ISSN 1734-3801 MEDIA – KULTURA – KOMUNIKACJA SPOŁECZNA Nr 20(2024)
e-ISSN 2450-081X MEDIA – CULTURE – SOCIAL COMMUNICATION 63–84
https://czasopisma.uwm.edu.pl/index.php/mkks DOI: 10.31648/mkks.9347

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

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

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

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

Wprowadzenie

Dzielenie się informacją i wiedzą jest rodzajem zachowań informacyjnych. Stanowi element systemu komunikacji międzyludzkiej, w której następuje wymiana informacji i wiedzy, a także ofert, opinii, poglądów i ocen pomiędzy jednostkami, grupami, organizacjami i innymi strukturami. Służy nie tylko porozumiewaniu się, lecz także wzbogacaniu wiedzy. Jest warunkiem powstawania, rozpowszechniania i efektywnego wykorzystania informacji i wiedzy (Świgoń, 2015). Obecnie istotnym pośrednikiem w tejże komunikacji jest technologia informacyjno-komunikacyjna, w tym Internet. Jest to system, a raczej zbiór systemów, czyli obiektów, metod, procedur i użytkowników połączonych wzajemnie w określony sposób, funkcjonujących jako całość. Dostępne na serwerach hostujących programy narzędziowe i aplikacje użytkowe oraz zasoby informacyjne to, wraz z aktywnością użytkowników, elementy internetowego systemu dzielenia się informacją i wiedzą.

Od prawie dwudziestu lat korzystamy z zasobów internetowych zwanych serwisami Web 2.0. Istotą tych rozwiązań (np. serwisy społecznościowe, serwisy wiki, serwisy social news, blogi, wideoblogi) jest stworzenie użytkownikom możliwości zapełniania własną treścią wcześniej przygotowanej struktury serwisu. Ocenia się, że serwisy Web 2.0 spowodowały zasadnicze zmiany w procesach dzielenia się informacją i wiedzą przez użytkowników Sieci. Obecnie zawartość informacyjna i struktura Sieci są w dużej mierze współtworzone przez użytkowników końcowych. Internauci stali się nie tylko odbiorcami informacji i wiedzy,

ale również jej autorami, stąd określenie „prosument" (producent + konsument). Tworzą oni społeczności wirtualne (*virtual communities*) i sieci powiązań (*networking*), w których zachodzą różnego rodzaju interakcje społeczne, w tym proces dzielenia się informacją i wiedzą. Funkcjonuje społecznościowe przetwarzanie informacji i wiedzy, czyli proces, który pozwala zbiorowo rozwiązywać problemy przekraczające możliwości jednostki (Cisek, 2009).

W literaturze naukowej wspomina się o koncepcji wiedzy kolektywnej, wiedzy opartej na współpracy (*collaborative knowledge*), która jest tworzona i udostępniana poprzez współpracę między jednostkami lub grupami. Jest to specyficzny rodzaj wiedzy, która jest wytwarzana przez ludzi pracujących razem na rzecz wspólnego celu, a przykładem mogą być działania społeczności tworzących zasoby serwisów Web 2.0, np. Wikipedii (Palermos, 2022). Uważa się, że wiedza może być budowana nie tylko w umyśle konkretnego człowieka, lecz także w umownym, zbiorowym umyśle grupy ludzi. Dowolna grupa i społeczność mogą więc posiadać wiedzę kolektywną. Posiadaczy takiej wiedzy łączy to, że funkcjonują w ramach tej samej sieci społecznej, motywuje ich uzupełnianie luk w wiedzy i chęć doskonalenia się, a także wyznają oni te same kryteria oceny jakości wiedzy oraz posiadają wspólne wartości (Fazlagić, 2008).

W obiegu naukowym funkcjonuje także pojęcie „społeczeństwo współpracy", pod którym kryją się realizowane w Sieci praktyki wirtualne (np. kultura daru, produkcja partnerska, ruch open source i open access, nauka obywatelska, haktywizm społeczny, grywalizacja, ruch prosumencki, współprodukcja mediów i innych wartości artystycznych) dostarczające znacznych ilości informacji, które można poddawać badaniom (Jemielniak i Przegalińska, 2020).

Równolegle rozwijana jest ta część Internetu, która nosi nazwę Dark Web. Termin ten określa sieci (np. TOR – The Onion Router, Freenet, I2P – Invisible Internet Project, Zeronet), w których cały ruch sieciowy jest w dużym stopniu anonimowy i kryptograficznie ukryty. Ruch sieciowy opiera się na sieci komputerów (ruterów zwanych węzłami lub serwerami pośredniczącymi) należących do ochotników i na algorytmach, które kierują komunikację internetową użytkowników przez serię komputerów innych internautów, co zasadniczo zapobiega skojarzeniu określonych działań z konkretnym użytkownikiem. Użytkownicy łączą się z serwerami pośredniczącymi poprzez wirtualne tunele zamiast bezpośredniego połączenia, co pozwala na anonimową aktywność. Zasoby Dark Web nie są indeksowane przez powszechnie wykorzystywane wyszukiwarki (np. Google i Bing), tak więc nie pojawiają się w wynikach wyszukiwania (Finklea, 2022; Hatta, 2020; Okyere-Agyei, 2022).

Oprócz tego funkcjonuje węższy znaczeniowo termin Dark Net obejmujący anonimowe węzły typu komputery, serwery, rutery połączone w techniczną sieć umożliwiającą funkcjonowanie zasobów, narzędzi i usług Dark Web (Finklea, 2022; Hatta, 2020). Zasoby internetowe, które znajdują się w Dark Web, dostępne są jedynie za pośrednictwem specjalnego oprogramowania, np. dla najpopularniejszej sieci TOR jest to Tor Browser (lub Onion Browser dla systemu iOS). Architektura sieci TOR zapewnia zarówno anonimowe udostępnianie zasobów,

jak i anonimowe ich przeglądanie. Według danych pochodzących z narzędzia analitycznego Tor Metrics (https://metrics.torproject.org/) z tej sieci korzysta codziennie od 2 do 2,5 mln użytkowników, głównie z USA, Niemiec, Indii, Indonezji, Rosji, Francji, Finlandii, Holandii, Wielkiej Brytanii i Egiptu.

Dotychczasowe badania pokazują, że aktywność użytkowników sieci TOR można podzielić na trzy główne kategorie: 1) aktywizm społeczny (np. ekologiczny), dziennikarstwo i sygnalizowanie nieprawidłowości; 2) działalność przestępcza na rynkach wirtualnych; 3) udostępnianie narzędzi do stwarzania zagrożenia bezpieczeństwa cybernetycznego, w tym botnetów oraz złośliwego oprogramowania, np. ransomware (Wang i in., 2019). Użytkownicy aktywni udostępniają głównie następujące tematyczne grupy treści: pornografia, kryptowaluta Bitcoin, narkotyki, hakerstwo, szkodliwe oprogramowanie, hazard, kwestie polityczne i religijne (Faizan i Khan, 2019).

