Krzysztof Kaczmarek*

Darknet jako przedmiot badań nauk społecznych

Streszczenie

W ciągu ostatnich dwudziestu lat znaczna część aktywności społecznych przeniosła się do Internetu. Spowodowało to głębokie przemiany społeczne i polityczne. Jednakże zdecydowana większość populacji nie zdaje sobie sprawy z tego, że ma dostęp jedynie do niewielkiej części informacji znajdujących się w cyberprzestrzeni. Zdecydowana ich większość znajduje się w tak zwanym ukrytym Internecie. Jego część stanowi z kolei darknet (ciemna sieć), który pozwala na zachowanie niemal zupełnej anonimowości użytkownika. Atrybuty tej części sieci powodują, że jest ona atrakcyjna dla bardzo ceniących sobie prywatność. Jednakże w tej grupie część osób to przestępcy, ekstremiści i terroryści. Powoduje to nowe wyznania dla służb odpowiedzialnych za bezpieczeństwo publiczne. Jednocześnie zagadnienia związane z darknetem mogą stanowić podmiot badań nauk społecznych.

Słowa kluczowe: darknet, ekstremizm, terroryzm, pedofilia, narkotyki, broń

* Dr Krzysztof Kaczmarek, Wydział Humanistyczny, Politechnika Koszalińska, e-mail: puola@tlen.pl, ORCID: 0000-0001-8519-1667.

Wstęp

Internet jest obecnie narzędziem, bez którego trudno sobie wyobrazić funkcjonowanie współczesnych społeczeństw i państw. Jest też miejscem, w którym można zapoznać się z niemal całą wiedzą ludzkości, bywa postrzegany jako repozytorium wszelkich informacji i jako encyklopedia zawierająca hasła na każdy temat. Jednakże okazuje się, że nie wszystkie zasoby Internetu są powszechnie dostępne. Część tych niedostępnych znajduje się w tzw. ciemnej sieci, która jest podzbiorem głębokiej sieci (ang. deep web) obejmującej m.in. witryny wymagające logowania. Szacuje się, że deep web jest 400 do 500 razy większy niż zwykły Internet[1]. Darknet jest stosunkowo mniejszy i składa się z wielu zaszyfrowanych sieci (sieć TOR – The Onion Router) będących w stanie ukryć tożsamość i lokalizację użytkownika. Dostęp do zasobów ciemnej sieci jest możliwy tylko przy pomocy specjalnego oprogramowania. Celem niniejszego artykułu jest analiza zagrożeń wynikających z nieumiejętnego przeglądania zasobów darknetu, korzyści z prawdopodobieństwa zachowania anonimowości oraz możliwości badawczych, jakie daje dostęp do informacji znajdujących w tej części Internetu.

Zasoby darknetu

Panuje powszechna opinia, że niemal wszystkie treści zawarte w darknecie są nielegalne i w związku z tym nawet możliwość ich biernego przeglądania może być przestępstwem. Tymczasem zarówno darknet, jak i dające do niego dostęp oprogramowanie są jedynie narzędziami. Tylko od użytkownika zależy do osiągnięcia, jakich celów zostaną one wykorzystane. Przede wszystkim sieć TOR, chociaż nie gwarantuje, ale daje użytkownikowi możliwość zachowania anonimowości. Korzyści wynikające z możliwości anonimowego poruszania się po Internecie opisał Antoni Krauz[2]. Według autora, anonimowe korzystanie z sieci pozwala m.in.: 1) chronić prywatność; 2) uniemożliwiać identyfikację lokalizacji użytkownika zamieszczającego w sieci treści nielegalne w niektórych

1 S.R. Choudhury, A. Kharpal, *The 'deep web' may be 500 times bigger than the normal web. Its uses go well beyond buying drugs*, CNBC, https://www.cnbc.com/2018/09/06/beyond-the-valley-understanding-the-mysteries-of-the-dark-web.html.

2 A. Krazu, *Mroczna strona Internetu – TOR niebezpieczna forma cybertechnologii*, [w:] *Dydaktyka informatyki*, red. A. Piecuch, Rzeszów 2017, s. 63–74.

państwach; 3) przeglądać strony cenzurowane; 4) działać służbom zajmującymi się zwalczaniem cyberprzestępczości bez obawy, że zostaną wykryte; 5) działać bez cenzury państwa i obawy o własne bezpieczeństwo; 6) przesyłać treści między państwami bez obawy, że zostaną zablokowane; 7) dziennikarzom w bezpieczny sposób komunikować się z informatorami; 8) zwiększyć bezpieczeństwo informacji; 9) zwiększyć bezpieczeństwo pracowników wywiadu; 10) koordynować działania grup przestępczych[3].

