Judyta Kasperkiewicz

ZAKUP KONTROLOWANY METODĄ WALKI Z ANONIMOWĄ SIECIĄ TOR

Sting operations as a method to fight anonymous net TOR

Wprowadzenie

Zagadnienie bezpieczeństwa i ochrony prywatności w cyberprzestrzeni stanowi już od kilku lat jeden z najczęstszych tematów rozważań i debat prawnych. Od czasu głośnej afery związanej z Edwardem Snowdenem (PRISM) użytkownicy Internetu dostrzegli, że trudno o anonimowość w sieci, i zdali sobie sprawę, że każdy przejaw ich działalności w sieci może stać się w pełni jawny i dostępny dla różnych instytucji państwowych. Dzięki bardzo popularnym portalom społecznościowym tym instytucjom (głównie służbom specjalnym) dużo łatwiej jest gromadzić dane o całym społeczeństwie. Szczególnie otwarty na współpracę z instytucjami państwowymi jest Facebook i dlatego też bardzo zaskakuje fakt, że ten portal dostępny jest również w anonimowej sieci TOR, gdzie przecież z założenia nie dochodzi do ujawniania prawdziwej tożsamości użytkowników i nie ma możliwości gromadzenia danych, które pozwalają przykładowo na wyświetlanie spersonalizowanych reklam. Zapewne na poznanie rzeczywistego celu tego posunięcia portalu przyjdzie nam jeszcze poczekać.

W odpowiedzi na potrzebę zachowania anonimowości niektórych użytkowników Internetu będących obywatelami państw rządzonych przez dyktaturę, np. Korei Północnej czy Chin, stworzono wspomnianą wyżej anonimową sieć TOR, tak aby umożliwić ludności tych państw niczym nieograniczony dostęp do niektórych zakazanych w ich krajach stron internetowych. Jednakże tego, co stało się później, nikt nie mógł nawet częściowo przewidzieć, gdyż obecnie sieć TOR stała się rajem dla przestępców, w tym głównie pedofilów, złodziei i hakerów.

Odpowiednie organy podejmują działania celem zahamowania nieprzewidzianego rozwoju tej sieci, a jednak ciągle jest to bardzo trudne. Zdarzają się działania organów ścigania podejmowane na szeroką skalę, ale po każdym z takich głośnych sukcesów pojawiają się nowi przestępcy, którzy zapełniają powstałą lukę.

Podstawowe pojęcia

Sieć TOR nazywana jest również ciemniejszą stroną Internetu, darknetem, *dark web* czy też *shadow* Internetu. Skrót TOR pochodzi od słów *The Onion Router*[1]. Sieć TOR została stworzona przez amerykańską Marynarkę Wojenną 20 września 2002 roku, a od 2005 roku rozwijana jest przez organizację non-profit Tor Project. Znakiem rozpoznawczym, a zarazem logo sieci jest cebula, a domenę stanowi .onion.

Jest to bezpłatny serwis, który prowadzi działalność równolegle do uniwersalnego Internetu, a jedyna różnica polega na tym, że aby z niej korzystać, należy posłużyć się specjalnym programem, który dostępny jest w Internecie.

Z założenia sieć TOR ma służyć zapewnieniu anonimowości użytkownikom, tak aby niemożliwe było namierzenie adresu IP danego użytkownika. W tym celu adres IP użytkownika przechodzi przez kilka serwerów.

Sieć TOR słynie z funkcjonujących na niej forów internetowych, które zawierają rady i wskazówki przydatne w działalności przestępczej i innej zabronionej. Przykładowo polskie fora zawierają działy dotyczące: kradzieży, przejmowania kont, podrabiania dokumentów, zemsty, szantażu czy też stalkingu. Ponadto prezentują ogromne ilości treści pornograficznych i pedofilskich. Te wpisy nie są jedynie poradami osób nieletnich, ale jak pokazują statystyki, z sieci TOR korzystają głównie osoby dorosłe, które zdają sobie sprawę z bezsilności policji, dlatego też często jawnie drwią z tej sytuacji. Popularne polskie fora w sieci to m.in. Polish Board & Market, Torowisko i ToRepublic.

Jak stwierdzają przedstawiciele policji różnych krajów, poza monitoringiem sieci TOR niewiele można obecnie zdziałać. Również taka instytucja jak EUROPOL jest bezradna w tej kwestii. W przeważającej mierze skuteczne działania policji bazują na błędach użytkowników sieci. Niektóre z większych operacji policyjnych, których efektem było zatrzymanie pedofilów, prowadziły właśnie do sieci TOR.

Za granicą zdarza się coraz częściej, że po kradzieży prywatnych zdjęć znanych osób przestępcy szantażują je lub nielegalnie wykorzystują. Nie jest problemem poruszanie się po sieci TOR, ale problem stanowi wejście do jej głębszych warstw, dokąd dostęp mają tylko nieliczni. Aby wejść na utworzone strony, należy uzyskać często bardzo skomplikowany ciąg znaków w domenie .onion, który składa się na adres sieci.

