place on the forums in the list below, which, however, is not a complete one of existing forums (Table 2).

Table 2

Discussion forums on the Dark Web

No.	Name	Description
1	2	3
1.	3h	political incorrectness plus various topics about Dark Web
2.	Abyss Forum	subjects: hacking, pornography, illicit trade, cryptocurrencies
3.	ACIEEED Forum	various topics, mainly hacking and trade in illicit goods
4.	ASAP Forum	about child pornography
5.	AskRaddle	multi-topic: ideologies, e.g. anarchism, feminism, fascism; programming, e.g. Linux, meta, games, climate changes, comics, prostitution, media, immigration, border crossing
6.	BreakingBad	for those dealing in and buying drugs and about encryption technologies, anonymity and trade on the web; also, Wiki with the knowledge of drug manufacturing
7.	Cebulka	in Polish, for those interested in illegal sale/purchase offers
8.	Cloud9 Forum	on illicit trade markets
9.	CryptBB	discussions on Bitcoin and on trading in this currency
10.	Dark Web Forums	for those interested in illicit trade on the Dark Web
11.	DEF Con Forums	a forum about hacking plus blogosphere plus a collection of articles on hacking and security on the web
12.	DFAS	various IT issues
13.	DimensionX	various Dark Web-related topics
14.	Dread Network	discussions on various Dark Web-related aspects
15.	Forum Bitcoin	various aspects of Bitcoin and Ethereum mining and their use for illegal payments
16.	French Poule Web	in French, topics: pornography, illicit trade, security and anonymity, and others
17.	French World Market	in French, for those interested in illicit trade

cont. Table 2

1	2	3
18.	Hidden Answer	various questions to experts in trade, hacking, anonymity, etc. plus answers
19.	Infocon	IT-related topics, mainly hacking
20.	Kick-ass	hacking, harmful software, stealing passwords and data, trade in illicit goods
21.	Mazafka	in Russian: about cryptocurrency-based payment systems, about harmful software
22.	NZ Darknet Market Forum	various aspects of illicit trade
23.	Onion Gun Forum	in Russian: for those interested in firearms
24.	PasteBox	about pornography
25.	Ramble	a collection of narrow-topic forums
26.	RuDark	multi-topic forum in Russian
27.	Russian Anonymous Platform	multi-topic forum in Russian
28.	SuprBay	for those interested in file sharing (music, films, applications, games, photography, books)
29.	The Hub	discussion on hidden services on the TOR network, illicit trade markets, cryptocurrencies and effective ways of staying anonymous
30.	The Majestic Garden	on “safe” drugs, on alleviating the effects of taking drugs
31.	The Stock Insider	exchange of or trade in insider information from listed companies
32.	The Tor Forum	topics related to sex and pornography and to trade in illicit goods
33.	VMN Almrauq Drugs Forum	about drug dealing
34.	XSS Forum	in Russian: tips for cybercriminals

A large majority of forums require setting up an account with the use of electronic mail that works within the Dark Web. There are at least a dozen servers which offer anonymous email accounts: Anonymous Temp Email (temporary, for several days), Alt Address (temporary for three days), Cook Mail, Cs.email (short-term), Daniel, DNMX, Elaude, Mail2Tor, Onion Mai, ProtonMail, Riseup, SecTor.City, Sonar, TorBox, TorMail and Xmpp.is.

Blogs are less visible elements of the system under study. Compared with the visible Internet (DNS system), their offer on the Dark Web is very modest. Ahmia and Torch search engines may give 876 items in their search results for “blog”, but the figure is inflated due to the issues described in the section about discussion forums. A smaller number of active blogs existed in spring 2023, especially those that share information without conducting illicit trade (Table 3).

