ACTA UNIVERSITATIS LODZIENSIS
FOLIA IURIDICA 82, 2018

http://dx.doi.org/10.18778/0208-6069.82.07

Hubert Wojciechowski[*]

DARKNET – WYBRANE ASPEKTY KRYMINOLOGICZNE, KRYMINALISTYCZNE I PRAWNE SZYFROWANYCH SIECI KOMPUTEROWYCH

Streszczenie. W artykule poruszono kwestie dotyczące sieci szyfrowanych, ich zawartości i bezpieczeństwa. Wyjaśnione zostały takie terminy, jak: Darknet, Deep Web i Dark Web. Opracowanie przedstawia aspekty techniczne programu The Onion Router oraz jego genezę. Omówiono również cechy charakterystyczne użytkowania takiego narzędzia oraz społeczności, która wokół niego się wytworzyła. Przedstawiona została ocena prawna i kryminalistyczna aktywności zlokalizowanej w Darknecie. Autor stoi na stanowisku, iż fenomen programu TOR nie powinien być oceniany negatywnie i przewiduje jego gwałtowny rozwój.

Słowa kluczowe: Darknet, The Onion Router Project, whistleblowing, bitcoin, Silk Road.

1. WPROWADZENIE

Wielu użytkowników Internetu, korzystając ze swoich skrzynek pocztowych, serwisów o różnorodnej tematyce czy kont na portalach społecznościowych, nie zdaje sobie sprawy z faktu, iż ich ulubione strony stanowią tylko niewielką część sieci. Istnieje także część sieci globalnej, zwana Deep Web, która nie jest dostępna w drodze zwykłego wyszukiwania poprzez przeglądarki internetowe (Wright 2009). Przykładem takiej zawartości mogą być konta chronione hasłami, serwisy archiwizujące stare wersje stron internetowych czy sieć stanowiąca zwykłe zaplecze techniczne. W ramach Deep Web można wyróżnić Dark Web (Greenberg 2014), czyli treści dostępne jedynie poprzez połączenia powstałe dzięki specjalnym oprogramowaniom. Tego typu sieć, wyodrębniona od pozostałej, powszechnie dostępnej zawartości, tworzy Darknet. Istniała ona już w ramach pierwotnego wojskowego ARPANETU (Advanced Research Projects Agency Network), zanim wyodrębnił się z niego cywilny, znany nam współcześnie Internet. Współcześnie spopularyzowaną nazwę stworzyli pracownicy korporacji Microsoft w artykule z 2002 r. (Biddle i in. 2002, 2) Istnieje wiele takich sieci, a każda z nich jest dostępna dzięki innemu oprogramowaniu, np.: I2P (Invisible Internet Project), Freenet czy TOR (The Onion Router). Szacuje się, że spośród wymienionych

[*] Uniwersytet Łódzki, Wydział Prawa i Administracji, Katedra Postępowania Karnego i Kryminalistyki, hubertw@poczta.onet.pl.

narzędzi największą liczbę użytkowników posiada TOR (*Anticounterfeiting…* 2015, 1). Na potrzeby artykułu pobrałem wskazany program i korzystałem z niego celem opisania zasad jego działania i użytkowania.

2. HISTORIA I ZASADA DZIAŁANIA

System trasowania cebulowego[1], na podstawie którego działa program TOR, został stworzony przez matematyka Paula Syversona oraz informatyków Michaela G. Reeda i Davida Goldschlaga, pracowników laboratoriów Marynarki Wojennej Stanów Zjednoczonych. Celem projektu była ochrona informacji w sieci komputerowej. Od 1997 r. projekt nadzorowała Defense Advanced Research Projects Agency (Fagoyinbo 2013, 258). Pierwotna wersja programu TOR została stworzona 20 września 2002 r. przez wcześniej wspomnianego Paula Syverona oraz informatyków Rogera Dingledine i Nicka Mathewsona. W roku 2004 rząd Stanów Zjednoczonych udostępnił kod programu do domeny publicznej. Projekt w latach 2004–2005 uzyskał patronat finansowy organizacji Electronic Frontier Foundation zajmującej się aktywizmem na rzecz praw cyfrowych[2]. Obecnie nad jego rozwojem czuwa TOR Project – organizacja *non-profit*, która stawia przed sobą cele badawczo-naukowe. Utrzymuje się z różnych źródeł; są to przede wszystkim darowizny. Do grona głównych sponsorów projektu należą m.in. rząd Stanów Zjednoczonych, Ministerstwo Spraw Zagranicznych Republiki Federalnej Niemiec, korporacje Google, Reddit czy organizacja Human Rights Watch. TOR Project wsparło także wiele pojedynczych osób[3].