Wewnątrz sieci dokonano podziału na zaufanych i nowych użytkowników. Co więcej, ustalono, że będą przyznawane punkty zaufania, a za przeprowadzone transakcje udzielane będą rekomendacje. Dla użytkowników sieci TOR użytkownicy „clear netu" stanowią cel pogardliwych wypowiedzi.

W sieci TOR najczęściej dochodzi do handlu dokumentami, danymi oraz kontami z portali aukcyjnych, np. Allegro. Nawet jeśli założymy, że część ofert jest fikcyjna, to i tak wiele z nich rzeczywiście jest zawieranych. Zwykle transakcje opłacane są za pomocą kart prepaidowych albo bitcoinami. Każdy użytkownik sieci TOR może założyć swój portfel będący kontem, na które składa się ciąg liczb. Na to konto

[1] https://www.torproject.org/, stan na dzień: 14 kwietnia 2015 r.

przekazywane są kryptowaluty, a następnie za pośrednictwem kantoru *on line* są one wypłacane na rzeczywiste konto bankowe.

Utworzone w sieci TOR fora internetowe pozostają ciągle poza jakąkolwiek kontrolą policji. Jedynie jej administratorzy na bieżąco monitorują każdego użytkownika i niekiedy stosują blokady według tylko sobie znanych zasad postępowania.

W skład sieci TOR wchodzą węzły wyjściowe oraz węzły pośredniczące, które stanowią stanowiska komputerowe na całym świecie, w odpowiedni sposób skonfigurowane i uruchomione. Obecnie funkcjonuje około kilku tysięcy węzłów obu rodzajów i dziewięć głównych serwerów. Zaszyfrowana informacja (inaczej pakiet) z komputera jednego użytkownika przesyłana jest do innego użytkownika komputera, następnie ten użytkownik rozszyfrowuje ją według klucza, który jest znany tylko jemu, i szyfruje ją w inny sposób. Kolejno dochodzi do przesłania tej nowo zaszyfrowanej informacji następnemu użytkownikowi komputera i cały proces się powtarza. Stąd wzięło się porównanie sieci TOR do cebuli, ponieważ cały proces przesyłu podlega rozwarstwieniu. Najbardziej narażony na wykrycie tożsamości jest użytkownik wyjściowy (ostatni, zwany również Tor Exit Node) oraz ten, który go poprzedza. Ta okoliczność stanowi najsłabszy punkt sieci. Natomiast pierwszy i pośredni użytkownicy są praktycznie niewykrywalni. Co dziesięć minut dochodzi do wyboru nowej, przypadkowej drogi w sieci dla działających aktualnie 8000 serwerów. Według ostatnich statystyk 11% użytkowników TOR pochodzi z USA, 7% z Niemiec, a 3,5% z Polski[2].

Sam program potrzebny do podłączenia się do sieci TOR jest legalny, dostępny w internecie, bazuje na przeglądarce Firefox. Istnieje możliwość pobrania go na trzy najpowszechniejsze systemy komputerowe, tj. Windows, Linux i Mac. Program dostępny jest również jako aplikacja mobilna dla telefonów komórkowych i tabletów. Jedną z głównych wad sieci jest powolne działanie i ciągle jeszcze ograniczona dostępność niektórych popularnych stron, które nie udostępniają swoich adresów w sieci TOR.

Kod programu określany jest jako *open source*, co oznacza, że jest publiczny. Umożliwia dzięki temu wykrywanie słabych punktów oraz uniemożliwia działanie funkcji szpiegowskich.

W nawiązaniu do funkcjonującej sieci TOR utworzony został blog „Arma", który publikuje zapewnienia, że sieć jest w pełni bezpieczna; na bieżąco umieszczane są na nim wpisy informujące o możliwych atakach na sieć i jej użytkowników.

Zakup kontrolowany oraz przesyłka niejawnie nadzorowana

Zakup kontrolowany jako czynność operacyjno-rozpoznawcza możliwy jest dzięki art. 19 ust. 1 i 2 ustawy o Policji i właśnie ta czynność operacyjno-rozpoznawcza najczęściej jest stosowana w przypadku walki policji z przestępcami z sieci TOR. Zakup kontrolowany niesłusznie czasami nazywany bywa prowokacją policyjną[3]. Wspomniany przepis jest zwykle stosowany w celu sprawdzenia uzyskanych

[2] www.metrics.torproject.org/users.html, stan na dzień: 14 kwietnia 2015 r.

[3] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Oficyna Wydawnicza Łośgraf, Warszawa 2011, s. 69.

wcześniej wiarygodnych informacji o przestępstwie, a następnie ustalenia sprawców oraz zdobycia dowodów przestępstwa.

Wyróżnia się cztery metody przeprowadzenia zakupu kontrolowanego:

- dokonanie w sposób niejawny nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przepadkowi albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione;
- przyjęcie lub wręczenie korzyści majątkowej;
- złożenie propozycji nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przepadkowi albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione;
- złożenie propozycji przyjęcia lub wręczenia korzyści majątkowej.

W czasie przeprowadzanych czynności podejmuje się wszelkie dopuszczalne przez prawo środki konieczne do zapewnienia bezpieczeństwa osobistego policjantów i osób udzielających pomocy Policji[4].

