

Daniel Mider

Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów

Powstanie i rozwój darkmarketów, to jest sklepów oferujących nielegalne towary i usługi, stało się przedmiotem debaty publicystycznej nacechowanej emocjonalnie, noszącej znamiona paniki moralnej¹, w której brakuje pogłębionej refleksji i weryfikacji źródeł. Elementami poddawany najsilniejszej krytyce są szeroko pojęte technologie anonimizujące, zapewniające anonimowość w sieci Internet². W niniejszym artykule zreferowano wyniki badań rozpoznawczych, które mają stanowić zracjonalizowany, empiryczny głos w dyskusji. Przedstawiono realny potencjał darkmarketów, wskazano nielegalne produkty i usługi będące przedmiotem obrotu gospodarczego oraz ich udział procentowy w rynku. Ważną przesłanką podjęcia badań była dynamika obserwowanych zjawisk – publikacje dotyczące darkmarketów, które zostały wydane ponad rok temu, należy traktować ostrożnie, a informacje w nich zawarte uważać za nieaktualne³.

W pierwszej kolejności wypada rozstrzygnąć kwestie dotyczące pojęć. W nomenklaturze naukowej, operacyjnej i publicystycznej powszechnie funkcjonują pojęcia: *Deep Web* i *Darknet*⁴. Ich rozumienie ma charakter metaforyczny, a nie

¹ S. Cohen, *Folk devils and moral panics*, London–New York 2011, s. 26–41.

² Publicystyka, w tym i polska, jest pełna nadinterpretacji, nieporozumień, poszukiwania sensacji i forsowania przesadnie restrykcyjnych projektów wobec technologii anonimizujących. Patrz na przykład: J. Chmielecka, *Po ciemnej stronie internetu*, Wyborcza.pl, Duży Format, 30 I 2013 r., http://wyborcza.pl/duzyformat/1,127290,13318724,Po_ciemnej_stronie_internetu.html [dostęp: 1 VIII 2018]; B. Świdorski, *Najciemniejszy zakątek internetu naprawdę istnieje. Ukryta sieć TOR: „Lewe” papiery, pedofilia, przekręty i narkotyki*, 21 IX 2012 r., <https://natemat.pl/32267,najciemniejszy-zakatek-internetu-naprawde-istnieje-ukryta-siec-tor-lewe-papiery-pedofilia-przekrety-i-narkotyki> [dostęp: 1 VIII 2018].

³ Ciekawe są wyniki badań Gwerna Branwena, pisarza i badacza niezależnego. Spośród 87 darkmarketów badanych przez niego w latach 2011–2015 w 2017 r. pozostało tylko pięć, obecnie zaś (wrzesień 2018 r.) funkcjonują tylko dwa z nich, co znamienne – rosyjskie (Tochka, przemianowany na Point Marketplace, oraz Hydra). Więcej na ten temat wraz ze szczegółowymi statystykami zob. G. Branwen, *Darknet market mortality risks*, <http://www.guern.net/DNM-survival> [dostęp: 13 IX 2018].

⁴ Takie nazewnictwo stosuje m.in. Federalne Biuro Śledcze USA oraz Europol (European Monitoring Centre for Drugs and Drug Addiction and Europol). Zob. *Drugs and the darknet: Perspectives for enforcement, research and policy*, Luksemburg 2017; S.R. Chabinsky, *Congressional Testi-*

dosłowny. Zakresy dwóch wymienionych nazw pozostają wobec siebie w stosunku podrzędności – drugie z pojęć jest podrzędne wobec pierwszego. Znaczenie pojęcia *Deep Web*, tj. Głębokiego Internetu, odwołuje się do asocjacji przestrzennych. Rozumienie dosłownego sensu będzie kierować uwagę ku temu, co położone na dnie, w otchłani, a więc trudno dostępne, a nawet niedosiężne. Do Głębokiego Internetu zalicza się treści, do których nie można dotrzeć za pomocą popularnych wyszukiwarek (Google/Yahoo/Bing/Yandex) najczęściej z następujących powodów: zablokowania dla robotów wyszukiwarek sieciowych, nieindeksowania z braku odnośników (Google), wymogu uwierzytelnienia (podanie nazwy użytkownika oraz hasła), użycia innych niż HTML języków programowania, lokalizacji geograficznej użytkownika uniemożliwiającej skorzystanie z niektórych treści i usług, a nawet historii wcześniejszych wyszukiwań. Ponadto w Głębokim Internecie lokują się trudniej dostępne sieci i kanały komunikacji, jak np. infrastrukturalne domeny najwyższego poziomu, alternatywne systemy nazw domen, pseudodomeny najwyższego poziomu, „stare” usługi internetowe, tj. istniejące przez wdrożeniem www (lub inaczej: Sieć 0.0., Web 0.0), intranety oraz ekstranety wydzielone z Internetu, informatyczne systemy zarządzania i sterowania, a także internetowe promieniowanie tła⁵. Dopelnieniem logicznym pojęcia *Deep Web* jest to, co położone płytko, a więc Sieć Powierzchniowa (*Surface Web*), określana także mianem *Cleartnet*, *Visible Web* lub *Indexable Web*⁶. Węższy w stosunku do *Deep Web* zakres znaczeniowy ma pojęcie *Darknet* (*Dark Web*). Odnosi się ono do sieci, które intencjonalnie mają charakter ukryty, są bowiem tak zaprojektowane, aby maksymalizować anonimowość ich użytkowników, przez co są dostępne przy użyciu odpowiednich przeglądarek lub specjalistycznego oprogramowania. Pojęcie *Darknet* zostało spopularyzowane w artykule *The Darknet and the future of content distribution* w 2002 r.⁷ W niniejszym artykule użyto też pojęcia *darknet market* lub – w skrócie – *darkmarket*.

W tytule artykułu wykorzystano pojęcia: czarny rynek oraz czerwony rynek. Należą one do zbioru pojęć zawierającego cztery kategorie relacji legalistyczno-etycznych, które mogą zachodzić między rynkiem towarów i usług a normami prawnymi i etycznymi: biały rynek, szary rynek, czarny rynek i czerwony rynek.

mony, 17 X 2009 r., <https://web.archive.org/web/20100412172853/http://www.fbi.gov/congress/congress09/chabinsky111709.htm> [dostęp: 1 VIII 2018]; tenże, *Major Executive Speeches*, 23 III 2010 r., <https://web.archive.org/web/20161227043937/https://www2.fbi.gov/pressrel/speeches/chabinsky032310.htm> [dostęp: 1 VIII 2018]. Takie określenie jest często używane również w publicystyce, m.in. w „The Guardian”, BBC News czy „Wired”. Patrz na przykład: *Organiser of Darkmarket fraud website jailed*, „The Guardian”, 26 II 2010 r., <https://www.theguardian.com/technology/2010/jan/14/darkmarket-online-fraud-trial-we> [dostęp: 1 VIII 2018].

⁵ Szerzej na ten temat zob. D. Mider, *Mappa Mundi ukrytego Internetu. Próba kategoryzacji kanałów komunikacji i treści*, „EduAkcja. Magazyn edukacji elektronicznej” 2015, nr 2, s. 55–70.

⁶ Por. C. Egger i in., G. Vigna, *Practical attacks against the I2P network*, 2013 r., <http://wwww.cip.cs.fau.de/~spjsschl/i2p.pdf> [dostęp: 1 VIII 2018].

⁷ P. Biddle i in., *The Darknet and the future of content distribution*, http://bearcave.com/misl/misl_tech/msdrm/darknet.htm [dostęp: 1 VIII 2018].

Kategoryzację zaproponował Samuel Edward Konkin III, twórca koncepcji agoryzmu i pojęcia minarchizm. Według tego filozofa biały rynek oznacza obrót legalnymi towarami i usługami w legalny sposób, szary rynek to obrót legalnymi towarami i usługami w nielegalny sposób (np. piracka płyta, film, program, unikanie opodatkowania). Czarny rynek to obrót nielegalnymi towarami i usługami w nielegalny sposób (np. zakazanymi substancjami psychoaktywnymi, bronią palną), jednak bez użycia przemocy („przestępstwa bez ofiar”). Natomiast pojęcie czerwony rynek odnosi się do obrotu nielegalnymi towarami i usługami, w ramach którego przemoc jest immanentnym elementem towaru lub usługi (np. rynki przemocy: płatni zabójcy)⁸. Ta klasyfikacja ma atrybut relatywności (rozmaitość uregulowań prawnych może lokować ten sam towar lub usługę w obrębie niemal dowolnego rynku; podobnie istnieje wiele systemów etycznych), jednak jako reguła kategoryzująca wydaje się wystarczająca, jeśli punktem odniesienia będzie rodzima legislacja.

Cele, hipotezy, zakres i metodyka badania

Zagadnienia związane z handlem towarami i usługami w sieci The Onion Router (TOR) są przedmiotem nielicznych, jak dotychczas, opracowań stricte naukowych, wśród których przeważają prace o charakterze technicznym⁹. Można tu znaleźć publikacje służb dyspozycyjnych¹⁰ oraz doniesienia klasyfikowane jako dziennikarstwo śledcze – w postaci licznych artykułów prasowych. Wymienione źródła charakteryzują się ograniczeniem tematycznym, np. skupiają się wyłącznie na zagadnieniach własności intelektualnej¹¹ lub środkach psychoaktywnych¹². Brakuje natomiast prac przeglądowych, w których zestawia się poszczególne towary i usługi dostępne w sieci

⁸ S.E. Konkin III, *New libertarian manifesto*, <http://agorism.info/docs/NewLibertarianManifesto.pdf> [dostęp: 13 VII 2018].

⁹ Spośród zwartych pozycji polskojęzycznych można wymienić tylko jedną. Zob. K.M. Mazur, *Polskojęzyczna społeczność przestępcza zorganizowana w sieci darknet*, Poznań 2016. Jest to ujęcie o charakterze prawnym i socjologicznym, jednak podane tam informacje są już nieaktualne.

¹⁰ *Drugs and the darknet. Perspectives for enforcement, research and policy*, Lisbon 2017, <https://www.emcdda.europa.eu/system/files/publications/6585/TD0417834ENN.pdf> [dostęp: 4 V 2019]. Grupy dyspozycyjne „(...) są różnie ujmowane i interpretowane w literaturze, ale ich wspólnym celem jest bezpośrednia, bezzwłoczna ochrona i obrona społeczeństwa przed wszelkimi zagrożeniami, niezależnie czy są to grupy militarne, paramilitarne, cywilne czy ochotnicze”. Cyt. za: <https://wydawnictwa.wspol.edu.pl/content/library/Grupy%20dyspozycyjneTOM1SP.pdf>, s. 5.

¹¹ Patrz na przykład: P. Biddlei in., *The Darknet and the future...* [dostęp: 4 V 2019].

¹² J. Broséus i in., *Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective*, „Forensic Science International” 2016, t. 264, https://www.researchgate.net/publication/297627993_Studying_illicit_drug_trafficking_on_Darknet_markets_Structure_and_organisation_from_a_Canadian_perspective, brak numeracji stron [dostęp: 4 V 2019].

TOR (wraz ze wskazaniem proporcji udziału w rynku)¹³. Należy również podkreślić istotność samego zjawiska handlu w sieci TOR, które charakteryzuje się stosunkowo łatwym, na ogół anonimowym oraz globalnym dostępem do nielegalnych towarów i usług. Impulsem do podjęcia badań stało się również publicystyczne przedstawianie darkmarketów w kategoriach przerysowanych, niepogłębionych, ogniskowanie się na ekstremalnych przypadkach, bez poprawnej, empirycznej weryfikacji źródeł.

Wyżej nakreślone przesłanki i problemy wyznaczyły zasadniczy cel postępowania badawczego: ilościowo-jakościową analizę realnego potencjału darkmarketów, ze wskazaniem typów produktów i usług nielegalnych będących przedmiotem obrotu gospodarczego oraz proporcji ich udziałów w rynku. Ma to najważniejsze znaczenie dla określenia zakresu i stopnia zagrożenia, jakie sieć TOR stwarza bezpieczeństwu narodowemu, państwowemu oraz globalnemu. W nawiązaniu do ukazujących się w prasie charakterystyk zjawiska darkmarketów, które odnoszą się do jego dynamicznych zmian, oraz tendencji dziennikarzy do szukania sensacji (np. sugerowanie przez nich istnienia rozbudowanego czerwonego rynku), w badaniach postawiono następującą hipotezę kierunkową: przedmiot obrotu gospodarczego w sieci TOR stanowią dobra szybkozbywalne, łatwe w produkcji, legalne w niektórych prawodawstwach (z reguły w lokalizacji, w której są wytwarzane oraz dystrybuowane), niezbyt kosztowne (ze względu na ryzyko, jakie ponosi kupujący) oraz skierowane do odbiorców indywidualnych.

