doi: 10.35757/KiS.2024.68.3.4

KULTURA i SPOŁECZEŃSTWO

POLSKA AKADEMIA NAUK
KOMITET SOCJOLOGII
INSTYTUT STUDIÓW POLITYCZNYCH
2024, nr 3

ISSN 0023-5172
2300-195x

A R T Y K U Ł Y I R O Z P R A W Y

ZBIGNIEW OSIŃSKI
Uniwersytet Marii Curie-Skłodowskiej w Lublinie

KULTUROWE ASPEKTY DARK WEB
PRZEGLĄD BADAŃ

WPROWADZENIE

Od ponad dwudziestu lat rozwijany jest obszar internetu nazywany „dark web". Terminem tym określa się sieci (np. TOR — The Onion Router, Freenet, I2P — Invisible Internet Project, Zeronet), w których cały ruch sieciowy jest w dużym stopniu anonimowy i kryptograficznie ukryty. Anonimowość jest istotnym czynnikiem przyciągającym użytkowników. Funkcjonowanie dark web opiera się na sieci komputerów (ruterów zwanych węzłami lub serwerami pośredniczącymi) należących do rozsianych po całym świecie osób prywatnych i na algorytmach, które kierują komunikację internetową użytkowników przez serię serwerów pośredniczących. Zasoby dark web nie są indeksowane przez powszechnie wykorzystywane wyszukiwarki (np. Google i Bing), nie pojawiają się zatem w wynikach wyszukiwania. Dla znaczącej części użytkowników internetu są więc niedostępne. W literaturze funkcjonuje też węższy znaczeniowo termin „dark net", obejmujący anonimowe węzły, typu komputery, serwery, rutery, połączone w techniczną sieć umożliwiającą funkcjonowanie zasobów, narzędzi i usług dark web (Finklea 2022; Hatta 2020).

Adres do korespondencji: zbigniew.osinski@mail.umcs.pl; ORCID: 0000-0003-4484-7265

Istnienie takiego obszaru internetu, który zapewnia użytkownikom duży poziom anonimowości, przyciąga tych, dla których anonimowość jest przydatna lub nawet niezbędna. Ogół wspomnianych zachowań, role przyjmowane przez użytkowników dark web, głoszone przez nich poglądy, normy i wartości funkcjonujące w tym środowisku, specyficzne kody kulturowe, tworzone grupy i sieci powiązań, stosowana terminologia, a także role pełnione przez samą sieć dark web, stanowią potencjalnie interesujące i ważne pole badań. W związku z tym pojawia się pytanie, czy badacze to pole eksplorują, jakimi aspektami funkcjonowania dark web się interesują, jakie metody i narzędzia badawcze stosują, jakie wnioski wysnuwają? Czy badania dark web wykraczają poza aspekty informatyczne i kryminalistyczne, czy pojawiły się badania kulturowych aspektów funkcjonowania tej części internetu? Na takie pytania odpowiedź może przynieść badanie literatury naukowej.

Wyjaśnienie, czym są aspekty kulturowe dark web, można oprzeć na tych definicjach, które pojęcie „kultura" wiążą z internetem. Przydatne będzie pojęcie „kultura internetu" wprowadzone przez socjologa Manuela Castellsa. W jego ujęciu na kulturę internetu składają się cztery warstwy: kultura techno-merytokratyczna (usprawnianie internetu, uznanie zasady otwartego oprogramowania i sieciowej współpracy), kultura hakerska (kreatywność technologiczna oparta na wolności, współpracy, zasadzie wzajemności i nieformalności, otwartym dzieleniu się kodem źródłowym), kultura wirtualno-komunitariańska (organizowanie zasad życia społecznego w przestrzeni internetowej, rozwijanie ruchów kontrkulturowych oraz alternatywnych środowisk) oraz kultura przedsiębiorczości (zarabianie w sieci). Opisując kulturę internetu, Castells (2003) wprowadził rozróżnienie na użytkowników-twórców oraz użytkowników-konsumentów. Kolejny przydatny terminem to „kultura uczestnictwa". Wprowadził go Henry Jenkins, który ocenił, że internet jest środowiskiem wyzwalającym synergię ludzi współpracujących na różne sposoby dla realizacji różnych celów. Kultura uczestnictwa w środowisku sieciowym według Jenkinsa (2006) polega na zacieraniu się granicy między producentem a konsumentem dóbr kultury. Jednym z wielu przykładów kultury uczestnictwa może być zmiana modelu dziennikarstwa. Dzięki narzędziom takim jak blogi i kanały YouTube każdy użytkownik sieci może stać się dziennikarzem relacjonującym wydarzenia czy publicystą dzielącym się swoimi przemyśleniami.

Bazując na powyższych definicjach, uznaję, że kulturowe aspekty dark web obejmują: funkcjonowanie w tej części internetu różnorodnych grup i społeczności, aktywne i pasywne role przyjmowane przez użytkowników

dark web, formy współpracy pomiędzy nimi, głoszone przez nich poglądy, przyjmowane normy i wartości, specyficzne kody kulturowe, zachowania, obyczaje, aktywność w zakresie tworzenia zasobów i udoskonalania rozwiązań technologicznych, a także motywacje generujące różne formy aktywności.

CELE I METODY BADAŃ

Głównym celem artykułu jest przegląd badań dotyczących kulturowych aspektów dark web. Prowadzenie badań oraz wiązanie ich wyników z istniejącą wiedzą jest podstawą funkcjonowania każdej dyscypliny naukowej. Znajomość dotychczasowego stanu badań jest więc koniecznością. Jednakże obserwowany od kilku dziesięcioleci gwałtowny przyrost liczby publikacji stwarza poważną trudność, zwłaszcza w przypadku zagadnień multi- i interdyscyplinarnych. Dlatego też przegląd literatury, potraktowany jako cel, a zarazem metoda badawcza, staje się bardziej istotny niż kiedykolwiek. Dobrze przeprowadzony przegląd, który można ogólnie opisać jako mniej lub bardziej systematyczny sposób syntezy wcześniejszych badań, tworzy solidne podstawy do pogłębiania wiedzy i rozwoju teorii. Jest także doskonałym sposobem syntezy wyników badań w celu odkrycia obszarów, w których potrzebne są dalsze badania, co jest kluczowym elementem tworzenia ram teoretycznych i budowania modeli koncepcyjnych (Snyder 2019).

Zostanie tu zastosowany półsystematyczny przegląd literatury, bowiem takie podejście pozwala na przegląd multi- lub interdyscyplinarnego obszaru badawczego. Podejście półsystematyczne z zasady jest przeznaczone dla zagadnień, które zostały skonceptualizowane w różny sposób i zbadane przez różne grupy badaczy w różnych dyscyplinach, co utrudnia systematyczny proces przeglądu. Tego rodzaju przegląd ma na celu zidentyfikowanie i zrozumienie potencjalnie istotnych podejść badawczych, które mają wpływ na badany temat. Do analizy i syntezy wyników przeglądu półsystematycznego można wykorzystać jakościową analizę tematyczną i jakościową analizę treści, które to techniki pozwalają na identyfikację i analizę perspektyw teoretycznych, wspólnych problemów, prawidłowości i tendencji występujących w zbiorze tekstów naukowych (Snyder 2019).

Przyjmujący podejście półsystematyczne badacz może odejść od dokładności i metodologicznego rygoryzmu przeglądu systematycznego, jednakże w zamian musi opracować własne standardy i szczegółowy plan, aby zapewnić wykorzystanie kompletnego zbioru odpowiedniej literatury i z naukową pewnością odpowiedzieć na swoje pytanie badawcze, jed-

nocześnie zachowując przejrzystość procesu badawczego. Ważne jest dokładne ustalenie, która literatura zostanie wybrana do przeglądu i w jaki sposób — muszą istnieć logiczne i ważne motywy. W zależności od tych decyzji badanie może zakończyć się bardzo różnymi odpowiedziami i wnioskami na te same pytania badawcze (Tranfield, Denyer, Smart 2003; Wong i in. 2013).