Celem TOR jest zapewnienie anonimowości swoim użytkownikom, tak aby wyśledzenie ich tożsamości, adresu IP oraz lokalizacji w sieci było możliwie najtrudniejsze. Istota działania programu opiera się na wielowarstwowym szyfrowaniu danych. Zakodowane pakiety informacji (pod postacią np. wiadomości e-mail, ogłoszeń na stronach czy postów na forach) przesyłane są przez szereg losowo wybranych serwerów pośredniczących[4], zwanych również węzłami komunikacyjnymi lub routerami. Urządzenia te utrzymywane są przez osoby prywatne wspierające rozwój projektu TOR. Router po otrzymaniu danych

[1] Nazywany tak ze względu na wykorzystywanie wielowarstwowego szyfrowania danych (od ang. *onion* – cebula). Więcej na temat zasad działania w dalszej części tekstu.

[2] Tzw. *digital rights*, czyli prawa związane z dostępem do mediów i urządzeń cyfrowych, takie jak: walka o prywatność, anonimowość i wolność słowa w Internecie. Wiele z nich nawiązuje do istniejących praw człowieka.

[3] Informacje z głównej strony internetowej fundacji TOR Project: https://www.torproject.org/about/overview.html.en [dostęp 06.02.2017].

[4] Komputer, który w ramach połączonej sieci pośredniczy w przekazywaniu danych między komputerami. Inne rodzaje serwerów mogą świadczyć także inne usługi, takie jak: udostępnianie zasobów (pamięci, treści stron internetowych) innym komputerom.

w pierwszej kolejności usuwa jedną warstwę szyfru, aby móc uzyskać dostęp do adresu kolejnego węzła komutacyjnego, a następnie przesyła je dalej. Klucz do szyfru bezpośrednio zabezpieczającego treść pakietu informacji posiada wyłącznie ostatni węzeł komunikacyjny, który przesyła dane do serwera docelowego. Z perspektywy użytkownika odczytującego odszyfrowane wiadomości dane pochodzą z ostatniego węzła komunikacyjnego, a właściwy nadawca treści pozostaje nieznany. W ten sposób prawdopodobieństwo wykrycia tożsamości użytkowników matematycznie spada do zera, jednak nie oznacza to, że obecnie nie dokonuje się przełomów technologicznych w tej dziedzinie. Steven J. Murdoch i George Danezis, naukowcy z Uniwersytetu Cambridge, w artykule z 2006 r. (Murdoch, Danezis 2006, 3–7) wykazali możliwość zredukowania anonimowości sieci TOR. Obserwując jedynie fragmenty sieci, mogli wywnioskować, które węzły były wykorzystywane do „cebulowego" przekazywania danych. Ponadto, gwarantowana przez program anonimowość tożsamości nadawcy informacji nie jest równoznaczna z bezpieczeństwem treści danych, o czym może zaświadczyć następujący przykład. Podstawą działania takiej sieci są wspomniane węzły komunikacyjne, które utrzymują ochotnicy na swój własny koszt. Szwedzki konsultant do spraw bezpieczeństwa Dan Egerstad założył i monitorował własne serwery tego typu. W 2007 r. udało mu się przechwycić e-maile z około setki kont pocztowych zarejestrowanych w TOR (*The hack…* 2007). Na podstawie treści tych wiadomości można było wywnioskować, iż należały one m.in. do: ambasad Australii, Japonii, Iranu, Indii i Rosji, ministerstwa spraw zagranicznych Iranu, biura wizowego Wielkiej Brytanii w Nepalu czy kilku organizacji walczących o prawa człowieka z Hong Kongu (Zetter 2007). Przechwycenie danych powiodło się, ponieważ – jak wcześniej wspomniano – informacje między ostatnim węzłem komunikacyjnym a serwerem docelowym nie są szyfrowane, o ile nie są stosowane dodatkowe rodzaje zabezpieczeń.