Table 3

Blogs on the Dark Web

No.	Name	Description
1	2	3
1.	AnonBlogs	a platform for microblogs plus a certain number of microblogs
2.	Blog Bitcoin	everything about Bitcoin
3.	Blog Joseph Duffy	a blog which is an element of the www service, subjects: specialist programming topic, open source
4.	Blog Random musing	considerations about various aspects of the Internet
5.	Blog Urof.net	blog (plus a separate tab: Articles) is an element of the www service, IT issues, mainly active presence on the Internet
6.	Bot Mans World	blog about firearms, part of a website
7.	Burny Liama's Blog	various aspects of the TOR network
8.	Coarse Enigma	specialist IT issues, especially those concerning privacy and cybersecurity
9.	Colin Cogle's Blog	issues related to amateur radio communication and IT
10.	CozyNet Blog	videoblog with various cartoons and music clips
11.	Endchan	a platform for microblogs plus a certain number of microblogs
12.	Etam Software	various IT issues
13.	Franco's technology blog	specialist programming knowledge
14.	Il blog di Leandro	various aspects of culture: cinema, TV, literature, music, IT, hacking
15.	Jake's Thoughs	open source software, computer games
16.	JS Blog	a blog which is an element of the www service, activities on the TOR network
17.	Kernal	specialist IT issues
18.	Mon blog Je sui Charlie	about computers
19.	ProPublica	investigative journalism, abuse of power
20.	Quantum	a blog by a programming engineer about various aspects of computer software
21.	Quantum Blog	various aspects of power engineering
22.	S-Config	providing information on interesting examples of creating pieces of digital cultural work on the Internet
23.	Security in a box	a blog presenting knowledge of privacy protection and security on the Web and cybersecurity in general
24.	SerHack	blog about anonymity, security, applications and cryptocurrencies
25.	Shen's Essays	a scientific blog about computers and information technology
26.	Tape News	about anonymity, illicit trade, hacking, cryptocurrencies
27.	Tech Learning Collective	a blog – part of the website, knowledge of security of IT infrastructure for organisations acting for the benefit of social justice
28.	The blog of ~vern	specialist IT issues

cd. tabeli 3

1	2	3
29.	The Dark Web Journal	posts about cryptocurrencies, what's new on the Dark Web, hacking, security on the Web
30.	Theyosh.nl	about application programming, especially for streaming services
31.	Vi Grey	blog by a programmer, part of the website
32.	Wizardy and Steamworks	about computer programs, their structure and use

Sharing information and knowledge also takes place on social media. The TOR network has its equivalents existing on the Internet of the DNS system: Facebook and Twitter. There are also social media specific to this network: Alogs.Space, Diaspora, Flashlight 2.0, Invidious – they allow for sharing materials found on the Dark Web and commenting on posts; Celebrity Underground – sharing photos and films featuring celebrities.

Services, which can be called social archives and libraries, are separate components of the information and knowledge-sharing system (Table 4).

The system is complemented by tools that support information and knowledge sharing on the TOR network (Table 5).

Table 4

Social archives and libraries

No.	Name	Description
1	2	3
1.	Anarch_Copy	e-books: scientific literature and fiction
2.	Anarcho-Copy Amusewiki Yansısı	e-books on various topics
3.	Anarşist Kütüphane	library of anarchistic books
4.	Bible4u	uncensored books that comprise the Bible, this resource is intended for individuals from countries where the Bible is banned; links to the Bible available in other services
5.	Booksi	e-books: scientific literature and fiction
6.	Comic Book Library	collection of comics
7.	Dailistormer	materials that do not find their way to liberal-leftist media for ideological and political reasons
8.	I'Lam Foundation	materials prepared by radical Muslims, links to many similar ones
9.	Imperial Library	about 1.5 million e-books in several dozen categories, epub and html
10.	Just Another Library	collection of courses in various scientific disciplines, e-books, audiobooks and photographs, hacking, security on the Web, drugs, occultism, health, electronics and IT, pornography
11.	Knowledge	knowledge of active use of the TOR network

cont. Table 4

1	2	3
12.	Library	several dozen e-books, for some reason absent from the visible Internet resources: IT, philosophy, politics (political incorrectness), security and anonymity, investigations, health
13.	Marxists Internet Archive	collection of classical Marxist works
14.	Monero	a guide for establishing a virtual wallet for trade in cryptocurrencies and on Dark Web markets
15.	Oil and Fish	a collection of materials on the principles of maintaining anonymity on the Web for religious and political dissenters
16.	Secret Junta's coffer (own translation from Ukrainian)	collection of materials that identify Russian war criminals
17.	Sustainable www	books, podcasts, courses, articles about website design
18.	The Library	several scientific books in the pdf format
19.	The Library of Thoughtcrime	a library of over 100 books and video clips (pdf, mp4) – Holocaust revisionism, cognitive abilities, crime (in the spirit of political incorrectness)
20.	Tor Guide	a guide on the structure and functioning of the TOR network
21.	Z Library	a huge collection of e-books and articles on many topics