Jako źródło danych bibliograficznych do przeglądu badań została wybrana baza Scopus, która ma charakter międzynarodowy i multidyscyplinarny. Zrezygnowano z bazy Web of Science, ponieważ przy identycznych kryteriach wyszukiwania dostarczyła blisko trzy razy mniej rekordów bibliograficznych. Zastosowano następujące kryteria wyszukiwania: Search documents — „dark web"; Search within — article title, abstract, keywords; Document type — article, conference paper, book chapter, book; Subject area: Social Sciences, Arts and Humanities, Psychology (zastosowane zawężenie miało na celu pominięcie publikacji dotyczących głównie kwestii informatycznych lub prawno-kryminalnych); Year — 2016–2023 (wcześniej rocznie ukazywały się tylko pojedyncze prace). W ten sposób uzyskano 208 rekordów bibliograficznych (stan w grudniu 2023 r.). Następnie przeanalizowano tytuły oraz słowa kluczowe i abstrakty celem wybrania publikacji, których treść przynajmniej częściowo dotyczy kulturowych aspektów funkcjonowania dark web. W ten sposób wyselekcjonowano 56 publikacji. Lektura tych tekstów pozwoliła na dodanie kolejnych 15 prac umieszczonych w bibliografiach artykułów z pierwszej grupy. Wzięto pod uwagę te pozycje z bibliografii, które poświęcone były dowolnym aspektom kulturowych aspektów dark web.

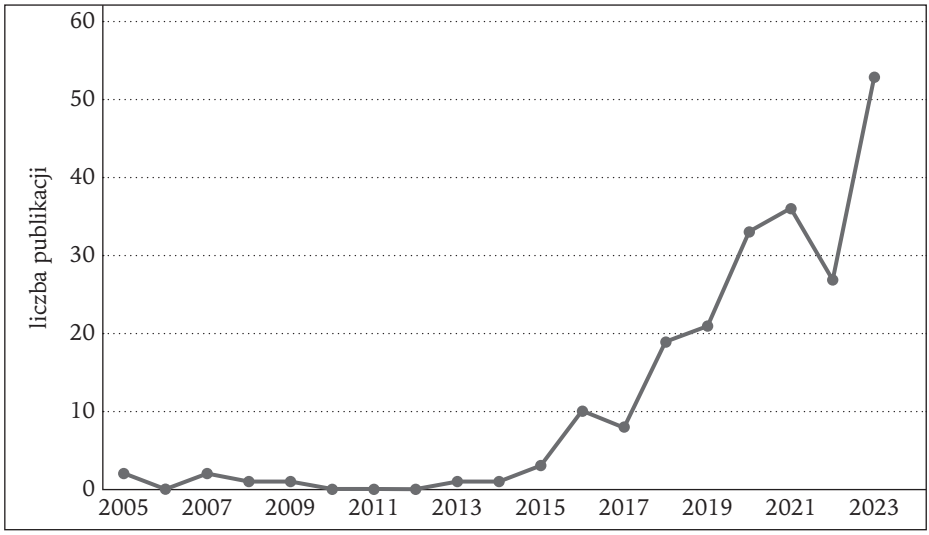
WYNIKI

Badania dark web wychodzące poza kwestie informatyczne lub prawno-kryminalistyczne mają stosunkowo krótką historię. Pierwsze publikacje, pośród teksów indeksowanych w bazie Scopus, pojawiły się dopiero w roku 2005 (wykres 1). W dalszym ciągu jest to niszowa sfera badań, z liczbą publikacji indeksowanych we wspomnianej bazie na poziomie kilkudziesięciu rocznie.

Jeżeli nie ograniczymy wyników wyszukiwania do określonych dziedzin nauki, to uzyskamy 707 rekordów bibliograficznych. Jednakże zdecydowana większość z nich zaklasyfikowa jest do dziedzin, w których badań o charakterze kulturoznawczym nie prowadzi się: Computer Science, Engineering i Mathematics (wykres 2). Po zastosowaniu ograniczenia wyników do dziedzin, w których mogą pojawić się badania kulturowych aspektów

Wykres 1

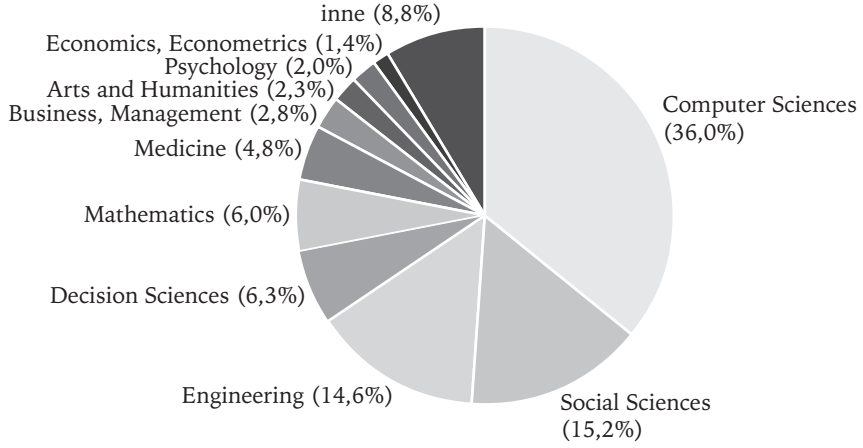
Przyrost liczby publikacji dotyczących dark web
(zaliczonych do: Social Sciences, Arts and Humanities, Psychology)



Źródło: badania własne.

Wykres 2

Przynależność dziedzinowa publikacji wykazanych po zastosowaniu terminu „dark web"
(wg bazy Scopus)



Źródło: badania własne.

dark web, otrzymano 208 rekordów, a po weryfikacji treści i uzupełnieniu o nowe prace, o czym już wspomniano, do badań przyjęto 71 publikacji.

W grupie zakwalifikowanych do badań tekstów można wyróżnić kilka nurtów tematycznych, które mają związek z zakresem terminu „aspekty kulturowe". Są to następujące grupy zagadnień:

- motywacje użytkowników dark web do korzystania z tej części internetu,
- wpływ istnienia dark web i zapewnionej tam anonimowości na zachowania ludzi,
- specyfika aktywności handlowej w dark web,
- działania podejmowane przez prowadzących nielegalny handel w celu poprawy reputacji i pozyskania zaufania klientów,
- praktyki komunikacyjne na forach dyskusyjnych,
- wolność rozpowszechniania informacji.

(1) Motywacje użytkowników dark web do korzystania z tej części internetu. Internauci korzystający z zasobów i usług dostępnych w dark web, czyli w sieciach o złej reputacji, zwłaszcza wśród prawników, przedstawicieli organów ścigania, a nawet wielu badaczy, kierują się różnymi motywami, nie zawsze o charakterze nielegalnym i przestępczym. Jednym z ważnych powodów jest potrzeba anonimowości i wolności wypowiedzi. Dark web zapewnia bowiem możliwość nieskrępowanej wymiany informacji i poglądów bez obawy późniejszych reperkusji. Pozwala również na w miarę bezpieczne prowadzenie działalności sprzecznej z prawem.

Dla użytkowników dark web istotna jest anonimowość. Badacze zidentyfikowali występowanie odczucia satysfakcji z anonimowych interakcji online, zwłaszcza w sytuacji bezpiecznego kupowania i sprzedawania nielegalnych towarów i usług (Bancroft, Reid 2017).

