DOI: 10.31648/kpp.8490

Łukasz Lenartowicz
Uniwersytet Warmińsko-Mazurski w Olsztynie
ORCID: 0000-0002-2185-238X
lukasz.lenartowicz@student.uwm.edu.pl

Rafał Pietraszuk
Uniwersytet Warmińsko-Mazurski w Olsztynie
ORCID: 0000-0001-9797-8782
rafal.pietraszuk@student.uwm.edu.pl

Darknet – nie tylko *The Onion Router*

Wstęp

Korzystanie z Darknetu przypomina zakupy online. Na szczególną uwagę zasługuje jednak proponowany tam asortyment. Darknet kusi zakupem m.in. kokainy, heroiny czy innych nielegalnych substancji. Daje możliwość wynajęcia płatnego mordercy. Nierzadko kilka kliknięć dzieli „konsumenta" od wynajęcia grupy wyspecjalizowanych komandosów, która zajmie się „niewygodnym" sąsiadem, mężem lub żoną.

Darknet to z technicznego punktu widzenia przede wszystkim anonimowa infrastruktura Internetu. Chcąc uzyskać dostęp do ciemnej warstwy sieci, bardzo ważne jest, aby pozostać anonimowym. Istnieje wiele protokołów i narzędzi, które zostały wykorzystane do jej opracowania. Podstawowe znaczenie mają tutaj dedykowane prywatności przeglądarki, techniki szyfrowania danych, Wirtualne Sieci Prywatne do przesyłania danych oraz algorytm routingu[1]. Te podstawowe narzędzia są niezbędne w celu uzyskania dostępu do ciemnej strony Internetu.

[1] E. Çalışkan, T. Minárik, A.M. Osula, *Technical and Legal Overview of the TOR Anonymity Network*, https://ccdcoe.org/library/publications/technical-and-legal-overview-of-the-TOR-anonymity-network/ (dostęp: 24.04.2022).

Darknet najczęściej jest kojarzony z *The Onion Router* (dalej: TOR). Celem artykułu nie jest jednak TOR jako taki, lecz przede wszystkim skupienie się na ukazaniu specyfiki funkcjonowania innych sieci (przeglądarek, aplikacji), które gwarantują zasadniczo anonimowy i niemożliwy do wyśledzenia dostęp, takich jak: I2P i Freenet[2]. Wspomniane sieci występują w roli nie tylko swoistego pomostu między ciemną stroną Internetu; posiadają ponadto zwiększoną funkcjonalność, co uwydatnia ich ewolucyjny charakter. W niniejszym opracowaniu wskazano możliwości uzyskania dostępu do zaciemnionej sfery sieci z uwzględnieniem podstaw technicznych takiego dostępu i ich charakterystyki. Rozważania dotyczące funkcjonowania sieci TOR, I2P oraz Freenet zostaną poprzedzone wyjaśnieniem, czym jest Darknet, jakie jest jego zasadnicze przeznaczenie (nie wszyscy bowiem korzystają z Darknetu w sposób sprzeczny z prawem), wraz ze wskazaniem jego miejsca w ogólnej strukturze Internetu. Problematyka ta zyskuje w ostatnim czasie na znaczeniu, co nie powinno dziwić, biorąc pod uwagę stale postępującą cyfryzację niemal każdej dziedziny życia nie tylko prywatnego, lecz także publicznego. Opisywane w ramach niniejszego artykułu techniki dostępu do Darknetu coraz częściej przewijają się również w pracy wymiaru sprawiedliwości, jak również prawników zatrudnionych w prywatnych kancelariach prawnych. Znajomość omawianej tematyki wśród prawników wydaje się zatem konieczna z uwagi na jej stale zwiększający się wpływ na tworzenie i stosowanie prawa.

Pojęcie Darknetu

Terminu „Darknet" używa się dla skategoryzowania sieci, które są anonimowe i zabezpieczone przed dostępem osób postronnych[3]. Utożsamiane są one z prowadzeniem działań, w tym transakcji o charakterze nielegalnym. Większość dostępnych w clearnecie (czyli „normalnym" Internecie) źródeł przedstawia Darknet jako miejsce na pograniczu „nieba i piekła – z jednej strony pełne cudów, z drugiej – niewyobrażalnej grozy"[4]. Samo pojęcie zostało użyte po raz pierwszy w artykule *The Darknet and the Future of Content Protection*, w którym autorzy zdefiniowali Darknet jako zbiór sieci i technologii służących do udostępniania treści cyfrowych[5].

Inna nazwą, która czasami jest błędnie używana jako synonim powyższego pojęcia, jest deepweb. Darknet to sieć komputerów, których zwykle nie można zobaczyć, a deepweb to system pozwalający na interakcję z nimi. Do cech charakterystycznych obu tych sieci można zaliczyć decentralizację polegającą na zabezpieczeniu przed

