BEZPIECZEŃSTWO • 2017 nr 4 TEORIA I PRAKTYKA

Marta Majorek

dr, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego

Darknet. Ostatni bastion wolności w internecie?

Wprowadzenie

Darknet, czy raczej Darknets[1] działają w specjalnie do tego celu zaprojektowanych przeglądarkach internetowych, których przykładem może być narzędzie, takie jak Tor. Przeglądarka ta wymieniona zostaje na samym początku, bowiem jest pierwszym tego typu narzędziem tak szeroko rozpowszechnionym w „zaszyfrowanej" sieci. Jej koncepcja jest wsparta na bezpłatnym oprogramowaniu, które maskuje lokalizacje i działania użytkowników. Początkowo, zaprojektowany przez Laboratorium Badań Marynarki Wojennej USA[2], Tor był wykorzystywany w celu ochrony wymiany informacji w ramach agencji rządowych. Jest to narzędzie, którego głównym i zarazem priorytetowym zadaniem jest ochrona prywatności[3]. W ciągu ostatniej dekady przeglądarki Darknetów umożliwiły aktywistom rozpowszechnianie informacji chociażby podczas wydarzeń Arabskiej Wiosny oraz w trakcie innych akcji mających na celu wzmocnienie ruchów wolnościowych i prodemokratycznych, sprzeciwiających się opresyjnym władzom[4]. Nie można pominąć również przydatności tych narzędzi dla

[1] W zależności od tego, jakiej aplikacji/ narzędzia używamy, mówić możemy o Freenecie, Torze i innych podobnych narzędziach umożliwiających nam poruszanie się po ukrytej sieci. Każde z tych narzędzi prowadzi nas do zamkniętej dla zwyczajnego użytkownika sieci. Z tego też względu nie ma jednego Darknetu, przeciwnie – jest ich co najmniej kilka i wciąż rozwijane są nowe technologie dające możliwość dostępu do tej przestrzeni.

[2] K. Swan, *Onion Routing and Tor*, „GEO. L. TECH. REV" 2016, s. 110, https://perma.cc/JV7Y-FNYH [dostep: 30.08.2017].

[3] C. Mc Manamon, F. Mtenzi, *Defending privacy: The development and deployment of a darknet.* „Internet Technology and Secured Transactions (ICITST), International Conference for IEEE" 2010, s. 2.

[4] R.B. Yetter, *Darknets, cybercrime & the onion router: Anonymity & security in cyberspace*, rozprawa doktorska, Utica College 2015, s. 24.

ofiar przemocy domowej, osób nękanych przez stalkerów, konsumentów chroniących swoją prywatność, chcących uchronić się przed natarczywymi reklamodawcami.

Celem artykułu jest w pierwszej kolejności zaprezentowanie koncepcji i charakterystyki Darknetu, wraz z przybliżeniem konkretnych technologii i narzędzi umożliwiających korzystanie z niego. Dla realizacji tego celu wybrano jedno z dostępnych obecnie narzędzi, jakim jest Freenet, które zostanie bardziej szczegółowo omówione, dając pełniejszy obraz możliwości, jakie otrzymuje użytkownik. W dalszej kolejności przedmiotem zainteresowania będzie stan wolności słowa i ochrony prawa do prywatności jednostki w przestrzeni internetu w krajach z reżimami wyraźnie limitującymi możliwości swobodnego przekazywania informacji w ramach sieci. W odpowiedzi na wskazane ograniczenia przeanalizowana zostanie kwestia możliwości, jakie stwarza poruszanie się w Darknecie dla podtrzymania swobodnej, nieocenzurowanej komunikacji. Przedstawione zostaną zarówno szanse, jak i zagrożenia, jakie niesie ze sobą korzystanie z ciemnego internetu, choć uwaga będzie skupiona na tych pierwszych, a to z racji szeroko pojmowanej wolności słowa. Jest ona w omawianym kontekście szczególnie istotna, zwłaszcza z punktu widzenia analizy sytuacji istniejącej we wspomnianych wyżej, opresyjnych reżimach. Po drugie zaś, ukazanie jaśniejszej strony Darknetu, jako przeciwwagi dla przeważającej ilości artykułów i opracowań koncentrujących się na jego negatywnym wymiarze[5], wydaje się z racji obranej tematyki zasadne.

Ogólna charakterystyka możliwości ciemnego internetu

Pomimo, że Darknet ma już dość długą historię, biorąc pod uwagę istnienie samego internetu, do chwili obecnej stanowi ciekawy przedmiot badań. Z drugiej zaś strony nadal wielu ludzi ma wątpliwości co do tego, czym jest tak zwana ciemna strona internetu. Po pierwsze jest on niejednokrotnie mylony z „Deep Web", czyli w bezpośrednim tłumaczeniu „głęboką siecią" – terminem, który odnosi się do wszystkich części internetu, jakie nie mogą być indeksowane przez wyszukiwarki, czyli nie są obecne w wynikach popularnych wyszukiwarek, takich chociażby jak Google, Bing czy Yahoo. Eksperci z dziedzin IT stoją na stanowisku, że głęboka sieć jest setki razy większa niż sieć ogólnodostępna. W rzeczywistości większość tak zwanej głębokiej sieci nie zawiera nic niepokojącego, czy tajemniczego. Są to bowiem głównie duże bazy danych, biblioteki czy witryny internetowe, które nie są dostępne dla ogółu społeczeństwa. Składa się głównie, co ciekawe, z zasobów akademickich prowadzonych przez uniwersytety. Przykładem są wewnętrzne sieci uczelniane i katalogi