Znawcy społeczności uczestniczących w handlu narkotykami sugerują, że w przekonaniu tych społeczności serwisy pośredniczące w takim handlu ułatwiają doświadczanie wolności osobistej w libertariańskich ramach filozoficznych. Zamiast angażować się w publiczny aktywizm przeciwko narkotykowej prohibicji, co byłoby sprzeczne z potrzebą ukrycia swojej tożsamości, wolą zanurzyć się w permisywnej rzeczywistości cyfrowej charakterystycznej dla dark web. Ich motywacją do korzystania z tej części internetu jest także możliwość wykorzystywania środowiska internetowego jako środka do budowania nowego świata, w którym zrealizują swoje idee towarzyszące konsumpcji narkotyków (Maddox i in. 2016).

Mieszkańców państw, w których stosuje się cenzurę internetu, do korzystania z dark web motywuje szansa na omijanie jej barier w trakcie

realizacji swoich potrzeb informacyjnych, zdobywania wiedzy oraz poznawania nowych technologii (Chen i in. 2024). Badacze wskazują też na istnienie potrzeby korzystania z technologii zapewniających anonimowość w celu wyrażania własnych poglądów politycznych i podejmowania działań w wysoce represyjnych reżimach (Jardine 2018).

Kolejnymi motywacjami do korzystania z dark web są postawy antyszczepionkowe, niski poziom zaufania do instytucji publicznych, a także samotność młodych mężczyzn. Dark web dla tych grup staje się miejscem poszukiwania osób o podobnych poglądach i w podobnej sytuacji oraz wiedzy zgodnej z ich postrzeganiem świata (Sirola i in. 2022).

Ogólnie rzecz biorąc, motywujące do aktywności w dark web są działanie poza kontrolą społeczeństwa i władzy oraz swoboda decydowania o swoich działaniach bez obawy przed represjami (Mirea, Wang, Jung 2019).

(2) Wpływ istnienia dark web i zapewnionej tam anonimowości na zachowania ludzi. Najliczniejsza grupa publikacji naukowych, spośród wybranych do badania, dotyczy wpływu istnienia dark web i anonimowości oferowanej przez te sieci na działania podejmowane przez różne grupy użytkowników internetu.

Dla autorów najnowszych przeglądów badań (Handalage, Prasanga 2021; Ofusori, Hendradi 2023) głównym skutkiem istnienia dark web jest wzrost cyberprzestępczości. Według Adriana Crawleya (2016) istotnym powodem takiego stanu rzeczy jest anonimowość, dzięki której każdy, kto chce i ma nawet niezbyt wyspecjalizowane kompetencje, może zaangażować się w działania przestępcze o stosunkowo niskim ryzyku wykrycia i ukarania. Ira Winkler i Araceli Gomes wyróżnili w tej części internetu nie tylko działania przestępcze, lecz także legalne. Do drugiej grupy zaliczyli: aktywność tzw. sygnalistów zgłaszających społeczności internetowej lub dziennikarzom nieprawidłowości w funkcjonowaniu firm, instytucji, urzędników i polityków; działania dziennikarzy z państw stosujących cenzurę, którzy dzielą się swoimi publikacjami; komunikację służb specjalnych ze swoimi agentami. Do aktywności przestępczej zaliczyli: nielegalny handel (narkotykami, bronią, lekarstwami, kryptowalutami, danymi, dokumentami, pornografią dziecięcą, oprogramowaniem hakerskim); nielegalne usługi (wynajmowanie hakerów, morderców); łamanie praw autorskich poprzez udostępnianie plików objętych tymi prawami, a także udostępnianie nielegalnych treści (głównie pornografii dziecięcej) (Winkler, Gomes 2017).

Autorzy innego przeglądu badań (Gupta, Maynard, Ahmad 2019) ustalili, że badacze problematyki dark web wyróżniają następujące role spo-

łeczne tej części internetu: rynek — handlu narkotykami, szkodliwym oprogramowaniem, kartami kredytowymi i identyfikacyjnymi, pornografią dziecięcą, bronią; platforma komunikacyjna — fora i czaty; miejsce zamawiania nielegalnych usług — hakerskich, terrorystycznych; źródło informacji o zagrożeniach wykorzystywane przez służby specjalne; zbiór narzędzi umożliwiających nielegalne transakcje; sposób na omijanie ograniczeń i blokad cenzorskich oraz na unikanie prześladowań ze strony władz.

Według Antoniego Krauza (2017) anonimowe korzystanie z sieci pozwala między innymi: chronić prywatność; uniemożliwiać identyfikację lokalizacji użytkownika zamieszczającego w sieci treści nielegalne; przeglądać strony blokowane przez cenzurę; działać służbom zajmującym się zwalczaniem cyberprzestępczości bez obawy, że zostaną wykryte przez przestępców; działać dziennikarzom bez cenzury państwa i obawy o własne bezpieczeństwo oraz w bezpieczny sposób komunikować się z informatorami; przesyłać treści między państwami bez obawy, że zostaną zablokowane; zwiększać bezpieczeństwo pracowników wywiadu; koordynować działania grup przestępczych.

Wielu badaczy zajmowało się różnymi szczegółowymi aspektami wykorzystywania dark web, która zapewniania anonimowość i ukryte usługi. Lev Topor (2022) badał społeczności neonazistowskie działające na anonimowych platformach komunikacyjnych. Ustalił, że w takich grupach rozprzestrzeniają się i kwitną nienawiść i teorie spiskowe oraz że ich uczestnicy często się radykalizują. Z kolei Nenad Denic i Sasa Devetak (2023) wykazali, że dark web jest platformą dla operacji psychologicznych i informacyjnych, rozpowszechniania propagandy, indoktrynacji online, rekrutacji i mobilizacji trolli, a także wirtualnego szkolenia, planowania i koordynacji operacji cybernetycznych w okresie zaburzeń wywołanych pandemią COVID-19 i wojną w Ukrainie. Badania Erica Jardine'a pozwoliły zidentyfikować ważną rolę dark web w rozpowszechnianiu treści bardzo krytycznych wobec firm, celebrytów, władz oraz systemów politycznych, a także niemieszczących się w ramach poprawności politycznej lub zaliczanych do mowy nienawiści. Wspomniane treści początkowo rozpowszechniane są w internecie dostępnym powszechnie. Następnie, na skutek interwencji firm, instytucji państwa, a nawet pojedynczych osób, są usuwane przez administratorów publikujących je serwisów. W takiej sytuacji niektórzy autorzy usuniętych treści publikują je ponownie, tym razem w dark web, skąd niejednokrotnie powracają do internetu powierzchniowego (Jardine 2019).

Innym nurtem badania zachowań użytkowników dark web jest poznawanie trudno dostępnych populacji przestępców. Zajmujący się ter-

roryzmem Gabriel Weimann ustalił, że istnieje wiele sposobów, w jakie terroryści wykorzystują dark web do realizacji swoich celów. Obejmują one wojnę psychologiczną i propagandę, zbieranie funduszy, rekrutację, eksplorację danych i koordynację działań. Użytkownicy tego rodzaju publikują w dark web materiały opisujące szczegółowo ich akcje. Przyjmują darowizny w bitcoinach, które następnie wykorzystują do zakupu broni na „czarnym rynku" w dark web (Weimann 2016a, 2016b).