Dominujący trend w badaniach Dark Web skupia się na tym, jak anonimowość sprzyja działalności przestępczej, oraz na technicznych aspektach funkcjonowania „ciemnych sieci" (Management Association…, 2018; Okyere-Agyei, 2022). Warto wspomnieć, że w ramach projektu Dark Web University of Arizona AI Lab zgromadzono treści internetowe generowane przez międzynarodowe grupy terrorystyczne, w tym strony internetowe, fora, czaty, blogi, serwisy społecznościowe, filmy. Opracowano różne techniki eksploracji danych, tekstu i stron internetowych ułatwiające zbadanie i zrozumienie zjawisk międzynarodowego terroryzmu poprzez podejście obliczeniowe i skoncentrowanie na danych (Chen, 2012).

Prace badawcze na temat Dark Web można podzielić m.in. ze względu na role, jakie autorzy przypisują zasobom tych sieci. Gupta, Maynard i Ahmad (2019) wyróżnili następujące role, które były badane: rynek handlu narkotykami, rynek handlu złośliwym oprogramowaniem, rynek handlu skradzionymi dokumentami i tożsamościami (karty kredytowe, dokumenty identyfikacyjne, dane personalne), rynek handlu pornografią dziecięcą, rynek handlu bronią, platformy umożliwiające anonimowe transakcje finansowe przy użyciu kryptowaluty Bitcoin, platformy do komunikacji (fora dyskusyjne, czaty), pole działań służb specjalnych zwalczających cyberprzestępczość, rynek serwerów hostujących ukryte usługi i zasoby, narzędzia do obchodzenia blokad cenzuralnych i ochrony przed prześladowaniami ze strony władz. Ustalono też, że w dotychczasowych badaniach dominują następujące problemy: rozwiązania techniczne i technologiczne (27% publikacji), analiza sieciowa Dark Web (24,5%), krajobraz cybernetycznych ataków na użytkowników (15%), nielegalny handel (12,5%), teoretyczne spojrzenie na prywatność i bezpieczeństwo „ciemnej sieci" (10%) oraz ewaluacja nielegalnych działań w Dark Web (9%). Prace, które skupiały się na analizie treści udostępnianych przez użytkowników w „ciemnych sieciach", stanowią zaś 8,5% publikacji wykrytych w trakcie tworzenia przeglądu badań Dark Web w roku 2022 (Tazi i in., 2022).

Z przeglądu literatury wynika, że nie wszystkie aspekty funkcjonowania Dark Web doczekały się kompleksowych badań. Według Wang, Mirea i Jung (2019)

nie poświęcono należytej uwagi problematyce korzystania przez użytkowników niebędących przestępcami z charakterystycznej dla Dark Web wolności słowa, zapewnionej przez anonimowość, w celu sygnalizowania różnorodnych nieprawidłowości, aktywizmu politycznego lub ekologicznego, omijania ograniczeń nakładanych na Internet przez reżimy autorytarne lub dzielenia się informacją i wiedzą z jakichkolwiek innych motywów. Konstatacja ta wydaje się nie do końca zasadna w kontekście informacji podanych w książce „Cyberpolityka. Internet jako przestrzeń aktywności politycznej" (Majorek i in., 2018). Autorzy wspomnieli o roli Dark Web w rozpowszechnianiu informacji w trakcie Arabskiej Wiosny, w szerzeniu wiedzy blokowanej przez totalitarne reżimy, w różnych akcjach sprzeciwu wobec opresyjnych władz państw niedemokratycznych oraz w ramach nieskrępowanej samoorganizacji aktywistów i rewolucjonistów. Powołali się przy tym na dwie publikacje prezentujące wyniki badań (Klimburg, 2014; Yetter, 2015).

Z ustaleń innych badaczy wiadomo, że w Dark Web zachodzą interakcje społeczne przy wykorzystaniu narzędzi znanych jeszcze z Internetu pierwszej generacji: czatów, tematycznych forów dyskusyjnych oraz e-maili. Oczywiście każde z tych narzędzi funkcjonuje w wersji właściwej dla sieci anonimowych (Xyan i in., 2020). Z kolei Pete i in. (2020) zidentyfikowali wzory interakcji i cechy społeczności uczestniczących w dyskusjach na forach w Dark Web oraz strukturę i węzły sieci uczestników dyskusji. Zaś Robert Gehl (2016) zaprezentował działania administratorów serwisu społecznościowego Dark Web Social Network zmierzające do wprowadzenia takich standardów, jak te stosowane przez Facebook i Twitter. Celem jest stworzenie bezpiecznego i moderowanego środowiska dla produktywnej wymiany informacji przez osoby ceniące sobie anonimowość. Jednakże należy podkreślić, że zdecydowana większość publikacji naukowych dotyczących funkcjonowania Dark Web (przynajmniej tych indeksowanych w bazie Scopus lub wykazywanych w wynikach wyszukiwania Google Scholar) koncentruje się na nielegalnych działaniach użytkowników, a także na kwestiach bezpieczeństwa w tejże sieci oraz aspektach etycznych i informatycznych.

Wspomniane publikacje nie prezentują zjawiska dzielenia się informacją i wiedzą w Dark Web jako kompleksowego systemu, który służy nie tylko przestępcom, lecz także uczciwym użytkownikom.

Cele, przedmiot i metodologia badań

Celem badań było opracowanie modelu systemu dzielenia się informacją i wiedzą, funkcjonującego w Dark Web w pierwszej połowie roku 2023; systemu w kształcie, w jakim jest on budowany, lecz także postrzegany przez jego uczestników – osoby dzielące się informacją i wiedzą. Zastrzeżenie dotyczące momentu istnienia opisywanego systemu wynika z faktu, że działające w Dark Web węzły stanowią własność osób prywatnych – ochotników. Nie zawsze

pozostają włączone i stosunkowo często zachodzi ich rotacja – jedne kończą swoją działalność, a inne zostają uruchamiane. Tak więc jest to system podlegający systematycznej i stosunkowo częstej ewolucji.

W kwestii zasadności badania systemu dzielenia się informacją i wiedzą w Dark Web należy podkreślić, że sieci tworzące tę część Internetu charakteryzują się daleko posuniętą anonimowością użytkowników. Mogą być wykorzystywane w celu ominięcia mechanizmów filtrowania treści, cenzury i innych ograniczeń komunikacyjnych. Powinno to przekładać się na tworzenie rozwiązań i zasobów cechujących się brakiem ograniczeń, a nawet anarchizmem, nieprzestrzeganiem prawa oraz dużo większym poziomem wolności słowa niż w powszechnie wykorzystywanym tzw. Internecie widzialnym. W związku z tym pojawia się pytanie – w jaki sposób anonimowość wpływa na zachowania informacyjne przekładające się na istnienie systemu dzielenia się informacją i wiedzą? Istotne wydaje się ustalenie nie tylko elementów i cech wspomnianego systemu, lecz także wykazanie ewentualnych różnic w sposobach dzielenia się informacją i wiedzą pomiędzy użytkownikami Internetu widzialnego i Dark Web. Należy także spróbować ustalić, czy użytkownicy badanego systemu przyjmują role prosumentów, czy tworzą społeczności wirtualne oraz czy efektem ich aktywności jest tworzenie wiedzy kolektywnej.