[5] J. Martin, *Drugs on the darknet: How cryptomarkets are transforming the global trade in illicit drugs*, Springer 2014; A. Bancroft, P.S. Reid, *Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge*, „International Journal of Drug Policy" nr 35, 2016; F. Wehinger, *The Dark Net: Self-regulation dynamics of illegal online markets for identities and related services*, „Intelligence and Security Informatics Conference (EISIC)", IEEE, 2011; J. Van Buskirk, *Characterising dark net marketplace purchasers in a sample of regular psychostimulant users*, „International Journal of Drug Policy" 2016, nr 35 ; M. Sutton, *Monitoring darknet access to identify malicious activity*, „U.S. Patent" 2013, nr. 8,413,238; S. Pang, *Malicious Events Grouping via Behavior Based Darknet Traffic Flow Analysis,* „Wireless Personal Communications" 2016.

biblioteczne, z których na co dzień korzystają studenci i wykładowcy. Zasadnicza różnica polega na tym, że zasoby Deep web mogą być odnalezione za pomocą alternatywnych, wewnętrznych wyszukiwarek. Przestrzeń ta, na chwilę obecną, nie jest w pełni możliwa do zbadania[6] (głównie ze względu na ogrom zasobów i unikatowe wyszukiwarki), a wiele projektów, tak zwanych „głębokich indeksów", nie powiodło się i zniknęło. Niemniej prace nad szeregiem rozwiązań umożliwiających skuteczne przeczesywanie tej przestrzeni trwają, są nieustannie implementowane i testowane[7].

Ciemna sieć, czy inaczej Darknet, to z kolei niewielki wycinek omówionego pokrótce Deep web. Jej treść nie tylko nie jest dostępna w wyszukiwarkach, ale jest czymś więcej: zasadza się bowiem na koncepcji prywatności i całkowitej anonimowości, których osiągnięcie możliwe jest dzięki zaawansowanym technikom kryptograficznym. W Darknecie zarówno internauci, jak i wydawcy stron internetowych mają, co do zasady, zapewnioną pełną ochronę prywatności[8]. Chociaż duże agencje rządowe są w stanie śledzić niektóre osoby funkcjonujące w teoretycznie anonimowej przestrzeni, to nastręcza to służbom szereg trudności, wymaga zaangażowania ogromnej ilości zasobów i koniec końców nie zawsze jest skuteczne. Wywołuje to dyskusje, które są niejednokrotnie bardzo spolaryzowane. Obrońcy zachowania pełnej prywatności argumentują, że udzielenie dostępu w celu egzekwowania prawa spowoduje osłabienie systemu i stworzy tylne drzwi dla tych, którzy będą chcieli używać narzędzia dla celów inwigilacji[9] lub innych praktyk naruszających prywatność oraz wolność jednostek.

Warto w tym miejscu pokrótce omówić, w jaki sposób użytkownik wspomnianą anonimowość może zyskać. Zazwyczaj anonimowość w „ciemnej sieci" uzyskuje się przy użyciu tak zwanej „sieci cebulowej". Zwykle przy wysłaniu żądania komputer automatycznie uzyskuje dostęp do serwera, na którym znajduje się odwiedzana witryna. W momencie użycia sieci cebulowej ten bezpośredni związek jest zerwany, a dane biegną do różnych serwerów, które w tysiącach kombinacji „odbijają je" i przekazują dalej. Dzięki temu, by wreszcie osiągnąć cel, nasze zapytanie przechodzi przez wielu pośredników. Otrzymany jest efekt w postaci zapytania, które jest rozpoznawane, ale jego nadawca pozostaje dla odbiorcy nieznany, co sprzyja anonimowej komunikacji dostępnej w większości popularnych systemów operacyjnych[10]. Pomimo nieustannego rozwoju różnorodnych narzędzi umożliwiających dostęp do sieci Darknet szerszej grupie odbiorców, wojsko oraz instytucje rządowe i organy ścigania nadal należą do głównych użytkowników ukrytego internetu. Dzieje się tak, ponieważ zwykłe przeglądanie internetu może ujawnić lokalizację użytkownika, a nawet, jeśli

---

6 Y. He, D. Xin, V. Ganti, S. Rajaraman, N. Shah, *Crawling deep web entity pages*, „Proceedings of the sixth ACM international conference on Web search and data mining", ACM 2013, s. 355.

7 D.K. Sharma, A.K. Sharma, *Deep Web Information retrieval Process*, „The Dark Web: Breakthroughs in Research and Practice", IGI-Global 2017, s. 114.

8 D. Omand, *The Dark Net Policing the Internet's Underworld,* „World Policy Journal" 2015, nr 32(4), s. 75–82.

9 E. Jardine, *The Dark Web dilemma: Tor, anonymity and online policing*, „Global Commission on Internet Governance" 2015, nr 21, s. 7.

10 P. Syverson, G. Boyce, *Genuine onion: Simple, fast, flexible, and cheap website authentication*, 2015, https://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/15-1231-0478.pdf [dostęp: 2.09.2017].

treść komunikatów jest dobrze zaszyfrowana, osoby niepożądane nadal mogą łatwo dojść do informacji personalnych osób komunikujących się i potencjalnie odkryć, gdzie dokładnie się znajdują. Dla żołnierzy i agentów w terenie, polityków prowadzących tajne negocjacje i w wielu innych okolicznościach, które można z łatwością przywoływać, stanowi to niedopuszczalne zagrożenie dla bezpieczeństwa[11].