Innym typem drastycznej przestępczości rozwijającej się dzięki anonimowości w dark web jest pedofilia. Badacze odkryli szereg charakterystycznych cech zachowań w sieci, które wskazują na to, że konkretne osoby aktywne w dark web (kryjące się pod nickami niemającymi nic wspólnego ze sferą seksualności) mogą być podejrzane o pedofilię. Osoby takie na forach i czatach dyskutują nie tylko o swoich doświadczeniach seksualnych. Rozmawiają też o różnych technikach aktów seksualnych, o zachowaniach seksualnych o charakterze dewiacyjnym, o etapach rozwoju seksualnego dzieci, o okaleczaniu narządów płciowych, a także o zasadach bezpieczeństwa i anonimowości chroniących przed zidentyfikowaniem danej osoby przez organy ścigania. Wypowiedzi mają cechy akceptacji dla pedofilii, a także dla sadyzmu, zoofilii i kazirodztwa. Autorzy takich postów podważają szkodliwość seksualnego wykorzystywania nieletnich. Część postów ma charakter instruktażu — jak znaleźć ofiary i jak nawiązać z nimi interakcje online i offline, jak od strony informatycznej zapewnić sobie pole do takich kontaktów, jakie stosować środki bezpieczeństwa i jak zachować anonimowość oraz gdzie wyszukiwać materiały pedofilskie (Woodhams in. 2021).

(3) Specyfika aktywności handlowej w dark web. Uwagę wielu badaczy przyciągnęła kwestia wpływu specyfiki dark web na działania o charakterze handlowym. Wymiana handlowa w tej sieci odbywa się na specjalnych platformach internetowych („ciemne rynki") i obejmuje głównie narkotyki, kryptowaluty, broń, podrobione lub skradzione dokumenty, nielegalnie pozyskane zbiory informacji, leki, pornografię dziecięcą oraz oprogramowanie i usługi hakerskie. Towar (z wyjątkiem tego, który ma postać cyfrową) wysyłany jest pocztą, a płatności dokonywane są kryptowalutami. Zarówno kupujący, jak i sprzedający muszą posiadać konto poczty elektronicznej na jednym z anonimowych serwerów w dark web, konto na konkretnej platformie handlowej oraz cyfrowy portfel kryptowalut (specjalna aplikacja). Według Roderica Broadhursta i in. (2017) kluczowe dla rozwoju handlu w dark web było pojawienie się kryptowalut, takich jak bitcoin, które pozwalają na niemal anonimową wymianę pieniędzy. Ta zdecentralizowana i rozproszona forma waluty istniejącej poza

systemem bankowym uzupełnia anonimowy charakter dark web, umożliwiając finansowanie operacji handlowych bez przypisywania im źródła pieniędzy. Funkcjonalności dostępne w portfelach kryptowalut utrudniają śledzenie wpłat i wypłat z poszczególnych portfeli cyfrowych oraz powiązanie ich z konkretnymi transakcjami.

James Martin (2023) zauważył pojawienie się na „ciemnych rynkach" dark web zjawiska zwanego gentryfikacją — rewitalizacją i unowocześnianiem procesu handlu. Zjawisko to wynika z preferencji administratorów witryn, sprzedawców i klientów, które w połączeniu z różnymi rozwiązaniami technologicznymi zachęcają do uczciwych praktyk handlowych, także w handlu nielegalnym. Jednocześnie karzą tych, którzy łamią zasady rynkowe i normy społeczne preferowane przez administratorów i klientów „ciemnych rynków". Okazuje się, że unikalne cechy strukturalne „ciemnych rynków", które obejmują opinie i oceny użytkowników, systemy rozstrzygania sporów oraz „policję" administratorów, a także internetowe fora dyskusyjne, pomagają we wspieraniu norm bezpieczeństwa i uczciwości handlujących. Wnioski te uwiarygodniają pogląd, że przemoc i niepewność, nieodłącznie związane z wieloma formami nielegalnego handlu w realnej rzeczywistości, w świecie online mogą zostać złagodzone, gdy groźba wykluczenia z tego czy innego „ciemnego rynku" narzuca konieczność przestrzegania zasad uczciwej wymiany. Martin twierdzi, iż istnieje coraz więcej dowodów sugerujących, że dostawców nielegalnych towarów i kryptowalut oraz ich klientów przyciąga do dark web przeświadczenie o zwiększonym bezpieczeństwie transakcji, a także o skutecznym działaniu norm rynkowych i procesów instytucjonalnych, które charakteryzują się uczciwością, szacunkiem i uprzejmym zaangażowaniem.

Jedna z grup badających handel w dark web (Booij i in. 2021) opracowała charakterystykę dominujących modeli karier sprzedawców działających w „ciemnych rynkach". Nieustanna walka między administratorami tych rynków a organami ścigania sprawia, że typowa żywotność nielegalnego rynku wynosi dwa lata. Kiedy rynek znika, aktywni sprzedawcy migrują na inne rynki z zamiarem kontynuowania działalności. Aby chronić swoją reputację na różnych rynkach, niektórzy próbują zachować ten sam pseudonim, ale inne osoby mogą ich uprzedzić. Znacznie bezpieczniejszą metodą jest zatem wygenerowanie klucza PGP (Pretty Good Privacy — narzędzie służące do szyfrowania, odszyfrowywania i uwierzytelniania między innymi poczty elektronicznej, plików, katalogów, a także kont w nielegalnym handlu) i użycie klucza publicznego jako identyfikacji na różnych rynkach. Okazuje się, że średnio 80% karier trwa zaledwie cztery miesiące i generuje bardzo małą sprzedaż. Tylko niewielka grupa (2%) dostawców ma długą

i nieprzerwaną karierę, która trwa latami i obejmuje wiele rynków. Wyróżniono wiec trzy typy karier: pozycja ugruntowana (wspomniane 2%), pretendenci (usiłujący podbić rynek) oraz kariery nieudane (wspomniane 80%).

(4) Działania podejmowane przez nielegalnych handarzy w celu poprawy reputacji i pozyskania zaufania klientów. Kluczowym aspektem funkcjonowania nielegalnego handlu w dark web jest reputacja sprzedawcy. Wynika to z faktu, że na „ciemnych rynkach" brak jest takich gwarancji prawnych i instytucjonalnych dla kupujących, jakie występują w handlu legalnym (prawo do odstąpienia, płatność przy odbiorze, gwarancja, rękojmia itp.). Brak mechanizmów egzekwowania odpowiedzialności w razie niedojścia transakcji do skutku lub innych problemów. Za to dominuje anonimowość, zarówno sprzedających, jak i kupujących. Obie strony muszą ustalić *ex ante*, czy po drugiej stronie nie czeka na nich policjant lub oszust. Robert A. Hardy i Julia R. Norgaard (2016) sugerują, że mechanizmy sprzężenia zwrotnego, w tym rabaty promocyjne (np. bezpłatna wysyłka), reklama i reputacja sprzedawcy, znacząco wpływają na wybory dokonywane przez kupujących. Te mechanizmy stworzyły nieformalne ramy instytucjonalne, wewnątrz których uczestnicy wymiany handlowej działają, kierując się zaufaniem i reputacją, czyli jedynymi czynnikami utrzymującymi funkcjonowanie rynku bez regulacji rządowych.

Budowaniu zaufania i reputacji służą funkcjonalności „ciemnych rynków", takie jak profile użytkowników i fora dyskusyjne, na których można umieszczać oceny, komentarze i opinie o transakcjach oraz o kupujących i sprzedających. Badacze ustalili, że istnieje wyraźny wpływ ocen formułowanych przez kupujących po zakończonych transakcjach na sukces biznesowy sprzedawców (Przepiorka, Norbutas, Corten 2017). W przypadku usług hakerskich mówi się nawet o istnieniu na forach dyskusyjnych specyficznego systemu wymiaru sprawiedliwości, który może zniszczyć karierę niekompetentnego i nieskutecznego hakera (Choi, Lee 2023). Niektóre badania sugerują, że bardzo istotnym czynnikiem budowy zaufania jest możliwość skontaktowania się ze sprzedawcą, który obok swojej oferty zamieszcza adres konta e-mail na jednym z serwerów pocztowych funkcjonujących w dark web. Oczywiście samo podanie adresu nie jest wystarczające. Zaufanie budzi bowiem jedynie ten sprzedawca, który szybko reaguje na zapytania i udziela wyczerpujących odpowiedzi (Foust i in. 2017).