Pełna anonimowość i brak cenzury mogą stanowić narzędzie wspomagające walkę o przestrzeganie praw człowieka w takich państwach, jak np. Chiny czy Arabia Saudyjska. Jednakże w o wiele większym stopniu atrybuty darknetu są wykorzystywane przez przestępców. Można tam odnaleźć strony z pornografią dziecięcą, fora pedofilskie, strony zoofilskie czy nawet nekrofilskie. Znajdują się tam sklepy z narkotykami czy ogłoszenia płatnych zabójców. Ze względu na często drastyczną zawartość stron dostępnych w darknecie autor nie zdecydował się na umieszczenie w niniejszym artykule odnośników do żadnej z nich. Autorowi udało się m.in. odnaleźć sklepy sprzedające dowolne narkotyki w dowolnej ilości z dostawą do dowolnego miejsca w Polsce w ciągu 24–48 godzin od chwili dokonania zapłaty lub przedpłaty. Warto zwrócić uwagę, że szczegółowa wiedza na ten temat może być niebezpieczna dla osób nieodpowiedzialnych, w tym nastolatków. Nie chodzi tutaj o zagrożenia, jakie niesie za sobą samo zażywanie substancji psychoaktywnych. Należy zdać sobie sprawę z tego, że wchodząc w jakikolwiek kontakt z handlarzami narkotyków, nie będzie już można tego kontaktu zerwać. Nawet dokonując płatności kryptowalutami, należy podać miejsce dostawy. Jednocześnie nie można mieć gwarancji, że nie zostanie się zidentyfikowanym w trakcie podejmowania takiej przesyłki. W takim przypadku zatrzymanie przez policję czy inne służby wydaje się być najmniejszym z możliwych problemów. Identyfikacja przez przedstawicieli karteli narkotykowych może skutkować szantażem i zmuszaniem to zachowań o charakterze przestępczym, np. przemytu narkotyków. Podobny mechanizm działa w przypadku handlu bronią. Zasoby darknetu pozwalają również uzyskać nielegalny dostęp do usług telewizyjnych, pirackiej muzyki, filmów czy oprogramowania.

Korzystanie z darknetu niesie za sobą również ryzyko zainfekowania komputera złośliwym oprogramowaniem, co może prowadzić do kradzieży tożsamości. Biorąc pod uwagę, że w tej części Internetu szczególnie aktywni są

3 Ibidem, s. 67–69.

przestępcy, skradziona tożsamość może posłużyć do popełnienia kolejnych przestępstw, nawet tych największego kalibru (zabójstwo, terroryzm, pedofilia). Zainfekowanie komputera daje również możliwość wykorzystania go do dokonywania przestępstw cybernetycznych. Wydaje się, że przeglądając zawartość darknetu, można zwiększyć własne bezpieczeństwo przez korzystanie z urządzenia przeznaczonego jedynie do tego celu. Wyklucza to niemal zupełnie możliwość kradzieży tożsamości. Oczywiście przy zachowaniu wszelkich środków ostrożności, z których najważniejszym jest zasada niepodawania żadnych danych mogących w jakikolwiek sposób zidentyfikować użytkownika.

Istnieją oczywiste trudności metodologiczne i praktyczne dotyczące analizy ilościowej i jakościowej treści dostępnych w darknecie. Poszukując informacji na ten temat, można spotkać dane dotyczące cech demograficznych użytkowników darknetu w funkcji przeglądanych przez nich treści. Ze względów oczywistych (niemal 100% anonimowość) dane te nie mogą być wiarygodne. Przeglądając ogólnodostępny Internet i literaturę przedmiotu, można spotkać informacje mówiące o tym, że np. wśród osób przeglądających treści pedofilskie największą grupę stanowią mężczyźni między 35 a 40 lat. Tego typu dane nie mogą być w żadnym wypadku wiarygodne. Dotarcie do najgłębiej ukrytych treści znajdujących się na nigdzie nieindeksowanych stronach wymaga znajomości bezpośrednich odnośników, które składają się najczęściej z losowo generowanych znaków. Treści te są dostępne tylko dla nielicznych, często za pokaźną opłatą.

Jednym z rodzajów treści hipotetycznie dostępnych w darknecie są tzw. czerwone pokoje (ang. red rooms), w których istnieje możliwość oglądania na żywo tortur, egzekucji czy okrutnych gwałtów. Wielu badaczy tej problematyki podaje w wątpliwość istnienie takich miejsc ze względu na ograniczenia techniczne sieci TOR[4], należy jednak pamiętać, że rozwój technologii, jeżeli nawet nie obecnie, to wkrótce może pozwolić na tego typu aktywność.