3. UŻYTKOWANIE I SPOŁECZNOŚĆ

Z przedstawionych wyżej zasad działania wynika, iż przesył danych przez TOR jest znacząco utrudniony i wydłużony w stosunku do zwykłych, niezaszyfrowanych sieci. Rodzi to szereg poważnych konsekwencji wpływających na sposób użytkowania. Na podstawie korzystania z programu TOR dokonałem licznych obserwacji. Przede wszystkim program ma charakter przeglądarki internetowej, której wygląd bazuje na popularnym, darmowym programie Mozilla Firefox. Cechą charakterystyczną adresów stron w tej sieci jest to, iż kończą się na frazę *.onion*. Oprócz możliwości przeglądania wcześniej wspomnianej specjalnej, kodowanej treści, istnieje też możliwość przeglądania zwykłych, ogólnodostępnych stron internetowych. Dostęp do szyfrowanych treści nie zawsze jest możliwy, gdyż jest to uzależnione od faktu, czy serwer z daną zawartością pozostaje włączony. Nie

zawsze tak jest, ponieważ węzły komunikacyjne zakładane są w dużej mierze przez osoby prywatne, a ich utrzymanie wiąże się z wysokimi kosztami. Sieci typu Darknet działają znacznie wolniej niż zwyczajny Internet, ze względu na ograniczone możliwości przesyłu danych. Z tego powodu wygląd stron jest zazwyczaj bardzo skromny, oszczędny w grafiki czy pliki filmowe, niejednokrotnie ograniczony jedynie do tekstu. Ponadto, węzły komunikacyjne bardzo często są zaprogramowane przez użytkowników na domyślne blokowanie sposobów wymiany i dystrybucji plików powodujących zbyt duży przesył danych, np. protokoły BitTorrent. Dotyczy to również użytkowników wysyłających tzw. spam[5]. Administratorzy społeczności wewnątrz Darknetu traktują tego typu zachowania jeszcze bardziej restrykcyjnie niż w ramach nieszyfrowanego Internetu.

Ze względu na pewną specyfikę działania programu TOR wśród jego użytkowników wykształciła się szczególna etykieta. W używanym języku istnieje podział na „wtajemniczonych" użytkowników Darknetu i niczego nieświadomych zwykłych internautów. Niezwykle silne poczucie anonimowości panujące wśród użytkowników spowodowało, że osoby zarządzające stronami nie stosują jakiejkolwiek formy cenzury. Nie gwarantuje to zaufania, gdyż nie każdy jest tym, za kogo się podaje. Z tego względu każda osoba korzystająca z Darknetu musi zachować szczególną ostrożność. Oferty sprzedaży nielegalnych towarów mogą być prowokacjami przeprowadzanymi w celu późniejszego szantażu. W związku z tym powstał system budowania opinii, w którym istotną rolę odgrywają rekomendacje i opinie innych użytkowników. W ramach istniejących w sieci TOR serwisów aukcyjnych osobom sprzedającym często przyznawane są punkty zaufania za przeprowadzane transakcje. Punktacje stosują zarówno kupujący, jak i administracja danego serwisu. Zaobserwowałem również, że w celu uwiarygodnienia ogłoszenia osoby prowadzące stronę niejednokrotnie wymagają uiszczenia drobnej opłaty za samo zamieszczenie ogłoszenia. Zgodnie z opinią niektórych osób dłużej porozumiewających w ramach społeczności Darknetu początkujący sprzedawcy często udostępniają darmowe próbki lub egzemplarze towaru w celu zdobycia reputacji rzetelnego kontrahenta (*Co to jest Darknet?* 2012).

Możliwe są różne rodzaje płatności za usługi oraz namacalne dobra dostępne w sieci TOR, jednak metodą najczęściej spotykaną i gwarantującą największą anonimowość są bitcoiny. Stanowią one jedną z wielu istniejących kryptowalut, czyli rozproszony system księgowości[6]. Przechowuje on informację o stanie posiadania użytkownika w umownych jednostkach. Waluta przechowywana

[5] Tzn. niechciane i niepotrzebne wiadomości elektroniczne pojawiające się nie tylko w ramach Internetu, ale także w sieci telefonów komórkowych. Cechą treści takich wiadomości jest fakt, iż jest ona niezależna od tożsamości odbiorcy i pozwala przypuszczać, że nadawca poprzez jej wysłanie może odnieść zyski nieproporcjonalne w stosunku do korzyści odbiorcy.