Przedmiotem badań uczyniono rozwiązania służące wspomaganiu procesu dzielenia się informacją i wiedzą oraz aktywne, w pierwszej połowie roku 2023, zasoby będące rezultatem tegoż dzielenia się, istniejące w jednej z sieci Dark Web – najbardziej popularnej sieci TOR. Jest to wirtualna sieć komputerowa wykorzystująca trasowanie cebulowe (technika służąca anonimizacji komunikacji w Internecie). W sieci TOR zaszyfrowane pakiety danych przesyłane są przez kilka węzłów sieciowych zwanych routerami cebulowymi, a technika szyfrowania/deszyfrowania, podobna do obierania warstw cebuli, zapewnia względną anonimowość zarówno twórcy zasobu internetowego, jak i wszystkim korzystającym z niego. Każdy węzeł pośredniczący zna bowiem jedynie lokalizację routera poprzedzającego i następnego. Zapobiega to analizie ruchu sieciowego, co stanowi podstawę anonimowości. Serwery i usługi sieci TOR dostępne są w pseudodomenie .onion, a nie w systemie DNS. Istniejące w sieci TOR usługi i zasoby nie są indeksowane przez roboty wyszukiwarek typu Google czy Bing. Konieczna jest znajomość bezpośredniego adresu w pseudodomenie .onion oraz korzystanie ze specjalistycznej przeglądarki Tor Browser. TOR umożliwia ukrycie tożsamości (lokalizacji) zarówno konsumenta treści (tj. zwykłego użytkownika), jak i jej dostarczyciela (Hatta, 2020, Okyere-Agyei, 2022).

Badania miały charakter empiryczny i polegały na pozyskiwaniu danych jakościowych bezpośrednio z przedmiotu badań. W tym celu wykorzystano dostępne w Internecie widzialnym zbiory linków do zasobów w pseudodomenie .onion, a także dwa typy narzędzi pozwalających na zidentyfikowanie zasobów w Dark Web i dotarcie do nich – wyszukiwarki działające w sieci TOR oraz dostępne w tejże sieci katalogi zasobów. W pierwszym etapie badań wykorzystano opracowane przez użytkowników sieci TOR katalogi serwisów (w „ciemnej sieci”

i Internecie widzialnym) w celu identyfikacji zasobów, których autorzy udostępniają informację i wiedzę (lub narzędzia i usługi pomocnicze) w Dark Web. W drugim etapie poszukiwano kolejnych zasobów „ciemnej sieci", korzystając z wyszukiwarek Ahmia i Torch. Stosowano terminy wyszukiwawcze powiązane ze zjawiskiem dzielenia się informacją i wiedzą, zidentyfikowane w pierwszym etapie badań. Zastosowano następujące terminy: blog, e-book, forum, library, freedom of information, freedom of speech, wiki. Badanie powtórzono kilkukrotnie. Zebrany materiał empiryczny został przeanalizowany przy wykorzystaniu metody analizy zawartości, pozwalającej na systematyczny i obiektywny opis treści. 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.

W badaniach zasobów Dark Web do pozyskiwania danych wykorzystuje się różnorodne techniki i narzędzia. Coraz popularniejsze staje się korzystanie z narzędzi informatycznych – crawlerów (roboty wyszukiwawcze) i skryptów w języku Python (np. Dark Web OSINT Tools https://github.com/apurvsinghgautam/dark-web-osint-tools), które pozwalają na automatyzację pobierania danych (Chen, 2012; Ferry i in., 2019). Jednakże autor zdecydował się na zastosowanie opisanej powyżej techniki opartej na katalogach i wyszukiwarkach, ponieważ jest ona wykorzystywana przez dominującą grupę użytkowników Dark Web, którzy nie są badaczami. Takie posunięcie wiąże się z głównym celem badań – opracowanie modelu 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, a nie przez badaczy Dark Web.

Wyniki badań

Do eksplorowania sieci TOR służy przeglądarka Tor Browser, która jest jednocześnie pierwszym elementem systemu dzielenia się informacją i wiedzą w badanej sieci, z jakim styka się użytkownik. Przycisk „New to Tor Browser" prowadzi do podstawowych wyjaśnień dotyczących zasad funkcjonowania sieci TOR i samej przeglądarki. Z kolei hiperłącze „Check our Tor Browser Manual" kieruje do bardziej rozbudowanych wyjaśnień wspomnianych zagadnień. Odsyła także do strony projektu TOR (https://www.torproject.org/). W ten sposób co prawda dociera się do elementów tzw. Internetu widzialnego, ale uzyskuje się wiedzę niezbędną do sprawnego korzystania z Dark Web (zob. zał. 1). Zasoby te stanowią przejaw dzielenia się informacją i wiedzą przez użytkowników „ciemnej sieci". Stąd też zarówno strona projektu, jak i zasoby o podobnym charakterze zaliczone zostały do badanego systemu. Opisane powyżej zasoby pozwalają na dotarcie do kolejnych serwisów Internetu widzialnego, w których użytkownicy sieci TOR dzielą się informacją i wiedzą (zob. zał. 2).

Zasadnicze elementy opisywanego systemu mieszczą się już w sieci TOR (w pseudodomenie .onion). Serwis Tor Status w styczniu 2023 roku wykazywał funkcjonowanie 6170 ruterów sieci TOR (zwanych też węzłami lub serwerami pośredniczącymi), w tym ok. 83% określanych było mianem stabilnych, 49% jako działających prawie bez przerwy, a 25% jako wyjściowe (pozwalające na komunikację z Internetem widzialnym). Zdecydowana większość ruterów opierała się na systemie Linux (ok. 5760) i FreeBSD (ok. 300). Zlokalizowane one były przede wszystkim w Niemczech (1660), Stanach Zjednoczonych (1350), Holandii (435), we Francji (325), w Serbii (180), Wielkiej Brytanii (165), Finlandii (160), Szwajcarii (160) i Kanadzie (155). Wspomniany serwis oraz inne źródła danych nie pozwalają na ustalenie, ile spośród urządzeń (komputerów) pełniących funkcję routerów posiada jednocześnie oprogramowanie pozwalające na pełnienie funkcji serwera WWW z usługami i zasobami, które można zaliczyć do systemu dzielenia się informacją i wiedzą. Skalę tego zjawiska ocenić można jedynie szacunkowo poprzez wyszukiwanie i przeglądanie serwisów w charakterystycznej dla sieci TOR pseudodomenie .onion. Tor Metrics pod koniec stycznia 2023 roku wykazywał dostępność, w zależności od dnia, od 650 tys. do 800 tys. unikalnych adresów .onion.