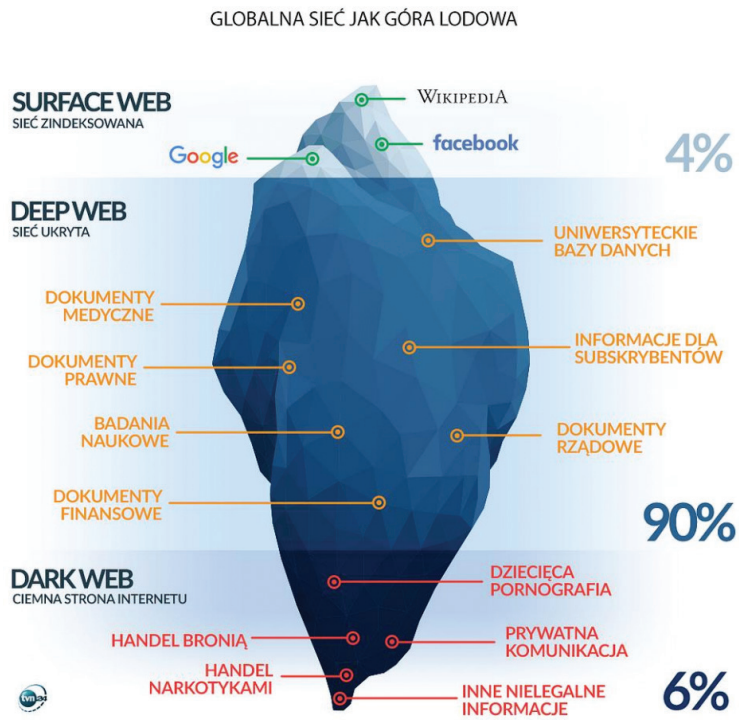
[2] W doktrynie jest mowa również o tzw. nieuczciwych domenach TLD – nie będą one jednak przedmiotem niniejszego artykułu z uwagi na ograniczenia edyTORskie. Zagadnienie to omawiają: V. Ciancaglini, M. Balduzzi, M. Goncharov, R. McArdle, *Deepweb and Cybercrime It's Not All About TOR*, s. 7 i nast., https://documents.trendmicro.com/assets/wp/wp-deepweb-and-cybercrime.pdf (dostęp: 24.04.2022).

[3] J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 137.

[4] P.H. Meland, Y.F.F. Bayoumy, G. Sindre, *The Ransomware-as-a-Service economy within the darknet*, „Computers & Security" 2020, vol. 92, s. 1.

[5] P. Biddle, P. England, M. Peinado, B. Willman, *The Darknet and the Future of Content Protection*, [w:] J. Feigenbaum (red.), *Digital Rights Management. DRM 2002. Lecture Notes in Computer Science*, vol. 2696, Berlin–Heidelberg 2003, https://doi.org/10.1007/978-3-540-44993-5_10 (dostęp: 3.12.2022).

inwigilacją i celowym bądź przypadkowym zastojem. Znaczącą wadą Darknetu jest kłopotliwy sposób docierania do potrzebnych informacji i brak skutecznych narzędzi służących ich wyszukiwaniu. Darknet przez wielu nazywany jest mrocznym Internetem bądź jego ciemną stroną. Popularne wyszukiwarki internetowe nie znajdują jego witryn (brak indeksacji), zaś serwis YouTube nie odtworzy zamieszczonych w nim nagrań[6].



Obraz 1. Warstwy Internetu

Źródło: T. Leżoń, *Głęboko pod powierzchnią jest miejsce, o którym wolałbyś nie wiedzieć*, https://tvn24.pl/magazyn-tvn24/gleboko-pod-powierzchnia-jest-miejsce-o-kTORym-wolalbys-nie-wiedziec,95,1850 (dostęp: 18.04.2022).

Globalna sieć składa się z trzech warstw: Surface Web, Deep Web i Dark Web. Sieć powierzchniowa, zwana również jako sieć widoczna lub indeksowana, jest łatwo dostępna za pośrednictwem standardowych wyszukiwarek internetowych[7]. Z kolei Deep Web nie jest dostępna dla ogółu społeczeństwa, z tego powodu w piśmiennictwie

[6] M. Majorek, *Darknet. Ostatni bastion wolności w internecie?* „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 4, s. 86.

[7] K. Shubhdeep, R. Sukhchandan, *Dark Web: A Web of Crimes*, „Wireless Personal Communications" 2020, nr 112(1), s. 2132.

określa się ją siecią niewidzialną lub ukrytą[8]. Deep Web zawiera głównie łagodne witryny, takie jak konto e-mail chronione hasłem, niektóre części płatnych usług subskrypcji, np. Netflix, oraz witryny, do których można uzyskać dostęp tylko za pośrednictwem formularza online. Cechą szczególną jest rozmiar tej warstwy Internetu – w 2001 r. szacowano, że jest 400–550 razy większa niż Surface Web i od tego czasu rośnie wykładniczo[9].

Darknet składa się z wielu rozproszonych węzłów, tzw. cebul, działających lokalnie, niewidocznych i niedostępnych z poziomu Internetu[10]. Dostać się do nich można jedynie w ramach sieci stworzonej przez dostawcę oprogramowania. Dzięki trasowaniu cebulowemu gospodarz i użytkownik spotykają się, ale żaden nie będzie wiedział, gdzie naprawdę znajduje się ten drugi. Nikt – łącznie z instytucjami zapewniającymi dostęp do witryn – nie posiada informacji o tym, kto nimi kieruje ani gdzie ma swoją siedzibę. Co więcej, nikt też nie może zamknąć witryn. Nacisk kładziony jest na prywatność oraz anonimowość, których osiągnięcie jest możliwe dzięki zastosowaniu zaawansowanej kryptografii[11].