Table 5

Tools that support information and knowledge sharing

No.	Name	Description
1	2	3
1.	AbleOnion	instant messaging client
2.	Adamant	instant messaging client and a cryptocurrency wallet based on the blockchain technology
3.	AfriLeaks	for anonymous sharing of information with journalists of several African services
4.	Bitmessage	P2P protocol for sending encrypted messages to another person or to multiple subscribers, protects against wiretapping, ensures anonymity
5.	Black Cloud	for file sharing
6.	Black Hat Chat	instant messaging client
7.	Dark Forest	instant messaging client
8.	FragDenStaat	reporting human rights abuse by the authorities for the relevant authorities to take proper measures
9.	MadIRC	instant messaging client
10.	Null Message	sending messages which self-destruct after 21 days
11.	SecureDrop	an open-source system for reporting irregularities, which media organisations and NGOs can install to receive secure documents from anonymous sources

cont. Table 5

1	2	3
12.	SVR	the Russian intelligence service implemented a system similar to the SecureDrop platforms to enable Russians who live abroad to send anonymous messages through the TOR network about threats to Russia's national security
13.	Theend	instant messaging client
14.	The Guardian	for sharing information anonymously with journalists of "The Guardian"
15.	Titan-XMPP	for anonymous communication and payments
16.	ZeroBin.net	for creating discussion forums

Conclusions

The presentation of the model of an Internet system of information and knowledge sharing should start with identifying its elements. Subsequently, interactions between those elements and with the surroundings should be determined.

Elements of the information and knowledge-sharing system on the TOR network can be grouped into the following categories:

1. Computers with suitable software installed – programs for the TOR node (depending on the computer operating system), WWW server package for PHP, e.g. XAMPP (Apache distribution), utility software for running websites, forums, blogs, etc., in the .onion pseudo-domain. Connected by telecommunication links, computers with such software make a network within the Internet and play the role of input/output nodes from the TOR network, an intermediary node and a hosting server.
2. Services that enable one to move around the TOR network – search engines and catalogues.
3. Information and knowledge resources that allow for acquiring skills in active and passive use of the TOR network.
4. Services that enable network users to communicate – e-mail, discussion forums, chats.
5. Specialist information and knowledge resources.

The hardware system component characteristics will be limited to the information provided above, as this paper is concerned with information science rather than information technology.

Therefore, let us pass on to the second element of the system in question. In order to move around the TOR network, it is necessary to have the addresses of individual websites and services shared by their developers/owners. An address is a string of characters generated separately for each website and service upon setting up, ending with the pseudo-domain name – .onion. Unlike the addresses in the DNS system Internet, those ending with .onion are not registered anywhere.

They do not consist of easy-to-read strings of characters (e.g. a company name read by a DNS server as an IP address) but a cryptographic public key. In order to reach the TOR network resources, one has to not only use a specialist browser but also enter (paste) into the address bar a string of 16 characters, which do not make any sequence of words. Therefore, catalogues of websites and browsers play a much more important role in this network than in the DNS system Internet. Unfortunately, due to the specificity of the TOR network, the usability of search engines and catalogues is not satisfactory. The search and index mechanisms of several dozen search engines do not manage to fit the search results with the search word too well. In the case of the search terms used in this study, only a small percent of addresses in the result list matched the search word (the main problems with the search results were listed in the part of the paper on the presentation of the search results). Catalogues of www services contain many inactive addresses (which is not uncommon in a volunteer-based network) and ones with the wrong classification. In effect, reaching a specific resource is difficult and time-consuming. One gets the impression that multiple search engines and catalogues were developed mainly as a place for paid advertising banners.