[6] Kryptowaluta, czyli waluta zabezpieczona kryptografią. System rozproszony polega zaś na tym, że zbiór niezależnych, ale obsługujących się nawzajem urządzeń technicznych (znajdujących się na różnych komputerach) jest połączony w jedną spójną całość za pomocą sieci.

jest w węzłach systemu zwanych „portfelami", do których dostęp mają tylko ich użytkownicy i została zabezpieczona przed wielokrotnym wydawaniem danej jednostki wartości (Nakamoto 2009, 2). Wymieniać ją można na zwykłe waluty, zarówno elektronicznie na odpowiednich serwisach, jak i poprzez gotówkę w specjalnych bankomatach. W przypadku opisywanych wcześniej bitcoinów ich status prawny nie jest uregulowany we wszystkich państwach. Wytwarzanie kolejnych jednostek tej kryptowaluty jest jednak legalne. Przykładowo, Niemcy uznają je za walutę elektroniczną dopuszczalną w transakcjach prywatnych (Węglewski 2013), z kolei Tajlandia jest pierwszym krajem na świecie, który zakazał jej stosowania (*Bitcoin nielegalny…* 2013). Polska również nie ma regulacji prawnych dotyczących bitcoina. Zdaniem Szymona Woźniaka z Ministerstwa Finansów nie można uznać go za środek płatniczy, a według dyrektyw unijnych nie spełnia on kryteriów waluty elektronicznej (MinFin 2013). Natomiast zgodnie z jedną z podstawowych zasad prawa to, co nie jest zabronione, jest dozwolone. Zatem użytkownicy mogą swobodnie dokonywać tego typu transakcji, ale urząd skarbowy oczekuje, że zyski z takich operacji będą podlegać opodatkowaniu, tak jak dochody z praw majątkowych. Niezgłoszenie dochodów z handlu bitcoinami może spowodować wszczęcie procedury ze strony aparatu skarbowego, choć nie ma w tym zakresie żadnej praktyki. Transakcje zaś kwitną, np. Polska zgodnie z wyliczeniami dra Krzysztofa Piecha z Zakładu Polityki Gospodarczej Szkoły Głównej Handlowej znajduje się na dziesiątym miejscu na świecie pod względem wytwarzanych bitcoinów. Wskazany proces generowania bitmonet nazywany jest „wydobywaniem". Polega on na wbudowanym w system mechanizmie, w którym każdy użytkownik sieci weryfikujący transakcje ma małe prawdopodobieństwo otrzymania losowej ilości kryptowaluty. System ten ma jednak ograniczenia, mające na celu uniknięcie nadmiernej jego eksploatacji. Uzyskiwane wartości nigdy nie mogą przekroczyć sumy 12,5 bitcoinów, a z biegiem czasu spadają do zera. W związku z tym w jednym momencie w obiegu nie może zaistnieć więcej niż 21 milionów monet. Prawdopodobieństwo uzyskania partii kryptowaluty jest uzależnione od mocy obliczeniowej, jaką użytkownik wnosi do sieci oraz od łącznej mocy obliczeniowej całego systemu (Nakamoto 2009, 5).

4. ZAWARTOŚĆ I JEJ OCENA PRAWNA

Sieć TOR może być użytkowana w bardzo różnorodny sposób. Podstawowym kryterium klasyfikacji treści udostępnianych za pośrednictwem programu TOR, wyróżnianym przez badaczy Darknetu, jest podział na materiały zgodne z prawem i z nim sprzeczne. W pracy naukowej poświęconej klasyfikacji zawartości sieci TOR, pochodzącej z lutego 2016 r., badacze z King's College London w przeciągu 5 tygodni pracy odnaleźli 5205 aktywnych stron, z czego 2723 mogło być klasyfikowanych ze względu na rodzaj udostępnianych treści. 1547 stron zawierało

materiały nielegalne (Moore, Rid 2016, 19). Wiele usług zgodnych z prawem niczym nie różni się od tych udostępnianych w ramach niezaszyfrowanego Internetu, np. adresy e-mail, wyszukiwarki internetowe, komunikatory internetowe, blogi, fora internetowe, radia internetowe, serwisy aukcyjne i informacyjne, strony oferujące przechowywanie danych czy usługi finansowe związane z kryptowalutą elektroniczną.