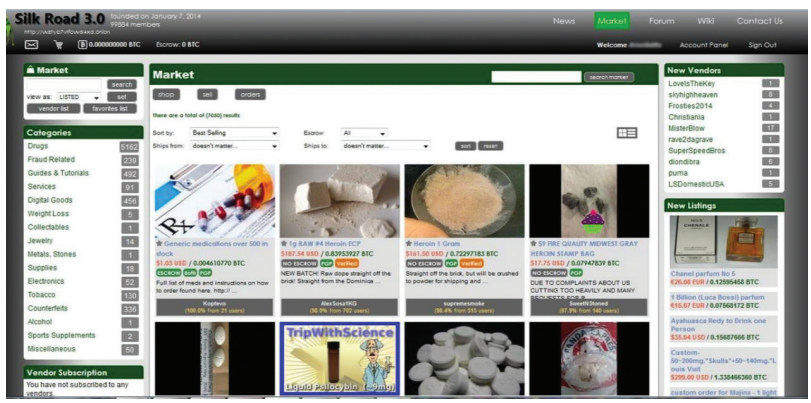
Dokonując przeglądu piśmiennictwa, można odnieść wrażenie, że Darknet to przede wszystkim miejsce, w którym dokonywane są czarnorynkowe transakcje. Istotnie, można tam napotkać witryny oferujące sprzedaż narządów, inne z kolei oferują dostęp do prawdziwych walk gladiatorskich, które kończą się śmiercią jednego z zapaśników, a jeszcze inne usługi morderstwa na zlecenie albo za odpowiednią opłatą dają możliwość oglądania tortur; część witryn reklamuje się jako dostawcy egzotycznych zwierząt. W literaturze wskazuje się, że dużym popytem cieszą się typowe produkty czarnorynkowe, takie jak broń, narkotyki, fałszywe dokumenty tożsamości. Zlecić też można kradzież na zlecenie, kupić gotową pracę naukową, a nawet zyskać możliwość zarobienia na ustawionych imprezach sportowych. Wachlarz produktów obejmuje również złoto, diamenty, konta na Netflixie, a także dziecięcą pornografię. W Darknecie można zlecić atak hakerski, a handel żywym towarem kwitnie tam od lat. Można także wykupić zabójstwo regularne, upozorowane na zaginięcie, śmierć w wypadku. W wyjątkowych okolicznościach przewidziano też ofertę obejmującą okaleczanie (regularne bądź z oszpeceniem twarzy), łamanie rąk, doprowadzenie do paraliżu wybranej części ciała oraz gwałty (najwyżej wyceniono gwałt na dzieciach polityków i innych osób publicznych)[12]. Usługodawcy wyceniają też zamachy bombowe i pobicia (w pakietach: od pojedynczej osoby po całą rodzinę). Oferowanie takiej palety produktów wiąże się z naruszeniem przepisów prawa, a zwłaszcza prawa karnego. Tytułem przykładu można

[8] Ibidem.
[9] C. Grannan, *What's the Difference Between the Deep Web and the Dark Web?*, https://www.britannica.com/sTORy/whats-the-difference-between-the-deep-web-and-the-dark-web (dostęp: 24.04.2022).
[10] E. Ormsby, *Darknet*, Kraków 2019, s. 20.
[11] M. Majorek, op. cit., s. 87.
[12] Ibidem.

wskazać na art. 148, 156, 157 197 i 263 Kodeksu karnego[13], jak również art. 59 ustawy o przeciwdziałaniu narkomani[14], penalizujący czyn polegający na udzieleniu innej osobie środka odurzającego celem osiągnięcia korzyści majątkowej lub osobistej.

W zależności od platformy, ceny za nielegalne towary lub usługi podawane są w dolarach amerykańskich lub euro. Anonimowe rynki wymagają anonimowych transakcji finansowych, dlatego powszechne są tam płatności, które nie angażują systemu bankowego. Przelew bankowy lub użycie karty płatniczej dają bowiem możliwość odtworzenia wędrówki pieniądza. Szczególnie pomocnym rozwiązaniem w dziedzinie płatności za nielegalny asortyment okazał się bitcoin. Jest to system płatności internetowych oparty na podstawach matematycznych, a zarazem wirtualna waluta, która przejęła funkcję gotówki w wirtualnym świecie[15]. Obecnie bitcoin jest wirtualną walutą najczęściej używaną w Internecie do prania pieniędzy[16].

Pierwszym nielegalnym sklepem internetowym w Darknecie był rynek internetowy Silk Road (Jedwabny Szlak), dostępny wyłącznie za pomocą przeglądarki internetowej TOR. Założony w roku 2011 Silk Road stał się synonimem dla wszystkich nielegalnych rynków internetowych znajdujących się w Darknecie. Liczba użytkowników z każdym dniem rosła wraz z oferowanymi towarami i usługami. Do publicznej świadomości Silk Road trafił za sprawą polityków, którzy postanowili wykorzystać walkę z internetowym handlem narkotykami w swoich kampaniach wyborczych.



Obraz 2. Przykładowa strona Silk Road

Źródło: P. Wierzbicki, *Gwałt na córce polityka? 36 000 dolarów. Przed wami najgorsze oblicze darknetu*, https://techsetter.pl/najgorsze-oblicze-darknetu/ (dostęp: 18.04.2022).

[13] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2022 r., poz. 1138 z późn. zm.).

[14] Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (t.j. Dz.U. z 2020 r., poz. 2050 z późn. zm.).

[15] G. Sobiecki, *Regulowanie kryptowalut w Polsce i na świecie na przykładzie Bitcoina: status prawny i interpretacja ekonomiczna*, „Problemy Zarządzania" t. 1, z. 3, s. 145 i nast.

[16] P. Opitek, *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo" 2017, nr 6, s. 40.

Przez dwa lata czarny rynek rozwijał się na platformie, aż do 2013 r., kiedy FBI udało się zatrzymać założyciela strony, 29-letniego Rossa Williama Ulbrichta. Admin wpadł nie przez niedoskonałość narzędzi, z których korzystał, ale przez błąd w konfiguracji serwera, co pozwoliło namierzyć tropiącym go agentom jego fizyczną lokalizację – serwerownię ulokowaną na Islandii[17]. Ross Ulbricht został skazany w 2015 r. Co prawda zarzuty obejmowały m.in. handel narkotykami, pranie pieniędzy, ale te najpoważniejsze dotyczyły prowadzenia organizacji o charakterze przestępczym, na co składało się m.in. organizowanie płatnych zabójstw. Ross Ulbricht trafił za kraty z karą podwójnego dożywocia, co w amerykańskiej praktyce karnej oznacza brak możliwości przedterminowego zwolnienia[18].