Dopełnieniem powyższego będą następujące przypuszczenia: brak w sieci TOR lub marginalizacja usług związanych z tzw. czerwonym rynkiem ze względu na trudność w dostarczaniu takich usług, ich nielegalność we wszystkich prawodawstwach, ponoszone koszty oraz stosunkowa łatwość wykrycia, choćby przez przeprowadzenie prowokacji.

Niniejszy artykuł to praca o charakterze empirycznym; w takich przedsięwzięciach badawczych źródła opisowe są zastępowane danymi pozyskiwanymi w toku standaryzowanego postępowania badawczego, w bezpośrednim kontakcie uczonego z przedmiotem jego zainteresowań. W tym przypadku wykorzystano obserwację nieuczestniczącą ukrytą¹⁴. Jest to metoda mająca długą i bogatą, w tym polską, tradycję¹⁵. Zebrany materiał empiryczny został przeanalizowany przy wykorzystaniu metody analizy zawartości (ang. *content analysis*). Jest ona definiowana jako technika badawcza służąca systematycznemu, obiektywnemu oraz ilościowemu opisowi treści komunikacyjnych¹⁶ lub jeszcze krócej – jako badanie artefaktów społecznych (to jest

¹³ *Anonymity Bibliography*, <https://www.freehaven.net/anonbib/full/date.html> [dostęp: 4 V 2019].

¹⁴ F. Liu, S. Maitlis, *Nonparticipant Observation*, w: *Encyclopedia of Case Study Research*, A.J. Mills, G. Durepos, E. Wiebe (red.), Thousand Oaks 2010, s. 610–612.

¹⁵ Zob. B. Malinowski, *Argonauci zachodniego Pacyfiku. Relacje o poczynaniach i przygodach krajozwojców z Nowej Gwinei*, Warszawa 1981.

¹⁶ B. Berelson, *Content analysis in communication research*, Glencoe 1952, s. 18. Do definicji Bernarda Berelsona nawiązuje i ją rozwija jeden z późniejszych klasyków tej metody Klaus Krippendorff. Zob. K. Krippendorff, *Models of messages: three prototypes*, w: *The analysis of communication content*, G. Gerbner i in. (red.), New York 1969.

intelektualnych i symbolicznych wytworów ludzkich)¹⁷. Metoda analizy polega na ocenie materiału symbolicznego w sposób zobiektywizowany i systematyczny. Oprócz jakościowej obróbki danych (kwalifikacji) dopuszcza ona ilościowe podejście do nich (kwantyfikację). Autor, korzystając z tej możliwości, zestawiał dane zgodnie ze standardami klasycznej statystyki opisowej (tabele brzegowe). Obie wymienione metody, to jest obserwacja nieuczestnicząca ukryta oraz analiza zawartości, są zaliczane do tak zwanych badań niereaktywnych (ang. *on-reactive research*), nazywanych również badaniami niejawnymi (ang. *unobtrusive research*)¹⁸.

Aktualnie jako sieci należące do Darknetu, czyli miejsca funkcjonowania darkmarketów, można rozpatrywać następujące cztery rozwiązania informatyczne (podane w kolejności ich powstawania): Freenet, The Onion Router, Invisible Internet Projec i Zeronet¹⁹.

Freenet to całkowicie zdecentralizowana sieć, nieposiadająca żadnego serwera sterującego ruchem lub przechowującego rejestr adresów. Jej zasoby są całkowicie rozproszone. Pomysłodawcą i autorem jest Ian Clarke, który napisał jej protokół i opracowanie w języku Java. Sieć jest rozwijana od marca 2000 r., zapewnia użytkownikom prywatność, lecz nie zapewnia anonimowości. Działanie Freenetu jest następujące: komputery połączone w sieć są równorzędne i każdy z nich jest jednocześnie serwerem danych (węzłem komunikacyjnym). Jest to topologia siatki (ang. *full mesh*), a więc bezserwerowa, ponieważ każdy z użytkowników przez zainstalowanie Freenetu udostępnia część przestrzeni swojego dysku twardego na potrzeby działania całości sieci. Ta przestrzeń jest ściśle odizolowana od reszty zasobów znajdujących się na komputerze. Służy ona do przechowywania danych wprowadzonych do sieci oraz do ich transferu. Użytkownik nie ma możliwości sprawdzenia, co zostało zdeponowane na dysku twardym, a także co zostało przesłane przez jego komputer. Jest to architektura rozproszonej sieci *peer-to-peer* (P2P), jednak z tą zasadniczą różnicą, że użytkownik po wprowadzeniu pliku do sieci traci kontrolę nad jego lokalizacją. Plik może się znaleźć w dowolnych miejscach, najczęściej więcej niż jednym (im bardziej popularny zasób, w tym większej liczbie lokacji jest on przechowywany). Dane z różną częstotliwością są automatycznie i losowo przenoszone z jednego komputera na inny, pobieranie danych zaś nigdy nie odbywa się bezpośrednio, lecz przez inne komputery (węzły sieci). Adresowania dokonuje się z użyciem kluczy występujących w kilku

¹⁷ A.M. Messinger, *Teaching Content Analysis through Harry Potter*, „Teaching Sociology” 2012, nr 4, s. 360.

¹⁸ Pojęcie badania niejawne wprowadził do słownika nauk społecznych w latach 60. XX w. profesor Uniwersytetu Stanforda Eugene J. Webb wraz z zespołem, a następnie w latach 80. wskazał tę metodę jako tożsamą z badaniami niereaktywnymi. Zob. E.J. Webb i in., *Unobtrusive Measures: Nonreactive Research in the Social Sciences*, Chicago 1966 oraz E.J. Webb i in., *Nonreactive Measures in the Social Sciences*, Dallas 1981.

¹⁹ Por. V. Ciancaglinii in., *Deepweb and cybercrime. It's not all about TOR*, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf> [dostęp: 12 IX 2018].

funkcjonalnych odmianach. Do podstawowych wad tej sieci przy zastosowaniu jej do funkcjonowania darkmarketów należą: powolne działanie, brak wyszukiwarek (istniejące wyszukiwarki nie dają relewantnych wyników), ubogie graficznie treści, znikome zainteresowanie nią potencjalnych klientów, konieczność samodzielnego i na ogół pozainternetowego poszukiwania kluczy do zasobów interesujących użytkowników²⁰.

The Onion Router został udostępniony do użytku cywilnego we wrześniu 2003 r. Pierwotnie rozwijano go jako projekt militarny – w ostatniej fazie tą siecią zajmowało się Laboratorium Marynarki Wojennej USA. Aktualnie funkcjonuje ona na licencji BSD i zarządza nią Fundacja TOR Project. TOR umożliwia ukrycie tożsamości (lokalizacji) zarówno konsumenta treści (to jest zwykłego użytkownika), jak i jej dostarczyciela. Komunikacja w sieci zachodzi przy użyciu niezależnych i wielowarstwowo szyfrowanych pakietów, stąd określenie „trasowanie cebulowe”, a także nazwa projektu oraz domeny, w której działa (ang. *onion*). TOR dobrze współpracuje z kryptowalutą bitcoin i zapewnia wysoki (choć nie idealny) poziom anonimizacji. Według TOR Metrics tej sieci używa ponad 2 mln użytkowników dziennie, ma ona ponad 6 tys. węzłów, a ruch przekracza 200 Gbit/s²¹. Darkmarkety od samego początku były silnie związane z tą właśnie siecią, tam też aktualnie znajduje się większość z nich²².

Invisible Internet Project (I2P) powstała w 2003 r. na licencji MIT (X11). Jest to sieć *peer-to-peer* (P2P) łącząca zalety TOR i Freenetu. Istota działania I2P polega na ustanawianiu krótkotrwałych (10-minutowych) jednokierunkowych tuneli w celu skomunikowania ze sobą węzłów sieci. Podstawowym rozwiązaniem jest jednokierunkowość, co ma utrudniać analizę ruchu. Nadawanie i odbieranie informacji między dwoma węzłami odbywa się różnymi kanałami. Baza węzłów i połączeń między nimi jest samoorganizująca się (nie wymaga żadnego serwera centralnego) i rozproszona. Każdy węzeł zawiera mapę sieci lokalnej. Wiadomości są łączone w struktury zwane „główkami czosnku”, są one szyfrowane w czterech warstwach. Sieć ma własną pseudodomenę – .i2p. Do zasadniczych wad I2P utrudniających, lecz nie uniemożliwiających funkcjonowanie tej sieci jako nośnika darkmarketów, należy zaliczyć: występowanie w wersji beta, a więc niestabilnej, powolność działania, utrudnienia w konfiguracji (większe niż w przypadku Freenet i TOR). Nie zaleca się używania tej sieci z systemem Windows i Mac ze względu na łatwiejszą deanonimizację. Bariery jest również świadomość społeczna, brak szerszej znajomości tej sieci, brak finansowania i dokumentacji porównywalnej z TOR i Freenet. Do wad zalicza się również utrudniony hosting stron. I2P ma jednak potencjał – lepszą (szybszą) komunikację P2P niż

²⁰ Oficjalna strona projektu Freenet: <https://freenetproject.org/author/freenet-project-inc.html> [dostęp: 4 VIII 2018].

²¹ TOR Metrics, <https://metrics.torproject.org/> [dostęp: 4 VIII 2018].

²² Oficjalna strona projektu TOR: <https://www.torproject.org/> [dostęp: 4 VIII 2018].

przez TOR, brak możliwości identyfikacji użytkownika z wykorzystaniem wzorców czasowych, brak możliwości ataku typu *Man in the Middle* (MITM)²³.

Zeronet to sieć, która powstała najpóźniej z omawianych projektów – w 2015 r. Podobnie jak pozostałe ma charakter zdecentralizowany. Jest to sieć *peer-to-peer*, w której identyfikacja zasobów odbywa się za pomocą kluczy (są nimi adresy bitcoin, wykorzystuje się również trackery BitTorrent). Zapewnienie anonimowości (ukrycie IP) wymaga równoległego użycia TOR²⁴.

Żaden z projektów nie występuje obecnie w edycji stabilnej, są to wersje tzw. beta, co oznacza, że funkcjonalność, bezawaryjność, niezawodność i działanie według specyfikacji nie są gwarantowane. Najczęściej używanym i najpopularniejszym programem, o najlepiej rozpoznanych właściwościach jest TOR, który osiągnął próg masowości²⁵. Na jego temat można znaleźć najwięcej materiałów edukacyjnych oraz instrukcji. W pozostałych sieciach nie odnotowano tak masowej wymiany bądź niemożliwe było jej stwierdzenie. Wydaje się, że największy potencjał techniczny jako ewentualny następcą sieci TOR ma I2P, jednak ta sieć nie osiągnęła progu masowości ze względu na mniejszą popularyzację, a także nieco trudniejszą instalację i konfigurację. Projekt Freenet nie nadaje się do wymiany towarów i usług z przyczyn technicznych (przede wszystkim ze względu na powolność jego działania), jest to raczej rozwiązanie, dzięki któremu można zamieszczać informacje w sposób możliwie anonimowy. Z kolei Zeronet jest na tyle nowym projektem, że zastosowane tu rozwiązania mogą nie być zrozumiałe i docenione przez szeroki krąg użytkowników.

W badaniach skupiono się na darkmarketach funkcjonujących w sieci TOR. Mają one swoją historię, jednak nie jest to przedmiotem niniejszego artykułu ze względu na złożoność i wielowątkowość zagadnienia²⁶. Aktualnie istniejące sklepy są już drugą generacją tzw. *cryptomarkets*, tj. pseudoanonimowych platform, których właściciele wyciągnęli wnioski dotyczące bezpieczeństwa z Operacji Onymous przeprowadzonej w listopadzie 2014 r.²⁷ Współczesne darkmarkety zostały ukształtowane przez dwa

²³ Oficjalna strona projektu I2P: <https://geti2p.net/> [dostęp: 4 VIII 2018].

²⁴ Oficjalna strona projektu Zeronet: <https://zeronet.io/> [dostęp: 15 IX 2018].

²⁵ J. Aldridge, D. Décary-Héту, *Not an 'ebay for drugs': The Cryptomarket 'Silk Road' as a paradigm shifting criminal innovation*, 2014, <http://ssrn.com/abstract=2436643> [dostęp: 15 IX 2018]; H. Rush, C. Smith, E. Kraemer-Mbula, P. Tang, *Crime online: Cybercrime and illegal innovation*, 2009, <http://eprints.brighton.ac.uk/5800/> [dostęp: 4 VIII 2018].

²⁶ Pierwsza w historii symboliczna wymiana handlowa w sieci z użyciem przodka współczesnego Internetu, sieci Arpanet, została zaaranżowana pomiędzy studentami Stanford Artificial Intelligence Laboratory i Massachusetts Institute of Technology w 1971 r. Doszło wówczas do handlu konopiami indyjskimi, których posiadanie i handel nimi (a także innymi środkami psychoaktywnymi), było karane pozbawieniem wolności na mocy ustawy federalnej z 1970 r.; S. Sharma, *Relationship between e-commerce and business*, „International Journal of Research & Development in Technology and Management Science – Kailash” 2014, nr 5, s. 22, 27–28. Por. także: J. Markoff, *What the Dormouse said: How the sixties counterculture shaped the personal computer industry*, New York 2005.