Due to these difficulties and the clearly different rules of the TOR network functioning compared to the DNS system Internet, there are a lot of resources which help users acquire competence in moving around the network. The authors of these resources assumed that the acquisition of knowledge of how the TOR network operates should begin on the “visible” Internet. Even the TOR Browser directs one to such materials. In effect, the number of specialist services, training courses, e-books, presentations and video clips intended both for those who want to expand TOR actively and for passive users, both beginners and specialists, is relatively large. Further, training materials and guides available within the TOR network are intended mainly for advanced users interested in active use of the network. This type of information and knowledge sharing takes place mainly in discussion forums and blogs. There is a visible prosumer movement in this element of the information and knowledge-sharing system, creating virtual communities and functioning as a mechanism of collective knowledge generation and the existence of collective knowledge.

Use of most forums requires setting up an anonymous e-mail account on the TOR network. At the moment (spring 2023), there are about a dozen servers offering this service, including those offering temporary e-mail accounts. Elements of the system that support communication between network users and facilitate information and knowledge sharing include applications for forum, chat, and blog development, not only on one’s computer, which acts as a server but also on an application provider’s server.

Apart from knowledge of various aspects of the TOR network, the resources available on this network provide information and knowledge of the following issues:

1. Operation of markets and shops with illicit goods (drugs, firearms, child pornography, stolen documents and databases, counterfeit products of well-known

brands) and services (hacking activities, creating hidden resources – servers, forums, shops – on the Dark Web).

2. Cryptocurrencies and systems of payment on the Dark Web.

3. Security and anonymity on the Dark Web.

4. Hackers' tools and methods.

5. Specialist IT issues (programming, administration).

6. Ideologies, especially Marxism and anarchism, political incorrectness, anti-leftism.

7. Methods and tools for systems of anonymous reporting of abuse and irregularities.

8. Knowledge of drugs and firearms.

Prosumers do not play a visible role in this element of the information and knowledge-sharing system in question. The types of resources mentioned above are not usually co-created but created by their authors and owners of the services. The virtual communities and networks developing around specialist servers are usually connected by buyer-seller-type relations.

Interactions in the process of information and knowledge sharing between the system and the surroundings consist mainly of providing knowledge to those interested in the Dark Web and the TOR system who do not have sufficient experience or competence to function in this part of the Internet.

The interactions within this system usually involve providing information and knowledge as if "as a side effect" for several reasons. Mainly, such actions are taken by those who offer illicit goods and services – owners of services, blogs and forums, whose main aim is to promote their own offer. The second reason is the willingness to earn money by promoting these offers owing to the solutions that make it easier for other users of the TOR network to move around the resources – catalogues and search engines with attached advertising banners.

However, not only mercantile motivations generate interactions in the information and knowledge-sharing system in question. There is a distinct group of users whose actions are driven by the idea of freedom of speech and anonymity on the Internet. Members of this group share e-books and articles, often in violation of copyright laws. The aim of some of these initiatives is to bypass censorship restrictions which are in force in some countries or to ensure the possibility of spreading information and reporting irregularities anonymously. Another group that shares information and knowledge without taking simultaneous actions aimed at earning money is a community of active users who are highly competent in IT, passionate developers of solutions used in the TOR network, and ensure anonymity and security.

Sharing information and knowledge on the TOR network takes place in a system in which the needs and motivations of the authors and those of resource users meet with the capabilities created owing to technologies, including anonymity, bypassing censorship restrictions and payment methods that employ the use of cryptocurrencies. This system is obviously affected by the specific culture of freedom, which can sometimes lead to anarchism and breaking the law.

Significant features of this system are its variability, ephemerality and instability of a considerable part of the resources and low effectiveness of tools used to search for specific content.

References

Chen, Hsinchun (2012). *Dark Web: Exploring and Data Mining the Dark Side of the Web*. New York: Springer. DOI: 10.1007/978-1-4614-1557-2.

Cisek, Sabina (2009). Dzielenie się wiedzą w Internecie. *Bibliotheca Nostra*, 3/4(19), 33–42.

Faizan, Mohd and Khan, Raees A. (2019). Exploring and analyzing the dark Web: A new alchemy. *First Monday*, 5(24). DOI: 10.5210/fm.v24i5.9473.