Przewiduje się dwa mechanizmy przeprowadzania zakupu kontrolowanego. Jako pierwszy wskazuje się zatrzymanie osoby podejrzewanej przez funkcjonariusza w momencie przekazywania przedmiotów lub korzyści, które są przedmiotem transakcji, przy nieujawnianiu powodów dokonania transakcji oraz danych osób uczestniczących w czynnościach. Natomiast drugim z tych mechanizmów jest przeprowadzanie kilku zakupów kontrolowanych w celu ustalenia wszystkich powiązań pomiędzy osobami biorącymi udział w transakcji, tj. dostawcy, sprzedawcy oraz odbiorcy[5].

Sama procedura przeprowadzenia czynności wskazanych w art. 19a ustawy o Policji przebiega zwykle w podobny sposób. Zwykle prowadzone są wcześniej inne czynności operacyjno-rozpoznawcze, które dają przypuszczenie, że zaistniał zamiar lub dokonanie jednego z czynów zabronionych wskazanych w art. 19a ust. 1 ustawy o Policji. W wyniku podjęcia takiego przypuszczenia rozpoczyna się od przygotowania do przeprowadzenia zakupu kontrolowanego. W przypadku sieci TOR najczęściej wystarczy informacja, że źródłem przestępczego działania jest ta sieć, tj. strona internetowa w domenie .onion.

Przed rozpoczęciem faktycznych przygotowań kierownik jednostki Policji lub kierownik komórki organizacyjnej jednostki Policji właściwej do wykonywania czynności operacyjno-rozpoznawczych kieruje pisemny wniosek do Komendanta Głównego Policji lub komendanta wojewódzkiego Policji o wydanie stosownego zarządzenia. Tymczasem Komendant Główny Policji lub komendant wojewódzki Policji może na czas określony zarządzić czynności, wcześniej jednak musi uzyskać pisemną zgodę właściwego miejscowo prokuratora okręgowego, chyba że stało się

[4] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 maja 2002 r. w sprawie szczególnych zasad i trybu wydawania, posługiwania się, przechowywania i ewidencji dokumentów, które uniemożliwiają ustalenie danych identyfikujących policjanta lub osobę udzielającą pomocy Policji oraz środków, którymi posługują się przy wykonywaniu zadań służbowych (DzU Nr 74, poz. 684).

[5] R. Zakrzewski, A. Woźniak, *Nowe metody operacyjnego działania Policji*, „Kontrola Państwowa" 1996, nr 4, s. 131.

to już niecelowe lub nie ma takiej możliwości bądź prokurator zarządził zaniechanie tych czynności.

Prokurator przed wydaniem pisemnej zgody zapoznaje się z materiałem będącym uzasadnieniem do przeprowadzenia wnioskowanych czynności. Czas, na jaki zarządza się czynności podejmowane celem przeprowadzenia zakupu kontrolowanego, nie może być dłuższy niż trzy miesiące. Czas stosowania zarządzonych czynności można przedłużyć na okres nie dłuższy niż kolejne trzy miesiące, jeżeli jest to celowe przy zastosowaniu odpowiedniej procedury, tj. na mocy kolejnego zarządzenia Komendanta Głównego Policji lub komendanta wojewódzkiego Policji, po uzyskaniu pisemnej zgody prokuratora.

Co istotne, takie przedłużenie możliwe jest tylko jednorazowo i tylko w razie pojawienia się nowych istotnych okoliczności dla sprawdzenia uzyskanych wcześniej, wiarygodnych informacji o przestępstwie oraz po ustaleniu sprawców i uzyskaniu dowodów przestępstwa można zarządzić kontynuację tych czynności na dalszy czas oznaczony.

Prokurator właściwy miejscowo na bieżąco informowany jest o wynikach przeprowadzonych czynności i w każdej chwili może zarządzić, aby zaniechano ich kontynuowania. W razie zgromadzenia dowodów umożliwiających wszczęcie postępowania karnego lub takich, które mają znaczenie dla toczącego się postępowania karnego, uzyskane materiały wraz z wnioskiem o wszczęcie postępowania przekazywane są prokuratorowi okręgowemu; materiały te wykorzystywane są z zastosowaniem art. 393 § 1 zd. 1 Kodeksu postępowania karnego.

Na podstawie art. 15 ust. 1 pkt 5a ustawy o Policji czynności związane z zakupem kontrolowanym mogą być niejawnie rejestrowane za pomocą urządzeń rejestrujących obraz lub dźwięk. Zgodnie z treścią art. 19a ust. 6 ustawy o Policji, który stanowi *lex specialis* w stosunku do art. 19 tej ustawy, ten sam organ może podjąć decyzję o przeprowadzeniu zakupu kontrolowanego oraz o rejestracji składających się nań czynności.