²⁷ D. Décary-Héту, L. Giommo, *Do police crackdowns disrupt drug cryptomarkets? A longitudi-*

zjawiska technologiczne, na które nałożyło się upowszechnienie Internetu. Pierwszym zjawiskiem było powstanie sieci The Onion Router (2003 r.), zapewniającej wysoki poziom anonimowości i jednocześnie funkcjonalnej, drugim – stworzenie pierwszego środka płatniczego gwarantującego względną anonimowość (pseudoanonimowość), czyli kryptowaluty bitcoin (2009 r.). Były to akty konstytutywne i przełomowe, jednak technologie zapewniające anonimowość są znacznie bogatsze, a stosowanie jedynie dwóch powyższych – niewystarczające²⁸.

Źródła

Metodyka wyszukiwania darkmarketów odbyła się na podstawie dwóch grup źródeł. Po pierwsze, skorzystano z gotowych zestawień, zbiorów i analiz znajdujących się zarówno w powierzchniowym Internecie, jak i *Deep Web*²⁹. Do najważniejszych tego typu źródeł zaliczono: strony rankingowe darkmarketów (Deep Dot Web – zawierająca największy zbiór informacji o darkmarketach³⁰, aktualizowany w czasie rzeczywistym, oraz nieaktualizowaną już stronę Darknet Markets³¹), fora dyskusyjne (The Hub – forum dyskusyjne ogniskujące się na darkmarketach i sprzedawcach³² oraz Kryptoanarchizm – polskie forum kryptoanarchistów³³), zbiory odnośników i tzw. *introduction points* (Daniel Onion Links List – zbiór kilku tysięcy skategoryzowanych, ocenionych i monitorowanych adresów stron w TOR³⁴ oraz The Uncensored Hidden Wiki – darknetową encyklopedię³⁵, nieocenzurowaną, ale też i nieaktualizowaną). Ponadto zastosowano wyszukiwania własne, wykorzystując: wyszukiwarki TOR, adresy zamieszczane w tzw. *pastebins* (usługa internetowa umożliwiająca zamieszczenie tekstu, a następnie podanie go w postaci łatwego do zapamiętania odnośnika) oraz informatorów rekru-

nal analysis of the effects of Operation Onymous, Dordrecht 2016, <http://www.gwern.net/docs/sr/2016-decaryhetu.pdf> [dostęp: 4 VIII 2018].

²⁸ Dobrym podręcznikiem dla średnio zaawansowanych użytkowników sieci TOR jest opracowanie L. Hendersona, *TOR and the dark art of anonymity*, [b.m.w.] 2015. Początkującym użytkownikom Darknetu warto wskazać: *Jolly Roger's security guide for beginners*, <https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/> [dostęp: 4 I 2018].

²⁹ Do najważniejszych należą opracowania: N. Malik, *Terror in the dark. How terrorists use encryption. The Darknet, and cryptocurrencies*, Millibank 2018; J. Mounteney, A. Bo, A. Oteo, *The internet and drug markets*, Luksemburg 2016; G.P. Paolii in., *Behind the curtain. The illicit trade of firearms, explosives and ammunition on the dark web*, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf.

³⁰ Deep.Dot.Web: <http://deepdot35wvmeyd5.onion> [dostęp: 13 IX 2018].

³¹ Darknet Markets: <https://darknetmarkets.co> [dostęp: 13 IX 2018].

³² The Hub: <http://thehub7xbw4dc5r2.onion> [dostęp: 13 IX 2018].

³³ Kryptoanarchizm: <http://kryptoanarchizm.liberatrianizm.net> [dostęp: 13 IX 2018].

³⁴ Daniel Onion Link List: <http://onionsnjajzkhm5g.onion> [dostęp: 13 IX 2018].

³⁵ The Uncensored Hidden Wiki: http://gxamjbnu7uknahng.onion/wiki/index.php/Main_Page [dostęp: 13 IX 2018].

towanych spośród znawców Darknetu. Należy podkreślić zasadniczą trudność badań jaką jest dynamika zjawiska³⁶. Ekosystem darkmarketów podlega bardzo szybkim zmianom, a dotychczasowe wyniki badań w dużym tempie ulegają dezaktualizacji³⁷.

Na pierwszym etapie wyszukiwania wyodrębniono 23 darkmarkety, głównie anglojęzyczne, a podczas dalszego postępowania wyeliminowano z analizy sześć sklepów (zestawienie sklepów oraz powody ich niezbadania zawarto w załączniku 1). W rezultacie poddano badaniu 17 sklepów, z których dziewięć to sklepy pojedynczych sprzedawców (tzw. *vendor shops*), a osiem to darkmarkety w pełnym tego słowa znaczeniu (realizujące model targowiska – wielu sprzedających, natomiast właściciel występuje jako tzw. zaufana trzecia strona)³⁸.

Obserwacja, prowadzona od 6 do 27 sierpnia 2018 r., polegała na systematycznej inwentaryzacji zasobów darkmarketów: spisu towarów i usług oraz ich kategoryzacji (systematyczna inwentaryzacja zasobów to określenie najlepiej oddające czynności badawcze).

Wyniki

Badaniu poddano 17 największych (pod względem liczby oferowanych usług) darkmarketów. Wyniki zestawiono w kolejności według liczby oferowanych towarów i usług. W wielu tabelach widnieje wiersz o nazwie „niesklasyfikowane”, ponieważ inwentaryzacji dokonano według poszczególnych kategorii towarów i usług, które są wyznaczone przez właścicieli darkmarketów, a nie przez analizę pojedynczych ofert. Pomiar przeprowadzony dla Dream Market, Berlusconi Market oraz Point Marketplace wykazał, że w kategoriach niesklasyfikowanych wartości rozkładają się według proporcji kategoryzacyjnych w przedziale ± 6 proc. Warto jednocześnie zaznaczyć czynnik błędu. Administracja sklepu pozostaje niekiedy niekonsekwentna – wielokrotnie można spotkać się z sytuacją, gdy w określonym dziale znajdują się oferty, które do danego działu nie powinny przynależeć. Poziom tych „zanieczyszczeń” wynosi dla Dream Market (największego ze sklepów) ± 8 proc.

³⁶ Przykładem może być artykuł V. Bhaskara, R. Linacre’a, S. Machina, *The economic functioning of online drug markets* („Journal of Economic Behavior & Organization” 2017, b.n.), który został złożony w 2016 r, a przyjęty do druku w 2017 r. Żaden z analizowanych przez autorów darkmarketów obecnie już nie funkcjonuje.

³⁷ Por. K. Soska, N. Christin, *Measuring the Longitudinal Evolution of Online Anonymous Marketplace Ecosystem*, Proceedings of the 24th USENIX Security Symposium, <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf>, 2015 [dostęp: 13 IX 2018].

³⁸ Mechanika funkcjonowania darkmarketów w wymiarze psychospołecznym, ekonomicznym i technicznym jest zagadnieniem złożonym i obszernym. Zainteresowanym polecam opracowanie RAND: G.P. Paolii in., *Behind the curtain. The illicit trade of firearms...*

Ogółem naliczono blisko ćwierć miliona (226 tys.) aktywnych ofert (tab. 1). Najliczniejszą kategorią dóbr sprzedawanych w darkmarketach są środki psychoaktywne stanowiące blisko połowę wszystkich ofert (47,6 proc.). W większości są to produkty nielegalne (czarny rynek). Druga kategoria – około jednej czwartej wszystkich ofert (26,9 proc.) – to towary legalne, choć w wielu przypadkach procedury ich dystrybucji są nielegalne (szary rynek). Trzecią pod względem liczebności grupą produktów i usług (15,2 proc.) są programy i sprzęt komputerowy. Jest to kategoria mieszana, w której można odnaleźć produkty zaliczane do białego, szarego i czarnego rynku. Lokują się tu programy służące do popełniania przestępstw finansowych, „pirackie” wersje programów i gier oraz sprzęt i oprogramowanie związane z bezpieczeństwem czy kryptowalutami. Pozostałe kategorie, z których żadna nie przekracza 3 proc., to towary i usługi przynależne w większości do szarego i czarnego rynku.

Tab. 1. Oferta darkmarketów – liczba i proporcje ogólnych kategorii ofert³⁹.

Typ oferty	Opis oferty	Liczba ofert	Udział ofert w rynku (w %)
Środki psychoaktywne	nielegalne i legalne środki psychoaktywne oraz pozostałe medykamenty i paraferalia (wyposażenie laboratoriów i użytkowników)	107 538	47,60
Informacje	bazy danych, książki elektroniczne i poradniki	60 891	26,90
Programy i sprzęt komputerowy	programy służące do popełniania przestępstw finansowych, „pirackie” wersje programów i gier, sprzęt i oprogramowanie związane z bezpieczeństwem oraz kryptowalutami	34 398	15,20
Dokumenty	falsyfikaty dokumentów, dokumenty w wersji papierowej i w wersji elektronicznej, elektroniczne tożsamości – głównie usług bankowych	6528	2,90
Usługi	usługi hakerskie i carderskie, legalizacja kryptowalut	6535	2,90
Falsyfikaty dóbr	falsyfikaty biletów bankowych, elektroniki, odzieży, kruszców i biżuterii oraz innych towarów ekskluzywnych	5537	2,40
Broń	broń palna, materiały wybuchowe i inna broń	1504	0,70
Inne, wyżej nie ujęte	oferty pracy, reklama	3278	1,40
Ogółem ofert		226 209	100,00

³⁹ Tabele zostały opracowane przez autora (przyp. red.).

Oferta darkmarketów dotycząca środków psychoaktywnych, innych medykamentów oraz utensyliów do produkcji i zażywania narkotyków

W rankingu zdecydowanie dominują stymulanty/empatogeny oraz tzw. narkotyki miękkie (definiowane jako nieuzależniające fizycznie, o umiarkowanej lub niskiej szkodliwości), którymi są różne odmiany konopi indyjskich. Razem stanowią one niemal trzy czwarte oferty środków psychoaktywnych. Pozostałe kategorie cieszą się znacznie mniejszą popularnością i choć jest ich dużo, to jednak żadna z nich nie przewyższa 10 proc. We wszystkich zbadanych darkmarketach można znaleźć szeroki wybór środków psychoaktywnych, natomiast sklepy pojedynczych dostawców specjalizują się raczej w sprzedaży konkretnych typów narkotyków, na ogół z kategorii „miękkich”.

Niektóre sklepy oferują ciekawą kategorię swoistych „nowości”, czyli środków jeszcze nie zdelegalizowanych, nazywanych w socjolekcie⁴⁰ branży narkotykowej RC's (wym. *are ceez*, ang. *research chemicals*). Desygnaty tego pojęcia zmieniają się w czasie wraz z pojawianiem się nowych środków psychoaktywnych i pracami legislacyjnymi penalizującymi posiadanie oraz wytwarzanie już istniejących substancji. Środki RC's, jako odrębna kategoria, są oferowane tylko w trzech z badanych darkmarketów: Dream Market, Wall Street Market oraz Olympus Market. W Point Marketplace (sklep rosyjski, obecnie już anglojęzyczny) można nabyć tzw. konstruktory, tj. usługę wytwarzania substancji psychoaktywnych na zamówienie (z przyczyn ekonomicznych narkotyki wytwarza się najczęściej na zamówienie). Mogą to być nowe mieszanki i substancje chemiczne bądź wskazana substancja psychoaktywna. W laboratorium gromadzi się tylko tyle prekursorów i odczynników oraz materiałów, aby zrealizować produkcję. W toku badań wyróżniono również ciekawą kategorię enteogenów (wyłączając z niej jednak psylocybinę – ze względu na liczebność oraz kulturowe dziedzictwo tej kategorii), tj. substancji (najczęściej) psychodelicznych wywołujących mistyczne, duchowe doświadczenia, odmienne stany świadomości, często wykorzystywanych w rozmaitych rytuałach szamańskich. Do tej kategorii zalicza się takie rośliny, które łatwo pozyskać samodzielnie – suszone kapelusze muchomorów czerwonych lub szałwię.

Handel pozostałymi medykamentami, które nie mają działania psychoaktywnego, tworzy szary rynek. Dominują wśród nich sterydy anaboliczne, głównie pochodzenia syntetycznego (dziewięć na dziesięć wszystkich ofert w tej kategorii). Dream Market i Wall Street Market oferują wartą odnotowania kategorię substytutów podawanych w leczeniu uzależnień (np. metadonu i buprenorfiny), podczas gdy w innych darkmarketach brakuje ofert tych substancji bądź są one rozproszone wśród innych kategorii.

⁴⁰ Odmiana języka charakterystyczna dla jakiejś grupy społecznej, <https://sjp.pwn.pl/sjp/socjolekt;2575733> (przyp. red.).