Fazlagić, Jan A. (2008). Wiedza kolektywna na przykładzie polskiej oświaty. *E-mentor*, 1(23). Access: https://www.e-mentor.edu.pl/artykul/index/numer/23/id/505.

Ferry, Nicolas, Hackenheimer, Thomas, Herrmann, Francine and Tourette, Alexandre (2019). Methodology of dark web monitoring. *11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Pitesti, Romania, 1–7. DOI: 10.1109/ECAI46879.2019.9042072.

Finklea, Kristin (2022). The Dark Web: An Overview. *Congressional Research Service*, IF12172. Access: https://crsreports.congress.gov/product/pdf/IF/IF12172.

Gehl, Robert W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, 7(18), 1219–1235. Access: https://journals.sagepub.com/doi/full/10.1177/1461444814554900.

Gupta, Abhineet, Maynard, Sean B. and Ahmad, Atif (2019). The Dark Web Phenomenon: A Review and Research Agenda. *Australasian Conference on Information Systems 2019*, Perth, WA.

Hatta, Masayuki (2020). Deep web, dark web, dark net: A taxonomy of "hidden" Internet. *Annals of Business Administrative Science*, 19(6), 277–292. DOI: 10.7880/abas.0200908a.

Jemielniak, Dariusz i Przegalińska, Aleksandra (2020). *Społeczeństwo współpracy*. Warszawa: Wydawnictwo Naukowe Scholar.

Klimburg, Alexander (2014). Roots Unknown – Cyberconflict Past, Present & Future. *Sicherheit und Frieden (S+F) / Security and Peace*, 1(32), 1–8.

Majorek, Marta, Olszyk, Sabina i Winiarska-Brodowska, Małgorzata (2018). *Cyberpolityka: Internet jako przestrzeń aktywności politycznej*. Warszawa: Wydawnictwo Texter.

Management Association, Information Resources (2018). *The Dark Web: Breakthroughs in Research and Practice*. Hershey, PA: IGI Global. DOI: 10.4018/978-1-5225-3163-0.

Okyere-Agyei, Stanley (2022). *The dark Web – A Review*. Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics, 209–214.

Palermos, Spyridon O. (2022). Collaborative knowledge: Where the distributed and commitment models merge. *Synthese*, 200. DOI: 10.1007/s11229-022-03459-7.

Pete, Ildiko, Hughes, Jack, Chua, Yi T. and Bada, Maria (2020). A Social Network Analysis and Comparison of Six Dark Web Forums. *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) 2020*, Genua, 484–493. DOI: 10.1109/EuroSPW51379.2020.00071.

Świgoń, Marzena (2015). *Dzielenie się informacją i wiedzą. Specyfika nieformalnej komunikacji w polskim środowisku akademickim*. Olsztyn: Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego w Olsztynie.

Tazi, Faiza, Shrestha, Sunny, De La Cruz, Junibel and Das, Sanchari (2022). SoK: An Evaluation of the Secure End User Experience on the Dark Net through Systematic Literature Review. *Journal of Cybersecurity and Privacy*, 2(2), 329–357. DOI: 10.3390/jcp2020018.

Wang, Victoria, Mirea, Mihnea and Jung, Jeyong (2019). The not so dark side of the darknet: a qualitative study. *Security Journal*, 32, 102–118.

Xyan, Chin W., Wei, Justin L. Z. and Juremi, Julia (2020). An Exploration into the Dark Web. *Journal of Applied Technology and Innovation*, 4(4), 10–13.

Yetter, Richard B. (2015). *Darknets, cybercrime & the onion router: Anonymity & security in cyberspace* [Dissertation]. New York: Utica College. Access: https://www.proquest.com/openview/376ea22b97714afcd76859eeec9e6ed9/1?pq-origsite=gscholar&cbl=18750.

Summary

Aim: To develop a model of an information and knowledge sharing system, existing on the Dark Web in early 2023, in a shape that it is constructed but also perceived by its users – an information and knowledge sharing individual.