Zakup kontrolowany określany bywa również jako „operacja pod przykryciem", a funkcjonariuszy uczestniczących w czynnościach nazywa się „policjantami pod przykryciem", natomiast tych, którzy wykonują działania zlecone – „tajnymi agentami"[6]. Całe przedsięwzięcie wymaga zwykle wielu przygotowań i pracy, gdyż należy przeniknąć do wnętrza środowiska przestępczego, dokonać obserwacji, nawiązać kontakty, zebrać potrzebne informacje i rozpracować wybrane osoby. Operacje z wykorzystaniem tajnych agentów mogą przynieść efekty w postaci zebrania materiału dowodowego, którego uzyskanie w inny sposób byłoby niemożliwe lub bardzo uciążliwe[7]. Celem czynności wykonanych przez wprowadzenie tajnego agenta do środowiska przestępczego jest:

[6] A. Szumski, *Wykorzystanie taktyki i techniki kryminalistycznej w ramach czynności operacyjno-rozpoznawczych*, Oficyna Wydawnicza Arboretum, Wrocław 2010, s. 178–188.
[7] J. Kudła, Z. Bielecki, *Przyjęcie lub wręczenie korzyści majątkowej i zakup kontrolowany. Raport z badań (część jawna). Cz. 1*, „Policja" 2007, s. 73.

- ustalenie zakresu podmiotowego i przedmiotowego działalności rozpracowywanych grup,
- uprzedzenie planowanych przedsięwzięć przestępczych,
- zwerbowanie informatora,
- zebranie informacji o konkretnych przestępstwach,
- ułatwienie czynności związanych z konfiskatą ukrywanego przez przestępców mienia,
- zatrzymanie sprawców przestępstwa[8].

Przeprowadzenie operacji tego rodzaju wymaga zwykle dużego zaangażowania finansowego i organizacyjnego ze strony organów ścigania, ich olbrzymiego doświadczenia w zwalczaniu struktur przestępczych, doskonałych informatorów, perfekcyjnej ochrony dla policjantów działających pod przykryciem[9]. Wzięcie udziału w takich czynnościach wiąże się również z wysiłkiem osób w nich uczestniczących. Należy ciągle mieć na uwadze to, że mogą z tego przedsięwzięcia wyniknąć nieprzewidziane skutki. Często są nimi stres spowodowany takim działaniem oraz załamanie nerwowe, popadanie w alkoholizm, narkotyzowanie się czy wręcz identyfikacja ze swoją przestępczą tożsamością, dlatego też niezwykle ważną rolę odgrywa specjalistyczne szkolenie tajnych agentów[10].

Omawiając zakup kontrolowany, należy poruszyć jeszcze trzy istotne zagadnienia. Po pierwsze, zwrócić uwagę na szczególną ochronę, jaką objęte są osoby biorące udział w czynnościach, ale niebędące funkcjonariuszami. Wszelkie dane ich dotyczące i mogące je zidentyfikować stanowią informację niejawną z nadaną klauzulą „ściśle tajne", a ich ujawnienie może nastąpić jedynie w trybie wskazanym w art. 9 ustawy. Udział takich osób w czynnościach jest dobrowolny. Opcjonalnie przyznaje się im wynagrodzenie i w razie utraty życia lub zdrowia przysługują stosowne świadczenia odszkodowawcze. Jednakże wydaje się, że trudno przyjąć, iż taką osobę współpracującą, na wzór innych porządków prawnych, można byłoby nazwać „tajnym agentem". Polskie regulacje nie są wystarczające dla przyjęcia takiego wniosku.

Po drugie, pozostało jeszcze zagadnienie, na które należy tylko zwrócić uwagę, tj. art. 144 ustawy o Policji, który pozwala przyjąć, że osoba uczestnicząca w opisywanych czynnościach nie popełnia przestępstwa, a więc mamy tutaj do czynienia z ustawowym kontratypem. Kontratyp ten odnosi się również do przesyłki niejawnie kontrolowanej, o której mowa będzie w dalszej części pracy.

Po trzecie, niezmiernie istotne jest odpowiednie dokumentowanie zarządzanych czynności, określonych w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji, a szczególnie w sprawach, w których miejscem dokonania czynu zabronionego jest Internet. Każdą z przeprowadzanych czynności dokumentuje się w postaci

[8] J. Kudła, B. Kupis, *Nowe uregulowania prawne dotyczące polskich działań pod przykryciem*, „Przegląd Policyjny" 2002, nr 3–4, s. 166.

[9] P. Podsiedlik, T. Czyłok, *Zakup kontrolowany, przyjęcie lub wręczenie korzyści majątkowej*, Wydawnictwo Szkoły Policji w Katowicach, Katowice 2012, s. 13.

[10] S. Waltoś, *Tajny agent (na obrzeżach odpowiedzialności karnej)*, „Państwo i Prawo" 1993, nr 11–12, s. 27.

notatki służbowej, a w razie potrzeby oddaje się do badań określonemu specjaliście. Co istotne, rejestrując każdą z czynności, wykonuje się również kopię tych rejestracji. Wszelkie materiały zawierające dowody przekazuje się organowi prowadzącemu postępowanie, a te, które ich nie zawierają, przechowuje przez dwa miesiące od dnia zakończenia lub zaniechania czynności. Następnie wydawane jest zarządzenie o protokolarnym, komisyjnym zniszczeniu zgromadzonych materiałów.

Zapisy utrwalone na nośnikach usuwa się w sposób uniemożliwiający odtworzenie tych zapisów z chwilą zniszczenia materiałów[11]. W przypadku gdy usunięcie z nośników utrwalonych na nich zapisów nie jest możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie albo dokonuje się ich fizycznego zniszczenia, przy zastosowaniu przepisów o ochronie informacji niejawnych[12].