Tab. 2. Środki psychoaktywne, inne medykamenty oraz utensylia do produkcji i zażywania narkotyków – liczba i proporcje ofert w darkmarketach.

Typ oferty	Nazwa lub rodzaj	Liczba ofert	Udział ofert w rynku w ramach podgrup (w %) – procentowanie w ramach podgrup (narkotyki vs pozostałe medykamenty)	Udział ofert w całości rynku (w %) – procentowanie do całości (narkotyki, pozostałe medykamenty oraz paraferalia)
Środki psychoaktywne nielegalne i legalne (czarny i szary rynek)	stymulanty/empatogeny	39 174	38,5	36,5
	konopie indyjskie/ THC	33 232	32,6	30,9
	opioidy/opiaty	8036	7,9	7,4
	psychodeliki	7850	7,7	7,2
	substancje psychoaktywne dostępne na receptę	6784	6,6	6,3
	sedatywno-nasenne	4743	4,7	4,4
	dysocjanty	1167	1,1	1,1
	legalne środki psychoaktywne (tzw. RC's)	670	0,6	0,6
	środki psychoaktywne na zamówienie (tzw. konstruktory)	236	0,2	0,2
	enteogeny	8	0,1	0,1
Środki psychoaktywne ogółem		101 900	100,0	94,7
Pozostałe medykamenty bez działania psychoaktywnego (szary rynek)	sterydy	4806	93,2	4,5
	środki na utratę wagi	255	4,9	0,2
	substytuty (<i>harm reduction</i>)	67	1,3	0,1
	środki na potencję	27	0,5	0,1
Pozostałe medykamenty ogółem		5155	100,0 (99,9)	4,9
Paraferalia (wyposażenie laboratoriów i użytkowników)		483	–	0,4
Ogółem ofert		107 538	–	100

Oferta darkmarketów dotycząca środków psychoaktywnych (stymulantów/empatogenów)

Wśród zbiorczej kategorii stymulantów/empatogenów dominują narkotyki okazjonalne, zażywane najczęściej podczas sobotnio-niedzielnych wyjazdów bądź wakacyjnych rozrywek w klubach lub na koncertach. Potocznie są nazywane ecstazy (także pixy, tablety, piguły, dropy, dropsy, pillsy). W mniejszym zakresie występują trzy klasyczne substancje, zdelegalizowane jeszcze w XX w.: kokaina, amfetamina i metamfetamina, a także dwie nowe substancje: nielegalny od początku drugiej dekady XXI w. mefedron oraz – jeszcze legalna w wielu krajach, tania, ale nieprzewidywalna w działaniu – α -PVP, nazywana potocznie flakka lub alfa.

Tab. 3. Środki psychoaktywne – stymulanty/empatogeny.

Nazwa stymulantu/empatogenu	Liczba ofert	Udział ofert w rynku (w %)
MDMA/ecstazy/XTC (3,4-metylenodioksymetamfetamina)	16 741	42,8
Kokaina (metylobenzoilokogonina)	3303	8,4
Amfetamina/speed (α -metylofenetyloamina)	2168	5,5
Metamfetamina/meth (N-metyloamfetamina)	1319	3,4
Mefedron (4-MMC, 4-metylometkatynon)	1036	2,6
Alfa/flakka (α -pirolidynopentiofenon, α -PVP)	826	2,1
Pozostałe niesklasyfikowane stymulanty/empatogeny (m.in. efedryna, MDEA, MDA, MDPV i in.)	13 781	35,2
Ogółem ofert	39 174	100

Oferta darkmarketów dotycząca środków psychoaktywnych (kannabinoidów roślinnych lub syntetycznych)

Jest to druga pod względem popularności grupa substancji obejmująca przede wszystkim związki pochodzenia naturalnego, w mniejszym stopniu zaś – syntetyczne. Na ogół nie są one klasyfikowane, lecz umieszczane w jednej zbiorczej kategorii. Występują w postaci suszu, skunu (liście charakterystycznie zwinięte w kulki), haszyszu (żywica konopi połączona spoiwem), jako olejki haszyszowe, żywność z dodatkiem marihuany (tzw. *edibles*), a nawet wkłady do e-papierosów (do waporyzacji). Dostępne są także nasiona konopi indyjskich oraz syntetycznie wytworzone THC (tetrahydrokannabinol). Charakterystyczne dla tej grupy substancji jest istnienie sklepów (głównie holenderskich, np. DutchDrugz, Dutch Magic, ElHerbolario oraz innych krajów, m.in. CharlieUK) oferujących wyłącznie albo prawie wyłącznie konopie indyjskie w różnych odmianach. Substancje z tej grupy są w zasadzie nielegalne w naszym prawodawstwie (art. 62 kk), z wyjątkiem nasion konopi indyjskich, które nie zawierają substancji aktywnej Delta 9-THC (tetrahydrokannabinolu) w wystarczającym stężeniu, aby zgodnie z literą prawa uznać je za środek psychotropowy.

Tab. 4. Środki psychoaktywne – kannabinoidy roślinne/syntetyczne.

Nazwa kannabinoidu	Liczba ofert	Udział ofert w rynku (w %)
Marihuana (susz, skun)	9171	27,6
Haszysz	1291	3,9
Olejki haszyszowe	1222	3,7
Żywność z dodatkiem marihuany (<i>edibles</i>)	433	1,3
Syntetyczne THC	291	0,9
Nasiona	152	0,4
Niesklasyfikowane lub inne*	20 672	62,2
Ogółem ofert	33 232	100

* W części sklepów te towary pozostały niesklasyfikowane.

Oferta darkmarketów dotycząca środków psychoaktywnych (psychodelików)

Szczegółowej klasyfikacji środków psychoaktywnych dokonali właściciele sześciu z siedemnastu zbadanych marketów (tab. 5). W największym z darkmarketów (Dream Market) posłużono się ogólną kategorią środków psychodelicznych. Wśród odnotowanych środków dominują tzw. narkotyki miękkie – LSD i psylocybina (naturalna i syntetyczna). W obrocie handlowym znajdują się też narkotyki, które obrosły swoistą legendą, na przykład 2C-B, czyli słynna „różowa kokaina”, znana jako: Nexus, Venus, Erox oraz MFR, stworzona w 1974 r. w kalifornijskim laboratorium przez Aleksandra Shulgina⁴¹.

Tab. 5. Środki psychoaktywne – psychodeliki.

Nazwa psychodeliku	Liczba ofert	Udział ofert w rynku (w %)
Niesklasyfikowane lub inne*	5576	71,1
LSD/LSD-25 (dietyloamid kwasu D-lizergowego)	1389	17,7
Psylocybina (4-PO-DMT)	355	4,5
2C-**	294	3,7
NBOM/NBOMe (25C-NBOMe)	211	2,7
Meskalina	25	0,3
Ogółem ofert	7850	100

* W części sklepów te towary pozostały niesklasyfikowane.

** Pochodne 2C-.

⁴¹ Aleksander Shulgin i jego małżonka Anna Shulgin to eksperci w dziedzinie substancji psychoaktywnych. A. Shulgin nie tylko wynalazł wiele z nich, lecz także opisał i sklasyfikował już istniejące substancje psychoaktywne, dostarczając na ich temat unikatowej wiedzy. Zob. np. A. Shulgin, *PiHKAL (Phenethylamines I Have Known And Loved): A chemical love story*, Berkeley 1991; tenże, *TiHKAL (Tryptamines I Have Known and Loved): The continuation*, Berkeley 1997.

Opioidy (w tym opiaty) oraz pozostałe środki rzadko są kategoryzowane. Dokładniejszej klasyfikacji w ramach tej kategorii dokonano zaledwie w dwóch sklepach: Rapture Market i Olympus Market, w których wyodrębniono m.in.: heroinę, kodeinę, morfinę, hydrokodon i oksykodon oraz opium. Również dysocjanty nie są kategoryzowane w większości darkmarketów (zaledwie w czterech) w których wyróżniono takie kategorie, jak ketamina oraz GHB (kwas γ -hydroksymasłowy), potocznie znany jako „narkotyk gwałtu”. Wśród środków sedatywno-nasennych dominują benzodiazepiny, które zostały wydzielone jako odrębna kategoria w sześciu darkmarketach. Rzadziej w ofercie znajdują się barbiturany, incydentalnie wystawia się do sprzedaży alkohol (raczej ekskluzywny, choć nie znaleziono ofert alkoholu zakazanego, jak na przykład absyntu o ponadnormatywnym stężeniu tujonu).

Oferta darkmarketów w zakresie informacji

Obejmuje ona dwie główne kategorie: podręczniki, poradniki i książki stanowiące przytłaczającą większość ofert (66,4 proc.) oraz bazy danych (margines, choć ważny i warty stałego monitorowania – zaledwie 107 ofert. Książki na ogół są sprzedawane w wersji elektronicznej – mogą być to wydania cyfrowe bądź skany publikacji istniejących w formie papierowej, najczęściej w formacie pdf (ang. *portable document format*). Przedmiotem handlu są w przeważającej mierze podręczniki na temat syntezy środków psychoaktywnych, hodowli grzybków halucynogennych i konopi indyjskich. Na przykład w Dream Market rozkłady liczbowe tematyki poszczególnych publikacji są następujące: narkotyki – 597, oszustwa (kategoria określana zbiorczo mianem „sca”, tj. oszustwa polegające na zdobyciu zaufania ofiary, a następnie nadużyciu tego zaufania, np. w jaki sposób korzystać za darmo z przewoźnika Uber, jadać za darmo w McDonald’s, czy otrzymywać za darmo produkty z sieci Walmart) – 3582, hacking – 2035, bezpieczeństwo sieci – 1484. Te oferty plasują się w sferze szarego rynku, polegającego m.in. na obrocie legalnymi publikacjami, jednak ze złamaniem tzw. prawa własności intelektualnej, lub wydawnictwami trzeciobiegowymi, niepublikowanymi według typowych procedur. Wartą odnotowania, choć nieliczną, kategorię stanowią wycieki baz danych, np. w czasie prowadzonych badań na sprzedaż zostały wystawione: baza serwisu zawodowego LinkedIn, a także dane kont serwisu Dropbox oraz Facebooka.

Tab. 6. Oferta darkmarketów – informacje.

Typ towaru	Przynależność towarów do rodzaju rynku	Liczba ofert	Udział ofert w rynku (w %)
Książki i poradniki	szary rynek	40 443	66,4
Bazy danych	czarny rynek	107	0,2
Niesklasyfikowane*	brak jednoznacznej klasyfikacji	20 341	33,4
Ogółem ofert		60 891	100

* W części sklepów te towary pozostały niesklasyfikowane.

Oferta darkmarketów w zakresie oprogramowania i sprzętu komputerowego

Jest to szeroka, zróżnicowana kategoria. Najliczniejszą podklasę stanowią programy i urządzenia służące do popełniania przestępstw o charakterze finansowym, przynależne do czarnego rynku. Można tu znaleźć oferty np. skimmerów, urządzeń w formie nakładek lub wkładek do bankomatów, a także skimmerów umożliwiających skopowanie karty, jeśli choć na chwilę wejdzie się w jej posiadanie. Oprócz urządzeń fizycznych oferta obejmuje oprogramowanie służące łamaniu zabezpieczeń oraz przejęciu kontroli nad urządzeniami zaatakowanej ofiary, a także dokonanie malwersacji finansowych. Ta kategoria jest uzupełniona o przewodniki (jest to świadome zaburzenie klasyfikacji, ponieważ mogłyby się one znaleźć wśród „książek i poradników”). Wymaga ona podjęcia dalszych pogłębionych badań, szczególnie w zakresie szkodliwego oprogramowania oraz skimmingu. Przedmiotem handlu są klucze do oprogramowania użytkowego i gier, a także do płatnych usług online, głównie pornografii (legalnej). Jest to zatem domena szarego rynku. Ofertę informatyczną darkmarketów dopełnia sprzęt i oprogramowanie umożliwiające zachowanie anonimowości w Internecie – tu większość ofert ma charakter legalny, ale są one nabywane w sposób anonimowy, co może – choć nie musi – świadczyć o ich przyszłym przeznaczeniu.

Tab. 7. Oferta darkmarketów – programy i sprzęt komputerowy.

Typ towaru	Przynależność towarów do rodzaju rynku	Liczba ofert	Udział ofert w rynku (w %)
Oprogramowanie, sprzęt i porady (<i>tutoriale</i>) do przestępstw/malwersacji finansowych (<i>botnety/malware/exploity</i>)	czarny rynek (przeważająco)	22611	65,8
Klucze do gier/klucze do oprogramowania użytkowego/pornografia – dostępy	szary rynek	4680	13,6
Sprzęt i oprogramowanie bezpieczeństwa	biały rynek	1252	3,6
Niesklasyfikowane*	brak jednoznacznej klasyfikacji	5855	17,0
Ogółem ofert		34 398	100

* W części sklepów te towary pozostały niesklasyfikowane.