Darknet jest także popularny wśród dziennikarzy i blogerów politycznych, zwłaszcza tych mieszkających w państwach, gdzie cenzura i więzienie polityczne są powszechne, co zostanie omówione wraz z konkretnymi przykładami w dalszej części artykułu. Anonimowość online pozwala ludziom, a także informatorom komunikować się ze swoimi „źródłami" i publikować informacje bez obaw o swoje bezpieczeństwo. Ta sama anonimowość może być również wykorzystywana przez czytelników wiadomości w celu uzyskiwania dostępu do informacji umieszczonej na sieci lokalnej, która jest blokowana przez różnorakie, stworzone do tego celu agencje, funkcjonujące głównie w reżimach autorytarnych, czy totalitarnych[12]. Aktywiści i rewolucjoniści używają również ciemnej sieci w celu niczym nieskrępowanej samoorganizacji, bez obawy o interwencję władz, w stosunku do których stoją w opozycji[13].

Z powyższego wynika, że pełna anonimowość jest możliwa do osiągnięcia w sieci, choć częstokroć dane jest nam słyszeć komunikaty, że wszystko, co robimy w sieci, może nas w prosty sposób zidentyfikować. Jest to niewątpliwie racja, a dla przeciętnego użytkownika sieci korzystanie z narzędzi Darknetu kojarzy się z czymś skomplikowanym, nieosiągalnym, kojarzone jest ze skomplikowanymi procedurami i superszybkimi, nowoczesnymi komputerami. Okazuje się jednak, że korzystanie z ciemnej sieci nie jest szczególnie skomplikowane – przynajmniej do pewnego stopnia – i nie pociąga za sobą konieczności inwestowania w nowinki technologiczne. Warto zatem pokrótce przyjrzeć się dostępnym narzędziom oferującym eksplorowanie zasobów Darknetu.

Dostęp do Darknetu – surfowanie po ciemnej stronie sieci

Dostęp do ukrytego internetu, wbrew powszechnie panującej opinii, jest zaskakująco prosty[14]. Przekonanie o skomplikowanym dostępie do tej części zasobów i kojarzenie przestrzeni Darknetu z wysoko wykwalifikowanymi hakerami bierze się raczej z niewiedzy, nieznajomości narzędzi i zasłyszanych, wyrywkowych informacji

[11] M. Aschmann, L.L. Michael, J. Jansen van Vuuren. *The utilisation of the deep web for military counter terrorist operations,* „Academic Conferences and publishing limited" 2017, https://researchspace.csir.co.za/dspace/bitstream/handle/10204/9261/Aschmann_18774_2017.pdf?sequence=1, [dostęp: 2.09.2017].

[12] Q. Wang, *Censorspoofer: asymmetric communication using ip spoofing for censorship-resistant web browsing*, „Proceedings of the 2012 ACM conference on Computer and communications security", ACM, 2012, https://www.researchgate.net/publication/221672885_CensorSpoofer_Asymmetric_Communication_with_IP_Spoofing_forCensorship-Resistant_Web_Browsing [dostep: 2.09.2017].

[13] A. Klimburg, *Roots Unknown–Cyberconflict Past, Present & Future*, „S&F Sicherheit und Frieden" 2014, nr 32.1, s. 2.

[14] A. Murray, *The dark web is not just for paedophiles, drug dealers and terrorists*, „Independent" 2014, http://www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html [dostep: 3.09.2017].

przekazywanych przez media głównego nurtu. Najbardziej popularnym, wspomnianym już wcześniej sposobem na rozpoczęcie eksploracji ukrytej sieci jest zainstalowanie narzędzia Tor, co oznacza The Onion Router (TOR). Jest to jedno z najwcześniejszych i najbardziej popularnych narzędzi sieci cebulowej[15]. Technicznie zaawansowani użytkownicy mogą znaleźć wiele różnych sposobów konfigurowania i używania Tor, niemniej korzystanie z niego dla przeciętnego użytkownika sieci, nieposiadającego głębszej wiedzy programistycznej, może być tak proste, jak instalacja nowej przeglądarki. Wystarczy być zatem średniozaawansowanym internautą, który potrafi zainstalować dowolny program na swoim komputerze. Zaledwie kilka kliknięć z witryny Tor jest wystarczające, aby uzyskać dostęp do zasobów ciemnej sieci. Omawiana przeglądarka jest zbudowana na bazie otwartego kodu źródłowego powszechnie dostępnej i wciąż popularnej przeglądarki Firefox, zatem każdy, kto kiedykolwiek korzystał z tego narzędzia, znajdzie przeglądarkę Tor przyjazną i łatwą w użyciu[16].

Przeglądarka Tor daje użytkownikowi zdecydowanie większy potencjał zachowania anonimowości w wirtualnej przestrzeni, może być używana do surfowania po stronach WWW dając jednocześnie użytkownikowi dodatkową ochronę przed niepożądanymi obserwatorami ruchu sieciowego[17], a przede wszystkim chroni użytkownika przed hakerami, różnymi formami szpiegostwa w internecie, gromadzeniem danych osobowych bez woli i zgody użytkownika oraz zbieraniem innych wrażliwych informacji. Narzędzie daje także możliwość odwiedzania witryn publikowanych anonimowo w sieci, które są niedostępne dla osób surfujących po wirtualnej przestrzeni w tradycyjny sposób. Jest to jedna z najczęściej wykorzystywanych funkcjonalności przeglądarki[18].