Natomiast przesyłka niejawnie kontrolowana (inaczej nazywana również dostawą niejawnie kontrolowaną)[13], pomimo że funkcjonuje w naszym systemie prawnym od 20 lat, nie cieszy się dużym zainteresowaniem. Została wprowadzona w myśl zaleceń zawartych w Konwencji Narodów Zjednoczonych o zwalczaniu obrotu środkami odurzającymi i substancjami psychotropowymi z 1988 roku. W Polsce została wprowadzona ustawą z 21 lipca 1995 roku zmieniającą ustawę o urzędzie Ministra Spraw Wewnętrznych, o Policji, o Urzędzie Ochrony Państwa, o Straży Granicznej oraz niektóre inne ustawy. Zaliczana jest do taktycznych czynności operacyjno-rozpoznawczych[14] oraz metod szczególnych „ofensywnych"[15].

Czynności dokonywane w celu niejawnego kontrolowania przesyłki polegają na niejawnym nadzorowaniu wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa, jeżeli nie stworzy to zagrożenia dla życia lub zdrowia ludzkiego. W ustawie w art. 19b ust. 1 wskazano również cele tych czynności, wymieniając:

- udokumentowanie przestępstw,
- ustalenie tożsamości osób uczestniczących w tych przestępstwach,
- przejęcie przedmiotów przestępstwa[16].

Obserwowanie odbywa się przy użyciu urządzeń technicznych utrwalających dźwięk lub obraz, a także przy użyciu urządzenia wykorzystującego *Global Positioning System – Navigation Signal Timing and Ranging* (GPS). Przesyłka okresowo może zostać wyłączona z obrotu, może również zostać otwarta celem sprawdzenia, oznakowania lub usunięcia przedmiotów lub zastąpienia ich innymi, a wszystko po to, aby ujawnić i utrwalić ślady kryminalistyczne.

---

[11] P. Podsiedlik, T. Czyłok, *Zakup kontrolowany*…, op. cit., s. 13.
[12] Tamże.
[13] A. Taracha, *Czynności operacyjno-rozpoznawcze: aspekty kryminalistyczne i prawnodowodowe*, Wydawnictwo Uniwersytetu Marii Skłodowskiej-Curie, Lublin 2006, s. 65-67.
[14] S. Pikulski, *Działania operacyjne policji*, „Wojskowy Przegląd Prawniczy" 1996, nr 2, s. 54.
[15] J. Kudła, *Wykorzystanie wyników czynności operacyjno-rozpoznawczych określonych w art. 19, 19a, 19b ustawy o Policji w postępowaniu karnym*, w: S. Lelental, J. Kudrelek, I. Nowicka (red.), *Czynności dochodzeniowo-śledcze i działania operacyjne policji a rola sądu w postępowaniu przygotowawczym*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2008, s. 246.
[16] T. Hanausek, *Kryminalistyka. Zarys wykładu*, Zakamycze, Kraków 2006, s. 142–143.

Wyróżnia się kilka rodzajów przesyłek niejawnie nadzorowanych:
- „czyste", w których przedmiot przestępstwa w całości lub w części został w sposób tajny podmieniony na identyczny albo usunięty;
- „brudne", w których nadzoruje się przesyłkę w stanie nienaruszonym;
- dostawy wewnątrzkrajowe – nadzorowanie dotyczy terytorium tylko jednego państwa;
- dostawy międzynarodowe, transgraniczne;
- międzynarodowe „wewnętrzne", w tym przypadku informacje np. o przemycie uzyskały organy ścigania kraju docelowego, który jednocześnie podejmuje czynności koordynujące operację od kraju nadania (wysyłającego) przez kraje tranzytowe;
- międzynarodowe „zewnętrzne", gdy wiadomość o nielegalnej dostawie powzięły władze innych państw, nie docelowego, i wówczas one uzgadniają warunki bezpiecznego przebiegu dostawy kontrolowanej do kraju docelowego[17].

Zarządzenie o wdrożeniu niejawnego nadzorowania, wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa wydaje Komendant Główny Policji lub komendant wojewódzki Policji. Po wydaniu tego zarządzenia zobowiązany jest poinformować prokuratora okręgowego właściwego według siedziby zarządzającego organu Policji. Również tutaj prokurator w każdym czasie może nakazać zaniechanie czynności i musi być informowany na bieżąco o wynikach czynności. Inaczej niż przy zakupie kontrolowanym ustawodawca nie wskazał czasu, na jaki można zarządzić tę czynność, zapewne z powodu braku możliwości przewidzenia, jak długo będzie to konieczne. Odmienność stanowi również zastrzeżenie, że nie przeprowadza się tych czynności, jeśli istnieje zagrożenie dla życia i zdrowia ludzkiego. Tego zastrzeżenia należy przestrzegać również wtedy, gdy istnieje potencjalne zagrożenie.