Z jednej strony zamknięcie rynku internetowego Silk Road przez FBI było wielkim sukcesem, z drugiej jednak strony dotychczasowy obrót dokonywany w ramach Silk Road został przeniesiony na inne tego typu platformy. Ponadto niemal miesiąc po zamknięciu strony Silk Road powstała platforma Silk Road 2.0. Następca najbardziej popularnego czarnego rynku w Darknecie przetrwał zaledwie rok, gdyż w ramach globalnej operacji „Onymous", przeprowadzonej w 2014 r. przez FBI, Interpol i inne służby, zatrzymano operatora, a wraz z tym zamknięto również portal i wiele innymi portalami handlowymi[19].

TOR

Do Darknetu można uzyskać dostęp przy pomocy narzędzi TOR[20], Freenet[21] czy też I2P[22]. Te skomplikowane pod względem zastosowanej technologii mechanizmy szyfrowania, mające na celu ukrycie tożsamości posługujących się nimi osób, nie są jednak trudne w obsłudze, gdyż ich konfiguracja jest stosunkowo łatwa, a interfejs przypomina ten, który jest wykorzystywany przez tradycyjne przeglądarki internetowe. Jednocześnie wykorzystywane techniki kryptograficzne stwarzają szereg wyzwań dla organów w zakresie identyfikacji i lokalizacji przestępców[23]. Ponieważ TOR zapewnia prawie nieograniczoną anonimowość swoim użytkownikom, skutkuje to tym, że zasadniczo wszystkie kroki uczynione pod „przykryciem" tej przeglądarki są nie do odtworzenia. Jak zauważa Marta Majorek, duże agencje rządowe są w stanie śledzić niektóre osoby funkcjonujące w teoretycznie anonimowej przestrzeni. Jednak nastręcza to służbom szeregu trudności, wymaga zaangażowania ogromnej ilości zasobów i nie zawsze okazuje się skuteczne[24].

---

[17] P. Wierzbicki, op. cit.

[18] United States of America v. Ross William Ulbricht, No. 15-1815-cr (2d Cir. May 31, 2017), https://sherloc.unodc.org/cld/en/case-law-doc/cybercrimecrimetype/usa/2017/united_states_of_america_v._ross_william_ulbricht_no._15-1815-cr_2d_cir._may_31_2017.html (dostęp: 3.12.2022).

[19] *Operation Onymous: International law enforcement agencies target the Dark Net in November 2014*, https://www.swansea.ac.uk/media/Operation-Onymous.pdf (dostęp: 3.12.2022).

[20] https://www.TORproject.org/.

[21] https://freenetproject.org/.

[22] https://geti2p.net/pl/.

[23] J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Warszawa 2020, s. 179.

[24] M. Majorek, op. cit., s. 87.

Symbolem tej sieci jest cebula, ponieważ sieć korzysta z trasowania cebulowego drugiej generacji, które polega na wysyłaniu wiadomości poprzez zaszyfrowane warstwy[25]. Obecnie sieć TOR uważana jest za sieć najbardziej bezpieczną, jeżeli chodzi o anonimowość[26]. Prywatność w sieci wynikająca z anonimowości sprawia, że sieć ta wykorzystywana jest do nielegalnych działań, w tym do popełniania cyberprzestępstw.

Choć genezy TOR można upatrywać już we wczesnych latach 90. XX w., to ważny epizod związany z rozwojem sieci przypada na rok 1997, bowiem wtedy prace nad siecią TOR finansowane były przez Marynarkę Wojenną Stanów Zjednoczonych, głównie przez Agencję Zaawansowanych Obronnych Projektów Badawczych (DARPA). Agencja ta zajmowała się także rozwojem Internetu w początkowych jego fazach i z tego względu posiada ona duży wkład w rozwój sieci na całym świecie. Badacze zwrócili uwagę, że korzystanie z popularnych sieci nie zapewnia dostatecznej prywatności dla użytkowników, bowiem sieci te nie zapewniają niezbędnej anonimowości, a co za tym idzie – w łatwy sposób osoby wykwalifikowane mogą prześledzić działania w sieci każdego człowieka. Zauważyli oni potrzebę stworzenia takiej sieci, która zapewni większą anonimowość swoim użytkownikom, lecz przede wszystkim dzięki której agenci rządowi mogliby np. przeglądać zasoby Internetu całkowicie anonimowo[27]. Hasłami, które przyświecały twórcom sieci TOR, była anonimowość oraz obrona praw demokratycznych, takich jak wolność słowa oraz dostęp do informacji.

Ściągniecie oprogramowania, dzięki któremu możemy używać TOR, jest całkowicie darmowe, a sam proces nie jest czasochłonny. Sieć nie zapisuje historii przeglądania ani danych logowania używanych przez użytkowników. Interfejs TOR jest bardzo zbliżony do tego występującego w przeglądarce Firefox. Anonimowość sieci TOR sprawia, że może być ona używana z pobudek zasługujących na aprobatę, jak również na potępienie pod groźbą poniesienia odpowiedzialności karnej. TOR umożliwia skorzystanie z platform, które w normalnej sieci są zablokowane przez cenzurę albo po prostu są nielegalne i prowadzą swoją działalność tylko w Darknecie. Platformy, takie jak Black Market Reloaded, Sheep Marketplace, czy Atlantis, oferują dostęp chociażby do pornografii dziecięcej, brutalnych zdjęć z morderstw czy wypadków. Za pośrednictwem tych witryn można całkowicie anonimowo kupić produkty, które w wielu krajach są wyłączone z obrotu handlowego: broń, narkotyki, nową tożsamość, sfałszowane dokumenty oraz dzieła sztuki.