Do przeglądania tych zasobów służy przeglądarka Tor Browser, która oferuje kluczowe narzędzie do przeszukiwania sieci TOR, jakim jest wyszukiwarka DuckDuckGo. Potrafi ona nie tylko przeszukiwać domenę spoza systemu DNS (a taką jest .onion), ale dodatkowo nie zbiera informacji o użytkownikach. W sieci TOR wyszukiwarek jest wiele, ich przydatność w świecie adresów .onion jest bowiem zdecydowanie większa niż podobnych narzędzi w świecie domen DNS. W styczniu 2023 roku czynnych było 37 wyszukiwarek (oprócz DucDuckGo): Ahmia, Amnesia, Bobby, Deep Search, Excavator, Find Tor, GDark, GoDeep, Grams, Haystak, Hologram (grupa Amnesia), Hoodle, Kraken, MetaGer, Ondex, OnionLand Search, OnionSearch, Onion Search Engine, Onion Search Serwer, Our realm, Phobos, Search Demon, Sentor, Stealth (grupa Amnesia), Submarine, Tor66, TorBook, Torch, TorDex, Torgle, TOR Google, TorLanD, Tornet Global Search, Tor Search, Tor Search Engine, TorTorGo, Venus Search Engine. Mnogość wyszukiwarek wynika nie tylko z tego, że adresy stron w sieci TOR stanowią skomplikowany i przypadkowy ciąg znaków. Zdecydowana większość wyszukiwarek spośród powyżej wymienionych eksponuje banery reklamowe rynków i sklepów w Dark Web, za co ich właściciele niewątpliwie pobierają wynagrodzenie.

Następnym kluczowym narzędziem, bez którego system dzielenia się informacją i wiedzą w sieci TOR byłby ułomny, są katalogi stron w pseudodomenie .onion (tab. 1).

Z tabeli 1 wynika, że w Dark Web rozwija się ten element systemu informacyjnego, który w powierzchniowym Internecie w zasadzie zanika – katalogi stron. Powody są podobne jak w przypadku ilościowego rozwoju wyszukiwarek – skomplikowane adresy .onion i zarabianie na banerach reklamowych.

Tabela 1

Katalogi stron w pseudodomenie .onion

Lp.	Nazwa	Kategorie stron
1	2	3
1.	BlackButterfly666's Link Collecion	linki do stron poświęconych kryptowalutom i do giełd Bitcoin
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	katalog stron związanych z nielegalnym handlem
5.	Darknet Home	Bitcoin, Blogs, cards, Catalogs, Drugs, E-Books, E-Mail, Escrow, Forums, Gambling, Hacking, Hosting, Markets, Money, News, Other, PayPal, Search, Weapons, Wikis
6.	Darknet Hub	linki do marketów i sklepów
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
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, Catalogs 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	linki do stron na temat kryptowalut, w tym giełdy Bitcoin
16.	Hidden Revievs	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

cd. tabeli 1

1	2	3
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	linki do sklepów i rynków
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	linki do sklepów i rynków
26.	Snow Bin	zbiór linków bez podziału na kategorie
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 (nowy)	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	kilkadziesiąt stron najczęściej odwiedzanych
35.	Topic Links	linki do kilkudziesięciu kategorii stron pornograficznych

cd. tabeli 1

1	2	3
36.	Tor.Fish	katalog stron związanych z nielegalnym handlem
37.	Tor Links 2023	Bitcoin, Blogs, Cards, Catalogs, 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	katalog stron prowadzonych przez oszustów i wyłudzaczy
40.	Truly Wiki	Search Engines, Marketplaces/Shops, Gambling, Hacking, Electronics, Wiki Link List/Catalog
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

Równie intensywny rozwój przeżywają fora dyskusyjne. Wyszukiwarka Torch wiosną 2023 roku w odpowiedzi na termin „Forum" wykazała istnienie 992 witryn, a Ahmia 285 (obie wyszukiwarki wybrano ze względu na stosunkowo dużą liczbę pozycji w wynikach wyszukiwania; DuckDuckGo została pominięta ze względu na jednoczesne uwzględnianie wyników z Internetu widzialnego). Jednakże zdecydowana większość spośród nich jest jedynie kanałem kontaktu przestępców (hakerów, złodziei, handlarzy narkotykami, politycznych ekstremistów itp.) z potencjalnymi klientami. Część forów od wielu miesięcy nie wykazuje aktywności użytkowników. Liczbę wyników zawyża też fakt, iż obie wyszukiwarki wykazały jako unikalne adresy .onion klony niektórych spośród forów. Na obu listach znajduje się ponadto stosunkowo dużo (nawet powyżej 80%) adresów serwisów niebędących forami dyskusyjnymi. Skuteczniejsze w dostarczaniu informacji o forach dyskusyjnych są katalogi zasobów sieci TOR. W miarę systematyczne dzielenie się informacją i wiedzą ma miejsce na forach z poniższej listy, która jednakże nie jest pełnym zestawem istniejących forów (tab. 2).

Zdecydowana większość forów wymaga założenia konta z wykorzystaniem poczty elektronicznej działającej wewnątrz Dark Web. Istnieje co najmniej kilkanaście serwerów oferujących anonimowe skrzynki poczty elektronicznej: Anonymous Temp Email (czasowa na kilka dni), Alt Address (czasowa na trzy dni), Cook Mail, Cs.email (na krótki czas), Daniel, DNMX, Elaude, Mail2Tor, Onion Mai, ProtonMail, Riseup, SecTor.City, Sonar, TorBox, TorMail, Xmpp.is.

Tabela 2

Fora dyskusyjne w Dark Web

Lp.	Nazwa	Opis
1	2	3
1.	3h	polityczna niepoprawność plus różne tematy o Dark Web
2.	Abyss Forum	tematyka: hakerstwo, pornografia, nielegalny handel, kryptowaluty
3.	ACIEEED Forum	różne tematy, głównie hackerstwo i handel towarami nielegalnymi
4.	ASAP Forum	o pornografii dziecięcej
5.	AskRaddle	wielotematyczne: ideologie, np. anarchizm, feminizm, faszyzm; programistyczne, np. linux, meta, gry, zmiany klimatyczne, komiksy, prostytucja, media, imigracja, przekraczanie granic
6.	BreakingBad	dla handlujących i kupujących narkotyki oraz o technologiach szyfrowania, anonimowości i handlu w sieci; do tego Wiki z wiedzą na temat produkcji narkotyków
7.	Cebulka	w języku polskim, dla zainteresowanych nielegalnymi ofertami kupna/sprzedaży
8.	Cloud9 Forum	o rynkach nielegalnego handlu
9.	CryptBB	dyskusje na temat Bitcoin i o handlu tą kryptowalutą
10.	Dark Web Forums	dla zainteresowanych nielegalnym handlem w Dark Web
11.	DEF Con Forums	forum o hakerstwie plus blogosfera plus zbiór artykułów o hakerstwie i bezpieczeństwie w sieci
12.	DFAS	różne zagadnienia informatyczne
13.	DimensionX	różne tematy związane z funkcjonowaniem Dark Web
14.	Dread Network	dyskusje o różnych aspektach Dark Web
15.	Forum Bitcoin	różnorodne aspekty „kopania" kryptowalut Bitcoin i Ethereum oraz ich wykorzystania do nielegalnych płatności
16.	French Poule Web	francuskojęzyczne, tematy: pornografia, nielegalny handel, bezpieczeństwo i anonimowość i inne
17.	French World Market	francuskojęzyczne dla zainteresowanych nielegalnym handlem
18.	Hidden Answer	różne pytania do znających się na handlu, hakerstwie, anonimowości itp. plus odpowiedzi
19.	Infocon	tematy informatyczne, głównie hakerstwo
20.	Kick-ass	hakerstwo, szkodliwe oprogramowanie, wykradanie haseł i danych, handel towarami nielegalnymi
21.	Mazafka	rosyjskojęzyczne o systemach płatności opartych na kryptowalutach, o szkodliwym oprogramowaniu
22.	NZ Darknet Market Forum	różnorodne aspekty nielegalnego handlu
23.	Onion Gun Forum	rosyjskojęzyczne dla zainteresowanych bronią strzelecką
24.	PasteBox	tematyka pornograficzna
25.	Ramble	zbiór wielu forów wąsko tematycznych
26.	RuDark	wielotematyczne forum rosyjskojęzyczne