Przyporządkowane witrynom Tor adresy nie wyglądają jak zwykłe adresy URL, do których przeciętny użytkownik jest przyzwyczajony. Składają się z losowo przyporządkowanych linijek tekstu składających się z losowego ciągu znaków[19]. Oto przykład ukrytego adresu WWW: http://dppmfxaacucguzpc.onion/. Połączenie z tego typu adresem spowoduje przeniesienie użytkownika bezpośrednio do katalogu ukrytych stron internetowych, jeśli jednak użytkownik nie ma zainstalowanego wymaganego oprogramowania, mimo że natrafi na link, po wysłaniu żądania połączenia z witryną nie wyświetli mu się jakakolwiek zawartość. Najprościej rzecz ujmując, korzystanie z Tora pozwala na znalezienie katalogów, plików wiki i bezpłatnych linków, które prowadzą użytkownika do pożądanych przez niego treści.

Warto również zaznaczyć, że Tor nie jest jedynym z grupy narzędzi umożliwiających niezauważalne przemykanie po zasobach ukrytej sieci. Do tego celu skonstruowano

---

15 *Darknet: ciemna strona internetu*, http://www.komputerswiat.pl/artykuly/redakcyjne/2016/10/darknet-ciemna-strona-internetu.aspx [dostęp: 6.09.2017].

16 *Ibidem*.

17 A. Chaabane, P. Manils, M.A. Kaafar, *Digging into anonymous traffic: A deep analysis of the tor anonymizing network*, „Network and System Security (NSS), 2010 4th International Conference on. IEEE", 2010, s. 167–168.

18 M. Spitters, S. Verbruggen, M. van Staalduinen, *Towards a comprehensive insight into the thematic organization of the tor hidden services*, „Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint", IEEE, 2014, s. 221–222.

19 Przykładem adresu strony w ramach przeglądarki TOR jest adres http://dppmfxaacucguzpc.onion.

i konstruuje się do tej pory rozmaite narzędzia oraz programy, które niejednokrotnie odznaczają się nieco bardziej rozbudowanymi funkcjonalnościami. Chodzi między innymi o aplikacje do udostępniania plików peer-to-peer (łączność bezpośrednia między danymi użytkownikami). W tym wypadku najpopularniejszy serwis, jakim jest Tor, nie daje użytkownikom komfortu wymiany plików p2p, ponieważ sieć ta nie została przystosowana do obsługi tak dużego ruchu[20]. Sieć, którą warto przywołać w pierwszej kolejności to I2P (Invisible Internet Project), a której to popularność notuje wzrost. Jest to projekt, który oferuje wiele ulepszeń, takich jak zintegrowane bezpieczne wiadomości e-mail, przechowywanie i udostępnianie plików plug-in oraz zintegrowane funkcje społecznościowe, takie jak blogowanie i czat[21].

Równie popularnym i zarazem sprawdzonym narzędziem jest przeglądarka Freenet, która podobnie jak omówiona wyżej, jest anonimową siecią typu peer-to-peer dostępną za pośrednictwem bezpłatnie pobranej aplikacji. W tym typie sieci nie ma scentralizowanych serwerów, które przechowują informacje lub przesyłają dane. Każdy komputer, który łączy się z siecią, bierze niejako na siebie zadanie dzielenia się informacjami[22].

Tabela 1. Podstawowe różnice pomiędzy obydwoma narzędziami

Darknet	URL	Wykorzystywane protokoły P2P	Wykorzystywane aplikacje P2P
I2P	http://www.i2p2.de	Gnutella, BitTorrent, eDonkey	I2Phex, I2PSnark, iMule
Freenet	https://freenetproject.org	Freenet	Frost

Źródło: S. Aked, *An investigation into darknets and the content available via anonymous peer-to-peer file sharing*, „Australian Information Security Management Conference", Perth Western Australia 2011, s. 11.

Gdy użytkownik instaluje Freenet, jego komputer nawiązuje połączenie z małą grupą istniejących już użytkowników Freenet. Każda z nich jest połączona z innymi komputerami użytkowników Freenet. Dzięki tym połączeniom cała zawartość sieci jest dostępna dla każdego użytkownika. Ten projekt pozwala Freenetowi być systemem skrajnie zdecentralizowanym, anonimowym i odpornym na nadzór i cenzurę[23].

Oprogramowanie Freenet wymaga od użytkowników udostępnienia części lokalnej przestrzeni dyskowej do przechowywania materiałów Freenet. Te informacje

[20] S. Aked, *An investigation into darknets and the content available via anonymous peer-to-peer file sharing*, „Australian Information Security Management Conference", Perth Western Australia 2011, s. 11.

[21] *Ibidem*.

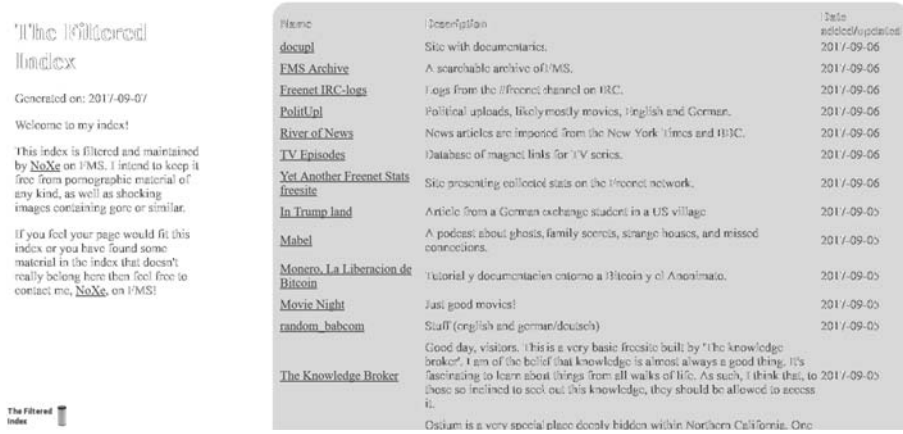
[22] T. Lu, *On Privacy and Anonymity in Freenet System*, „International Journal of Security and Its Applications" 2016, Vol. 10, nr 5, s. 41–42.