Oferta darkmarketów w zakresie dokumentów

Jest ona różnorodna i niewątpliwie wymaga dalszego, czasochłonnego porządkowania. Przedmiotem obrotu są dokumenty: w wersji papierowej (kradzione, podrobione i nielegalizowane, podrobione i legalizowane) oraz w formie elektronicznej (skany dokumentów). Ogółem stanowią one 41,7 proc. ofert w tej kategorii. Najliczniejszą grupę reprezentują kompletne tożsamości lub informacje dotyczące usług o charakterze

finansowym tj. skradzionych identyfikatorów bankowych, kart bankomatowych, płatniczych, kredytowych oraz portfeli elektronicznych. Mogą one posłużyć do bezpośredniego pozyskania środków finansowych lub dokonywania kolejnych przestępstw o charakterze finansowym albo innych. Tę kategorię uzupełniają anonimowe, zarejestrowane na sprzedawcę karty SIM. Przedmiotem obrotu są także konta, polubienia i subskrypcje w serwisach społecznościowych w powierzchniowym Internecie (Facebook, YouTube, Instagram).

Tab. 8. Oferta darkmarketów – dokumenty.

Typ towaru	Przynależność towarów do rodzaju rynku	Liczba ofert	Udział ofert w rynku (w %)
Falsyfikaty dokumentów	czarny rynek	519	7,9
Dokumenty w sensie fizycznym	czarny rynek	542	8,3
Fizyczne falsyfikaty i kradzione dokumenty	czarny rynek	113	1,7
Skany dokumentów i dokumenty fizyczne	czarny rynek	1381	21,1
Skany dokumentów	czarny rynek	175	2,7
Identyfikatory bankowe/kart bankomatowych/płatniczych/kredytowych, portfele elektroniczne	czarny rynek	2897	44,5
Karty SIM	szary rynek	72	1,1
Konta, polubienia, subskrypcje z serwisów społecznościowych	biały rynek (przeważająco)	472	7,2
Niesklasyfikowane*	brak jednoznacznej klasyfikacji	357	5,5
Ogółem ofert		6528	100

* W części sklepów te towary pozostały niesklasyfikowane.

Oferta darkmarketów dotycząca broni

Dla tego asortymentu oferta jest uboga, zawiera nieco ponad tysiąc propozycji. Przeważa broń automatyczna samopowtarzalna, w większości przypadków – krótka (pistolety). Stwierdzono także obecność ofert broni nieautomatycznej powtarzalnej (strzelby i rewolwery). Sprzedaż broni proponują dwa darkmarkety: włoski Berlusconi Market oraz rosyjska Hydra. Incydentalnie, siedem ofert odnotowano również w Empire Market (wystawiono tam na sprzedaż trzy pistolety oraz pistolet automatyczny UZI w pakiecie z amunicją). Pozostała broń to przedmioty zabronione przez prawodawstwa niektórych państw, a dopuszczane przez prawodawstwa innych (nie traktowane jako broń), jak np.: kubotany, kastety, broń ukryta (np. w laskach, piórach wiecznych), gazy łzawiące, tasery, granaty dymne, a także lasery o dużej mocy i broń biała, w tym noże.

Zaledwie cztery oferty dotyczyły materiałów wybuchowych, wszystkie pochodziły z Berlusconi Market.

Tab. 9. Oferta darkmarketów – broń.

Typ towaru	Przynależność towarów do rodzaju rynku	Liczba ofert	Udział ofert w rynku (w %)
Broń palna	czarny rynek	1004	66,7
Materiały wybuchowe	czarny rynek	4	0,3
Inna broń	brak jednoznacznej klasyfikacji	12	0,8
Niesklasyfikowane*	brak jednoznacznej klasyfikacji	484	32,2
Ogółem ofert		1504	100

* W części sklepów te towary pozostały niesklasyfikowane.

Falsyfikaty dóbr

Darkmarkety oferują przede wszystkim fałszywe metale szlachetne pod różnymi postaciami: kruszców, biżuterii, monet bulionowych, sztabek inwestycyjnych i monet kolekcjonerskich, w tym (w niewielkiej liczbie) historycznych. Ważną kategorię stanowią fałszywe środki płatnicze oraz dobra luksusowe (markowa odzież, zegarki). Te dobra są obecne w niemal wszystkich badanych darkmarketach (wyjątek stanowi Olympus Market oraz sklepy pojedynczych sprzedawców), można je odnaleźć przede wszystkim w Dream Market oraz w Point Marketplace.

Tab. 10. Oferta darkmarketów – falsyfikaty dóbr.

Typ towaru	Przynależność towarów do rodzaju rynku	Liczba ofert	Udział ofert w rynku (w %)
Bilety bankowe	czarny rynek	772	13,9
Elektronika/zegarki	czarny rynek	319	5,8
Odzież	czarny rynek	94	1,7
Kruszce, biżuteria	brak jednoznacznej klasyfikacji	1402	25,3
Niesklasyfikowane*	brak jednoznacznej klasyfikacji	2950	53,3
Ogółem ofert		5537	100

* W części sklepów te towary pozostały niesklasyfikowane.

Usługi

Można tu znaleźć usługi o charakterze programistycznym oraz wsparcie w zakresie konfiguracji programów. Usługi można podzielić tematycznie na: usługi hakerskie (odnoszące się do usług typowo internetowych – od włamań do kont poczty

elektronicznej i serwisów społecznościowych do konfiguracji i programowania botnetów oraz carderskie (związane z nadużyciami w zakresie bankowości elektronicznej). Te dwa typy usług należy zaklasyfikować do czarnego rynku.

Tab. 11. Oferta darkmarketów – usługi.

Typ towaru	Przynależność towarów do rodzaju rynku	Liczba ofert	Udział ofert w rynku (w %)
Usługi hakerskie	czarny rynek	995	15,2
Usługi carderskie	czarny rynek	258	3,9
Programowanie/grafika	brak jednoznacznej klasyfikacji	37	0,6
Niesklasyfikowane*	brak jednoznacznej klasyfikacji	5245	80,3
Ogółem ofert		6535	100

* W części sklepów te towary pozostały niesklasyfikowane.

Inne, wyżej nieujęte oferty

Jest to kategoria obecna wyłącznie w jednym rosyjskim darkmarkecie – Point Marketplace. Można tu znaleźć oferty pracy, w przeważającej części w branży narkotykowej, dotyczące dystrybucji, transportu i wytwarzania narkotyków, a czasem kierowania tymi zespołami na określonym terenie. Zamieszcza się również oferty pracy dla programistów. W subkategorii „reklama” przeważają oferty promocji usług związanych z narkotykami. Jest to zróżnicowany zbiór obejmujący zarówno oferty reklamy BTL⁴² (np. zaprojektowania naklejek, tzw. wlepek, oraz ich dystrybucji na określonym terenie), jak i ATL⁴³ (np. reklamy radiowej, niewykluczone, że zamieszczonej przez dziennikarza radiowego – swoisty *product placement* w audycji radiowej jego autorstwa).

Tab. 12. Oferta darkmarketów – inne, wyżej nieujęte.

Typ towaru	Przynależność towarów do rodzaju rynku	Liczba ofert	Udział ofert w rynku (w %)
Oferty pracy	czarny rynek (przeważająco)	3163	96,5
Reklama	biały rynek, szary rynek	115	3,5
Ogółem ofert		3278	100

* W części sklepów te towary pozostały niesklasyfikowane.

⁴² BTL (ang. *below the line*) – działania reklamowe skierowane do konkretnego klienta, niebędące reklamą w środkach masowego przekazu, za: https://pl.wikipedia.org/wiki/Below_the_line (przyp. red.).

⁴³ ATL (ang. *above the line*) – oznacza strategię działań marketingowych bezpośrednio rozpoznawalnych, prowadzonych w mediach tradycyjnych, za: https://pl.wikipedia.org/wiki/Above_the_line (przyp. red.).

W poszukiwaniu czerwonego rynku

W powyższych zestawieniach usług i towarów oferowanych w darkmarketach zwraca uwagę nieobecność ofert przynależnych czerwonemu rynkowi. Istnienie tego rynku jest jednak niezaprzeczalnym faktem. Oszacowanie rynku płatnych zabójców jest spekulacyjne i przybliżone, ale jest możliwe dokonanie przybliżonego wyliczenia: w pierwszej dekadzie XXI w. w Polsce odsiadywało wyrok około półtorej setki płatnych zabójców. Przyпуска się, że około jedna czwarta zabójstw to były zabójstwa na zlecenie⁴⁴. Jak wskazuje Scott Carney, amerykański dziennikarz śledczy, czerwony rynek jest rozległy i prężny. Przykładem jego funkcjonowania może być kilka udokumentowanych przejawów. Na przykład działalność boliwijskich seryjnych morderców sprzedających europejskim koncernom farmaceutycznym tłuszcz ofiar potrzebny do produkcji luksusowych kremów do twarzy, kradzież dziesiątek tysięcy przysadek mózgowych w Wielkiej Brytanii wykorzystywanych do produkcji hormonu wzrostu (ostatnia dekada ubiegłego wieku), a także zbieranie rogowek palestyńskich bojowników poległych w walce przez izraelskich żołnierzy⁴⁵.

Skalę czerwonego rynku oddaje istniejący od 2013 r. portal Havoscope korzystający ze źródeł typu: weryfikowane doniesienia czytelników, publikacje prasowe i naukowe. Zestawienia zaprezentowano w tabelach 13–14.

Tab. 13. Zestawienie cen zabójstw na zlecenie.

Miejsce, szczegóły	Cena (w dolarach amerykańskich)
Argentyna	3749–5555
Australia	13 610–83 000
Boliwia	4000–15 000
Kolumbia	minimum 600, 2000–4000 za skuteczne wykonanie zadania
Francja, Monako	330 000
Indie, Mombaj	35–900
Włochy (wykonawcy: Mafia Hitman)	3700 (postrzelenie – <i>kneecapping</i>), 27 000 (zabójstwo)
Meksyk, Ciudad Juarez	85 (w nielicznych przypadkach – mniej)
Meksyk (cel: szef policji)	20 382

⁴⁴ Zob. Z Lasocik, *Zabójca zawodowy i na zlecenie*, Kraków 2005; R. Lane, *Murder in America: A history*, Columbus 1997; K. Wójcik, *Mafia na Wybrzeżu*, Warszawa 2016; *Mordercy do wynajęcia*, Newsweek.pl, www.newsweek.pl/polska/mordercy-do-wynajecia,19153,1,1.html [dostęp: 17 IX 2018]. Warto jednak na marginesie odnotować, że w toku postępowania sądowego nie potwierdzono prokuratorskiej hipotezy o istnieniu „klubu płatnych zabójców” w Polsce na przełomie XX i XXI w.

⁴⁵ S. Carney, *Czerwony rynek. Na tropie handlarzy organów, złodziei kości, producentów krwi i porywaczy dzieci*, Wołowiec 2014, s. 29.

Filipiny (wykonawcy: szwadrony śmierci)	110
Hiszpania	27–69 000
USA / Wielka Brytania	od kilkuset do 25 000
USA (za zabójstwo agenta DEA i informatora)	800 000

Źródło: *Global Black Market Information*, <https://www.havocscope.com/black-market-prices/contract-killing/> [dostęp: IX 2018].

Tab. 14. Zestawienie cen w handlu żywym towarem.

„Przedmiot” transakcji	Cena (w dolarach amerykańskich)
Niemowlę w Chinach	7800
Niemowlę w Indonezji	160–250
Dziecko w Ghanie	50 (bezpośrednio od rodzica), 300 (od handlarza)
Dziecko w Indiach	45–350
Dziecko w Mali	600 (jako żołnierz)
Dziecko w Wielkiej Brytanii	25 000
Dziewczynka w Indiach	24
Dziewczynka w Rumunii	3000–6000
Dziewczynka w Bangladeszu	250
Dziewczynka w Kenii	600
Dziewczynka w Mozambiku	2
Dorosły w Kanadzie	4879
Romska „panna młoda”	270 000
Dziewczynka w Iraku	5000 lub 2500
Dziewczynka w Kanadzie	5989
Dziecko w Kambodży	500–800
Dziewczynka w Kolumbii	2600
Kobieta z Północnej Korei	1066 (ok. 20 lat), 761 (ok. 30 lat), 457 (ok. 40 lat)
Żona z Wietnamu (do Chin)	11 800

Źródło: Havoscope, *Human Trafficking: Prices and Statistics of the Modern Day Slave Trade*, <https://www.havocscope.com/black-market-prices/human-trafficking-prices/> [dostęp: IX 2018].

Znikoma obecność usług i produktów czerwonego rynku w Darknecie, pomimo niewątpliwego istnienia tego rynku, wydaje się spowodowana przede wszystkim incydentalnym zapotrzebowaniem na tego typu towary i usługi. Popyt na narządy do przeszczepów, na zniewolonych ludzi czy usługi płatnych zabójców jest rzadkie i niecykliczne, a zatem nieadekwatna wydaje się dla tego rodzaju usług formuła darkmarketowego targowiska jako sposobu ich sprzedaży. Inaczej jest w przypadku

narkotyków – są one nabywane cyklicznie (na potrzeby spotkań towarzyskich) lub regularnie (uzależnienie). Z tego powodu należy się spodziewać, że oferty zaliczane do czerwonego rynku nie będą masowe w ofercie darkmarketów. I tak jest w istocie.