Można spotkać się z opiniami, że budowaniu zaufania służy także technologia. Nathalie Nahai ustaliła, że ludzie dokonują podświadomych osądów na temat stron internetowych, kierując się „wskazówkami zaufania" uwarunkowanymi tym, jak zaprojektowana jest witryna (obecność nazwy

i logo, symetria stron, strona z FAQ, listy produktów i możliwość utworzenia konta). W związku z tym administratorzy serwisów w dark web, zarówno tych, które pełnią rolę rynku handlowego, jak i tych mających charakter forów dyskusyjnych, dbają o taki ich kształt, który buduje pozytywne odczucia u użytkowników (Nahai 2017). Innym rozwiązaniem służącym budowie zaufania są systemy depozytów kryptowalut. Zamawiający towar/usługę przesyła należną kwotę do takiego depozytu, a sprzedawca dostaje ją na swoje konto dopiero po potwierdzeniu, że towar dodarł do kupującego lub że usługa została wykonana (Laferrière, Décary-Hétu 2023).

Z kolei Kim Moeller (2023) pisze o trzech wymiarach zaufania w dark web: zaufanie procesowe, które wywodzi się z powtarzających się transakcji ze znanymi partnerami; zaufanie oparte na postaciach, mierzone reputacją danej osoby w sieci; zaufanie instytucjonalne do platformy i jej administratorów.

(5) P r a k t y k i k o m u n i k a c y j n e na forach dyskusyjnych. Zachowania użytkowników dark web analizowane są także na podstawie badania postów. Uczestnicy dyskusji w dark web wykazują potrzebę skutecznego komunikowania się z innymi osobami, jednocześnie chroniąc swoją prywatność. Obie potrzeby mogą naraz zrealizować jedynie na forach i czatach funkcjonujących w „ciemnej" części internetu.

Według Roberta W. Gehla (2016) serwisy dark web, które umożliwiają prowadzenie dyskusji, podobnie jak analogiczne serwisy w internecie powierzchniowym, charakteryzują się zarówno praktykami władzy — w postaci inwigilacji przez administratorów, algorytmicznej regulacji działań użytkowników oraz ograniczeń programistycznych i infrastrukturalnych, jak i wolnością — w postaci treści tworzonej przez użytkowników oraz rozwoju nowych, spontanicznych form społeczności online. Od uczestników dyskusji wymaga się zachowania anonimowości, dlatego na forach i w serwisach dark web nie występują zjawiska znane na przykład z Facebooka — nawiązywanie relacji w ramach kręgu koleżeńskiego, miejscowości lub miejsca pracy, chwalenie się zdjęciami z wakacji, wybudowanym domem, awansem, podwyżką itp. Polityka prywatności w dark web wymaga, aby dyskutanci nie ujawniali jakichkolwiek danych osobowych ani innych pozwalających na identyfikację. Jednocześnie administratorzy narzucają, tak jak na Facebooku, reguły wypowiadania się i udostępniania materiałów. Niektóre fora i serwisy nie pozwalają na reklamę nielegalnej działalności handlowej lub usługowej prowadzonej w dark web ani na zamieszczenie nielegalnych materiałów typu pornografia dziecięca. Gehl dostrzegł, że w tego typu miejscach dominuje technoelitaryzm, czyli dyskusje o kodowaniu, hakowaniu, inwigilowaniu, programach komputerowych i prowa-

dzeniu pirackich rozgłośni radiowych. Częstym zjawiskiem jest udzielanie porad technicznych i informatycznych.

Z kolei Hussein Alnabulsi i Rafiqul Islam (2018) odkryli, że na większości forów dominują dyskusje na temat narkotyków, piractwa, hakerstwa, przemocy i fałszywych dokumentów, czyli działalności nielegalnej. Konstatację taką potwierdziły także najnowsze badania. Fora zostały zdominowane przez działania nielegalne i nieetyczne, w szczególności przez nielegalny handel narkotykami i cyberprzemoc. Duża aktywność związana z narkotykami sugeruje, że fora w dark web działają jako substytut nielegalnych rynków. Pojawiły się tam również nielegalne treści, takie jak informacje związane z oszustwami, kradzieżą tożsamości i sprzedażą fałszywych dokumentów tożsamości oraz hakowaniem, a także różne rozmowy o przestępstwach (Hiramoto, Tsuchiya 2024).

Osoby zainteresowane hakerstwem i handlem najczęściej uczestniczą w wielu społecznościach internetowych, są bowiem zainteresowane zebraniem jak największej liczby informacji. Użytkownicy odgrywający na poszczególnych forach centralną rolę wykazują tendencję do przyjaznego dzielenia się wiedzą z nowymi członkami danego forum. Badacze dostrzegli też, że osoby odgrywające role moderatorów i technicznych guru wyraźnie wpływają na opinie i poglądy użytkowników niedoświadczonych w danej problematyce (Pete i in. 2020).

Na forach poświęconych „ciemnemu handlowi" i kryptowalutom badacze (Chen, Meng, Wang 2023) zaobserwowali, że większość dyskusji obraca się wokół zasad handlu w dark web i tematów zorientowanych na początkujących, takich jak porady o skutecznym przeprowadzeniu zakupów, jak używać bitcoina oraz jak korzystać z usługi Escrow (rachunek powierniczy, który przeznaczony jest do gromadzenia środków i prowadzenia rozliczeń pomiędzy konkretnymi, określonymi w umowie partnerami handlowymi). Ma to zapewnić bezpieczeństwo zawartych transakcji. Ustalili też, że na badanych forach nie obserwuje się pojawiania się przywództwa i dominacji w dyskusji. Co więcej, użytkownicy, którzy angażują się w większą liczbę dyskusji i używają słownictwa o szerszym zakresie, są bardziej skłonni do rezygnacji z udziału w forum. Najprawdopodobniej tracą motywację po zrealizowaniu celu, dla którego pojawili się na danym forum. Można też przyjąć, że gdy skumulowane ryzyko odkrycia tożsamości i późniejszych konsekwencji przeważa nad przewidywanymi korzyściami, użytkownicy są skłonni do podjęcia trudnej decyzji o całkowitym opuszczeniu społeczności.

Inni badacze (Baele, Brace, Coan 2021) doszli do wniosku, że przynajmniej na kilku forach dyskusyjnych rozwija się subkultura białej supre-

macji oraz antysemityzmu. Analizując zamieszczane tam posty, dostrzegli proces systematycznej radykalizacji postaw uczestników. Badane środowisko charakteryzuje się trójpoziomową strukturą, zarówno pod względem gradacji skrajności poglądów wyrażanych na forach, jak i popularności poszczególnych forów. Subkultura ta podzieliła się na kilka odrębnych, ale nakładających się na siebie skrajnie prawicowych podkultur. Przeprowadzona analiza wykazała, że najbardziej popularne wśród osób głoszących supremację białej rasy i antysemityzm jest najmniej radykalne forum 4chan. Z kolei najbardziej radykalne poglądy pojawiają się na forach najmniej popularnych i znanych.