Jeżeli chodzi o użytkowanie sieci TOR w Polsce, to w sieci działa 25 stron, głównie forum Polish Board and Market. Użytkownicy na tym forum dzielą się rożnymi kwestiami typu, jak pozbyć się zwłok, gdzie można kupić narkotyki czy broń. W 2009 r.

---

[25] Więcej o tym, jak działa trasowanie cebulowe: T. Szydłowski, *TOR – wszystko, co trzeba wiedzieć o sieci cebulowej*, https://www.komputerswiat.pl/artykuly/redakcyjne/TOR-wszystko-co-trzeba-wiedziec-o-sieci-cebulowej/lp69phy (dostęp: 18.04.2022).

[26] C. Zielińska, *„Cybercrime" – wyzwanie dla kryminologii*, [w:] D. Dajnowicz-Piesiecka, E. Jurgielewicz-Delegacz, E.W. Pływaczewski (red.), *Przestępczość XXI wieku. Szanse i wyzwania dla kryminologii*, Warszawa 2020, s. 541.

[27] R.A. Haraty, B. Zantout, *The TOR dota communication system: A survey*, „Journal of Cummunications and Networks" 2014, t. 16, nr 4, s. 415.

poseł Krzysztof Brejza wniósł do Ministerstwa Spraw Wewnętrznych i Administracji interpelacje na temat bezkarności rozpowszechniania dziecięcej pornografii, w której postulował zdelegalizowanie sieci TOR. W ramach odwetu internauci włamali się na jego stronę internetową i napisali post, w którym przyznawał się do bycia pedofilem oraz wychwalał sieć TOR, pisząc: „Chciałem polecić wszystkim doskonałe i działające strony z pornografią dziecięcą. Strony są na TOR, więc są bezpieczne”[28]. Ze względu na anonimowość nie można było stwierdzić, kto napisał ten post i inne komentarze, więc sprawców nie ujęto.

W literaturze wskazuje się na pewne pozytywne zastosowania sieci TOR. Jak zauważa Filip Rodniewicz, „(...) służyć on ma z założenia obronie przed wszelkimi formami sieciowej inwigilacji, będącej zagrożeniem dla wolności, prywatności czy swobody prowadzenia działalności gospodarczej. Wskazują oni na pozytywne aspekty wykorzystania TOR w krajach niedemokratycznych (zwłaszcza w Chinach i w Iranie), gdzie umożliwia on opozycji i dziennikarzom swobodną wymianę informacji przez Internet”[29]. Ciekawym przykładem jest Mauretańczyk Nasser Weddady, który za pośrednictwem sieci TOR rozpoczął walkę z praktykowanym w Mauretanii niewolnictwem[30]. Wskazuje się, że z sieci tej korzystali także aktywiści, którzy organizowali demonstracje w ramach Arabskiej Wiosny w 2010 r., a także w trakcie innych akcji mających na celu wzmocnienie ruchów wolnościowych i prodemokratycznych, sprzeciwiających się opresyjnym władzom[31].

Nieznajomość przedstawionego zagadnienia skutkuje tym, że wiele osób traktuje sieć TOR jako naturalne siedlisko przestępstw, jednak trzeba pamiętać, iż z sieci TOR korzystają również osoby, które po prostu chcą być anonimowe, cenią sobie swoją prywatność. Osoby, które korzystają z sieci w celach popełniania czynów przestępczych stanowią mniejszość. W wyniku działań niewielkiego odsetka użytkowników sieć TOR ma bardzo negatywną renomę na świecie, a w Polsce osoby z niej korzystające uznawane są za potencjalnych przestępców[32].

Freenet

Równie popularnym narzędziem wykorzystywanym w celu nawiązywania łączności z Darknetem jest przeglądarka Freenet, która stanowi przykład anonimowej sieci typu P2P – *peer-to-peer*. P2P, czyli osoba do osoby, to model komunikacji w sieci komputerowej, który – w odróżnieniu od architektury klient-serwer – zapewnia wszystkim hostom te same uprawnienia. Każdy z uczestników logujący się do sieci zgadza się na udostępnienie

[28] I. Kacprzak, *Poseł Brejza na celowniku pedofilów*, https://www.rp.pl/spoleczenstwo/art16829681-posel-brejza-na-celowniku-pedofilow (dostęp: 18.04.2022).

[29] F. Radoniewicz, *Formy zjawiskowe i stadialne*, [w:] idem, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, 2016, Lex.

[30] A. Nastuła, *Dilemmas related to the functioning and growth of Darknet and the Onion Router network*, „Social Development & Security” 2020, vol. 10, nr 2, s. 8.

[31] M. Majorek, op. cit., s. 85.

[32] Ł. Michalik, *Sieć TOR, czyli jak zostałem przestępcą*, https://gadzetomania.pl/4011,siec-TOR-czyli-jak-zostalem-przestepca (dostęp: 18.04.2022).