cd. tabeli 2

1	2	3
27.	Russian Anonymous Platform	wielotematyczne forum rosyjskojęzyczne
28.	Suprbay	dla zainteresowanych wymianą plików (muzyka, filmy, aplikacje, gry, fotografia, książki)
29.	The Hub	dyskusje na temat ukrytych usług sieci TOR, o rynkach nielegalnego handlu, o kryptowalutach i skutecznym dbaniu o anonimowość
30.	The Majestic Garden	o „bezpiecznych" narkotykach, o łagodzeniu skutków brania narkotyków
31.	The Stock Insider	wymiana lub handel poufnymi informacjami w spółkach giełdowych
32.	The Tor Forum	tematy związane z seksem i pornografią oraz z handlem towarami nielegalnymi
33.	VMN Almrauq Drugs Forum	o handlu narkotykami
34.	XSS Forum	rosyjskojęzyczne z poradami dla cyberprzestępców

Mniej widocznym elementem badanego systemu są blogi. W porównaniu do Internetu widzialnego (system DNS) ich oferta w Dark Web jest bardzo skromna. Co prawda wyszukiwarki Ahmia i Torch po zastosowaniu terminu wyszukiwawczego „blog" wykazały po 876 pozycji na liście wyników, jednakże wynik ten został znacznie zawyżony przez problemy opisane już przy omawianiu forów dyskusyjnych. Lista rzeczywiście istniejących i aktywnych wiosną 2023 roku blogów jest znacznie mniejsza, zwłaszcza jeżeli uwzględnimy jedynie te, których autorzy dzielą się informacją i wiedzą, ale nie prowadzą nielegalnego handlu (tab. 3).

Tabela 3

Blogi prowadzone w Dark Web

Lp.	Nazwa	Opis
1	2	3
1.	AnonBlogs	platforma do prowadzenia mikroblogów plus pewna liczba mikroblogów
2.	Blog Bitcoin	wszystko o kryptowalucie Bitcoin
3.	Blog Joseph Duffy	blog elementem serwisu www, tematyka: specjalistyczne zagadnienia programowania, open sources
4.	Blog Random musing	przemyślenia na temat różnych aspektów Internetu
5.	Blog Urof.net	blog (plus oddzielna karta: Articles) elementem serwisu www, tematyka informatyczna, głównie aktywne funkcjonowanie w Internecie
6.	Bot Mans World	blog o broni strzeleckiej, część witryny www
7.	Burny Liama's Blog	różne aspekty sieci TOR
8.	Coarse Enigma	specjalistyczne zagadnienia z informatyki, zwłaszcza dotyczące prywatności i cyberbezpieczeństwa

cd. tabeli 3

1	2	3
9.	Colin Cogle's Blog	zagadnienia z zakresu radioamatorstwa i informatyki
10.	CozyNet Blog	wideoblog z różnymi filmami animowanymi i klipami muzycznymi
11.	Endchan	platforma do prowadzenia mikroblogów plus pewna liczba mikroblogów
12.	Etam Software	różne problemy informatyczne
13.	Franco's technology blog	specjalistyczna wiedza z zakresu programowania
14.	Il blog di Leandro	różne aspekty kultury: kino, telewizja, literatura, muzyka, technologia informatyczna, hakerstwo
15.	Jake's Thoughs	oprogramowanie open source, gry komputerowe
16.	JS Blog	blog elementem serwisu www, tematyka funkcjonowania w sieci TOR
17.	Kernal	specjalistyczne zagadnienia informatyczne
18.	Mon blog Je sui Charlie	o komputerach
19.	ProPublica	dziennikarstwo śledcze, przypadki nadużyć władzy
20.	Quantum	blog inżyniera oprogramowania o różnych aspektach programów komputerowych
21.	Quantum Blog	różnorodne aspekty energetyki
22.	S-Config	dostarczanie informacji o ciekawych przykładach tworzenia dzieł kultury cyfrowej w Internecie
23.	Security in a box	blog z wiedzą na temat ochrony prywatności i bezpieczeństwa w Sieci oraz ogólnie komputerowego
24.	SerHack	blog o anonimowości, bezpieczeństwie, aplikacjach i kryptowalutach
25.	Shen's Essays	naukowo o komputerach i informatyce
26.	Tape News	o anonimowości, nielegalnym handlu, hakerstwie, kryptowalutach
27.	Tech Learning Collective	blog częścią witryny www, wiedza w zakresie bezpieczeństwa infrastruktury IT dla organizacji działających na rzecz sprawiedliwości społecznej
28.	The blog of ~vern	specjalistyczne zagadnienia informatyczne
29.	The Dark Web Journal	posty na temat kryptowalut, nowości w Dark Web, hakerstwa, bezpieczeństwa w Sieci
30.	Theyosh.nl	o programowaniu aplikacji, przede wszystkim do streamingu
31.	Vi Grey	blog programisty, część witryny www
32.	Wizardy and Steamworks	o programach komputerowych, wiedza o ich budowie i użytkowaniu

Dzielenie się informacją i wiedzą można zaobserwować także w mediach społecznościowych. W sieci TOR mają swoje odpowiedniki serwisy znane z Internetu systemu DNS: Facebook i Twitter. Funkcjonują tam także serwisy społecznościowe specyficzne dla tejże sieci: Alogs.Space, Diaspora, Flashlight 2.0, Invidious – pozwalają na dzielenie się materiałami znalezionymi w Dark Web oraz komentowanie postów; Celebrity Underground – dzielenie się zdjęciami i filmami z celebrytami w roli głównej.