Dla niektórych przedstawicieli doktryny przesyłka niejawnie kontrolowana stanowi odmianę zakupu kontrolowanego[18]. W tym przypadku dochodzi również najczęściej do nawiązania współpracy z innymi organami zarówno publicznymi, jak i prywatnymi (np. firmą kurierską) celem osiągnięcia zamierzonego celu. To jednak generuje dodatkowe zagrożenie dla powodzenia przedsięwzięcia. W wyniku przedsięwziętych czynności można doprowadzić do:
- zatrzymania sprawcy lub sprawców na gorącym uczynku, np. przemytu,
- przejęcia przedmiotów przestępstwa, np. alkoholu, broni,
- niedopuszczenia przedmiotów przestępstwa do dalszego obrotu,
- pełnego ustalenia odbiorców przedmiotów przestępstwa, np. paserów;
- likwidacji szlaków przemytniczych;
- ustalenia składu osobowego grup i związków przestępczych;

[17] D. Potakowski, *Nowe uprawnienia Policji w walce z przestępczością zorganizowaną*, „Przegląd Policyjny" 1996, nr 1–6, s. 90.
[18] A. Woźniak, R. Zakrzewski, *Nowelizacja ustawy o Policji – rozszerzenie uprawnień operacyjno-rozpoznawczych*, „Monitor Prawniczy" 1996, nr 1, s. 6.

– zebrania bardzo mocnego i należycie udokumentowanego materiału dowodowego jeszcze przed wydaniem postanowienia o wszczęciu postępowania przygotowawczego.

Przesyłka (dostawa) niejawnie kontrolowana jest działaniem podejmowanym w celu stwierdzenia tożsamości uczestników przestępstwa w sytuacji, gdy określone przedmioty są nielegalnie przemieszczane, przechowywane lub dochodzi do obrotu nimi. Zamiast zająć je natychmiast po stwierdzeniu, że pochodzą z przestępstwa, służba policyjna nadzoruje ich „ruch", by w rezultacie sporządzić dokumentację, mającą walor dowodowy w przyszłym procesie karnym. Przyjmuje się, iż w wielu przypadkach w celu potwierdzenia zasadności podjęcia niejawnej kontroli przesyłki niezbędne jest przeprowadzenie tajnego przeszukania[19].

Przykłady walki organów ścigania w Polsce i na świecie z siecią TOR

Tylko pozornie wydaje się, że nie jest możliwe dotarcie do użytkowników sieci TOR. Doskonałym przykładem możliwości przełamania anonimowości w tej sieci jest operacja przeprowadzona przez amerykańskie FBI, które po kilku miesiącach intensywnej pracy zatrzymało kilkadziesiąt osób zaangażowanych w działalność pedofilską w jej ramach.

W październiku 2013 roku amerykańskie służby federalne zamknęły pierwszy internetowy bazar, czyli serwis pod nazwą Silk Road, a w wyniku tych działań zatrzymano domniemanego założyciela serwisu Williama Ulbrichta oraz, na wniosek władz amerykańskich, 28-letniego Erika Eoina Marquesa (w Irlandii)[20]. W tym samym czasie doszło do zastanawiającego zbiegu okoliczności i zamknięcia wielu ukrytych serwisów, m.in. poczty Tormail i systemu płatności bitcoinowych Onionbank. Jak się okazało, FBI ustaliło IP osób odwiedzających witryny na serwerze Freedom Hosting, wykorzystując błąd w podstawowym oprogramowaniu (exploit 0-day Firefox 17).

Po roku te same służby odniosły kolejny sukces i ramach zakrojonej na szeroką skalę operacji doszło do zlikwidowania serwisów, w tym serwisu Silk Road 2.0, a tym samym zatrzymano domniemanego założyciela tego serwisu Blake'a Benthala, który powszechnie znany jest pod pseudonimem „Defcon". Został on oskarżony o utworzenie serwisu, który umożliwił ponad stu tysiącom osób prowadzenie transakcji kupna-sprzedaży narkotyków i innych nielegalnych towarów, np. sfałszowanych dokumentów. „Defcon" może zostać skazany nawet na karę dożywotniego pozbawienia wolności. Zgodnie z oficjalnym oświadczeniem nowojorskiego Prokuratora Generalnego obroty Silk Road 2.0 sięgały 8 mln dolarów miesięcznie.

Mowa tutaj o operacji „Onymous" przeprowadzonej w listopadzie 2014 roku, podczas której FBI zlokalizowało i zamknęło 410 serwisów w sieci TOR. Działalność tych serwisów związana była ze sprzedażą narkotyków, broni, fałszywych banknotów oraz kart kredytowych. Operacja została przeprowadzona w 16 krajach. Wzięły w niej udział następujące jednostki: European Cybercrime Centre (EC3) Europol, FBI,

[19] J. Widacki, *Kryminalistyka*, Wydawnictwo C.H. Beck, Warszawa 2012, s. 138.

[20] http://www.dobreprogramy.pl/FBI-triumfuje-najwiekszy-hosting-sieci-Tor-przejety-tysiace-uzytkownikow-zdemaskowanych,News,45424.html, stan na dzień: 14 kwietnia 2015 r.