Należy również zwrócić uwagę na to, że jeżeli jakieś zjawiska nie są obserwowalne, to nie znaczy, że nie istnieją. W darknecie część stron pojawia się tylko o określonych porach, dlatego są trudniejsze do wyśledzenia. Szczególnie wtedy, kiedy algorytm określający czas ich działania nie jest wprost związany z powszechnie stosowanymi jednostkami czasu.

4 F. Velázquez, *Red Room Deep Web*, „Science & Technology", https://wsimag.com/science-and-technology/61203-red-rooms-deep-web.

Podsumowując tę część artykułu, na podstawie własnych badań, autor pozwala sobie postawić tezę, że istnieje możliwość przybliżonego jakościowego określenia treści dostępnych w darknecie. Jednakże nie można dokonać analizy ilościowej i określić, jakich treści jest najwięcej. Jedną z przyczyn są różnice w ilości informacji i danych dostępnych pod poszczególnymi adresami darknetu. Przeszukując zasoby darknetu, autor natrafił także na treści, których nie opisał w sposób szczegółowy ze względu na ich drastyczny charakter i potencjalną możliwość dostępu do niniejszego artykułu osób nieletnich.

Ekstremizmy i terroryzm w darknecie

Ugrupowania o charakterze terrorystycznym działały na platformach internetowych od końca lat 90. wieku XX. Bardzo szybko okazało się, że dla terrorystów korzystanie ze zwykłego Internetu jest zbyt ryzykowne. Ich działania były monitorowane, a oni sami lokalizowani[5]. Możliwość zachowania anonimowości spowodowała, że darknetem zainteresowały się ugrupowania ekstremistyczne i terrorystyczne. Po raz pierwszy zostało to udowodnione, kiedy w roku 2013 amerykańska Agencja Bezpieczeństwa Narodowego (NSA) przechwyciła zaszyfrowany plik zawierający korespondencję pomiędzy szefem Al-Kaidy Aymanem Al-Zawahirim a Nasirem Al-Wuhaysim, szefem Jemeńskiej Al-Kaidy. Zostało wówczas ujawnione, że już od około dekady Al-Kaida przynajmniej częściowo do komunikowania się wykorzystywała darknet. W szczególności komunikowali się w ten sposób jej przywódcy. Po atakach terrorystycznych w Paryżu dokonanych w listopadzie 2015 roku Państwo Islamskie (ISIS) przeniosło swoją działalność propagandową do darknetu, żeby chronić tożsamość swoich zwolenników, a zawartość swoich stron przed haktywistami[6].

W kwietniu 2018 roku opublikowano przygotowany przez Henry Jackson Society raport zatytułowany „Terror in the Dark". Zawierał on informacje o wzroście liczby ukrytych w darknecie platform organizacji terrorystycznych i ekstremistycznych. Według wspomnianego raportu, platformy te służą przede wszystkim do planowaniu zamachów, zdobywaniu funduszy oraz rekrutowaniu nowych członków. Według autorów raportu, organizacje terrorystyczne

5 G. Weimann, *Going Darker? The chellenge of Dark Net terrorism*, https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf.

6 Ibidem.

i ekstremistyczne wykorzystują platformy umieszczone w darknecie: 1) żeby się ukryć. Monitorowanie powierzchniowej sieci (zwykłego Internetu) oraz mediów społecznościowych przez instytucje zajmujące się bezpieczeństwem powoduje szybkie usuwanie treści ekstremistycznych z platform mediów społecznościowych; 2) do prowadzenia rekrutacji. Najczęściej pierwszy kontakt jest nawiązywany przy wykorzystaniu powierzchniowych platform internetowych. Dopiero później przekazywane są informacje dotyczące dostępu do witryn terrorystów w darknecie; 3) jako rezerwuar propagandy. Usuwane z sieci powierzchniowej treści często pojawiają się również w darknecie; 4) do używania kryptowalut, żeby uniknąć wykrycia i móc zbierać fundusze na swoją działalność[7].