Korzystanie z sieci TOR w określony sposób może realizować znamiona czynów zabronionych przez ustawy karne. Na forach dyskusyjnych w Darknecie można wymieniać się dowolnymi informacjami. Ich treść może być mocno zróżnicowana, m.in. dowiemy się, jak skonstruować bombę z łatwo dostępnych materiałów, uzyskamy porady dotyczące manipulacji czy dokonywania oszustw. W ten sposób można podżegać do dokonania przestępstwa (nakłaniać inną osobę do popełnienia czynu zabronionego) lub udzielać pomocnictwa (w tym przypadku ułatwiać popełnienie czynu zabronionego przez udzielanie rady lub informacji). Kara za podżeganie i pomocnictwo jest wymierzana w granicach zagrożenia przewidzianego za sprawstwo według art. 18 i art. 19 ustawy z dnia 6 czerwca 1997 r. − Kodeks karny (t.j. Dz. U. 2017, poz. 2204). Należy pamiętać, iż wspomnianych czynności można dopuścić się także w ramach niezaszyfrowanego Internetu, jednak wykrycie osób odpowiedzialnych za nie jest dużo łatwiejsze.

Pornografia jest bardzo rozpowszechniona nie tylko w Darknecie, lecz także w szeroko dostępnym Internecie. Stosunkowo łatwo można wejść w posiadanie pornografii z udziałem osób małoletnich poniżej 15 lat, co jest zagrożone karą od 3 miesięcy do 5 lat pozbawienia wolności zgodnie z art. 202 § 4a k.k.

Specyfiką Darknetu jest to, iż dość często można natknąć się na oferty z bardzo szerokiego wachlarza nielegalnych usług niedostępnych w zwykłym Internecie, jak np. wynajęcie hakera. Ze swoimi umiejętnościami ogłaszają się hakerzy, którzy proponują wykradanie informacji od osób prywatnych czy firm. Stanowi to czyn bezprawnego uzyskania informacji zgodnie z art. 267 k.k. i jest zagrożone grzywną, karą ograniczenia albo pozbawienia wolności do lat 2. Podobnie tyczy się to czynu niszczenia danych informatycznych zgodnie z art. 268a k.k., za który grozi kara pozbawienia wolności do lat 3. Obydwa wymienione czyny zabronione ścigane są na wniosek pokrzywdzonego.

Kolejnym typem nielegalnych usług, jakie można znaleźć w Darknecie, są zabójstwa na zlecenie. W ramach korzystania z programu TOR w ciągu zaledwie jednej godziny odnalazłem pięć stron, które oferowały usługi tzw. *contract killing*. Na podstawie analizy treści tych stron doszedłem do różnych wniosków dotyczących ich wiarygodności. Dwie strony stanowiły ewidentny żart i przedstawiały absurdalne informacje. Jedna strona została dezaktywowana przez samego jej administratora, który ujawnił ją jako oszustwo mające na celu wyłudzanie pieniędzy od osób chcących zlecać zabójstwa. Dwie strony natomiast można było z dużą dozą prawdopodobieństwa określić jako prawdziwe oferty. Przemawiały za tym duże środki ostrożności, jakie powzięli ich administratorzy. Przede wszystkim

kontakt miał odbywać się jedynie przez adres e-mail zabezpieczony przez TOR. Ponadto, osoba oferująca te usługi zalecała zabezpieczenie treści wiadomości dodatkowym programem szyfrującym i oznajmiała, że nie będzie odpowiadać na wiadomości niezaszyfrowane. W zleceniu miały być zawarte wszelkie ważne informacje na temat potencjalnego celu, wraz z aktualnym zdjęciem. Oferent odmawiał zabijania polityków i osób poniżej 18. roku życia. Koszt miał być wyceniany po dokładniejszym zapoznaniu się zabójcy z celem i wynosić ok. 10 tys. funtów brytyjskich. Wykonanie zlecenia miało zostać rozpoczęte po wpłaceniu połowy sumy przez wcześniej wspomniane bitcoiny. Druga połowa ceny miała zostać uiszczona po okazaniu dowodu śmierci (zdjęcia) przez zabójcę. Czas wykonania zlecenia został określony na około dwa tygodnie, jeżeli cel znajdował się na terenie Unii Europejskiej. Zgodnie z polskim prawem za zabójstwo grozi kara pozbawienia wolności na czas nie krótszy od lat 8, kara 25 lat pozbawienia wolności lub kara dożywotniego pozbawienia wolności. Zlecenie zabójstwa jest jedną z niesprawczych form zjawiskowych popełnienia przestępstwa i podlega karalności tak jak w przypadku podżegania i pomocnictwa opisanego wcześniej.