Posługując się przykładem usługi płatnego kwalifikowanego zabójstwa (morderstwa), można rozważyć potencjalne zyski i straty wykorzystania Darknetu jako miejsca oferowania tego rodzaju świadczeń.

- 1. Duże ryzyko zdekonspirowania zleceniodawcy i wykonawcy oraz poniesienia przez nich odpowiedzialności.** Potencjalna dekonspiracja i schwytanie wykonawcy może nastąpić podczas wykonywania usługi zabójstwa na zlecenie. Z kolei zleceniodawcę – niekiedy jednoznacznie – dekonspiruje wybór ofiary. Najprawdopodobniej zleceniodawcą będzie osoba z kręgu rodzinnego, towarzyskiego lub zawodowego, odnosząca stosunkowo duże korzyści ze śmierci ofiary, a jednocześnie dysponująca siłą nabywczą pozwalającą na skorzystanie z usługi. Dodatkowym czynnikiem obciążającym może być wiedza i umiejętności zamawiającego, dzięki którym będzie on miał możliwość skorzystania z usługi w Darknecie (znajomość darkmarketów, umiejętność posługiwania się kryptowalutami). Czyn kwalifikowanego zabójstwa jest obłożony wysokimi karami we wszystkich prawodawstwach, tak więc służby dyspozycyjne będą skłonne monitorować takie usługi, a nawet posługiwać się prowokacją, aby im zapobiegać. Ogłoszenie, które jest stale obecne w Darknecie, potencjalnie stanowi czynnik ryzyka.
- 2. Niski poziom zaufania transakcji.** Im bogatsze doświadczenie wykonawcy, tym łatwiejsza jego identyfikacja na podstawie dowodów, a także tym większy nacisk na jego ściganie przez służby dyspozycyjne. Z kolei z punktu widzenia zleceniodawcy istnieją silne przesłanki, aby publicznie nie potwierdzać dokonanego zlecenia, tym bardziej, jeśli na przykład zabójstwo było pozorowane na samobójstwo lub nieszczęśliwy wypadek. Wykorzystanie mechanizmu rozpowszechnionego w Darknecie, jakim jest transakcja z pomocą „zaufanej trzeciej strony”, jest trudne, a w zasadzie niemożliwe do zrealizowania, ponieważ użytkownik Darknetu uznawany za „zaufaną trzecią stronę” nie podejmie się współudziału w zabójstwie lub porwaniu za niewielką kwotę. Model płatności bezpośredniej to jednocześnie ryzyko oszustwa ze strony zleceniobiorcy. Taki rachunek zysków i strat zdecydowanie utrudnia budowanie kultury zaufania tak potrzebnej dostawcom i odbiorcom korzystającym z darkmarketów.
- 3. Wysokie ceny usług.** Jest to niewątpliwie bariera rozwoju czerwonego rynku. Ceny za dokonanie kwalifikowanego zabójstwa to zazwyczaj kwoty przekraczające kilka tysięcy złotych, a czasami sięgające nawet kilkuset tysięcy złotych. W przypadku handlu narkotykami są to na ogół niewielkie kwoty, nieprzekraczające jednorazowo kilkuset złotych. Dlatego też potencjalne ryzyko związane z wykonaniem usługi jest pomijane, gdyż strata – w wyniku wpadki – nie będzie dotkliwa.

Przytoczona argumentacja wyjaśnia nieopłacalność oferowania usług. Jednocześnie skłania do wniosku, że oferty usług i produktów czerwonego rynku obecne w darkmarketach niekoniecznie są tym, czym się wydają. Analiza treści wykazuje, że oferty czerwonego rynku mogą należeć do jednej z czterech kategorii, którymi są: oszustwo (tzw. *scam*⁴⁶), prowokacja służb dyspozycyjnych, incydentalna, nieprofesjonalna oferta oraz oferty nierozstrzygnięte lub potencjalnie prawdziwe. Do pierwszej i przypuszczalnie drugiej kategorii najprawdopodobniej można zaliczyć ogłoszenia ukazujące się na stronie Besa Mafia – oferty albańskiej mafii dotyczące dokonania morderstw na zlecenie. Wyciek danych z serwisu (między innymi korespondencji) ujawnił, że najprawdopodobniej było to oszustwo: klienci wpłacali zaliczki, administratorzy zaś przestawali odpowiadać na ich wiadomości bądź zapewniali, że kolejny przelew spowoduje realizację usługi. Odnotowano także przypadki, że administratorzy serwisu przesyłali amerykańskiej policji informacje dotyczące zleciodawców zabójstw, do których miało dojść na terenie Stanów Zjednoczonych⁴⁷. Do trzeciej kategorii ofert czerwonego rynku – przestępstw incydentalnych i źle zaplanowanych – należy porwanie brytyjskiej modelki Chloe Ayling w 2017 r. przez Polaka Łukasza Herbę (vel Daniela Zawadę). Do porwania doszło w Mediolanie, gdzie sprawca zorganizował sesję fotograficzną, podczas której odurzył ofiarę za pomocą wstrzykniętej ketaminy i w obszernej walizce przewiózł w bagażniku samochodu do swojej kryjówki w okolicach Turynu. Następnie wystawił modelkę na aukcji w sieci TOR za równowartość 300 tys. euro płatnych w bitcoinach. Żądanie analogicznego okupu otrzymała rodzina i menedżer modelki (według innych źródeł aukcja rozpoczynała się od ceny wywoławczej 150 tys. dolarów). Ostatecznie, po upływie około tygodnia, sprawca uwolnił porwaną. Przewiózł ją do brytyjskiego konsulatu, gdzie został aresztowany. Ł. Herba został skazany na 16 lat i 9 miesięcy pozbawienia wolności (notabene, obrona utrzymywała, że zdarzenie było ustalone pomiędzy stronami i w całości upozorowane, w tle zaś pojawiła się przynależność Ł. Herby do prawdopodobnie istniejącej organizacji o nazwie Czarna Śmierć)⁴⁸. Do ostatniej kategorii – oferty nierozstrzygnięte lub potencjalnie prawdziwe – należy zakwalifikować dwie sprawy: dotyczące nowojorskiego su-

⁴⁶ *Scam* jest definiowany jako oszustwo, którego immanentną cechą jest wzbudzenie czyjegoś zaufania, a następnie wykorzystanie tego faktu.

⁴⁷ *Besa Mafia: Dark Web hitman for hire site takes a hit*, RiskBased Security, <https://www.riskbased-security.com/2016/05/besa-mafia-dark-web-hitman-for-hire-site-takes-a-hit> [dostęp: 13 IX 2018]; A. Haertle, *Jak naprawdę działa serwis zabójców do wynajęcia w darknecie*, „Zaufana trzecia strona”, 15 V 2016 r., <https://zaufanatrzeciastrona.pl/post/jak-naprawde-dziala-serwis-zabojcow-do-wynajecia-w-darknecie/> [dostęp: 13 IX 2018].

⁴⁸ Szerzej na ten temat w doniesieniach prasowych. Zob. A. Haertle, *Porwana modelka wystawiona na aukcji w deep webie za 300 000 EUR w bitcoinach*, „Zaufana Trzecia Strona”, 5 VIII 2017 r., <http://zaufanatrzeciastrona.pl/post/porwana-modelka-w-bitcoinach/> [dostęp: 13 IX 2018]; C. Aliens, *Timeline: British model supposedly kidnapped for darknet auction*, 11 VIII 2017 r., <http://www.deepdotweb.com/2017/08/11/timeline-british-model-supposedly-kidnapped-darknet-auction/> [dostęp: 13 IX 2018].

tenera Froilana Rosado, który w Darknecie oferował usługi nieletnich prostytutek (15–18 lat), oraz porywacza Beniamina Gastona, skazanego na 50 lat więzienia za porwanie, handel żywym towarem oraz przyczynienie się do śmierci jednej ze swoich ofiar⁴⁹.

Zakończenie

Przeprowadzone badania ujawniły obecność rozwiniętego czarnego rynku zogniskowanego na środkach psychoaktywnych i – w mniejszym stopniu – rynku szarego (z elementami czarnego), w którego przypadku przedmiotem obrotu są informacje (bazy danych, książki elektroniczne i poradniki) oraz programy i sprzęt komputerowy, w tym służące do popełniania przestępstw finansowych, a także „pirackie” wersje programów i gier. Obserwacje poczynione przez autora mają charakter wstępnego rozpoznania pola badawczego, które oprócz przybliżenia swego „landszaftu” darkmarketów, ma wyznaczać dalsze obszary i kierunki eksploracji. Wśród przyszłych kierunków badawczych powinny znaleźć się następujące zagadnienia:

- 1. Psychospołeczne aspekty funkcjonowania darkmarketów**, a szczególnie analiza mechanizmów budujących zaufanie i czyniących wymianę handlową możliwą i bezpieczną dla stron⁵⁰. Warto poznać swoiste modus operandi sprzedawców, a także stosowane przez nich techniki, aby unikać dekonspiracji i ponoszenia odpowiedzialności. Istotne wydaje się zbadanie ram etycznych funkcjonowania tego typu giełd. Należałoby je rozpocząć od analizy treści regulaminów darkmarketów, sposobu i zasad rozstrzygnięcia sporów na linii klient–sprzedawca, analizy traktowania osób łamiących regulaminy, przede wszystkim – oszustów. Ważnym wątkiem, jak się wydaje, jest studium społecznych konsekwencji funkcjonowania darkmarketów. Bez wątpienia powstaje rynek nielegalnych środków psychoaktywnych oraz ich dystrybutorów, wzbogacony o zupełnie nowe jakości. Joshua L. Dratel, obrońca Rossa Ulbrichta (założyciela Silk Road – pierwszego darkmarketu w historii),

⁴⁹ Wymienione zdarzenia łączy taki sam sposób ich wykrycia: za pomocą programu Memex opracowanego przez Christophera White’a. Szerzej na temat programu Memex, jego działania i zastosowań w sprawach kryminalnych zob. T. Brewster, *Memex in action: Watch DARPA artificial intelligence search for crime on the „Dark Web”*, „Forbes”, 10 IV 2015 r., <https://www.forbes.com/sites/thomasbrewster/2015/04/10/darpa-memex-search-going-open-source-check-it-out/#f071d152812b> [dostęp: 13 IX 2018]; L. Greenemeier, *Human traffickers, caught on hidden internet*, „Scientific American”, 8 II 2015 r., <https://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-internet/> [dostęp: 13 IX 2018]; W. Shen, *Memex*, <https://www.darpa.mil/program/memex> [dostęp: 13 IX 2018]; B. Spice, *Carnegie Mellon developing online tools to detect and identify sex traffickers*, 13 I 2015 r., <https://www.cmu.edu/news/stories/archives/2015/january/detecting-sex-traffickers.html> [dostęp: 13 IX 2018].

⁵⁰ Incydentalnie tego typu próby badań są podejmowane. Zob. D.S. Zindros, *Trust in decentralized anonymous marketplaces*, Ateny 2014–2015.

wykazał, że istnienie darkmarketów przyczyniło się do zmniejszenia przestępczości związanej z narkotykami i poprawy bezpieczeństwa na ulicach amerykańskich miast⁵¹. W tym celu powołał na świadków przedstawicieli służb dyspozycyjnych. Wnioski sformułowane na potrzeby obrony oskarżonego zostały potwierdzone w raporcie European Monitoring Centre for Drugs and Drug Addiction, którego autorzy wskazują, że sprzedawane produkty są wyższej jakości, sprzedawcy zaś muszą sprostać wyższym standardom w zakresie jakości obsługi i zaufania spowodowanej upublicznieniem w sieci dyskusji o jakości zarówno obsługi, jak i sprzedawanych towarów⁵².