(6) Wolność rozpowszechniania informacji. Mechanizmy dostępne w dark web (fora dyskusyjne, anonimowa poczta elektroniczna) wykorzystywane są także do zwiększania poziomu bezpieczeństwa w trakcie korzystania z wolności słowa. Przykładem takiego zjawiska jest przekazywanie informacji dziennikarzom, gdy informator ma podstawy do obawy o własne bezpieczeństwo. W takich kontaktach informatorzy ukrywają swoją tożsamość, identyfikując się wyłącznie nickiem oraz wykorzystując jeden z wielu dostępnych w dark web serwerów anonimowej poczty elektronicznej. Badacze zaobserwowali zjawisko zwane *whistle-blowing*, czyli działanie polegające na ujawnianiu rządowych lub firmowych niejawnych informacji. Uczestnicy tego procederu twierdzą, że opinia publiczna ma prawo być informowana także o tajnych, pozaprawnych lub wstydliwych działaniach zarówno rządów, jak i dużych firm (Mirea, Wang, Jung 2019).

W kontekście problematyki wolności słowa w dark web istotna jest praca, w której Michael Chertoff (2017) przypomniał cele stworzenia szczególnych sieci składających się na tę część internetu. Ich twórcy wskazują na przydatność tego typu rozwiązań między innymi dla opozycji politycznej i obrońców praw człowieka w krajach totalitarnych, mogących dzięki nim uzyskać anonimowy, czyli bezpieczny, dostęp do internetu powierzchniowego, który jest monitorowany przez służby specjalne. Zdecentralizowana struktura wspomnianych sieci chroni zawarte w nich zasoby przed ingerencją władz, które nie mogą danych serwerów wyłączyć ani ocenzurować zawartych w nich treści. Twórcy dark web twierdzą, że swoboda wymiany informacji i pomysłów, wyrażania poglądów, opinii i ocen jest fundamentem demokracji i praw człowieka. Przekonują, że przyświecał im szczytny cel, jakim jest ochrona wolności internetu i prywatności użytkowników. Służą temu serwisy z kolekcjami e-booków o treści zwalczanej przez niektóre rządy, stworzone dla dziennikarzy strony ułatwiające nawiązywanie kontaktów z sygnalistami i rozpowszechnianie materiałów

niedopuszczanych przez władze, a także fora dyskusyjne, na których panuje swoboda wymiany poglądów. Chertoff ocenił, że w dużej mierze dzięki istnieniu dark web rozwinęły się takie zjawiska jak wspomniany już *whistle-blowing* oraz haktywizm. Drugie z wymienionych zjawisk polega na aktywności hakerskiej o charakterze pozytywnym. Hakerzy odnajdują luki w oprogramowaniu komputerowym i wskazują je twórcom tychże programów, by je naprawili. Ponadto wyszukują serwisy udostępniające pornografię dziecięcą i przeprowadzają na nie ataki celem uniemożliwienia działania. W obu przypadkach wykorzystanie dark web pozwala hakerom uniknąć problemów prawnych (Chertoff 2017).

PODSUMOWANIE

Badania różnych aspektów funkcjonowania dark web prowadzą głównie przedstawiciele informatyki, nauk inżynieryjnych i matematyki. Dotyczą one kwestii technicznych, technologicznych i programistycznych o charakterze specjalistycznym. Druga dominująca grupa badań obejmuje kwestie prawne i kryminalistyczne. Taka tematyka realizowana jest przez badaczy funkcjonujących w ramach nauk prawnych oraz nauk o bezpieczeństwie. Publikacje tej grupy sprowadzają się głównie do szczegółowych analiz prawnych i kryminalistycznych konkretnych zasobów i działań w dark web.

Kulturowe aspekty dark web to niszowa sfera badań, z historią zaledwie kilkunastoletnią oraz z liczbą publikacji indeksowanych w bazie Scopus na poziomie kilkudziesięciu rocznie, autorstwa przedstawicieli ekonomii, nauk o zarządzaniu, psychologii, socjologii, kulturoznawstwa, a także nauk o mediach i komunikacji. Zajmują się oni badaniami, których tematykę można podzielić na kilka grup wyróżnionych ze względu to, że dotyczą podobnych aspektów aktywności ludzkiej.

W ramach pierwszej z nich badacze starają się odpowiedzieć na pytanie, d l a c z e g o niektórzy ludzie k o r z y s t a j ą z z a s o b ó w i u s ł u g dostępnych w dark web, czyli w sieciach kojarzących się z przestępczością? Ustalono, że często występującą motywacją jest anonimowość zapewniająca względne bezpieczeństwo przy popełnianiu przestępstw. Ważną motywacją jest także chęć komunikowania się bez ograniczeń cenzuralnych i bez ryzyka represji ze strony totalitarnych reżimów. Ogólnie rzecz biorąc, motywujące do aktywności w dark web jest działanie poza kontrolą społeczeństwa i władzy oraz swoboda decydowania o swoich działaniach bez obawy przed represjami.

Jeżeli chodzi o kwestie motywacji do korzystania z dark web, to można wskazać istotny problem wart objęcia systematycznymi badaniami. Jest

nim wykorzystywanie tej części internetu w celu ugruntowania i potwierdzenia swojej tożsamości i poglądów. Ludzie często angażują się w różnego rodzaju społeczności internetowe, takie jak fora dyskusyjne, grupy na mediach społecznościowych czy blogi. Poprzez udział w tych społecznościach mogą potwierdzać swoje przekonania, dzielić się doświadczeniami i wymieniać poglądy z innymi. Jednakże nie wszystkie poglądy i tożsamości znajdują swoje miejsce w internecie widzialnym. Cała gama treści bywa blokowana i usuwana z mediów społecznościowych i innych serwisów. Dotyczy to przede wszystkim poglądów kwalifikowanych jako mowa nienawiści, łamanie poprawności politycznej, radykalna prawicowość, antysemityzm, biała supremacja czy nawet (w niektórych państwach) opozycyjność wobec reżimów totalitarnych. Zwolennicy tego typu poglądów szukają potwierdzenia swojej tożsamości i możliwości wyrażania swoich racji między innymi w dark web. Dlatego też zasadny wydaje się postulat rozwoju badań tego aspektu aktywności ludzkiej.

Druga grupa badań poświęcona jest analizie rodzajów aktywności użytkowników dark web uwarunkowanych anonimowością. Badacze w większym stopniu zajmują się aktywnością przestępczą, a w znacznie mniejszym aktywnością legalną (przynajmniej w państwach demokratycznych). Prawdopodobnie jest to związane z dominującym w publikacjach naukowych przekonaniem, że głównym skutkiem istnienia dark web jest wzrost cyberprzestępczości. Dlatego też najczęściej badane są takie zachowania jak: nielegalny handel i usługi, tworzenie społeczności pedofilskiej, łamanie praw autorskich, werbunek i indoktrynacja realizowane przez grupy terrorystyczne oraz udostępnianie nielegalnych treści (głównie pornografii dziecięcej). Stosunkowo nieliczne są publikacje poświęcone badaniu takich problemów jak: aktywność tzw. sygnalistów, działania dziennikarzy z państw stosujących cenzurę, rozpowszechnianie poglądów zaliczanych do radykalnych, pozyskiwanie wiedzy niedostępnej ze względu na ograniczenia cenzuralne. Także ten obszar badawczy można objąć postulatem rozwoju systematycznych badań.

Do trzeciej grupy można zaliczyć publikacje poświęcone specyfice nielegalnego handlu w środowisku cyfrowym. Ustalono, że takie kontakty handlowe odbywają się na specjalnych platformach internetowych („ciemne rynki"), a ich przedmiotem są głównie narkotyki, kryptowaluty, broń, podrobione lub skradzione dokumenty, nielegalnie pozyskane zbiory informacji, leki, pornografia dziecięca oraz oprogramowanie i usługi hakerskie. Fundamentem rozwoju handlu w dark web są kryptowaluty, takie jak bitcoin, które pozwalają na niemal anonimowe płacenie. Mechanizmy „ciemnych rynków" zachęcają do uczciwych praktyk

handlowych (także w handlu nielegalnym), a jednocześnie karzą tych, którzy łamią zasady i normy społeczne preferowane przez administratorów i klientów. Okazuje się, że o sukces w handlu na dark web jest niezwykle trudno. Pozycję ugruntowaną, czyli obecność na rynku dłuższą niż kilka miesięcy, zdobywa jedynie około 2% handlujących.