W ramach aukcji organizowanych w Darknecie można wejść w posiadanie różnych nielegalnych przedmiotów. Na odpowiednich serwisach można łamać prawa autorskie, kopiując nielegalnie pliki, zakupić narkotyki, broń, sfałszowane dokumenty, sfałszowaną walutę, kradzione towary, numery kart kredytowych (Jones 2005, 133). Posiadanie broni bez zezwolenia zgodnie z art. 263 § 2 k.k. podlega karze od 6 miesięcy do 8 lat pozbawienia wolności. Według wcześniej wspomnianego badania (Moore, Rid 2016, 19) najczęstszym typem nielegalnej działalności w Darknecie jest handel narkotykami. Zgodnie z art. 62 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (t.j. Dz. U. 2017, poz. 783) za posiadanie środków odurzających lub substancji psychotropowych grozi kara pozbawienia wolności do 3 lat. Spis substancji zabronionych jest stale aktualizowany, jednak szybki rozwój wytwórstwa tzw. „dopalaczy" sprawia, że ustawodawca pozostaje cały czas daleko w tyle za przestępcami.

Dość specyficznym procederem, który umożliwia program TOR jest tzw. *whistleblowing*, czyli ujawnianie lub nagłaśnianie informacji lub działalności uważanej za nielegalną czy nieetyczną wewnątrz organizacji prywatnych i publicznych. Tymi kanałami najczęściej dochodzi do zdobywania i przekazywania tajnych, poufnych lub nielegalnych informacji, które później są ujawniane opinii publicznej. Wikileaks jest najbardziej znanym przykładem portalu zajmującego się tego typu działalnością. Takie magazyny, jak: „The Guardian", „The New Yorker", „The Intercept" czy organizacja „ProPublica" korzystają z programu TOR w celu ochrony tożsamości swoich informatorów (Ellis 2014). Działalność tzw. „demaskatorów" może być jednak wątpliwa i poddawana różnym ocenom. *Whistleblowing* może realizować znamiona czynu ujawniania lub wykorzystania informacji niejawnych zgodnie z art. 265 § 1 k.k. i jest zagrożone karą pozbawienia wolności od 3 miesięcy do 5 lat. Typ kwalifikowany tego przestępstwa,

uregulowany w ramach art. 265 § 2 k.k., dotyczy sytuacji, gdy do ujawnienia informacji doszło na rzecz podmiotu zagranicznego – wtedy wymiar kary wynosi od 6 miesięcy do 8 lat.

Wymienione sytuacje stanowią tylko niewielką część czynów zabronionych, jakie można popełnić w Darknecie. Przestępcy stale tworzą nowe metody dokonywania przestępstw i stale pozostają w nieustannym wyścigu z organami śledczymi.