Tabela 4

Społeczne archiwa i biblioteki

Lp.	Nazwa	Opis
1.	Anarch_Copy	e-booki: literatura naukowa i piękna
2.	Anarcho-Copy Amusewiki Yansısı	e-booki różnorodne tematycznie
3.	Anarşist Kütüphane	biblioteka pozycji anarchistycznych
4.	Bible4u	nieocenzurowane teksty składające się na Biblię, zasób stworzony z myślą o osobach z państw, w których Biblia jest zakazana; linki do Biblii dostępnej w innych serwisach
5.	Booksi	e-booki: literatura naukowa i piękna
6.	Comic Book Library	zbiór komiksów
7.	Dailistormer	materiały, które ze względów ideologiczno-politycznych nie przebijają się do mediów liberalno-lewicowych
8.	I'Lam Foundation	materiały radykalnych islamistów, linki do wielu podobnych
9.	Imperial Library	ok. 1,5 mln e-booków w kilkudziesięciu kategoriach, formaty epub i html
10.	Just Another Library	zbiór kursów z różnych dyscyplin naukowych, e-booków, audiobooków i zdjęć, tematyka hakerska, bezpieczeństwo w Sieci, narkotyki, okultyzm, zdrowie, elektronika i informatyka, pornografia
11.	Knowledge	wiedza o aktywnym korzystaniu z sieci TOR
12.	Library	kilkadziesiąt e-booków z różnych powodów nieobecnych w zasobach Internetu widzialnego: tematyka komputerowa, filozofia, polityka (polityczna niepoprawność), bezpieczeństwo i anonimowość, śledztwa, zdrowie
13.	Marxists Internet Archaive	zbiór dzieł klasyków marksizmu
14.	Monero	poradnik zakładania wirtualnego portfela do handlu kryptowalutami oraz na rynkach Dark Web
15.	Oil and Fish	zbiór materiałów o zasadach zachowania anonimowości w Sieci dla dysydentów religijnych i politycznych
16.	Sekretna skrzynka junty (własne tłumaczenie z j. ukraińskiego)	zbiór materiałów identyfikujących rosyjskich zbrodniarzy wojennych
17.	Sustainable www	książki, podcasty, kursy, artykuły poświęcone projektowaniu stron www
18.	The Library	kilkaset książek naukowych w formacie pdf
19.	The Library of Thoughtcrime	biblioteka ponad 100 książek i plików wideo (pdf, mp4) – rewizjonizm holokaustu, zdolności poznawcze, przestępczość (w duchu niepoprawnym politycznie)
20.	Tor Guide	poradnik budowy i funkcjonowania sieci TOR
21.	Z Library	ogromny zbiór e-booków i artykułów z wielu tematów

Odrębnym składnikiem systemu dzielenia się informacją i wiedzą są serwisy, które można nazwać społecznymi archiwami i bibliotekami (tab. 4).

Dopełnieniem badanego systemu są narzędzia wspierające dzielenie się informacją i wiedzą w sieci TOR (tab. 5).

Tabela 5

Narzędzia wspierające dzielenie się informacją i wiedzą

Lp.	Nazwa	Opis
1.	AbleOnion	komunikator
2.	Adamant	komunikator i portfel kryptowalut oparty na technologii blockchain
3.	AfriLeaks	do anonimowego udostępniania informacji dziennikarzom kilkunastu serwisów afrykańskich
4.	Bitmessage	protokół komunikacyjny P2P służący do wysyłania zaszyfrowanych wiadomości do innej osoby lub do wielu subskrybentów, chroni przed podsłuchiwaniem, zapewnia anonimowość
5.	Black Cloud	do udostępniania plików
6.	Black Hat Chat	komunikator
7.	Dark Forest	komunikator
8.	FragDenStaat	zgłaszanie łamania prawa przez władze w celu podjęcia przeciwdziałania przez odpowiednie organizacje
9.	MadIRC	komunikator
10.	Null Message	wysyłanie wiadomości ulegających samozniszczeniu po 21 dniach
11.	SecureDrop	system open source do zgłaszania nieprawidłowości, który organizacje medialne i pozarządowe mogą zainstalować, aby bezpiecznie przyjmować dokumenty z anonimowych źródeł
12.	SVR	służba wywiadowcza Rosji wdrożyła system podobny do platformy SecureDrop, aby umożliwić Rosjanom mieszkającym za granicą bezpieczne przesyłanie anonimowych informacji za pośrednictwem sieci Tor o zagrożeniach dla bezpieczeństwa narodowego Rosji
13.	Theend	komunikator
14.	The Gardian	do anonimowego udostępniania informacji dziennikarzom „The Gardian”
15.	Titan-XMPP	do anonimowej komunikacja i płatności
16.	ZeroBin.net	do tworzenia forów dyskusyjnych

Wnioski

Chcąc zaprezentować model internetowego systemu dzielenia się informacją i wiedzą, wypada rozpocząć od wyodrębnienia elementów tego systemu. Następnie należy ustalić interakcje zachodzące pomiędzy elementami systemu oraz jego interakcje z otoczeniem.

Elementy systemu dzielenia się informacją i wiedzą w sieci TOR można pogrupować w następujące kategorie:

1. Komputery z zainstalowanym odpowiednim oprogramowaniem – oprogramowanie węzła TOR (zależne od systemu operacyjnego komputera), pakiet serwera WWW dla PHP, np. XAMPP (dystrybucja Apache'a), oprogramowanie użytkowe pozwalające na uruchamianie w pseudodomenie .onion stron www, forów, blogów itp. Komputery z takim oprogramowaniem, połączone łączami telekomunikacyjnymi, tworzą sieć wewnątrz Internetu i odgrywają w niej rolę węzła wejściowego/wyjściowego z sieci TOR, węzła pośredniczącego i serwera hostującego.

2. Usługi umożliwiające poruszanie się po sieci TOR – wyszukiwarki i katalogi.

3. Zasoby informacji i wiedzy pozwalające na nabycie kompetencji w zakresie aktywnego lub biernego korzystania z sieci TOR.

4. Usługi umożliwiające kontaktowanie się użytkowników sieci – poczta e-mail, fora dyskusyjne, czaty.

5. Zasoby informacji i wiedzy o charakterze specjalistycznym.

Charakterystyka sprzętowego komponentu systemu zostanie ograniczona do już podanych informacji, niniejszy artykuł mieści się bowiem w ramach nauki o informacji, a nie informatyki.

Przejdźmy więc do drugiego elementu omawianego systemu. Do poruszania się po sieci TOR oprócz przeglądarki Tor Browser niezbędne są adresy poszczególnych witryn i usług udostępnionych przez ich twórców/właścicieli. Adresem jest ciąg znaków, wygenerowany oddzielnie dla każdej witryny i usługi w momencie konfiguracji, zakończony nazwą pseudodomeny .onion. W przeciwieństwie do adresów w Internecie systemu DNS te z końcówką .onion nie są nigdzie rejestrowane. Nie tworzy ich ciąg łatwych do odczytania znaków (np. nazwa firmy odczytywana przez serwer DNS jako adres IP), lecz kryptograficzny klucz publiczny. Chcąc dotrzeć do zasobów sieci TOR, należy użyć nie tylko specjalnej przeglądarki, lecz także w pasek adresu wpisać (wkleić) ciąg 16 znaków, które nie układają się w jakikolwiek ciąg wyrazów. W związku z tym w tejże sieci katalogi stron i wyszukiwarki pełnią dużo ważniejszą funkcję niż w Internecie systemu DNS. Niestety, specyfika sieci TOR powoduje, że przydatność wyszukiwarek i katalogów nie jest zadowalająca. Mechanizmy wyszukiwania i indeksowania kilkudziesięciu wyszukiwarek nie radzą sobie zbyt dobrze z dopasowaniem listy wyników do terminu wyszukiwawczego. W przypadku terminów zastosowanych w opisywanym badaniu jedynie kilkanaście procent adresów z listy wyników było adekwatnych do terminu wyszukiwawczego (główne problemy z listami wyników wymienione zostały w części artykułu poświęconej prezentacji wyników badań). Z kolei katalogi serwisów WWW zawierają wiele adresów nieczynnych (o co nietrudno w sieci opartej na ochotnikach) oraz błędnie przyporządkowanych do danej kategorii. W efekcie dotarcie do poszukiwanego zasobu jest trudne i czasochłonne. Można odnieść wrażenie, że liczne wyszukiwarki i katalogi powstały głównie w celu zamieszczania płatnych banerów reklamowych.