Sukces sprzedających i kupujących uwarunkowany jest między innymi zdobyciem odpowiedniej reputacji i zaufania w realiach anonimowości obu stron transakcji. Problematyka działań mających na celu zdobycie i utrzymanie reputacji na „ciemnych rynkach" wydzielona została jako czwarta grupa badanych problemów. Ustalono, że budowaniu zaufania i reputacji służą funkcjonalności „ciemnych rynków", takie jak profile użytkowników i fora dyskusyjne, na których można umieszczać oceny, komentarze i opinie o transakcjach oraz o kupujących i sprzedających. Ważna jest możliwość skontaktowania się ze sprzedawcą (e-mail) oraz odpowiednia budowa i jakość serwisu z ofertami.

Do piątej grupy badanych problemów można zaliczyć analizy postów zamieszczanych na forach dyskusyjnych. Badacze doszli do wniosku, że zachowania dyskutujących charakteryzują trzy cechy: zachowywanie anonimowości, korzystanie z wolności wypowiedzi oraz przyjazne dzielenie się wiedzą. Dominują dyskusje o hakerstwie, zachowywaniu bezpieczeństwa i anonimowości, porady w zakresie uczestniczenia w „ciemnym handlu" oraz dzielenie się poglądami radykalnymi politycznie i ideologicznie. O ile w dyskusjach dotyczących kwestii informatycznych i handlowych dostrzega się przyjazne dzielenie się wiedzą, o tyle dyskusje polityczno-ideologiczne wzmagają radykalizację postaw.

W trakcie przeglądu badań można było odkryć, ze zdziwieniem, że niewiele publikacji dotyczy roli dark web we wspomaganiu wolności słowa. Tak więc do szóstej grupy tematów zostało zaliczonych jedynie kilka prac wykazujących, że w dużej mierze dzięki istnieniu tej części internetu rozwinęły się takie zjawiska jak anonimowy dostęp do zasobów internetu powierzchniowego, *whistle-blowing* (sygnalizowanie nieprawidłowości) oraz haktywizm (informowanie o lukach w oprogramowaniu). Czy niewielka liczba publikacji świadczy o niewielkiej skali wymienionych zjawisk? Przegląd zasobów dark web sugeruje, że problemem jest raczej nastawienie badaczy na szukanie głównie ciemnych stron tej sieci.

Dużym problemem w badaniu dark web jest anonimowość użytkowników, trudność pozyskania danych oraz ich niepewna wiarygodność. Istotnym wyzwaniem jest także badanie tych społeczności, które nie są nastawione na popełnianie przestępstw, a dark web traktują jako oazę wolności słowa. Ponieważ internet widzialny poddawany jest coraz większej

kontroli, że pojawiają się głosy wskazujące na konieczność ograniczania rozpowszechniania niektórych poglądów (np. tych określanych jako mowa nienawiści lub niemieszczących się w ramach poprawności politycznej), a nawet karania za ich publiczne głoszenie, należy spodziewać się rozwoju sieci tworzących dark web. Ograniczenia nakładane na użytkowników internetu widzialnego niewątpliwie będą skłaniać coraz większe grupy ludzi do korzystania z wolności i anonimowości panującej w dark web. Dlatego też można spodziewać się znacznego poszerzenia wyzwań badawczych stwarzanych przez tę sieć. Staną przed nimi zarówno humaniści, jak i przedstawiciele nauk społecznych, otwierają się bowiem nowe obszary eksploracji i tematy. Jednakże poważnym wyzwaniem będą metody badań, a zwłaszcza techniki pozyskiwania danych i informacji oraz sposoby ich uwiarygodniania w anonimowym środowisku. Niemniej apel o bardziej intensywne niż dotychczas eksplorowanie dark web wydaje się zasadny.

BIBLIOGRAFIA

Alnabulsi Hussein, Islam Rafiqul, 2018, *Identification of Illegal Forum Activities inside the Dark Net*, w: *Proceedings — International Conference on Machine Learning and Data Engineering*, IEEE, s. 30–34.

Baele Stephane J., Brace Lewys, Coan Travis G., 2021, *Variations on a Theme? Comparing 4chan, 8kun, and Other Chans' Far-Right '/pol' Boards*, „Perspectives on Terrorism", t. 15(1), s. 65–80.

Bancroft Angus, Reid Peter S., 2017, *Challenging the Techno-Politics of Anonymity: The Case of Cryptomarket Users*, „Information, Communication & Society", t. 20(4), s. 497–512 (https://doi.org/10.1080/1369118X.2016.1187643).

Barratt Monica J., Maddox Alexia, 2016, *Active Engagement with Stigmatised Communities through Digital Ethnography*, „Qualitative Research", t. 16(6), s. 701–719.

Booij Tim M., Verburgh Thijmen, Falconieri Federico, van Wegberg Rolf S., 2021, *Get Rich or Keep Tryin. Trajectories in Dark Net Market Vendor Careers*, w: *Proceedings — 2021 IEEE European Symposium on Security and Privacy Workshops*, IEEE, s. 202–212.

Broadhurst Roderic, Woodford-Smith Hannah, Maxim Donald, Sabol Bianca, Orlando Stephanie, Chapman-Schmidt Ben, Alazab Mamoun, 2017, *Cyber Terrorism: Research Review: Research Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology* (https://dx.doi.org/10.2139/ssrn.2984101).

Castells Manuel, 2003, *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem*, tłum. Tomasz Hornowski, Rebis, Poznań.

Chen Zhicong, Jardine Eric, Fan Liu Xiao, Zhu Jonathan J. H., 2024, *Seeking Anonymity on the Internet: The Knowledge Accumulation Process and Global Usage of the Tor Network*, „New Media & Society", t. 26(2), s. 1074–1095 (https://doi.org/10.1177/14614448211072201).

Chen Zhicong, Meng Xiang, Wang Cheng-Jun, 2023, *The Dark Web Privacy Dilemma: Linguistic Diversity, Talkativeness, and User Engagement on the Cryptomarket Forums*, „Humanities and Social Sciences Communications", t. 10 (https://doi.org/10.1057/s41599-023-02424-0).

Chertoff Michael, 2017, *A Public Policy Perspective of the Dark Web*, „Journal of Cyber Policy", t. 2(1), s. 26–38 (https://doi.org/10.1080/23738871.2017.1298643).

Choi Kyung-Shick, Lee Claire S., 2023, *In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services and the Underground Justice System*, „Journal of Contemporary Criminal Justice", t. 39(2), s. 201–221.

Crawley Adrian, 2016, *Hiring Hackers*, „Network Security", t. 9, s. 13–15.

Denic Nenad V., Devetak Sasa, 2023, *Dark Web — As Challenge of the Contemporary Information Age*, „Trames", t. 27(2), s. 115–126.

Finklea Kristin, 2022, *The Dark Web: An Overview*, Congressional Research Service (https://crsreports.congress.gov/search/#/?termsToSearch=Kristin%20Finklea&orderBy=Relevance).

Foust Jeremy, Ghee Chariah, Hartung Mateusz, Hynes Kathleen, Li Chong, Mandrich Patrycja, McMaster Kymberlee, Reibel Jared, Tadlock Kamilah, 2017, *The Dark Internet: An Exploration of Culture and User Experience*, Digital Repository at the University of Maryland (https://api.drum.lib.umd.edu/server/api/core/bitstreams/be66a81a-d9cc-42aa-a952-035461495ad1/content).