2. **Aspekty ekonomiczne.** Warto przyjrzeć się bliżej poszczególnym kategoriom dóbr i usług oferowanych w darkmarketach, a także spróbować określić zmiany w ich rodzaju i proporcjach zachodzące w czasie, ze szczególnym uwzględnieniem proporcji między poszczególnymi kategoriami ofert oraz między liczbą ofert nielegalnych i legalnych (czarny rynek kontra szary rynek, kontra biały rynek). Interesujące poznawczo wydaje się również studium mechanizmów dokonywania transakcji, regulacji cen oraz używanych kryptowalut.
3. **Aspekty techniczne i organizacyjne.** Należy poznać mechanizmy dystrybucji dóbr, a także techniczno-informatyczną stronę funkcjonowania darkmarketów (zabezpieczenia, problemy techniczne itp.). Jest to istotne w kontekście potencjalnej deanonimizacji kupujących i sprzedających oraz właścicieli platform sprzedażowych. Równie wartościowe poznawczo byłoby odtworzenie sposobów i kanałów dystrybucji poszczególnych dóbr – techniki kamuflowania wysyłanych produktów, a także typowe sposoby ich bezpiecznego odbioru.
4. **Dynamika zmian darkmarketów.** Istotne wydaje się przeanalizowanie trendów rozwojowych darkmarketów i podjęcie próby sformułowania prognoz, a także wyciągnięcie wniosków i ustalenie wzorców modus operandi użytkowników i sprzedawców z jednej strony oraz służb dyspozycyjnych z drugiej. Pierwsi z wymienionych sięgają po wciąż nowe pomysły zabezpieczeń, ci ostatni zaś opracowują coraz bardziej wysublimowane techniki deanonimizacji sprzedających i kupujących. W tym kontekście swoistą miarą przyszłości może być projekt OpenBazaar, eliminujący podstawową słabość darkmarketów, czyli konieczność obecności „zaufanej trzeciej strony” każdej transakcji⁵³.

⁵¹ J.L. Dratel, *Document 251*, 22 V 2015 r., <https://cryptome.org/2015/05/ulbricht-251.pdf>, s. 36 [dostęp: 13 IX 2018].

⁵² *European drug report. Trends and developments*, European Monitoring Centre for Drugs and Drug Addiction, 2016 r., <http://www.emcdda.europa.eu/system/files/publications/2637/TDAT16001ENN.pdf> [dostęp: 13 IX 2018].

⁵³ Więcej na ten temat na stronie projektu: OpenBazaar, <https://openbazaar.org/> [dostęp: 13 IX 2018].

5. Monitorowanie zdarzeń rzadkich, ze szczególnym uwzględnieniem epizodów z zakresu czerwonego rynku, a także próby dotarcia do takich rynków, jeśli one istnieją.

Nasuwają się również uwagi o charakterze metodycznym. Badanie darkmarketów wykracza poza standardowe kompetencje badacza z obszaru nauk społecznych. Konieczne zatem jest opanowanie technik informatycznych co najmniej z zakresu konfiguracji oprogramowania służącego do korzystania z badanych obszarów Internetu oraz kryptografii. Niezbędne jest również poznawanie socjolekty bogatego w pojęcia informatyczne i technologiczne (odnoszące się do usług i towarów będących przedmiotem wymiany), a także specyficznej nomenklatury użytkowników i sprzedawców darkmarketów. Nieodzowne jest swoiste towaroznawstwo (narkotyki, broń, dokumenty, informacje, podrabiane towary) oraz rudymetarna wiedza o popełnieniu typowych oszustw podczas tego typu transakcji. Znaczna liczba ofert darkmarketów oraz ich zróżnicowanie wymagają zastosowania zautomatyzowanej eksploracji za pomocą robotów sieciowych. Problemem metodycznym jest brak możliwości (ocenianej subiektywnie) badania niektórych ofert dotyczących nielegalnych treści, a także realnych sposobów nabywania i dystrybucji towarów. Ponadto jednostki uczestniczące w wymianie handlowej tworzą specyficzne, hermetyczne grupy. Nawiązanie z kimkolwiek kontaktu wymaga więc dużego wysiłku. Powyższe problemy skłaniają do poszukiwania oryginalnej metodyki badania, która jednocześnie będzie spełniać wymogi pracy naukowej, wdrożenia niektórych elementów pracy operacyjnej (np. legendowania), a także zastosowania zautomatyzowanych sposobów pozyskiwania i kategoryzowania danych.

Załącznik 1. Lista darkmarketów (stan na sierpień 2018 r.).

Lp.	Nazwa sklepu (skrót nazwy)	Adres(y) sklepu	Adres forum sklepu	Typ dostępu	Model bezpieczeństwa płatności	Typ waluty	Ranking epdofweb.com	Ranking darknetmarkets.com	Data utworzenia sklepu	Status (sklep zbadany/niezbadany – z podaniem z przyczyny)
1.	Berlusconi Market	http://55j6kjwki4vjtmzp.onion/ http://55j6kjwki4vjtmzp.onion/ http://3m2pyft7fyzjqymu.onion/ http://hky3mzk3jtm4z44.onion/	http://lokwo54utdfvr4r.onion	rejestracja otwarta	Escrow Market/FE-dla zaufanych	bitcoin/monero/litecoin	3,67 (67 recenzji)	3,7 (74,29%) 7 wpisów (26 XI 2017 r.)	7 VII 2017 r.	zbadany
2.	Cannazon	http://cannazon4gbjluus.onion	–	rejestracja otwarta	Multisig or trusted/FE – dla zaufanych	bitcoin/monero	4,13 (15 recenzji)	–	21 III 2018 r.	zbadany
3.	CharlieUK	http://eeyovrly7charuku.onion/	–	rejestracja otwarta	Vendor Shop	–	4,75 (84 recenzje)	3,7 (73,85%) 13 wpisów (28 X 2016 r.)	–	zbadany

4.	Dream Market	http://jd6yhuwcivehvdt4.onion/ http://lchudifyeqm4ldjj.onion/ http://jd6yhuwcivehvdt4.onion/ http://l3e6ly3uoi4zcv2.onion/ http://7ep7acrkunzdcw3l.onion/ http://vilpaqbrmvizecjo.onion/ http://igyirhvxq3sy5.onion/ http://6qlocfg6zq2kyael.onion/ http://x3x2qwb7jasax6tq.onion/ http://bkjcpa2kikkmowwq.onion/ http://xytjqcfendzeby22.onion/	http://tmsk-hzavkyedupbr.onion/	rejestracja otwarta	Escrow Market/FE	bitcoin	4,04 (1707 recenzji)	3,3 (66,88%) 32 wpisy (6 IX 2016 r.)	15 XI 2013 r.	zbadany
5.	Dutch Magic	http://x75csj7vzprjji5v.onion/	–	rejestracja otwarta	Vendor Shop	bitcoin	3,86 (163 recenzje)	–	2012 r.	zbadany
6.	DutchDrugz	http://dutchdr5gsol4dde.onion/	–	rejestracja otwarta	Vendor Shop	bitcoin/ ethereum/ monero/ litecoin/ dash	4,25 (42 recenzje)	–	–	zbadany
7.	ElHerbolario	http://elherbotsiddaroL.onion/	–	rejestracja otwarta	Vendor Shop	bitcoin	3,90 (198 recenzji)	–	–	zbadany
8.	EmpireMarket	http://empiremktx.gov/hm.onion/ref/12186	http://empforumgfttfqmq.onion/	rejestracja otwarta	FE – tyłko dla zaufanych	bitcoin/ monero/ litecoin	–	–	2018 r.	zbadany

9.	GammaGo- blin - Pushing Taboo	http://pushingtabu7itqj.onion	https://dark-netmarkets.co/gammagoblin/gammagoblin-pushing-taboo-custom-payment-2/	rejestracja otwarta	Vendor Shops	bitcoin	4,01 (85 recenzji)	3,3 (66%) 10 wpisów 20 X 2016 r.	-	zbadany
10.	Hydra	http://wayawaytel3k66fl.onion/	-	rejestracja otwarta	-	bitcoin	4,14 (73 recenzje)	4,2 (84,56%) 79 wpisów 28 XII 2016 r.	-	zbadany
11.	Olympus Market	http://xc7oyzq4cz3ki7sa.onion/signup/MATQP3	http://olptial-kpybezjlhx.onion/	rejestracja otwarta	Multisig or trusted/FE częściowo możliwe	bitcoin/ monero	3,85 (26 recenzji)	-	1 I 2018 r.	zbadany
12.	QualityKing	http://quality2ui4uooy.m.onion	-	zamknięty	Vendor Shop	bitcoin	3,19 (18 recenzji)	-	-	zbadany
13.	Rapture Ma- kret	http://rtexijfqcndum5v.onion/	-	rejestracja otwarta	Multisig or trusted/FE – tylko zaufani sprzedawcy	bitcoin/ monero	4,11 (23 recenzje)	-	18 I 2018 r.	zbadany
14.	RechardSport	http://rechardsp4x6tdrh.onion/	-	rejestracja otwarta	Vendor Shop	-	4,06 (9 recenzji)	-	-	niezbadany – spoza grupy docelowej – falsyfikaty dóbr, sklep jest w Internecie powierzchnio- wym

15.	RuTOR	http://rutorzmmfllzk5.onion/ http://pointgg34ghbo2s.onion/auth/register/563636d36a-b740e4720f44e8328441d3 http://mlotvmf5wjmovl57.onion/auth/register/563636d36a-b740e4720f44e8328441d3 http://dw5f7gf7lkwvekj3.onion/auth/register/563636d36a-b740e4720f44e8328441d3 http://zo7o7hksuj7laxo.onion/auth/register/563636d36a-b740e4720f44e8328441d3 http://q3ckokmc4ha5en6m.onion/auth/register/563636d36a-b740e4720f44e8328441d3 http://qfc5pxlr5f6e4wg3.onion/auth/register/563636d36a-b740e4720f44e8328441d3 http://tochka3evlj3sxdv.onion/auth/register/563636d36a-b740e4720f44e8328441d3	-	rejestracja otwarta	-	-	2,67 (6 recenzji)	3,5 (70%) 4 wpisy 5 XII 2016 r.	-	niezbadany – spoza grupy docelowej, forum z możliwością handlu
16.	T•chka (obecnie: Point Market- place)	http://q3ckokmc4ha5en6m.onion/auth/register/563636d36a-b740e4720f44e8328441d3 http://qfc5pxlr5f6e4wg3.onion/auth/register/563636d36a-b740e4720f44e8328441d3 http://tochka3evlj3sxdv.onion/auth/register/563636d36a-b740e4720f44e8328441d3	-	rejestracja otwarta	Multisig or trusted/FE	3,78 (165 recenzji)	-	30 I 2015 r.	zbadany	
17.	The Cannabis Growers and Merchants Cooperative (CGMC)	http://cgmcoopwhempo6a5.onion/ http://joinegmc5soplano.onion/	-	wyłącznie na zaproszenie	Multisig or trusted	4,69 (68 recenzji)	-	7 VI 2016 r.	niezbadany – tylko na zaproszenie	

18.	The Church (JOR)	http://artsmankindxgcv5.onion/	–	rejestracja otwarta	Vendor Shop	bitcoin	3,33 (3 recenzje)	–	zbadany
19.	The French Connection	http://abyssopyps3z4xof.onion/	–	rejestracja otwarta	Vendor Shop	bitcoin	3,61 (98 recenzji)	4,3 (86,29%) 105 wpisów 18 X 2016 r.	zbadany
20.	The Majestic Garden	http://talismanrestz7mr.onion/	http://talismanrestz7mr.onion/	generowanie klucza	Escrow Market/FE	–	3,50 (13 recenzji)	4,0 (80%) 5 wpisów 25 X 2016 r.	niezbadany – konieczny klucz
21.	ToYouTeam	http://tybeta57rw2onit.onion/	–	zamknięty	Vendor Shop	–	3,85 (15 recenzji)	–	niezbadany – brak połączenia podczas trwania badania
22.	Wall Street Market	http://wallst4qihu6lvs.a.onion/	http://x7bwsm-core5fmx56.onion/	rejestracja otwarta	Multisig or trusted/FE-lv3	bitcoin/ monero	4,23 (162 recenzje)	3,5 (70,91%) 11 wpisów 21 XII 2016 r.	zbadany
23.	WayAway	http://wayawaytcl3k66fl.onion/	–	na zaproszenie	–	–	4,39 (19 recenzji)	3,0 (60%) 2 wpisy 11 XII 2016 r.	niezbadany – spoza grupy docelowej

Źródło: Opracowanie własne autora.

Załącznik 2. Środki psychoaktywne – potentaci Darknetu.