części swojego dysku oraz udostępnienia łącza na cele pracy Freenetu. Elementy poszczególnych witryn są w tym wypadku dzielone na fragmenty, a następnie umieszczone na komputerach wielu przypadkowych użytkowników. W tym typie sieci nie ma scentralizowanych serwerów, które przechowują informacje lub przesyłają dane. Każdy komputer, który połączy się z siecią, staje się niejako zwykłym użytkownikiem (odbiorcą treści), serwerem i swego rodzaju „słupem przesyłowym". Dzięki temu nie jest możliwe zweryfikowanie, który komputer jest faktycznym źródłem strony. Nigdy nie wiadomo, czy komputer, przez który przechodzi treść, jest jej autorem, odbiorcą czy jedynie stanowi punkt przesyłowy dla treści. Podstawową wadą takiego rozwiązania jest niezwykle powolna infrastruktura, gdyż Freenet „(...) działa jako sieć identycznych węzłów, które wspólnie udostępniają swoją przestrzeń dyskową do przechowywania plików i współpracują w celu ukrycia ich faktycznej lokalizacji"[33]. *File sharing* opiera się na modelu, w którym pliki przechowywane są i udostępniane bezpośrednio przez komputery użytkowników, bez konieczności ich załadowania (*upload*) na serwer. Użytkownicy takich sieci mają możliwość pobierania plików poprzez bezpośrednie połączenie do komputera użytkowników, które takowe udostępniają. Stosowana technologia może umożliwiać również wyszukiwanie udostępnianych plików w celu bezpośredniego połączenia dwóch nieznających się wzajemnie użytkowników: posiadającego poszukiwane materiały i poszukującego materiałów do pobrania. Najbardziej znane sieci działające w tożsamy sposób to Napster, Kazaa, Morpheus, Gnutella, Freenet, Audiogalaxy, BitTorrent, eDonkey (eMule)[34].

Użytkownik Freenetu ma niewielki wpływ na to, co jest zapisane w jego magazynie danych. Pliki są przechowywane lub usuwane w zależności od ich popularności. Użytkownicy przechowują jedynie części poszczególnych plików i są bezpośrednio połączeni z niewielką liczbą węzłów (maksymalnie pięciu). Jeśli użytkownik chce pobrać plik, musi wysyłać zapytania do sąsiadujących węzłów. Jeśli pytany węzeł ma żądany plik, to wysyła go zamawiającemu[35]. Nie ulega wątpliwości, że sieć została skonstruowana w taki sposób, aby zapewnić możliwie wiele rodzajów interakcji między użytkownikami, od dostępu do ciemnej warstwy Internetu, przez usługi wymiany plików i ich przechowywania, po wewnętrzne serwisy społecznościowe[36].

I2P

Dostęp do ciemnej części Internetu zapewnia również Invisible Internet Project (I2P). Wskazuje się, że nie jest ona tak popularna jest TOR, ale obydwie wspólnie stanowią „dobrze znane sieci anonimowości używane przez wiele osób w celu ochrony

[33] I. Clarke, O. Sandberg, B. Wiley, T.W. Hong, *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, [w:] H. Federrath (red.), *Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science*, Berlin–Heidelberg 2009, s. 46.

[34] Z. Okoń, *Prawo autorskie w społeczeństwie informacyjnym*, [w:] P. Podrecki (red.), *Prawo Internetu*, Warszawa 2007, s. 400.

[35] J. Kosiński, op. cit., s. 138.

[36] M. Majorek, op. cit., s. 85.

ich prywatności i anonimowości w Internecie"[37]. I2P to anonimowa warstwa sieci z komutacją pakietów (komutacja pakietów polega na dzieleniu ciągłego strumienia danych na mniejsze kawałki nazywane pakietami, które przesyłane są następnie między kolejnymi węzłami sieci), wielokrotnym, wielowarstwowym szyfrowaniem transmisji, mechanizmem znajdowania połączenia poprzez komputery proxy oraz w pełni rozproszoną organizacją, w której nie ma żadnych centralnych serwerów. Wskazana komutacja pakietów w istocie przypomina *sharding*, polegający na podziale zadań na wiele porcji i przetwarzania ich w wielu węzłach jednocześnie[38], co z kolei zapewnia swoiste maskowanie ruchu.

I2P powstała na bazie modyfikacji sieci Freenet[39]. Umożliwia aplikacjom wysyłanie między sobą wiadomości pseudonimowo i bezpiecznie za pomocą routingu czosnkowego[40]. Przesyłane między węzłami wiadomości mogą być grupowane i zamykane w strukturze nazywanej główką czosnku (ang. *garlic*). Oprócz upakowanych w główce czosnku wiadomości, znajdują się tam również informacje o tunelu nadawczym, przez który wysyłana została paczka, co przyspiesza ustalanie trasy, którą można przesyłać wiadomość zwrotną od węzła docelowego.

Pakiety danych przesyłane w sieci I2P noszą nazwę wiadomości. Aby wysłać dane do wybranego węzła sieci I2P, węzeł nadawczy sprawdza w rozproszonej, samoorganizującej się bazie połączeń jak oznaczony jest identyfikator bramy, poprzez którą można się skomunikować z węzłem docelowym. Następnie wiadomość jest przekazywana do odpowiedniego tunelu nadawczego, z poleceniem przesłania jej do jednego z tuneli odbiorczych węzła docelowego. Warto dodać, że każdy z węzłów przechowuje i na bieżąco uaktualnia swoją część rozproszonej bazy połączeń. Powyższe to z kolei nic innego jak łączność bezpośrednia między użytkownikami *peer-to-peer* w celu wymiany plików, co jest totalnym odstępstwem od dominującego modelu klient-serwer.

Podczas transmisji danych w sieci I2P wszystkie informacje są szyfrowane na czterech warstwach, przy czym zarówno źródłowy, jak i docelowy adres IP są ukryte przed sobą i stronami trzecimi[41]. Pierwsza warstwa szyfrowania (warstwa wiadomości) służy do zaszyfrowania danych użytkownika, przesyłanych od węzła źródłowego do docelowego. Druga z warstw szyfrowania obejmuje szyfrowanie główki czosnku, czyli zbioru połączonych (i już wcześniej zaszyfrowanych) ze sobą wiadomości przesyłanych tunelami. Trzeci poziom szyfrowania to szyfrowanie warstwy transportowej wewnątrz tunelu.

---

[37] N.P. Hoang, P. Kintis, M. Antonakakis, M. Polychronakis, *An Empirical Study of the I2P Anonymity Network and its Censorship Resistance*, [w:] *Proceedings of the Internet Measurement Conference 2018 (IMC '18). Association for Computing Machinery*, New York 2018, s. 379.