[23] R. Graham, B. Pitnam, *Far beyond crime-ridden depravity, darknets are key strongholds of freedom of expression online*, https://theconversation.com/far-beyond-crime-ridden-depravity-darknets-are-key-strongholds-of-freedom-of-expression-online-71598 [dostęp: 6.09.2017].

są automatycznie szyfrowane, więc właściciel komputera nie wie, jakie pliki są przechowywane, a także, jaka jest zawartość tych plików. Pliki udostępnione w sieci są przechowywane na wielu komputerach, zapewniając dostęp do nich nawet wtedy, gdy część użytkowników wyłączy swoje maszyny[24].

Sieć skonstruowana została tak, że umożliwia wiele różnych rodzajów interakcji, co w wyraźny sposób odróżnia ją od Tor. Nie brakuje tam takich funkcjonalności, jak wewnętrzne serwisy społecznościowe, dające możliwość budowania bezpośrednich relacji z innymi użytkownikami[25]. Istnieje kilka witryn programu Freenet, które wykorzystują wyszukiwarki sieciowe do indeksowania stron, oferując katalogi dostępnej zawartości. Witryny z indeksami są częścią sieci Freenet, a zatem mogą być dostępne tylko dla użytkowników, którzy pobrali i zainstalowali dedykowane oprogramowanie. Co zrozumiałe, standardowe wyszukiwarki nie mają zastosowania do wyszukiwania witryn na stronie Freenet.

Rysunek 1. Przykładowe katalogi w ramach Freenet



Źródło: badania własne.

Darknet w służbie wolności informacji

Większość form szyfrowania stała się podstawą nowoczesnego internetu i wszechobecnej infrastruktury informatycznej. Szyfrowanie zostało powszechnie uznane za kluczowe dla ochrony wolności słowa, prywatności i handlu. Darknet to miejsce, które dysponuje pięcioma głównymi właściwościami – bezpieczeństwem przesyłu danych, uwierzytelnianiem, anonimowością, cyfrowymi walutami i ukrytą wymianą plików[26]. Rząd brytyjski szyfruje prawie wszystkie swoje strony, a rząd Stanów Zjednoczonych planuje to zrobić w najbliższej przyszłości. Daje to szansę ochrony przed

[24] *Ibidem*.

[25] T. Lu, *On Privacy and Anonymity…*, *op. cit.,* s. 48.

[26] D. Moore, T. Rid, *Cryptopolitik and the Darknet*, „Survival" 2016, vol. 58, nr 1, s. 26.

działalnością hakerów paraliżujących rządowe systemy. Głównie przez wzgląd na bezpieczeństwo, najbardziej liberalne demokracje przyjęły zakrojone na szeroką skalę wdrożenia systemów szyfrowania, jako korzystny i niezbędny element rozwoju wewnętrznej infrastruktury informatycznej.

Zgodnie z przyjętym założeniem badawczym, należy w tym miejscu przejść do problemu, który wydaje się niejednokrotnie pomijany w rozważaniach na temat ciemnej sieci, koncentrujących się na ukazaniu możliwości, jakie stwarza korzystanie z Darknetu dla różnego typu organizacji przestępczych. Chodzi mianowicie o miejsca, w których opresyjne reżimy nie tylko limitują dostęp do internetu, ale śledzą poczynania swoich obywateli na szeroką skalę. Wszechobecna cenzura hamuje kiełkujące ruchy prodemokratyczne i wolnościowe, eliminując podejmowane próby zmiany systemu. Przykładem krajów znacząco limitujących dostęp do samej sieci są Erytrea i Korea Północna. Zgodnie z listą opracowaną przez Komitet Ochrony Dziennikarzy (Committee to Protect Journalists) z 10 krajów, w których prasa jest najbardziej ograniczona, państwa te zajęły niechlubne dwa pierwsze miejsca. Lista oparta jest na badaniach nad wykorzystywaniem przez reżimy różnorodnych taktyk, począwszy od więzienia dziennikarzy i represyjnych przepisów, po ograniczanie dostępu do internetu[27].

Obawiając się rozprzestrzeniania się ruchów rewolucyjnych w ramach Arabskiej Wiosny w 2011 roku, Erytrea zrezygnowała z planów zapewnienia swoim obywatelom internetu mobilnego, ograniczając tym samym możliwość dostępu do niezależnych informacji[28]. Chociaż internet jest w pewnym (mocno ograniczonym) stopniu dostępny, to jedynie przez połączenia typu dial-up, a do tego mniej niż 1% populacji ma możliwość korzystania z sieci.

Drastycznie odmienna sytuacja panuje obecnie w Chinach, bowiem pomimo setek milionów użytkowników internetu, chińskie władze podtrzymują tak zwaną „Wielką Zaporę" (Great Firewall), polegającą na utrzymywaniu rzeszy cenzorów wykorzystujących zaawansowane narzędzia technologiczne w celu blokowania stron internetowych z treściami krytykującymi poczynania rządu[29]. Infiltracji podlegają też serwisy społecznościowe, gdzie nie dość, że publikowane treści są usuwane, to stosuje się również propagandową działalność przybierającą formę agitacji na rzecz rządu.