5. ASPEKTY KRYMINALISTYCZNE

Rzecznik Komendy Głównej Policji w 2012 r. oświadczył, iż Wydział do Walki z Cyberprzestępczością monitoruje użytkowników oraz zawartość sieci TOR (Świderski 2012). Namierzenie osób łamiących prawo przy użyciu tego programu jest niezwykle trudne; problemy z tym ma zarówno europejska, jak i amerykańska policja. Podczas rozpracowywania siatek pedofilskich funkcjonariusze często natrafiają na kanały komunikacyjne w programie TOR. Stosowane są różnorodne techniki operacyjne, takie jak infiltrowanie środowisk internetowych czy prowokacje. Policja zakłada i utrzymuje serwery komunikacyjne w celu przejmowania danych w sposób opisany w przypadku wcześniej wspomnianego Dana Egerstada. Jednym ze środków operacyjnych, które oferuje prawo w razie zakupu nielegalnych towarów, są zakupy kontrolowane i niejawnie nadzorowane. Pierwszy wariant dotyczy kupna nielegalnych materiałów przez funkcjonariusza działającego pod tzw. przykrywką. Druga metoda polega na przejęciu przesyłki, zarekwirowaniu zawartości i wysłaniu paczki dalej do adresata wraz z dołączonym sygnalizatorem otwarcia. Doręczyciel musi wyrazić zgodę na taką operację. Ze względu na trudności wykrywcze związane z technologią policja musi liczyć na błędy popełniane przez samych przestępców. Jednym z największych serwisów giełdowych oferujących obrót nielegalnym towarem była strona Silk Road, na której oferowano narkotyki i inne substancje psychotropowe. Działalność strony była trzykrotnie powstrzymywana przez amerykańską i europejską policję. Do ostatecznego jej zamknięcia i aresztowania jej twórcy Rossa Ulbrichta doszło 5 listopada 2014 r. (Chen 2011). Ulbricht został oskarżony o tzw. pranie brudnych pieniędzy, hakerstwo oraz o pomocnictwo w handlu narkotykami. Akt oskarżenia dotyczył również zlecenia kilku morderstw, jednak zarzuty te wycofano, ponieważ nie udowodniono, że którekolwiek z nich rzeczywiście doszło do skutku. W 2015 r. Ulbricht został skazany na karę dożywotniego pozbawienia wolności bez uzyskania możliwości wcześniejszego zwolnienia.

6. PODSUMOWANIE

Twórcy terminu „Darknet" nie przewidzieli tego, jak wiele zastosowań znajdzie się dla tego typu sieci. Nie przypuszczali, jak bardzo to narzędzie ułatwi zwykłym obywatelom zejście na drogę przestępstwa. W swoim artykule opisywali je tylko jako jedną z metod przekazywania danych. Przewidzieli jednak jej gwałtowny rozwój i określili ją mianem „dżina z butelki, który raz wypuszczony, nie da się z powrotem w niej zamknąć" (Biddle i in. 2002, 15). Nie wszyscy korzystają z Darknetu w sposób sprzeczny z prawem. Przekrój użytkowników programu TOR jest bardzo szeroki. Posługują się nim dysydenci polityczni, aktywiści i bojownicy o prawa człowieka w krajach autorytarnych. Z tego powodu organizacje zajmujące się ochroną tychże praw bardzo często korzystają z tego narzędzia i wspierają finansowo jego utrzymanie. Do największych jego darczyńców należy jednak zaliczyć rząd Stanów Zjednoczonych (zgodnie z danymi ze strony TOR Project). Państwa również wykorzystują Darknet do zabezpieczania i przesyłania informacji zdobytych w drodze działalności wywiadowczej, czego dowodem mogą być wcześniej wspomniane dane przechwycone przez Dana Egerstada. Celem przyświecającym stworzeniu tego programu było zagwarantowanie prywatności i anonimowości przesyłu danych – zgodnie z pierwotnym założeniem z sieci TOR korzystają zarówno osoby prywatne, jak i przedsiębiorstwa. Należy przypuszczać, iż w dobie coraz większej inwigilacji prywatnego życie obywateli, zarówno przez państwa, jak i wielkie korporacje, pragnienie ochrony tych wartości będzie coraz większe. Z tego powodu liczba użytkowników omawianego narzędzia będzie stale rosła.

BIBLIOGRAFIA

Anticounterfeiting on the Dark Web. 2015. Anticounterfeiting Committee – U.S. Subcommittee Public Awareness Task Force. http://www.inta.org/Advocacy/Documents/2015/ACC%20Dark%20Web%20Report.pdf [dostęp 6.02.2017].

Biddle, Peter, Paul England, Marcus Penaido, Bryan Willman. 2002. *The Darknet and the Future of Content Distribution*. http://msl1.mit.edu /ESD10/docs/darknet5.pdf [dostęp 6.02.2017].

„Bitcoin nielegalny w Tajlandii. Kłopot wirtualnej waluty". 2013. *Wyborcza.biz.* 30 lipca. http://web.archive.org/web/20131206083558/http://wyborcza.biz/biznes/1,100896,14357543,Bitcoin_nielegalny_w_Tajlandii__Klopot_wirtualnej.html [dostęp 6.02.2017].