Kategoria	Nazwa darkmarketu (w kolejności najczęściej odwiedzanych)	Udział w rynku narkotykowym (w proc. liczonych od liczby ofert w danej kategorii)
Środki psychoaktywne ogółem	1. Dream Market	56,8
	2. Olympus Market	19,5
	3. Hydra	11,1
	4. Wall Street Market	4,3
	5. Berlusconi Market	4,2
Kannabinoidy	1. Dream Market	57,3
	2. Olympus Market	16,4
	3. Hydra	13,0
Stymulanty/empatogeny	1. Dream Market	52,0
	2. Olympus Market	24,2
	3. Hydra	14,8
Psychodeliki	1. Dream Market	62,4
	2. Olympus Market	17,8
	3. Hydra	8,7

Bibliografia

- Aldridge J., Décary-Héту D., *Not An 'ebay For Drugs': The Cryptomarket 'Silk Road' as A Paradigm Shifting Criminal Innovation*, 2014, <http://ssrn.com/abstract=2436643> [dostęp: 4 VIII 2018].
- Aliens C., *Timeline: British model supposedly kidnapped for darknet auction*, 11 VIII 2017 r., <https://www.deepdotweb.com/2017/08/11/timeline-british-model-supposedly-kidnaped-darknet-auction/> [13 IX 2018].
- Anonymity Bibliography*, <https://www.freehaven.net/anonbib/full/date.html> [dostęp: 4 V 2019].
- Berelson B., *Content analysis in communication research*, Glencoe 1952, The Free Press.
- Besa Mafia: Dark Web hitman for hire site takes a hit*, RiskBased Security, <https://www.riskbasedsecurity.com/2016/05/besa-mafia-dark-web-hitman-for-hire-site-takes-a-hit/> [dostęp: 13 IX 2018].
- Bhaskar V., Linacre R., Machin S., *The economic functioning of online drug markets*, „Journal of Economic Behavior Organization” 2019, nr 159, s. 426–441.
- Biddle P. i in., *The Darknet and the Future of Content Distribution*, Levine’s Working Paper Archive, <https://ideas.repec.org/p/cla/levarc/618897000000000636.html> [dostęp: 4 V 2019].
- Brewster T., *Memex In Action: Watch DARPA Artificial Intelligence Search For Crime On The „Dark Web”*, „Forbes”, 10 IV 2015 r., <https://www.forbes.com/sites/thomas->

brewster/2015/04/10/darpa-memex-search-going-open-source-check-it-out/#f071d152812b [dostęp: 13 IX 2018].

Broséus J. i in., *Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective*, „Forensic Science International” 2016, t. 264, także: https://www.researchgate.net/publication/297627993_Studying_illicit_drug_trafficking_on_Darknet_markets_Structure_and_organisation_from_a_Canadian_perspective [dostęp: 4 IV 2019].

Carney S., *Czerwony rynek. Na tropie handlarzy organów, złodziei kości, producentów krwi i porywaczy dzieci*, Wołowiec 2014, Wydawnictwo Czarne.

Chabinsky S.R., *Congressional Testimony*, 17 X 2009 r., <https://web.archive.org/web/20100412172853/http://www.fbi.gov/congress/congress09/chabinsky111709.htm> [dostęp: 1 VIII 2018].

Chabinsky S.R., *Major Executive Speeches*, 23 III 2010 r., <https://web.archive.org/web/20161227043937/https://www2.fbi.gov/pressrel/speeches/chabinsky032310.htm> [dostęp: 1 VIII 2018].

Chmielecka J., *Po ciemnej stronie internetu*, Wyborcza.pl, „Duży Format”, 30 I 2013 r., http://wyborcza.pl/duzyformat/1,127290,13318724,Po_ciemnej_stronie_internetu.html [dostęp: 1 VIII 2018].

Ciancaglini V. i in., *Deepweb and Cybercrime. It's Not All About TOR*, A Trend Micro Research Paper, <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf> [dostęp: 12 IX 2018].

Cohen S., *Folk devils and moral panics*, London–New York 2011, Routledge.

Décary-Héту D., Giommo L., *Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous*, Springer, Dordrecht 2016, <http://www.gwern.net/docs/sr/2016-decaryhetu.pdf>. [dostęp: 13 IX 2018].

Dratel J.L., *Document 251*, <https://cryptome.org/2015/05/ulbricht-251.pdf> [dostęp: 13 IX 2018].

Drugs and the darknet: Perspectives for enforcement, research and policy, Luksemburg 2017, European Monitoring Centre for Drugs and Drug Addiction and Europol, Publications Office of the European Union; a także: <https://www.emcdda.europa.eu/system/files/publications/6585/TD0417834ENN.pdf> [dostęp: 13 IX 2018].

Egger C. i in., *Practical Attacks Against The I2P Network*, 2013 r., <http://www.cip.cs.fau.de/~spjsschl/i2p.pdf> [dostęp: 1 VIII 2018].

European drug report. Trends and developments, European Monitoring Centre for Drugs and Drug Addiction, 2016 r., <http://www.emcdda.europa.eu/system/files/publications/2637/TDAT16001ENN.pdf> [dostęp: 13 IX 2018].

- Global Black Market Information*, <https://www.havocscope.com/black-market-prices/contract-killing/> [dostęp: 13 IX 2018].
- Greenemeier L., *Human traffickers, caught on hidden internet*, „Scientific American”, 8 II 2015 r., <https://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-internet/> [dostęp: 13 IX 2018].
- Haertle A., *Jak naprawdę działa serwis zabójców do wynajęcia w darknecie*, „Zaufana trzecia strona”, 15 V 2016 r., <https://zaufanatrzeciastrona.pl/post/jak-naprawde-dziala-serwis-zabojcow-do-wynajecia-w-darknecie/> [dostęp: 13 IX 2018].
- Haertle A., *Porwana modelka wystawiona na aukcji w deep webie za 300 000 EUR w bitcoinach*, „Zaufana Trzecia Strona”, 5 VIII 2017 r., <https://zaufanatrzeciastrona.pl/post/porwana-modelka-wystawiona-na-aukcji-w-deep-webie-za-300-000-eur-w-bitcoinach/> [dostęp: 13 IX 2018].
- Henderson L., *TOR and the dark art of anonymity*, [b.m.w.] 2015, CreateSpace Independent Publishing Platform.
- Human Trafficking: Prices and Statistics of the Modern Day Slave Trade*, <https://www.havocscope.com/black-market-prices/human-trafficking-prices/> [dostęp: IX 2018].
- Jolly Roger's security guide for beginners*, <https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/> [dostęp: 4 I 2018].
- Konkin III S.E., *New Libertarian Manifesto*, <http://agorism.info/docs/NewLibertarianManifesto.pdf> [dostęp: 13 VII 2018].
- Krippendorff K., *Models of messages: three prototypes*, w: *The analysis of communication content*, G. Gerbner i in. (red.), New York 1969, Wiley.
- Lane R., *Murder in America: A History*, Columbus 1997, Ohio State University Press.
- Lasocik Z., *Zabójca zawodowy i na zlecenie*, Kraków 2005, Zakamycze.
- Liu F., Maitlis S., *Nonparticipant Observation*, w: *Encyclopedia of Case Study Research*, A.J. Mills, G. Durepos, E. Wiebe (red.), Thousand Oaks 2010, Fairfield University.
- Malik N., *Terror in the Dark. How Terrorists Use Encryption. The Darknet and Cryptocurrencies*, Millibank 2018, The Henry Jackson Society.
- Malinowski B., *Argonauci zachodniego Pacyfiku. Relacje o poczynaniach i przygodach krajozców z Nowej Gwinei*, Warszawa 1981, PWN.
- Markoff J., *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry*, New York 2005, Penguin Group.
- Mazur K.M., *Polskojęzyczna społeczność przestępcza zorganizowana w sieci darknet*, Poznań 2016, nakładem własnym autora.

- Messinger A.M., *Teaching Content Analysis through Harry Potter*, „Teaching Sociology” 2012, nr 4, s. 360–367.
- Mider D., *Mappa Mundi ukrytego Internetu. Próba kategoryzacji kanałów komunikacji i treści*, „EduAkcja. Magazyn edukacji elektronicznej” 2015, nr 2, s. 55–70.
- Mordercy do wynajęcia*, Newsweek.pl, www.newsweek.pl/polska/mordercy-do-wynajecia,19153,1,1.html [dostęp: 17 IX 2018].
- Mounteney J., Bo A., Oteo A., *The internet and drug markets*, Luksemburg 2016, European Monitoring Centre for Drugs and Drug Addiction.
- Organiser of Darkmarket fraud website jailed*, „The Guardian”, 26 II 2010 r., <https://www.theguardian.com/technology/2010/jan/14/darkmarket-online-fraud-trial-we> [dostęp: 1 VIII 2018].
- Paoli G.P. i in., *Behind the curtain. The illicit trade of firearms, explosives and ammunition on the dark web*, Santa Monica 2017, RAND Corporation, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf.
- Rush H. i in., Tang P., *Crime Online: Cybercrime and Illegal Innovation*, 2009, <http://eprints.brighton.ac.uk/5800/> [dostęp: 4 VIII 2018].
- Sharma S., *Relationship between e-commerce and business*, „International Journal of Research & Development in Technology and Management Science – Kailash” 2014, nr 5, s. 17–28.
- Shen W., *Memex*, <https://www.darpa.mil/program/memex> [dostęp: 13 IX 2018].
- Shulgin A., *PiHKAL (Phenethylamines I Have Known And Loved): A chemical love story*, Berkeley 1991, Transform Press.
- Shulgin A., *TiHKAL (Tryptamines I Have Known and Loved): The Continuation*, Berkeley 1997, Transform Press.
- Soska K., Christin N., *Measuring the Longitudinal Evolution of Online Anonymous Marketplace Ecosystem*, Proceedings of the 24th USENIX Security Symposium, 2015, <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf> [dostęp: 13 IX 2018].
- Spice B., *Carnegie Mellon developing online tools to detect and identify sex traffickers*, Carnegie, 13 I 2015 r., Mellon University, <https://www.cmu.edu/news/stories/archives/2015/january/detecting-sex-traffickers.html> [dostęp: 13 IX 2018].
- Świdorski B., *Najciemniejszy zakątek internetu naprawdę istnieje. Ukryta sieć TOR: „Lewe” papiery, pedofilia, przekrety i narkotyki*, 21 IX 2012 r., <https://natemat.pl/32267,najciemniejszy-zakatek-internetu-naprawde-istnieje-ukryta-siec-tor-lewe-papiery-pedofilia-przekrety-i-narkotyki> [dostęp: 1 VIII 2018].

Webb E.J. i in., *Nonreactive Measures in the Social Sciences*, Dallas 1981, Houghton Mifflin.

Webb E.J. i in., *Unobtrusive Measures: nonreactive Research in the Social Sciences*, Chicago 1966, Rand McNally.

Wójcik K., *Mafia na Wybrzeżu*, Warszawa 2016, MUZA.

Zindros D.S., *Trust in decentralized anonymous marketplaces*, Athens 2014–2015, National Technical University of Athens.

Źródła internetowe

I2P, <https://geti2p.net/>.

Daniel Onion Link List, <http://onionsnjajzkhm5g.onion>.

Darknet Markets, <https://darknetmarkets.co>.

Deep.Dot.Web, <http://deepdot35wvmeyd5.onion>.

Freenet, <https://freenetproject.org/author/freenet-project-inc.html>.

Kryptoanarchizm, <http://kryptoanarchizm.liberatrianizm.net>.

OpenBazaar, <https://openbazaar.org/>.

The Hub, <http://thehub7xbw4dc5r2.onion>.

The Uncensored Hidden Wiki, http://gxamjbnu7uknahng.onion/wiki/index.php/Main_Page.

TOR Metrics, <https://metrics.torproject.org/>.

TOR, <https://www.torproject.org/>.

Zeronet, <https://zeronet.io/>.

Abstrakt

Artykuł prezentuje wyniki obserwacji nieuczestniczącej ukrytej targowisk (tzw. darkmarketów) w sieci The Onion Router (TOR). Przedstawiono realny potencjał darkmarketów, które są przedmiotem obrotu gospodarczego, wskazując rodzaje produktów i usług nielegalnych oraz proporcje ich udziału w rynku. Obserwację prowadzono w sierpniu 2018 r. Zidentyfikowano dynamiczny czarny rynek środków psychoaktywnych zażywanych incydentalnie (towarzysko), wśród których są obecne stymulanty, empatogeny oraz kanabinoidy. Oferta czarnego rynku obejmuje także inne środki psychoaktywne, przede wszystkim opioidy (opiaty), psychodeliki, środki sedatywno-nasenne i dysocjanty.

Na czarny rynek składa się również oferta kradzionych baz danych, oprogramowanie i sprzęt służące do informatycznych malwersacji finansowych, nielegalne dokumenty (kradzione i podrabiane), a także falsyfikaty (biletów bankowych, odzieży, elektroniki, kruszców), broń palna i materiały wybuchowe. Natomiast obecność czerwonego rynku ma charakter przypadkowy i niejednoznaczny (porwania, zabójstwa na zlecenie).

Słowa kluczowe: cyberzagrożenia, Darknet, darkmarkety, kontrekononomia, The Onion Router.

Abstract

The article presents the results of the non-participation hidden observation of market-places (the so-called “darkmarkets”) in The Onion Router. The real potential of darkmarkets was measured: the proportions and types of illegal content, products and services traded. The observation was carried out in August 2018. A dynamic black market of psychoactive substances used incidentally (socially), as stimulants/empatogens and cannabinoids was identified. The offer of the black market also includes other psychoactive substances, above all opioids / opiates, psychedelics, sedatives, and dissociatives. The black market also includes the offer of stolen databases, software and hardware used for financial embezzlements, illegal documents (stolen and counterfeit), as well as counterfeits of banknotes, clothing, electronics, gold), also firearms and explosives. In turn, the presence of the red market is accidental and ambiguous (abductions, contract killings).

Keywords: cyber threats, Darknet, darkmarkets, counter-economy, The Onion Router.