Służby Imigracyjne i Celne USA (ICE) oraz Departament Bezpieczeństwa USA. Jak się przypuszcza, w tej sprawie wiele zawdzięczać można eksperymentowi wykonanemu przez ekspertów z CERT University Carnegie Mellon, którzy wykorzystali w tym celu 115 bardzo szybkich serwerów. Ich eksperyment polegał na oznaczeniu w sieci pewnych elementów i identyfikacji ich drogi od nadawcy do odbiorcy. Eksperyment trwał od stycznia do lipca 2014 roku. W lipcu serwery te zostały wyłączone. Stanowi to doskonały przykład zastosowania niejawnego nadzorowania przesyłki. Wspomniani eksperci wystąpili na konferencji Black Hat w 2014 roku, opisując mechanizm tego doświadczenia. W swoim wystąpieniu poinformowali: „In our analysis, we've discovered that a persistent adversary with a handful of powerful Server and a coupe gigabit links can deanonymize hundreds of thousands TOR clients and thousands of hidden services within a couple of months. The total investment cost? Just under $3,000"[21]. Tłumacząc ich wypowiedź, należy stwierdzić: „odkryliśmy, że zdeterminowany atakujący, dysponujący kilkoma serwerami dużej mocy i kilkoma połączeniami o przepuszczalności kilku gigabitów, może w ciągu paru miesięcy odkryć tożsamość setek tysięcy klientów sieci TOR oraz tysięcy ukrytych serwerów. Całkowity koszt inwestycji? Niecałe 3000 dolarów". Zaskakuje zarówno prostota podejścia do problemu, jak i skala skuteczności.

Po ujawnieniu informacji o przeprowadzonej operacji magazyn „The Economist" stwierdził, że zlikwidowane serwisy wraz z serwisem Silk Road 2.0 obsługiwały 30% rynku, gdyż od czasu Silk Road 1.0 pojawiły się nowe. Wbrew temu, co utrzymuje FBI, nie zlikwidowano głównego ośrodka internetowego handlu niedozwolonymi towarami. Prawdą jest jednak, że doszło do zlikwidowania jednego ze znaczących centrów. Natomiast w dzienniku „The Washington Post" opublikowano krytyczny artykuł o działaniach FBI, w którym stwierdzono, że operacja uwieńczona sukcesem spowoduje wzrost zagrożenia przestępczością narkotykową na ulicach miast, gdyż dzięki przeniesieniu się nielegalnego handlu z ulicy do sieci te zagrożenia w rzeczywistym świecie się zmniejszyły.

FBI ujawniło przykłady zamkniętych w wyniku operacji serwisów, tj.:

- „Pandora" (pandora3uym4z42b.onion), „Blue Sky" (blueskyplzv4zv4fsti.onion) będące sklepami z narkotykami,
- „Executive Outcomes" (http://iczyaan7hzkyjown.onion) będący sklepem z bronią,
- „Fake Real Plastic" (http://igvmwp3544wpnd6u.onion) będący sklepem z kartami kredytowymi,
- „Fast Cash!" (http://5oulvdsnka55buw6.onion) handlujący fałszywymi banknotami.

Zamknięte serwery znajdowały się w Bułgarii, Czechach, Finlandii, Francji, Niemczech, na Węgrzech, w Irlandii, na Łotwie, Litwie, w Luksemburgu, Holandii, Rumunii, Hiszpanii, Szwecji, Szwajcarii i w Wielkiej Brytanii. Dziwi fakt, że lista ta nie uwzględnia np. Rosji.

Aby zniwelować ryzyko objęcia pozycji „stanowiska wyjściowego", czyli najbardziej narażonego na ujawnienie IP, specjaliści polecają takie skonfigurowanie

[21] http://www.belowgotham.com/Tor-trust.pdf, stan na dzień: 14 kwietnia 2015 r.

ruchów stacji roboczej, aby możliwy był jedynie ruch wyjściowy przez Proxy do sieci TOR. W tym celu istnieje możliwość skorzystania z gotowej konfiguracji dystrybucji Tails. Szczególnie narażeni na różne niebezpieczeństwa, jakie wiążą się z siecią TOR, są użytkownicy urządzeń mobilnych, tj. telefonów i tabletów, gdyż w ich przypadku łatwiejsze pozostaje ustalenie tożsamości. Taka możliwość zwiększa się zwłaszcza w razie umieszczenia w kodzie strony obiektu wideo lub audio w standardzie HTML5 z opcją autoodtwarzania. Ta czynność powoduje, że program uruchomi bez wcześniejszego zapytania wewnętrzny odtwarzacz, który łączy się z siecią, ignorując ustawienia Proxy i przekierowując ruch do sieci TOR[22]; w ten sposób umożliwia ujawnienie prawdziwego adresu IP użytkownika urządzenia mobilnego.

Na początku 2014 roku Kaspersky Lab poinformował, że odkryto ponad 900 usług rozsyłających *malware* z sieci TOR.

W 2014 roku również w Polsce doszło do rozesłania z sieci TOR wiadomości mailowych zawierających fałszywe alarmy bombowe. Jednak specjaliści zakładają, że policji nie udałoby się ustalić tożsamości ich nadawcy, gdyż pomimo iż doszło do zatrzymania osoby podejrzanej o nadanie tych alarmów dzięki połączeniu ze sobą wszystkich istotnych okoliczności dotyczących poszczególnych zdarzeń, dopiero po kilku dniach do tych czynów przyznała się inna osoba, która sama określała się mianem „CyberBrevika”[23]. W związku z tym zatrzymano kolejnego podejrzanego. Przypuszcza się, że ten pierwszy podejrzany został zatrzymany na podstawie wyciągnięcia przez policję zbyt pochopnych wniosków.