Method: The study was empirical and consisted of the acquisition of quality data directly from the study object (TOR network). Qualitative data processing (qualification) was performed, which resulted in identifying resources in which users share information and knowledge, and the resources were divided into relatively homogeneous groups comprising the model of an information and knowledge-sharing system. Subsequently, the TOR-specific system features were identified.

Results: Sharing information and knowledge on the TOR network takes place in the system in which the needs and motivations of the authors (mainly mercantile) and those of resource users meet with the capabilities created owing to technologies, including anonymity, bypassing censorship restrictions and payment methods that employ the use of cryptocurrencies. This system is significantly influenced by the culture of freedom, sometimes leading to anarchy and violation of laws. Significant features of this system include its variability, ephemerality and instability of a considerable part of the resources and low effectiveness of tools used to search for specific content.

Specyfika systemu dzielenia się informacją i wiedzą w sieci TOR (The Onion Router)

Streszczenie

Cel: Opracowanie modelu istniejącego w Dark Web, w pierwszej połowie roku 2023, systemu dzielenia się informacją i wiedzą w kształcie, w jakim jest on budowany, lecz także postrzegany przez jego uczestników – osoby dzielące się informacją i wiedzą.

Metoda: Badania miały charakter empiryczny i polegały na pozyskiwaniu danych jakościowych bezpośrednio z przedmiotu badań (sieci TOR). Przeprowadzono jakościową obróbkę danych (kwalifikację), w efekcie czego wyróżniono zasoby, w których użytkownicy dzielą się informacjami i wiedzą, oraz dokonano podziału tychże zasobów na w miarę jednorodne grupy składające się na model systemu dzielenia się informacją i wiedzą. Następnie wyróżniono te cechy systemu, które okazały się specyficzne dla sieci TOR.

Rezultaty: W sieci TOR dzielenie się informacją i wiedzą zachodzi w systemie kojarzącym ze sobą potrzeby i motywacje twórców (głownie merkantylne) oraz użytkowników zasobów z możliwościami stworzonymi przez technologie, w tym anonimowość, obchodzenie ograniczeń cenzuralnych oraz metody płacenia z wykorzystaniem kryptowalut. W sposób bardzo wyraźny na kształt tegoż systemu wpływa specyficzna kultura wolności bazująca na wspomnianych możliwościach technologicznych; specyficzna, często przeradzająca się bowiem w anarchizm i łamanie prawa. Istotną cechą opisywanego modelu systemu jest zmienność, efemeryczność i nietrwałość znacznej części zasobów oraz niska skuteczność narzędzi służących do wyszukiwania konkretnych treści.

Appendix 1

The Tor Project service provides, on several pages, knowledge of the following issues:

1. Community – training in Dark Web-related issues: presentations, courses, tutorials, e-books (protecting social movements); links to resources on other sites: Surveillance Self-Defense (https://eff.org) – defence against surveillance on the web; Totem (https://totem-project.org) – courses on security and privacy on the web and on methods of bypassing attempts at censorship on the Internet; Consumer Reports Security Planner (https://securityplanner.consumerreports.org) – data security, including TOR Browser as a privacy-protecting tool; Committee to Protect Journalists (https://cpj.org) – protection of journalists and their sources of information; Freedom of the Press Foundation (https://freedom.press) – protection of journalists' freedom, e.g. with the use of the TOR network; Exposing the Invisible (https://exposingtheinvisible.org) – knowledge and tools for activists who conduct investigations based on collecting information, including the use of the TOR network.
2. Support – answers to frequently asked questions: all aspects of the TOR network and TOR Browser, problems faced by operators of TOR nodes/servers, developing .onion websites.
3. Forum – for seeking professional help for those with ideas for improving the TOR Browser and TOR Project websites.
4. Manual – TOR Browser user's manual.