Gehl Robert W., 2016, *Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network*, „New Media & Society", t. 18(7), s. 1219–1235 (https://doi.org/10.1177/1461444814554900).

Gupta Abhineet, Maynard Sean B., Ahmad Atif, 2019, *The Dark Web Phenomenon: A Review and Research Agenda*, w: *ACIS 2019: Making the World a Better Place with Information Systems*, Freemantle, Australia (https://acis2019.io/pdfs/ACIS2019_PaperFIN_004.pdf).

Handalage Upulie, Prasanga Tereen, 2021, *Dark Web, Its Impact on the Internet and the Society: A Review*, ResearchGate.net (http://dx.doi.org/10.13140/RG.2.2.11964.36484).

Hardy Robert A., Norgaard Julia R. 2016, *Reputation in the Internet Black Market: An Empirical and Theoretical Analysis of the Deep Web*, „Journal of Institutional Economics", t. 12(3), s. 515–539.

Hatta Masayuki, 2020, *Deep Web, Dark Web, Dark Net: A Taxonomy of 'Hidden' Internet*, „Annals of Business Administrative Science", t. 19(6), s. 277–292 (https://doi.org/10.7880/abas.0200908a).

Hiramoto Naoki, Tsuchiya Yoichi, 2024, *Dark Web Activity in the Japanese Language between 2004 and 2020: A Case Study of the Onion Channel*, „Deviant Behavior" (https://doi.org/10.1080/01639625.2024.2311751).

Jardine Eric, 2018, *Tor, What Is It Good For? Political Repression and the Use of Online Anonymity-Granting Technologies*, „New Media and Society", t. 20(2), s. 435–452.

Jardine Eric, 2019, *Online Content Moderation and the Dark Web: Policy Responses to Radicalizing Hate Speech and Malicious Content on the Darknet*, „First Monday", t. 24(12) (https://doi.org/10.5210/fm.v24i12.10266).

Jenkins Henry, 2006, *Kultura konwergencji. Zderzenie starych i nowych mediów*, tłum. Małgorzata Bernatowicz, Mirosław Filiciak, Wydawnictwa Akademickie i Profesjonalne, Warszawa.

Krauz Antoni, 2017, *Mroczna strona Internetu — TOR niebezpieczna forma cybertechnologii*, „Dydaktyka Informatyki", t. 12, s. 63–74.

Laferrière Dominique, Décary-Hétu David, 2023, *Examining the Uncharted Dark Web: Trust Signalling on Single Vendor Shops*, „Deviant Behavior", t. 44(1), s. 37–56.

Maddox Alexia, Barratt Monica J., Allen Matthew, Lenton Simon, 2016, *Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital 'Demimonde'*, „Information Communication and Society", t. 19(1), s. 111–126.

Martin James, 2023, *Cryptomarkets and Drug Market Gentrification*, w: Meropi Tzanetakis, Nigel South (red.), *Digital Transformations of Illicit Drug Markets: Reconfiguration and Continuity*, Emerald Publishing, s. 127–139.

Mirea Mihnea, Wang Victoria, Jung Jeyong, 2019, *The Not So Dark Side of the Darknet: A Qualitative Study*, „Security Journal", t. 32, s. 102–118 (https://link.springer.com/article/10.1057/s41284-018-0150-5#Sec6).

Moeller Kim, 2023, *Trust in Cryptomarkets for Illicit Drugs*, w: Meropi Tzanetakis, Nigel South (red.), *Digital Transformations of Illicit Drug Markets: Reconfiguration and Continuity*, Emerald Publishing, s. 29–43.

Nahai Nathalie, 2017, *Webs of Influence: The Psychology of Online Persuasion*, Pearson Education Limited, London.

Ofusori Lizzy O., Hendradi Rimuljo, 2023, *Understanding the Impact of the Dark Web on Society: A Systematic Literature Review*, „International Journal of Information Science and Management", t. 21(4), s. 1–21.

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

Przepiorka Wojtek, Norbutas Lukas, Corten Rense, 2017, *Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs*, „European Sociological Review", t. 33(6), s. 752–764.

Sirola Anu, Nuckols Julia, Nyrhinen Jussi, Wilska Terhi-Anna, 2022, *The Use of Dark Web as a COVID-19 Information Source: A Three-Country Study*, „Technology in Society", t. 70 (https://www.sciencedirect.com/science/article/pii/S0160791X22001531).

Snyder Hannah, 2019, *Literature Review as a Research Methodology: An Overview and Guidelines*, „Journal of Business Research", t. 104, s. 333–339 (https://doi.org/10.1016/j.jbusres.2019.07.039).

Topor Lev, 2022, *Phishing for Nazis: Conspiracies, Anonymous Communications and White Supremacy Networks on the Dark Web*, Routledge, New York.

Tranfield David, Denyer David, Smart Palminder, 2003, *Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review*, „British Journal of Management", t. 14(3), s. 207–222 (https://doi.org/10.1111/1467-8551.00375).

Tsuchiya Yoichi, Hiramoto Naoki, 2021, *Dark Web in the Dark: Investigating When Transactions Take Place on Cryptomarkets*, „Forensic Science International: Digital Investigation", t. 36 (http://dx.doi.org/10.2139/ssrn.3754071).

Weimann Gabriel, 2016a, *Terrorist Migration to the Dark Web*, „Perspectives on Terrorism", t. 10(3), s. 40–44.

Weimann Gabriel, 2016b, *Going Dark: Terrorism on the Dark Web*, „Studies in Conflict & Terrorism", t. 39(3), s. 195–206.

Winkler Ira S., Gomes Araceli T., 2017, *Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies*, Syngress Publishing, Rockland.

Wong Geoff, Greenhalgh Trish, Westhorp Gill i in., 2013, *RAMESES Publication Standards: Meta-Narrative Reviews*. „BMC Medicine", t. 11, nr 20 (https://doi.org/10.1186/1741-7015-11-20).

Woodhams Jessica, Kloess Juliane A., Jose Brendan, Hamilton-Giachritsis Catherine E., 2021, *Characteristics and Behaviors of Anonymous Users of Dark Web Platforms Suspected of Child Sexual Offenses*, „Frontiers in Psychology", t. 12 (https://doi.org/10.3389/fpsyg.2021.623668).

CULTURAL ASPECTS OF THE DARK WEB. RESEARCH REVIEW

Zbigniew Osiński
(Maria Skłodowska University in Lublin)

Abstract

The article contains a review of research on the cultural aspects of the Dark Web. A semi-systematic literature review was used for this purpose, as such an approach enables the reviewing of a multi- or interdisciplinary research area. Scopus, an international and multidisciplinary database indexing academic publications, was the source of bibliographic data. It turned out that there is a relatively short history of research on the cultural aspects of the Dark Web. The first publications on the topic only appeared in the Scopus database in 2005, and it continues to be a niche area of research, with the annual number of indexed publications around a few dozen. The author distinguished the following groups of issues that researchers deal with: (1) motivations among Dark Web users for making use of this part of the internet; (2) the impact of the Dark Web's existence and the anonymity it provides on human behaviour; (3) the specificity of trading activity on "dark markets"; (4) steps taken by illegal traders to gain a reputation and customer trust; (5) communication practices on discussion forums; (6) the freedom to disseminate information; and (7) the methodology for studying communities on "dark networks".

key words: cultural aspects of the Dark Web, dark markets, Scopus, semi-systematic literature review

słowa kluczowe: kulturowe aspekty Dark Web, ciemne rynki, Scopus, półsystematyczny przegląd literatury