W krajach zaawansowanych technologicznie, takich jak wspomniane wyżej Chiny, wszechobecna cenzura internetu idzie w parze z surowymi karami i groźbami więzienia w celu zagwarantowania konsekwentnego uciszania krytycznych głosów w sieci. Egzemplifikacją tego jest fakt, że aż 32 z 44 więzionych w Chinach dziennikarzy pracowało online. Prześladowanie przez rząd jest zatem powszechną taktyką stosowaną w co najmniej pięciu najbardziej cenzurowanych krajach. Przykładowo w Wietnamie wielu blogerów znajduje się pod ścisłym nadzorem władz w celu zapobieżenia upowszechniania informacji o niewygodnych dla władz wydarzeniach. W Iranie krewni dziennikarzy zostali wezwani przez władze i poinformowani, że mogą stracić pracę oraz emerytury z powodu publikacji niepochlebnych treści w sieci.

---

[27] *Ibidem*.

[28] Zob.: A. Zieliński, K. Zieliński, *Mobile telecommunication systems changed the electronic communications and ICT market*, „Journal of Telecommunications and Information Technology" 2013, nr 2, s. 8.

[29] *Beijing moves to bolster its Great Firewall of China*, „The Telegraph" 2017, http://www.telegraph.co.uk/news/2017/07/11/beijing-moves-bolster-great-firewall-china/ [dostęp: 8.09.2017].

Co więcej, władze są podejrzewane o tworzenie fałszywych wersji popularnych witryn i wyszukiwarek w ramach rozbudowanych technik nadzoru[30].

Ograniczanie swobodnej działalności dziennikarzy i zakaz przyjmowania korespondentów zagranicznych jest nader powszechną taktyką stosowaną przez cenzurę opresyjnych rządów. Lista najbardziej cenzurowanych krajów dotyczy tylko tych, w których rządy ściśle kontrolują media, a istnieje szereg przykładów, gdzie praktyki tego typu są stosowane na nieco mniejszą skalę. W niektórych krajach, zwłaszcza w Syrii, warunki są niezwykle niebezpieczne – dziennikarze są represjonowani, przetrzymywani i zabijani, niektórzy przez siły lojalne wobec reżimu Bashara al-Assada, inni przez grupy bojowe tak zwanego państwa islamskiego[31].

Przykłady tego typu można mnożyć i jak widać, wolność słowa, do której przyzwyczajeni są obywatele krajów demokratycznych, w różnych obszarach globu pozostaje jednak mocno nadszarpnięta. A zatem warto się zastanowić, w jaki sposób pokonać tę machinę zewnętrznej opresji albo choć w pewnym stopniu ją osłabić. Z pewnością nie kosztem bezpieczeństwa dziennikarza. Sytuacja w krajach, gdzie sieć internet praktycznie nie istnieje jest zdecydowanie trudniejsza, natomiast w obszarach, gdzie istnieje pokrycie, w sukurs mogą przyjść omówione wyżej narzędzia Darknetu. Ciemna strona sieci może okazać się światełkiem w tunelu i pomóc upowszechniać informację bez narażania się na tak wielkie niebezpieczeństwo.

Ciemna sieć, jak już było wcześniej argumentowane, jest obszarem często niezrozumianym przez rząd i ogół społeczeństwa. Publikacje poczytnych gazet, zarówno tradycyjnych, jak i internetowych, wydają się być jednoznacznie negatywne w stosunku do Darknetu, przywołują głównie czarnorynkowe transakcje i nielegalną działalność grup handlarzy narkotykami czy pedofilów. Podobnie jak w przypadku wszystkich obszarów życia, element kryminalny w ciemnej sieci jest obecny, niemniej jednak prawdopodobnie nie występuje w większym nasileniu, niż w ramach tradycyjnej sieci[32]. Niewątpliwie można znaleźć witryny oferujące narkotyki, obecne są też nadużycia związane z dziecięcą pornografią, ale można je również znaleźć w ogólnodostępnym internecie. Sieć, do której dostęp jest możliwy wyłącznie poprzez oprogramowanie korzystające z silnej kryptografii, zapewnia osobiste bezpieczeństwo i anonimowość osobom zagrożonym oraz represjonowanym przez niedemokratyczne reżimy, umożliwiając im swobodne przekazywanie obiektywnych treści na zewnątrz, dzięki czemu informacja może trafić do szerszej grupy odbiorców, przede wszystkim tych za granicą.

Co interesujące, Reporterzy bez Granic zalecają użycie narzędzi Darknetu dla blogerów, dziennikarzy i aktywistów w krajach, w których mogą być zagrożone z powodu cenzury lub nawet aresztowania[33]. Międzynarodowe Biuro Broadcastingu (które

---

30 https://cpj.org/2015/04/10-most-censored-countries.php [dostęp: 8.09.2017].

31 J. Ball, B. Schneier, G. Greenwald, *NSA and GCHQ target Tor network that protects anonymity of web users*, „The Guardian", 14.10.2013, https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption [dostęp: 11.09.2017].

32 M. Spitters, S. Verbruggen, M. Staalduinen, *Towards a comprehensive insight into the thematic organization of the tor hidden services*, „Intelligence and Security Informatics Conference" (JISIC) 2014*,* IEEE, s. 223.

33 M. Mahdian, *Fighting censorship with algorithms,* [w:] P. Boldi, L. Gargano, *Fun with Algorithms,* Berlin/Heidelberg 2010, s. 296–297.

emituje Głos Ameryki i Radio Free Asia) jest głównym sponsorem Tora i rekomenduje jego wykorzystanie przez osoby znajdujące się pod władzą represyjnych reżimów, aby umożliwić im dostęp do globalnych mediów. Tor jest także zalecany i wspierany przez takie organizacje jak Human Rights Watch i Global Voices, a nawet giganta ogólnodostępnych serwisów internetowych – firmę Google[34].