Appendix 2

The following services can be regarded as having the largest amount of expert materials:

1. **Reddit** (https://www.reddit.com) – a service for sharing materials found on the Internet, with subreddits:
   - Darknet – contains materials on the use of VPN, the Tails system, the TOR Browser, PGP keys, virtual wallets, trade on the Dark Web, and creating and transferring Bitcoin;
   - TOR – contains materials on the risks in using the TOR network and other applications, expanding the network of TOR servers/nodes, problems with connecting with the TOR network, versions of TOR Browser for various systems, guidance on how to set up the TOR Browser for various purposes, e.g. for bypassing geographic blockades.
2. **GitHub** (https://github.com) – hosting Internet service with groups:
   - Dark Web – information on public repositories on GitHub which contain materials on the Dark Web;
   - Tor Project – information on repositories of the TOR Project.
3. **GitLab** – TorProject (https://gitlab.torproject.org/tpo) group in the hosting service, content in subgroups:
   - Anti-censorship – bypassing censorship on the Internet, applied by totalitarian or authoritarian states;
   - BSD – installing and using the TOR Browser in BSD, i.e. Unix operating systems;
   - Communities – help for TOR-related projects, e.g. TOR training resources (how to maintain anonymity on the web, how to use Tails and Tor Browser);
   - Core – how to use various applications for the TOR network, e.g. for scanning the web;
   - .onion services – implementing and monitoring resources of the .onion pseudo-domain;
   - Organisation – everything about the TOR project (guideline materials, e.g. wiki).
4. **Slideplayer** (https://slideplayer.com) – service with presentations, selected materials:
   - TOR Project – explanation of the principles of operation, anonymity;
   - Improvement of operation of the TOR network;
   - Onion tracing;
   - Anonymous browsing of the TOR network;
   - Traffic on the TOR network;
   - Second generation of onion routing.

5. **YouTube** (https://www.youtube.com) – selected mini-lectures:
   - How does the TOR network operate, what it is;
   - How to enter the darknet through the TOR network;
   - Using TOR Browser;
   - Privacy is ensured by the TOR network;
   - Getting to know the Dark Web;
   - Buying on the Dark Web;
   - Dark Web Red Rooms, do they exist?
   - Films on the Dark Web;
   - Purchase services on the Dark Web;
   - Hackers on the Dark Web;
   - Using TOR Browser;
   - Dangers on the Dark Web.
6. Portals on Dark Web-related issues, examples:
   - DarkWebFans – https://darkwebfans.com/ – catalogue of websites and services on the Dark Web, knowledge of how this part of the Internet works;
   - DarkWeb.Link – https://darkweb.link/ – blog with knowledge of several issues related to “dark web” plus a catalogue of links to the .onion pseudo-domain;
   - Dark Web Links – https://darkweblinks.com/ – catalogue of websites in the .onion pseudo-domain plus knowledge of how the Dark Web works;
   - DarkWebLinksSites – https://darkweblinkssites.com – links to websites related to trade on the “dark web”, Bitcoin, gambling, anonymity;
   - Dark Web Magazine – https://darkwebmagazine.com/ – a service with the latest news, reviews and links from “the dark web”;
   - Dark Web Markets – https://darkwebmarket.net/ – a catalogue of links (with a closer presentation of some of them) to Internet markets on “the dark web” and to services that facilitate the use of Bitcoin and anonymous payments, knowledge of the financial side of the Dark Web operation;
   - Dark Web Official – https://darkwebofficial.com/ – reviews of websites in the .onion pseudo-domain, a list of websites used for frauds; knowledge of how the Dark Web works;
   - DarkWeb-Sites – https://darkweb-sites.org/ – blog with knowledge of several issues related to “the dark web” plus a catalogue of links to the .onion pseudo-domain resources;
   - Dark Web URLs – https://darkweburls.com/ – a catalogue of websites in the .onion pseudo-domain plus knowledge of how the Dark Web works;
   - Darkweb.wiki – https://darkweb.wiki/ – knowledge of various aspects of the Dark Web, a catalogue of websites in the .onion pseudo-domain, including those used for committing fraud;
   - GlobaLeaks – https://www.globaleaks.org/ – a platform for running on the Dark Web, used for reporting irregularities anonymously, knowledge of investigative journalism;
   - Onion Ranks – https://onionranks.com/ – a catalogue of websites in the .onion pseudo-domain;
   - The Hidden Wiki – https://thehiddenwiki.org/ – what’s new in the world of the Dark Web, a catalogue of websites in the .onion pseudo-domain.