Na zagrożenia związane z przejściem organizacji ekstremistycznych i terrorystycznych oraz handlu bronią do darknetu zwrócił uwagę Europejski Komitet Regionów w swojej opinii dotyczącej przeciwdziałaniu radykalizacji postaw i brutalnemu ekstremizmowi z 18 stycznia 2017 roku. Punkt 44 wspomnianej opinii brzmi: „[…] konieczne jest nasilenie wymiany informacji i współpracy operacyjnej, poczynienie postępów w dziedzinie walki z nielegalnym handlem bronią palną oraz z finansowaniem terroryzmu. Dostrzega także konieczność wprowadzenia skutecznych narzędzi kontroli nad »ukrytą siecią« (deep web, darknet), która stanowi często instrument rozprzestrzeniania radykalnych treści”[8].

Ekstremizm i terroryzm to pojęcia, które nie są związane jedynie z organizacjami islamistycznymi. Darknet jest wykorzystywany także przez skrajną prawicę i organizacje rasistowskie, a służby porządkowe nie zawsze potrafią sobie z tym poradzić. Przykładem jest chociażby działalność skrajnej prawicy w Niemczech, która wykorzystując darknet, nie tylko rozpowszechnia neonazistowskie treści propagandowe, lecz także zaopatruje się w broń i materiały pirotechniczne[9]. Analogicznie działają skrajnie prawicowe i neonazistowskie oraz skrajnie lewicowe ugrupowania w innych państwach.

Jednakże nie cała aktywność sieciowa terrorystów przeniosła się do darknetu. Według Pierluiginiego Paganiniego, włoskiego publicysty i eksperta od

7 Ibidem.

8 *Opinia Europejskiego Komitetu Regionów – Przeciwdziałanie radykalizacji postaw i brutalnemu ekstremizmowi: mechanizmy zapobiegania na poziomie lokalnym i regionalnym*, Dz. Urz. UE 2017, C 017/07.

9 T. Lejman, *Terror, z którym nie radzą sobie Niemcy*, „Tygodnik Polsat”, https://tygodnik.polsatnews.pl/news/2020-02-29/terror-z-ktorym-nie-radza-sobie-niemcy/.

cyberbezpieczeństwa, całkowite przeniesienie kanałów propagandy do darknetu doprowadziły do tego, że jej zasięg znacznie by się zmniejszył. Szeroką propagandę i wstępną rekrutację przeprowadzają wciąż za pomocą tradycyjnych platform takich, jak Twitter czy Facebook[10].

Perspektywy badań nad darknetem w ujęciu społecznym

Dotychczas nie przeprowadzano kompleksowych badań koncentrujących się na socjologicznym wymiarze darknetu. Większość prób przeprowadzenia tego typu analiz dotyczyła jedynie małej części zagadnienia. W istniejącej literaturze jest przedstawiana w zdecydowanej większości ciemna wersja darknetu[11]. Mimo że zagadnienia związane z darknetem są coraz częściej omawiane w kręgach zajmujących się zagadnieniami cyberbezpieczeństwa, niewiele osób zdaje sobie sprawę z jego istnienia. W trakcie prowadzenia zajęć ze studentami autor dowiedział się, że o darknecie słyszało zaledwie 6 osób na ponad 200. Jednakże żadna z nich nie korzystała z tego narzędzia w obawie, że mogłoby to być niezgodne z prawem.

Mimo że w tej sieci ma miejsce wiele działań przestępczych, darknet nie jest kryminogenny. Obserwowane tam działania przestępcze istnieją również poza nim. Biorąc pod uwagę wirtualne rynki w darknecie, nie można zaprzeczyć, że nielegalny handel narkotykami jest dominującą działalnością na wielu rynkach darknetu.

Nie można również zaprzeczyć, że darknet stanowi poważne zagrożenie bezpieczeństwa. Ze względu na jego wyjątkowe cechy, jak: anonimowość, wirtualne rynki i wykorzystanie kryptowalut, w sieci tej można z łatwością popełniać przestępstwa. W rezultacie darknet należy zbadać bardziej poważnie. Należy także zauważyć, że celem istnienia darknetu nie jest szkodzenie jednostkom, organizacjom i społeczeństwom. Nie powinno się również arbitralnie określać środowisk korzystających z darknetu jedynie jako kryminogenne. Wydaje się, że potrzebne są pogłębione badania holistyczne nad społecznymi aspektami darknetu. Ich wyniki mogłyby pomóc w opracowaniu narzędzi zwiększających bezpieczeństwo korzystania z Internetu. Ostatecznie darknet

10 B. Józefiak, *Terroryści niechętnie korzystają z darknetu*, „CyberDefence24", https://www.cyberdefence24.pl/terrorysci-niechetnie-korzystaja-z-darknetu.