[38] I. Bashir, *Blockchain. Zaawansowane zastosowania łańcuchów bloków*, 2019, s. 487.

[39] M. Bienkowski, *Sieć I2P. Część 6*, https://www.benchmark.pl/testy_i_recenzje/siec-i2p.html (dostęp: 18.04.2022).

[40] A. Ali i in., *TOR vs I2P: A comparative study*, 2016 IEEE International Conference on Industrial Technology (ICIT), 2016, s. 1748.

[41] S. Aked, *An investigation into darknets and the content available via anonymous peer-to-peer file sharing*, 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia 2011, s. 11.

Polega ono na szyfrowaniu wszelkich informacji „wpuszczanych" do tunelu. Ostatnim poziomem szyfrowania jest szyfrowanie informacji przekazywanych w węźle między różnymi tunelami[42].

W sieci I2P transmisja danych realizowana jest poprzez jednokierunkowe tunele (nadawcze i odbiorcze) o krótkim czasie życia wynoszącym 10 min. Jednokierunkowość tuneli upraszcza wyszukiwanie dróg dostępu do innych węzłów sieci oraz utrudnia analizę ruchu. Wskazuje się również, że takie rozwiązanie zwiększa bezpieczeństwo[43].

Mimo wielu podobieństw, system I2P nie jest konkurencyjną siecią w stosunku do TOR. Zamierzeniem twórców TOR było stworzenie w miarę szybkiej, anonimowej sieci służącej do przeglądania przede wszystkim stron WWW znajdujących się w Internecie. Celem powstania sieci I2P było zaś zbudowanie zdecentralizowanej wirtualnej sieci, działającej jak gdyby pod powierzchnią Internetu, jednak o zwiększonej funkcjonalności. Dlatego wewnątrz sieci I2P zaimplementowano mechanizmy pozwalające na korzystanie z usług o funkcjonalności identycznej z ich odpowiednikami w sieci Internet, a więc serwerów WWW umożliwiających publikację stron, które nazywane są Eepsite, serwerów IRC, mechanizmów wymiany plików między użytkownikami, a także stworzono anonimowe serwery pocztowe oraz anonimowe serwery proxy, działające dla stron WWW znajdujących się poza siecią I2P w normalnym Internecie.

Podobnie jak w sieci TOR, na potrzeby sieci I2P stworzono pseudodomenę najwyższego poziomu z rozszerzeniem .i2p, która działa tylko w sieci I2P[44]. Odpowiedniki stron WWW z rozszerzeniem .i2p, czyli wspomniane przed chwilą Eepsite, można przeglądać zwykłą przeglądarką internetową po wcześniejszej instalacji oprogramowania I2P i skonfigurowaniu EepProxy. Program EepProxy odpowiada za komunikacje między przeglądarką internetową a dowolną stroną Eepsite. Działa on podobnie do zwykłego serwera proxy, z którego usług można korzystać w dowolnej przeglądarce internetowej. Na potrzeby sieci I2P powstała m.in. usługa blogowa Syndie, klient poczty Susimail, a także klient sieci BitTorrent I2PSnark oraz klient sieci ed2k – iMule (*invisible Mule*)[45].

Zakończenie

Termin „Darknet" oznacza ciemną strefę Internetu. W tym jednym słowie mieści się ogół witryn, za pośrednictwem którym można zostać właścicielem asortymentu zabronionego przez obowiązujące prawo. Działalność *e-commerce* zaliczana do Darknetu pozwala również nabyć swoiste usługi, których wykonanie wypełnia znamiona ciężkiego uszczerbku na zdrowiu, a w skrajnych przypadkach stanowi zamach na prawo do życia, w tym działalność terrorystyczną. W szerokim rozumieniu Darknet to również różnego rodzaju narzędzia technologiczne, takie jak przeglądarki, sieci, protokoły,

[42] *I2P*, https://pl.wikipedia.org/wiki/I2P (dostęp: 18.04.2022).
[43] S. Aked, op. cit., s. 11.
[44] Ibidem, s. 12.
[45] Ibidem.

których wykorzystywanie zapewnia możliwości wykorzystania tego, co oferuje Darknet. Występowanie przymiotnika *dark* może wywoływać pewne negatywne wyobrażenia dotyczące tej części Internetu. I choć nierzadko są one w pełni uzasadnione, gdyż Darknet jest wykorzystywany do działań przestępczych, to jego cechy, takie jak prywatność i anonimowość, mogą przysłużyć się również w dobrej sprawie.

Chcąc zostać „użytkownikiem" Darknetu, należy wyposażyć się w odpowiednie przeglądarki internetowe, o czym była mowa w niniejszym artykule. Jest to warunek *sine qua non*, ponieważ tradycyjne przeglądarki nie zapewniają wymaganej prywatności oraz anonimowości, a w tym maskowania lokalizacji oraz aktywności użytkowników. W literaturze można spotkać się również z opiniami, że celem przyświecającym stworzeniu infrastruktury, którą z czasem zaczęto określać jako Darknet, było zagwarantowanie prywatności i anonimowości przesyłu danych. Deweloperzy, mając na względzie postępującą inwigilację życia prywatnego obywateli, zarówno przez państwa, jak i wielkie korporacje, przeczuwali, że narzędzia, takie jak TOR, Freenet czy I2P, staną się coraz popularniejsze, nie przypuszczali jednak, jak bardzo omówione w niniejszym artykule rozwiązania wsparte kryptografią ułatwią życie przestępcom.

TOR jawi się jako rozwiązanie podstawowe, umożliwiające surfowanie po Internecie bez obawy o śledzenie aktywności. Freenet oraz I2P wykraczają znacznie dalej ze swoją funkcjonalnością, ponieważ przypominają w istocie aplikacje oparte na technologii łańcucha bloków.