Bardzo często przedmiotem transakcji w sieci TOR stają się konta na Allegro posiadające dużą liczbę pozytywnych komentarzy czy też konta bankowe ze zgromadzonymi środkami finansowymi.

Innym obrazowym przykładem problemu z siecią TOR jest zdarzenie z lutego 2014 roku, kiedy to umieszczono w niej materiały o jednym z kapitanów ABW, który był w przeszłości ekspertem wydziału bezpieczeństwa teleinformatycznego. W sieci tej dostępne były jego pełne dane osobowe, łącznie ze zdjęciem, numerem PESEL oraz informacjami o jego rodzinie. Dowodzi to, że wiele ze skradzionych danych gromadzonych jest właśnie w sieci TOR i tam są one wykorzystywane do przestępczych celów.

Podsumowanie

Pomimo złej reputacji, jaką obecnie cieszy się sieć TOR, pozostaje ona nadal w oczach wielu symbolem wolności i wzorcem w dążeniu do ochrony prywatności w ramach komunikacji internetowej.

Przykładami pozytywnych skutków jej funkcjonowania są przykładowo dostęp do Internetu użytkowników będących dziennikarzami w krajach, gdzie sieć poddawana jest cenzurze, dostęp do Internetu osób przebywających na urlopie w krajach,

[22] http://zaufanatrzeciastrona.pl/post/korzystasz-z-sieci-tor-na-telefonie-lepiej-uwazaj/, stan na dzień: 14 kwietnia 2015 r.

[23] http://wyborcza.pl/1,75478,16404430,CyberBrevik__To_ja_wyslalem_maile_o_bombach__W_areszcie.html, stan na dzień: 14 kwietnia 2015 r.

w których istnieją ograniczenia ze względu na ich położenie geograficzne czy też ochronę przed poniesieniem odpowiedzialności za działalność w Internecie klientów różnych instytucji, np. hoteli.

Liczyć należy na to, że w przyszłości wzrośnie skala działań podejmowanych na rzecz przeciwdziałania problemom pojawiającym się w związku z funkcjonowaniem sieci TOR i dzięki temu uda się uniknąć wielu niebezpiecznych zdarzeń, do których aktualnie dochodzi za pośrednictwem tej sieci. Pocieszające wydaje się to, że szybki postęp technologiczny sprzyja nie tylko przestępcom, lecz także organom ścigania, i wszyscy spodziewamy się, że w przyszłości eksperci znajdą sposób na zniwelowanie zagrożeń płynących z tej sieci. Już teraz bowiem docierają do nas niepotwierdzone jeszcze informacje o tym, że FBI posiada *malware* pozwalający namierzyć użytkowników sieci TOR, czyli przypuszczać można, że jesteśmy coraz bliżej kresu bezkarności jej użytkowników.

Streszczenie

W związku z pojawieniem się nowego zagrożenia, jakim jest anonimowa sieć TOR, występuje coraz więcej problemów wynikających z przekształcenia jej w narzędzie wyrafinowanych przestępców. W założeniu celem twórców tej sieci było ułatwienie dostępu do informacji zawartych w sieci komputerowej tym, którzy mieszkają w państwach, gdzie Internet jest cenzurowany, np. dla dziennikarzy w Korei. Stało się jednak inaczej i aktualnie siecią tą posługują się głównie złodzieje, hakerzy, handlarze narkotyków i pedofile. Organy ścigania zdają sobie sprawę z płynącego stąd zagrożenia i podejmują działania w celu wykrywania sprawców przestępstw, których źródło pochodzi z sieci TOR, np. poprzez zakup kontrolowany. Choć jest to niezmiernie trudne, to zagraniczne służby odnoszą sukcesy. Pocieszające wydaje się to, że szybki postęp technologiczny sprzyja nie tylko przestępcom, lecz także organom ścigania, i wszyscy spodziewamy się, że w przyszłości eksperci znajdą sposób na zniwelowanie zagrożeń płynących z tej sieci.

Słowa kluczowe: sieć TOR, anonimowa sieć, zakup kontrolowany, przesyłka niejawnie nadzorowana

Summary

With the new threat which is anonymity network TOR appeared a huge number of problems which are connected with a transformation of this new network as a tool for sophisticated offenders. The creator of this specific network wanted to make easier to have an access to Internet by people in same countries which decided to censor e.g. for journalists from North Korea. But we have now different reality and the TOR is currently using by thieves, hackers, drug dealers and paedophiles who are dealing with this network. The law enforcement agencies realized that it is a very dangerous threat and they are making an effort to descry a real offenders of these crimes which source comes from the TOR e.g. through a sting operation. It is extremely difficult, however the overseas services are getting off the ground. It is comforting that a quick technological development encourage offender but the law enforcement agencies as well, and we expected that in future the experts will find a way to level this threat which is deriving from the TOR.

Keywords: TOR network, anonymity network, sting operation, controlled delivery