Wyżej opisane trudności oraz wyraźna odmienność zasad funkcjonowania sieci TOR w porównaniu do zasad Internetu systemu DNS powodują, że powstało wiele zasobów pozwalających nabyć kompetencje w poruszaniu się po tej sieci.

Twórcy tych zasobów wyszli z racjonalnego założenia, że poznawanie wiedzy o funkcjonowaniu sieci TOR powinno rozpocząć się jeszcze w tzw. Internecie widzialnym. Nawet Tor Browser kieruje do tego typu materiałów. W efekcie liczba specjalistycznych serwisów, szkoleń, e-booków, prezentacji i filmów, przeznaczonych zarówno dla osób chcących aktywnie rozbudowywać TOR, jak i dla użytkowników biernych, zarówno dla poczatkujących, jak i specjalistów, jest stosunkowo duża. Z kolei materiały szkoleniowe i poradniki dostępne wewnątrz sieci TOR przeznaczone są głównie dla użytkowników zaawansowanych, zainteresowanych aktywnym działaniem. Miejscem udostępniania tego typu informacji i wiedzy są przede wszystkim fora dyskusyjne i blogi. W tym elemencie systemu dzielenia się informacją i wiedzą możemy dostrzec ruch prosumencki, powstawanie społeczności wirtualnych, funkcjonowanie mechanizmu kolektywnego tworzenia wiedzy oraz istnienie wiedzy kolektywnej.

Korzystanie z większości forów wymaga założenia konta anonimowej poczty elektronicznej działającej w sieci TOR. Obecnie (wiosna 2023) funkcjonuje kilkanaście serwerów z tą usługą, w tym także oferujących skrzynkę poczty tymczasowej. Elementem systemu, który wspiera komunikację pomiędzy użytkownikami sieci i ułatwia dzielenie się informacją i wiedzą, są także aplikacje do tworzenia forów, czatów i blogów, nie tylko na własnym komputerze stanowiącym serwer, lecz także na serwerze dostawcy tego typu aplikacji występującej w roli usługi.

Oprócz wiedzy na temat różnorodnych aspektów funkcjonowania sieci TOR zasoby tejże sieci dostarczają informacji i wiedzy z następujących zagadnień:

1. Funkcjonowanie rynków i sklepów z nielegalnymi towarami (narkotyki, broń, pornografia dziecięca, skradzione dokumenty i bazy danych, podróbki znanych marek) i usługami (działania hakerskie, tworzenie ukrytych zasobów – serwisów, forów, sklepów – w Dark Web).
2. Kryptowaluty i systemy płatności w Dark Web.
3. Bezpieczeństwo i anonimowość w Dark Web.
4. Narzędzia i metody hakerstwa.
5. Specjalistyczne zagadnienia informatyczne (programowanie, administrowanie).
6. Ideologie, zwłaszcza marksizm i anarchizm, tzw. niepoprawność polityczna, antylewicowość.
7. Metody i narzędzia dla systemów anonimowego informowania oraz zgłaszania nadużyć i nieprawidłowości.
8. Wiedza o narkotykach i broni strzeleckiej.

W przypadku tego składnika badanego systemu dzielenia się informacją i wiedzą prosumenci nie odgrywają widocznej roli. Wymienione rodzaje zasobów najczęściej nie są bowiem współtworzone, lecz tworzone przez osoby będące twórcami i właścicielami poszczególnych serwisów. Społeczności wirtualne i sieci powiązań, które powstają wokół specjalistycznych serwisów, najczęściej posiadają charakter relacji sprzedawca – kupujący.

Interakcje w zakresie dzielenia się informacją i wiedzą, zachodzące pomiędzy opisanym systemem, a otoczeniem zewnętrznym, polegają głównie na dostarczaniu

wiedzy zainteresowanym Dark Web i systemem TOR, którzy nie posiadają należytego doświadczenia i odpowiednich kompetencji, by funkcjonować w tej części Internetu.

Interakcje zachodzące wewnątrz tego systemu najczęściej polegają na dostarczaniu informacji i wiedzy niejako „przy okazji" z kilku powodów. Przede wszystkim działania takie podejmują oferenci nielegalnych towarów i usług – właściciele serwisów, blogów i forów, których głównym celem jest promocja własnej oferty. Drugi powód sprowadza się do chęci zarobienia na promowaniu wspomnianych oferentów, dzięki rozwiązaniom ułatwiającym innym użytkownikom sieci TOR poruszanie się po zasobach – katalogom i wyszukiwarkom z dołączonymi banerami reklamowymi.

Jednakże nie tylko motywacje merkantylne generują interakcje w omawianym systemie dzielenia się informacją i wiedzą. Wyraźnie dostrzegalną grupą są użytkownicy kierujący się ideą wolności słowa i anonimowości w Internecie. Ta grupa udostępnia zasoby e-booków i artykułów, często z pogwałceniem praw autorskich. Część takich inicjatyw ma na celu obchodzenie ograniczeń cenzuralnych obowiązujących w niektórych państwach lub zapewnienie możliwości anonimowego rozpowszechniania informacji i zgłaszania nadużyć. Kolejna grupa, która dzieli się informacją i wiedzą bez jednoczesnego podejmowania działań zarobkowych, to społeczność aktywnych użytkowników o wysokich kompetencjach informatycznych, pasjonatów rozwiązań tworzących sieć TOR, a także zapewniających anonimowość i bezpieczeństwo.

W sieci TOR dzielenie się informacją i wiedzą zachodzi w systemie kojarzącym ze sobą potrzeby i motywacje twórców oraz użytkowników zasobów z możliwościami stworzonymi przez technologie, w tym anonimowość, obchodzenie ograniczeń cenzuralnych oraz metody płacenia z wykorzystaniem kryptowalut. W sposób bardzo widoczny na kształt tegoż systemu wpływa specyficzna kultura wolności bazująca na wspomnianych możliwościach technologicznych. Specyficzna, często bowiem przeradzająca się 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.

Bibliografia

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). Dostęp: 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.

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.

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

S u m m a r y

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.