Nie tylko organizacje praw człowieka i grupy medialne, zalecają wykorzystanie narzędzi Darknetu; specjaliści IT i kadra zarządzająca także wykorzystuje silnie szyfrowane połączenia między innymi do testowania skuteczności implementowanych systemów Firewall, zapewnienia awaryjnego dostępu do internetu podczas awarii DNS i zagwarantowania poufności sieciowej korespondencji.

Wskazać można tutaj pewną prawidłowość. Biorąc pod uwagę państwa, w których dostęp do internetu nie jest limitowany, można zauważyć istotny rozziew między tymi, które odnoszą się do szyfrowania i Darknetu w sposób stosunkowo przyjazny a tymi, które wszelkimi sposobami próbują dyskredytować, a nawet blokować dostęp do ciemnej sieci. W Rosji powołano wyspecjalizowane organy, mające na celu cenzurować przestrzeń internetu. Przykładowo Tor opisywany jest jako „niewidzialny internet", który umożliwia kryminalistom ukrywanie swoich działań przed władzami i organami wymiaru sprawiedliwości, w celu popełniania przestępstw, takich jak: handel narkotykami oraz bronią, rozpowszechnianie pornografii dziecięcej, angażowanie się w sprawy handlu ludźmi i prowadzenie nielegalnych kampanii politycznych[35]. Prawdą jest to, że stwierdzenia te nie są wcale błędne, niemniej jednak jest to obraz wyrywkowy, mający uzasadnić walkę z ciemną siecią i ukazywać ją wyłącznie w niekorzystnym świetle. Polityka Chin i Rosji w zakresie szyfrowania nie może być łatwo pominięta, bowiem kształtuje ona rzeczywistość 1,5 miliarda osób w sieci. Te dwa potężne kraje ustanawiają de facto normy dla dużej liczby krajów nienależących do świata demokratycznego[36].

Szczególna wartość anonimowej, ciemnej sieci w krajach o rozwiniętej demokracji znajduje swoje odzwierciedlenie w raporcie finansowym projektu Tor. Widzimy, że otrzymał on ponad 1,8 miliona dolarów dotacji od rządu Stanów Zjednoczonych w 2013 roku, co stanowi ponad 50% całkowitych dochodów przedsięwzięcia na wskazany rok. Dotacje pochodzą z wielu zasobów, w tym ponad 555 000 dolarów z Internetwork News, organizacji typu non-profit działającej na rzecz demokracji i praw człowieka, finansowanej przez Departament Stanu USA oraz ponad 830 000 dolarów pochodzących z Departament Obrony USA[37]. Wydaje się zatem mało prawdopodobne, aby rząd USA finansował narzędzia wspomagające nielegalne działania w sieci, na czele z pedofilią, handlem narkotykami i terroryzmem. Dodając do tego argumenty wcześniej wskazane, a dotyczące prostej obsługi narzędzi i braku szczególnych wymagań technicznych, można przyjąć, że Darknet stwarza takie możliwości dla dziennikarzy i blogerów z obszarów dotkniętych cenzurą, jakich nie daje jakikolwiek inny instrument komunikacji online.

---

[34] K.D. Watson, *The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks*, „Wash. U. Global Stud. L. Rev." 2012, 11, s. 718.

[35] D. Moore, T. Rid, *Cryptopolitik…*, *op. cit.,* s. 30.

[36] *Ibidem*.

[37] J. Cole, *Dark Web 101*, Air Force Air Command and Staff College Maxwell AFB United States 2016, http://www.dtic.mil/get-tr-doc/pdf?AD=AD1005862, s. 3–4 [dostęp: 11.09.2017].

Podsumowanie

Niewątpliwie anonimowość technologii Darknetu posiada dwie, przeciwstawne moralnie strony. Podczas gdy ludzie mogą korzystać z ukrytej sieci w celach przestępczych, mogą też używać jej dla dobra ogółu i w celu ochrony swojej prywatności, czy zapewnieniu sobie bezpieczeństwa. Anonimowość jest ważna przez wzgląd na możliwości, jakie stwarza dla krzewienia demokracji i podtrzymywania jej fundamentów. Zapewnia przestrzeń dla wolności ekspresji oraz wyrażania opinii sprzecznych z tymi, które głosi władza. I dalej, anonimowość zapewnia zarówno ochronę jednostki, która niejednokrotnie pełni rolę rzecznika mniejszości, a także kreuje szanse, aby przyjęte przez władzę rozwiązania były krytykowane i kwestionowane przez ludzi o odmiennych poglądach. Innymi słowy anonimowość to swego rodzaju tarcza chroniąca przed zakusami rządzącej większości, stanowiąca niejednokrotnie ostatni bastion demokracji. W krajach niedemokratycznych, jak zostało wykazane, istnienie anonimowości jest jedynym sposobem, dzięki któremu ludzie mogą prezentować odmienne – względem despotycznych reżimów – punkty widzenia, w nadziei na zapewnienie choć częściowej wolności politycznej.

Tor Project, poprzez swoją stronę internetową, zachęca działaczy politycznych, dysydentów, dziennikarzy i reformatorów – ludzi, którym bliskie są prawa i wolności obywatelskie, by używać narzędzi Darknetu w krajach stosujących represje wobec dziennikarzy oraz limitujących wolność słowa[38]. Aplikacje te są zatem jednym z niewielu możliwych rozwiązań pozwalających nie tylko obejść cenzurę opresyjnej władzy, lecz również chronić się przed poważnymi represjami z jej strony[39].