Chen, Adrian. 2011. "The Underground Website Where You Can Buy Any Drug Imaginable". *Gawker*. http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160 [dostęp 6.02.2017].

Co to jest Darknet?. 2012. http://libertarianin.org/co-to-jest-darknet [dostęp 6.02.2017].

Ellis, Justin. 2014. „The Guardian introduces SecureDrop for document leaks". *Nieman Journalism Lab*. http://www.niemanlab.org/2014/06/the-guardian-introduces-securedrop-for-document-leaks [dostęp 6.02.2017].

Fagoyinbo, Joseph Babatunde. 2013. *The Armed Forces: Instrument of Peace, Strength, Development and Prosperity*. Bloomington: AuthorHouse.

Greenberg, Andy. 2014. "Hacker lexicon: what is the dark web?". *Wired.* http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web [dostęp 6.02.2017].
Jones, Robert. 2005. *Internet Forensics. Using Digital Evidence to Solve Computer Crime*. Boston: O'Reilly.
„MinFin: Bitcoin nie jest nielegalny". 2013. *Puls Biznesu*. http://www.pb.pl/3485125,94998,minfin--bitcoin-nie-jest-nielegalny [dostęp 6.02.2017].
Moore, Daniel, Thomas Rid. 2016. "Cryptopolitik and the Darknet". *Survival: Global Politics and Strategy*. http://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1142085?needAccess=true [dostęp 6.02.2017].
Murdoch, Steven, George Danezis. 2006. *Low-Cost Traffic Analysis of Tor*. 3–7. http://www.cl.cam.ac.uk/~sjm217/papers/oakland05torta.pdf [dostęp 6.02.2017].
Nakamoto, Satoshi. 2009. *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf [dostęp 6.02.2017].
Świderski, Bartosz. 2012. „Najciemniejszy zakątek Internetu naprawdę istnieje. Ukryta sieć TOR: »Lewe« papiery, pedofilia, przekręty i narkotyki". http://natemat.pl/32267,najciemniejszy-zakatek-internetu-naprawde-istnieje-ukryta-siec-tor-lewe-papiery-pedofilia-przekrety-i-narkotyki [dostęp 6.02.2017].
"The hack of the year". 2007. *The Sydney Morning Herald*. http://www.smh.com.au/news/security/the-hack-of-the-year/2007/11/12/1194766589522.html?page=fullpage#contentSwap1 [dostęp 6.02.2017].
TOR Project. 2017. https://www.torproject.org/about/overview.html.en [dostęp 6.02.2017].
Węglewski, Miłosz. 2013. „Bitcoin. Zamiana psa na dwa koty". *Newsweek*. http://www.newsweek.pl/opinie/bitcoin--zamiana-psa-na-dwa-koty,107731,1,1.html [dostęp 6.02.2017].
Wright, Alex. 2009. "Exploring a 'Deep Web' That Google Can't Grasp". *New York Times*. http://www.nytimes.com/2009/02/23/technology/internet/23search.html?pagewanted=2&_r=0&th&emc=th [dostęp 6.02.2017].
Zetter, Kim. 2007. "Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise". *Wired*. http://archive.wired.com/politics/security/news/2007/09/embassy_hacks?currentPage=1 [dostęp 6.02.2017].

Akty prawne

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz. U. 2017, poz. 2204).
Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (t.j. Dz. U. 2017, poz. 783).

Hubert Wojciechowski

DARKNET – SELECTED CRIMINOLOGICAL, FORENSIC AND LEGAL ASPECTS OF ENCRYPTED COMPUTER NETWORKS

Abstract. The article raises issues concerning encrypted networks, their content and security. The following terms are explained: Darknet, Deep Web and Dark Web. The article presents some technical aspects of The Onion Router software and its origins. It also includes some characteristic features of the usage of such a tool and of the community which has developed around it. A legal and forensic assessment of the activity placed in the Darknet is presented. The author believes that the phenomenon of TOR software should not be evaluated negatively and the author predicts its rapid development.

Keywords: Darknet, The Onion Router Project, whistleblowing, Bitcoin, Silk Road.