Załącznik 1

Serwis Tor Project na kilku stronach dostarcza wiedzy o następujących zagadnieniach:

1. Community – szkolenia w problematyce Dark Web: prezentacje, kursy, tutoriale, e-booki (ochrona ruchów społecznych); linki do zasobów na innych stronach: Surveillance Self-Defense (https://eff.org) – obrona przed inwigilacją w sieci; Totem (https://totem-project.org) – kursy na temat bezpieczeństwa i prywatności w sieci oraz o metodach omijania prób cenzury Internetu; Consumer Reports Security Planner (https://securityplanner.consumerreports.org) – bezpieczeństwo danych, w tym TOR Browser jako narzędzie do ochrony prywatności; Committee to Protect Journalists (https://cpj.org) – ochrona dziennikarzy i ich źródeł informacji; Freedom of the Press Foundation (https://freedom.press) – ochrona wolności dziennikarzy, m.in. z wykorzystaniem sieci TOR; Exposing the Invisible (https://exposingtheinvisible.org) – wiedza i narzędzia dla aktywistów prowadzących śledztwa oparte na zbieraniu informacji, w tym wykorzystanie sieci TOR.
2. Support – odpowiedzi na najczęściej zadawane pytania: wszelkie aspekty sieci TOR i przeglądarki TOR Browser, problemy operatorów węzłów/serwerów TOR, tworzenie stron .onion.
3. Forum – dla szukających fachowej pomocy, dla mających pomysły na ulepszenie TOR Browser oraz stron Projektu TOR.
4. Manual – instrukcja obsługi przeglądarki TOR Browser.

Załącznik 2

Do najbardziej zasobnych w materiały eksperckie można zaliczyć następujące serwisy:

1. **Reddit** (https://www.reddit.com) – serwis dzielenia się materiałami znalezionymi w Internecie, a w nim subreddity:
   - Darknet – zawiera materiały na temat: korzystania z VPN, z systemu Tails, przeglądarki TOR Browser, kluczy PGP, wirtualnych portfeli, handlu w Dark Web, kreowania i transferowania Bitcoin;
   - TOR – zawiera materiały na temat: zagrożeń przy korzystaniu z JavaScript, bezpieczeństwa korzystania z sieci TOR i różnych aplikacji, rozbudowy sieci serwerów/węzłów TOR, problemów z łączeniem się z siecią TOR, wersji TOR Browser dla różnych systemów, porady, jak wykorzystywać ustawienia TOR Browser do różnych celów, np. do likwidacji blokad geograficznych.
2. **GitHub** (https://github.com) – hostingowy serwis internetowy z grupami:
   - Dark Web – informacje o repozytoriach publicznych na GitHub zawierających materiały o Dark Web;
   - Tor Project – informacje o repozytoriach projektu TOR.
3. **GitLab** – grupa TorProject (https://gitlab.torproject.org/tpo) w hostingowym serwisie internetowym, merytoryczne treści w podgrupach:
   - Antycenzura – obchodzenie metod cenzury w Internecie stosowanych przez państwa totalitarne lub autorytarne;
   - BSD – instalowanie i używanie TOR Browser w BSD, czyli systemach operacyjnych z rodziny Unix;
   - Społeczności – pomoc dla projektów związanych z siecią TOR, np. zasoby szkoleniowe TOR (jak zachować anonimowość w Sieci, jak korzystać z Tails i Tor Browser);
   - Core (rdzeń) – jak korzystać z różnych aplikacji dla sieci TOR, np. do skanowania sieci;
   - Usługi. onion – wdrażanie i monitorowanie zasobów pseudodomeny. onion;
   - Organizacja – wszystko o projekcie TOR (materiały poradnikowe typu wiki).
4. **Slideplayer** (https://slideplayer.com) – serwis z prezentacjami, wybrane materiały:
   - Projekt TOR – wyjaśnienie zasad działania, anonimowość;
   - Ulepszanie funkcjonowania TOR;
   - Trasowanie cebulowe;
   - Anonimowe przeglądanie sieci TOR;
   - Ruch w sieci TOR;
   - Druga generacja onion routingu.

5. **YouTube** (https://www.youtube.com) – wybrane miniwykłady:
   - Jak działa sieć TOR, czym jest;
   - Jak dostać się do darknetu za pomocą sieci TOR;
   - Posługiwanie się TOR Browser;
   - Prywatność zapewniana przez sieć TOR;
   - Poznawanie Dark Web;
   - Kupowanie w Dark Web;
   - Dark Web Red Room, czy istnieją?
   - Filmy w Dark Web;
   - Serwisy zakupowe w Dark Web;
   - Hakerzy w Dark Web;
   - Posługiwanie się TOR Browser;
   - Niebezpieczeństwa w Dark Web.
6. Portale o tematyce (głównej) Dark Web, przykłady:
   - DarkWebFans – https://darkwebfans.com/ – katalog stron i usług w Dark Web, wiedza o funkcjonowaniu w tej części Internetu;
   - DarkWeb.Link – https://darkweb.link/ – blog z wiedzą na temat kilku zagadnień związanych z „ciemną siecią" plus katalog linków do zasobów pseudodomeny .onion;
   - Dark Web Links – https://darkweblinks.com/ – katalog stron w pseudodomenie .onion plus wiedza o funkcjonowaniu Dark Web;
   - DarkWebLinksSites – https://darkweblinkssites.com – linki do stron typu handel w „ciemnej sieci", Bitcoin, hazard, anonimowość;
   - Dark Web Magazine – https://darkwebmagazine.com/ – serwis dostarczający aktualnych wiadomości, recenzji i linków z „ciemnej sieci";
   - Dark Web Markets – https://darkwebmarket.net/ – katalog linków (wraz z omówieniami części z nich) do internetowych marketów w „ciemnej sieci" oraz do serwisów ułatwiających posługiwanie się Bitcoin i anonimowe płatności, wiedza o finansowej stronie funkcjonowania Dark Web;
   - Dark Web Official – https://darkwebofficial.com/ – recenzje stron w pseudodomenie .onion, lista stron wykorzystywanych do popełniania oszustw; wiedza o funkcjonowaniu Dark Web;
   - DarkWeb-Sites – https://darkweb-sites.org/ – blog z wiedzą na temat różnych zagadnień związanych z „ciemną siecią" plus katalog linków do zasobów pseudodomeny .onion;
   - Dark Web URLs – https://darkweburls.com/ – katalog stron w pseudodomenie .onion plus wiedza o funkcjonowaniu Dark Web;
   - Darkweb.wiki – https://darkweb.wiki/ – wiedza o różnych aspektach Dark Web, katalog stron w pseudodomenie .onion, w tym stron służących ich autorom do popełniania oszustw;
   - GlobaLeaks – https://www.globaleaks.org/ – platforma do uruchomienia w Dark Web, która służy anonimowemu zgłaszaniu nieprawidłowości, wiedza na temat dziennikarstwa śledczego;
   - Onion Ranks – https://onionranks.com/ – katalog stron w pseudodomenie .onion;
   - The Hidden Wiki – https://thehiddenwiki.org/ – nowości w świecie Dark Web, katalog stron w pseudodomenie .onion.