11 M. Mirea, V. Wang, J. Jung, *The not so dark side of the darknet: a qualitative study*, „Security Journal" 2019, No. 32.

nie jest społeczeństwem, w którym przestępczość jest normą. W rzeczywistości jest to platforma technologiczna używana przez różne osoby do różnych celów[12], podobnie jak w przypadku ogólnodostępnych stron i portali internetowych. Treści tam zamieszczane zależą jedynie od użytkowników.

Zakończenie

Istnieje niewiele publikacji dotyczących badań nad treściami dostępnymi w darknecie, a większość dostępnych na ten temat informacji jest najczęściej powielana. Część osiągalnych opisów zawartości darknetu należy traktować w kategorii miejskich legend. Jednakże na podstawie własnych badań autor doszedł do wniosku, że korzystanie z tej części ukrytego Internetu może sprowadzić różnorakie zagrożenia, szczególnie na osoby ich nieświadome. Podejmując badania nad aktywnością społeczną, polityczną czy biznesową w darknecie, należy zawsze zwracać uwagę na to, żeby do niektórych treści nie miały dostępu osoby niepowołane, w tym dzieci. Treści w nim dostępne można sklasyfikować pod względem stopnia trudności ich odnalezienia. Na pierwszym miejscu znajdują się te, które najłatwiej wyszukać; na kolejnych miejscach stopień trudności dotarcia jest większy: 1) treści legalne w większości państw; 2) narkotyki i inne środki psychoaktywne; 3) kradzione środki płatnicze (karty kredytowe, karty podarunkowe, kody doładowujące w usługach pre-paid itp.); 4) pirackie oprogramowanie, filmy i muzyka; 5) broń (w tym niemal wszystkie rodzaje broni palnej); 6) podrabiane dokumenty (najwięcej ofert pochodzi ze Stanów Zjednoczonych i Wielkiej Brytanii); 7) nielegalna pornografia (nagrania z ukrytych kamer, pedofilia, zoofilia i inne materiały przedstawiające nieakceptowalne społecznie formy zachowań seksualnych). Do innych rodzajów treści autorowi nie udało się dotrzeć w stopniu pozwalającym na ich zhierarchizowanie pod względem trudności dostępu. Przykładem jest odnalezienie w darknecie przez autora linku do strony propagującej treści rasistowskie przeznaczone dla mieszkańców Stanów Zjednoczonych. Tego typu linki bywają ukryte w treściach powszechnie dostępnych w normalnym Internecie.

Prowadzenie dalszych badań nad darknetem i jego roli w aktywności społecznej wymaga odpowiedniego przygotowania metodologicznego i, być może, opracowania nowych metod badawczych przeznaczonych do badania tego medium.

12 Ibidem.

Bibliografia

Choudhury S.R., Kharpal A., *The 'deep web' may be 500 times bigger than the normal web. Its uses go well beyond buying drugs*, CNBC, https://www.cnbc.com/2018/09/06/beyond-the-valley-understanding-the-mysteries-of-the-dark-web.html.

Józefiak B., *Terroryści niechętnie korzystają z darknetu*, „CyberDefence24", https://www.cyberdefence24.pl/terrorysci-niechetnie-korzystaja-z-darknetu.

Krazu A., *Mroczna strona Internetu – TOR niebezpieczna forma cybertechnologii*, [w:] *Dydaktyka informatyki*, red. A. Piecuch, Rzeszów 2017.

Lejman T., *Terror, z którym nie radzą sobie Niemcy*, „Tygodnik Polsat", https://tygodnik.polsatnews.pl/news/2020-02-29/terror-z-ktorym-nie-radza-sobie-niemcy/.

Mirea M., Wang V., Jung J., *The not so dark side of the darknet: a qualitative study*, „Security Journal" 2019, No. 32.

Velázquez F., *Red Room Deep Web*, „Science & Technology", https://wsimag.com/science-and-technology/61203-red-rooms-deep-web.

Weimann G., *Going Darker? The chellenge of Dark Net terrorism*, https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf.

The darknet as a subject of social science research

Abstract

Over the past twenty years, a significant proportion of social activity has moved to the Internet. It caused profound social and political changes. However, the vast majority of the population is unaware that they only have access to a small part of the information in the cyberspace. The vast majority of them are on the so-called hidden Internet. Part of it, in turn, is the darknet, which allows almost complete anonymity of the user. The attributes of this part of the web makes it attractive to those who value privacy highly. However, in this group, some people are criminals, extremists and terrorists. This causes new confessions for the services responsible for public safety. At the same time, darknet issues can be a subject of social science research.

Key words: darknet, extremism, terrorism, pedophilia, drugs, weapons