BIBLIOGRAFIA

Literatura

Aked S., *An investigation into darknets and the content available via anonymous peer -to-peer file sharing, 9th Australian Information Security Management Conference*, Perth Western Australia 2011.

Ali A. i in., *TOR vs I2P: A comparative study*, 2016 IEEE International Conference on Industrial Technology (ICIT), 2016.

Biddle P., England P., Peinado M., Willman B., *The Darknet and the Future of Content Protection*, [w:] J. Feigenbaum (red.), *Digital Rights Management. DRM 2002. Lecture Notes in Computer Science*, vol 2696, Berlin–Heidelberg 2003.

Haraty R.A., Zantout B., *The TOR dota communication system: A survey*, „Journal of Cummunications and Networks" 2014, t. 16, nr 4.

Hoang N.P., Kintis P., Antonakakis M., Polychronakis M., *An Empirical Study of the I2P Anonymity Network and its Censorship Resistance*, [w:] *Proceedings of the Internet Measurement Conference 2018 (IMC '18). Association for Computing Machinery*, New York 2018.

Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

Majorek M., *Darknet. Ostatni bastion wolności w Internecie?*, „Bezpieczeństwo. Teoria i Praktyka" 2017, nr 4.

Meland P.H., Bayoumy Y.F.F., Sindre G., *The Ransomware-as-a-Service economy within the darknet*, „Computers & Security" 2020, vol. 92.

Nastuła A., *Dilemmas related to the functioning and growth of Darknet and the Onion Router network*, „Social Development & Security" 2020, vol. 10, nr 2.

Okoń Z., *Prawo autorskie w społeczeństwie informacyjnym*, [w:] P. Podrecki (red.), *Prawo Internetu*, Warszawa 2007.

Opitek P., *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo" 2017, nr 6.

Ormsby E., *Darknet*, Kraków 2019.

Radoniewicz F., *Formy zjawiskowe i stadialne*, [w:] idem, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, 2016, Lex.

Sobiecki G., *Regulowanie kryptowalut w Polsce i na świecie na przykładzie Bitcoina: status prawny i interpretacja ekonomiczna*, „Problemy Zarządzania" t. 1, z. 3.

Worona J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Warszawa 2020.

Zielińska C., *„Cybercrime" – wyzwanie dla kryminologii*, [w:] D. Dajnowicz-Piesiecka, E. Jurgielewicz-Delegacz, E.W. Pływaczewski (red.), *Przestępczość XXI wieku. Szanse i wyzwania dla kryminologii*, Warszawa 2020.

Akty prawne

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2022 r., poz. 1138 z późn. zm.).

Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (t.j. Dz.U. z 2020 r., poz. 2050 z późn. zm.).

Źródła internetowe

Bienkowski M., *Sieć I2P. Część 6*, https://www.benchmark.pl/testy_i_recenzje/siec-i2p.html.

Çalışkan E., Minárik T., Osula A.M., *Technical and Legal Overview of the TOR Anonymity Network*, https://ccdcoe.org/library/publications/technical-and-legal-overview-of-the-tor-anonymity-network/.

Ciancaglini V., Balduzzi M., Goncharov M., McArdle R., *Deepweb and Cybercrime It's Not All About TOR*, https://documents.trendmicro.com/assets/wp/wp-deepweb-and-cybercrime.pdf.

Grannan C., *What's the Difference Between the Deep Web and the Dark Web?*, https://www.britannica.com/sTORy/whats-the-difference-between-the-deep-web-and-the-dark-web.

I2P, https://pl.wikipedia.org/wiki/I2P.

Kacprzak I., *Poseł Brejza na celowniku pedofilów*, https://www.rp.pl/spoleczenstwo/art16829681-posel-brejza-na-celowniku-pedofilow.

Leżoń T., *Głęboko pod powierzchnią jest miejsce, o którym wolałbyś nie wiedzieć*, https://tvn24.pl/magazyn-tvn24/gleboko-pod-powierzchnia-jest-miejsce-o-kTORym-wolalbys-nie-wiedziec,95,1850.

Operation Onymous: International law enforcement agencies target the Dark Net in November 2014, https://www.swansea.ac.uk/media/Operation-Onymous.pdf.

Opulski P., *Ciemna strona Internetu*, https://sekTOR3-0.pl/blog/ciemna-strona-internetu/.

Szydłowski T., *TOR – wszystko, co trzeba wiedzieć o sieci cebulowej*, https://www.komputerswiat.pl/artykuly/redakcyjne/TOR-wszystko.

United States of America v. Ross William Ulbricht, No. 15-1815-cr (2d Cir. May 31, 2017), https://sherloc.unodc.org/cld/en/case-law-doc/cybercrimecrimetype/usa/2017/united_states_of_america_v._ross_william_ulbricht_no._15-1815-cr_2d_cir._may_31_2017.html.

Wierzbicki P., *Gwałt na córce polityka? 36 000 dolarów. Przed wami najgorsze oblicze darknetu*, https://techsetter.pl/najgorsze-oblicze-darknetu/.

Darknet – more than The Onion Router

Summary

This paper describes the possibilities of gaining access to the darkened sphere of the network, taking into account the technical basis of such access and their characteristics. The features of these programs determine their usefulness in criminal activity, which is why knowledge of how they work becomes a kind of standard in legal practice. Considerations regarding the functioning of the TOR, I2P and Freenet networks will be preceded by an explanation of what Darknet is, what is its main purpose (not everyone uses the Darknet illegally) together with an indication of its place in the general structure of the Internet.

Keywords: Darknet, The Onion Router, TOR, Silk Road, Freenet, I2P