Jak wcześniej zostało podkreślone, korzystanie z anonimowej sieci było i jest rekomendowane przez grupy i organizacje zajmujące się ochroną praw człowieka, pośród których wymienić można chociażby Human Rights Watch, Reporterów bez Granic, czy Global Voices. Wszystkie sugestie dotyczące korzystania z ciemnej sieci zdają się pomijać istniejące w jej ramach nadużycia, niemniej jednak prasowe doniesienia, czy nawet naukowe analizy dotyczące aktów przestępczych, są zdecydowanie powszechniejsze, niż przykładowo ukazywanie znaczenia tego narzędzia dla kształtowania postaw prodemokratycznych i wolności słowa. W chwili obecnej nie potrafimy sprostać idealistycznym założeniom Darknetu, który ma być przede wszystkim miejscem wolnej wymiany idei i poglądów oraz przestrzenią wolną od manipulacji i zapewniającą bezpieczny oraz anonimowy dostęp do prawdy. Najogólniej rzecz ujmując, najlepszym z możliwych, choć w chwili obecnej utopijnym, scenariuszem byłaby sytuacja, w której ludzie przestaliby używać Darknetu do prowadzenia nielegalnej

---

[38] Państwa takie jak Chiny czy Rosja, a więc należące do grupy państw o wysokim zaawansowaniu infrastruktury informatycznej, w tym internetu, robią wszystko, by blokować usługi posługujące się silnym szyfrowaniem. Walka chińskiego rządu z Torem trwa od kilku lat, a w chwili obecnej coraz częściej słyszy się, że do tejże przyłącza się również Rosja. Zob.: K. McCarthy, *Russia, China vow to kill off VPNs, Tor browser New laws needed because today's censorship not good enough, apparently*, „The Register" 2017, https://www.theregister.co.uk/2017/07/11/russia_china_vpns_tor_browser [dostęp: 12.09.2017].

[39] Pomimo że Tor cieszy się szczególnym zainteresowaniem władz państw niedemokratycznych, istnieje szereg innych możliwości poruszania się w ciemnej sieci, a część z nich została w ramach niniejszego artykułu omówiona.

działalności. Jednakże mimo że nie można wykorzenić „ciemnej strony" ciemnej sieci, nie należy zdyskredytować, pomijać i lekceważyć jej jasnej strony, ponieważ w pewnych okolicznościach może się okazać, że jest to jedyne dostępne narzędzie wolnego i rzetelnego dziennikarstwa.

Darknet. Ostatni bastion wolności w internecie?
Streszczenie

Przedmiotem artykułu jest analiza możliwości zastosowania różnego typu narzędzi Darknetu, czyli ciemnej sieci do ochrony prywatności i zapewnienia bezpieczeństwa aktywistom oraz dziennikarzom działającym w rejonach świata, gdzie dostęp do rzetelnej informacji jest limitowany, bądź blokowany przez opresyjne reżimy. Dokonano przeglądu wspartych na bezpłatnym oprogramowaniu narzędzi, w kontekście ich głównych funkcjonalności polegających na maskowaniu lokalizacji i działań użytkowników, dając tym samym możliwość rzetelnego i bezpiecznego przekazywania informacji na zewnątrz. W ciągu ostatniej dekady przeglądarki Darknetów umożliwiły aktywistom rozpowszechnianie informacji o wydarzeniach toczących się między innymi podczas Arabskiej Wiosny oraz w trakcie innych akcji, mających na celu wzmocnienie ruchów wolnościowych i prodemokratycznych, sprzeciwiających się opresyjnym władzom.
Słowa kluczowe: Darknet, Tor, Freenet, ciemna sieć, dziennikarstwo, bezpieczeństwo, wolność informacji, prywatność

Darknet. The Last Bastion of Freedom on the Internet?
Abstract

The purpose of the article is an analysis of the potential use of various types of Darknet tools in privacy protection and ensuring the safety of activists or journalists operating in places, where access to reliable information is limited or blocked. An overview of free software tools will be provided in the context of their main functionality such as: masking user locations and activities, free spreading of the information, and finally providing the possibility of reliable and secure communication. During the last decade, Darknet's browsers have enabled activists to disseminate information concerning events taking place during The Arab Spring, and other actions aimed at strengthening the libertarian and pro-democracy movements opposed to the oppressive authorities.
Key words: Darknet, Tor, Freenet, journalism, security, freedom of information, privacy

Даркнет. Последний оплот свободы в Интернете?
Резюме

В статье дан анализ возможности применения различных типов инструментов Даркнета (темной сети), для защиты конфиденциальности и обеспечения безопасности активистам и журналистам, работающим в тех регионах мира, в которых доступ к достоверной информации ограничивается или блокируется существующими режимами. Дан обзор основанных на бесплатном программном обеспечении инструментов в контексте их основных функциональных возможностей, заключающихся в маскировке местонахождения и действий пользователей, тем самым

давая возможность надежной и безопасной передачи информации. В течение последнего десятилетия браузеры Даркнета позволили активистам распространять информацию о событиях, происходящих, напр., во время Арабской Весны, а также в ходе других действий освободительных или демократических сил, ведущих борьбу с деспотическими властями.
Ключевые слова: Даркнет (Darknet), Tor, Freenet, темная сеть, журналистика, безопасность, свобода информации, неприкосновенность частной жизни