ISSN 2080-1807

TORUŃSKIE STUDIA BIBLIOLOGICZNE
2017, nr 1 (18)

Katarzyna Jarczewska-Walendziak*
Uniwersytet Mikołaja Kopernika w Toruniu
e-mail: kaja@doktorat.umk.pl

Wykorzystywanie otwartych źródeł informacji przez służby śledcze

DOI: http://dx.doi.org/10.12775/TSB.2017.008

Streszczenie: Postępujący przyrost zasobów informacji jawnej oraz możliwość szybkiego i łatwego ich pozyskiwania sprawiają, że coraz częściej różne podmioty wykorzystują je w podejmowanych przez siebie działaniach. Sytuację taką obserwuje się m.in. w służbach śledczych, które korzystają z tego typu zasobów przed przystąpieniem do wykonywania dalszych działań wywiadowczych prowadzonych innymi środkami oraz w ich trakcie. Niniejszy artykuł jest próbą opisu możliwości wykorzystywania otwartych źródeł informacji w pracy służb śledczych. Autorka przybliża istotę i znaczenie informacji jawnoźródłowych, etapy ich analizy, rodzaje istniejących źródeł oraz przykłady ich wykorzystywania przez służby śledcze w Polsce i za granicą. Osobne miejsce w artykule zajmuje prezentacja zalet i wad wywiadu białego oraz ograniczeń w wykorzystywaniu otwartych źródeł informacji wynikających z przyrostu zasobów informacyjnych oraz automatyzacji procesów wyszukiwania informacji.

Słowa kluczowe: analiza informacji, otwarte źródła informacji, służby bezpieczeństwa, służby śledcze.

* Uczestniczka studiów doktoranckich z zakresu bibliologii i informatologii, prowadzonych na Wydziale Nauk Historycznych Uniwersytetu Mikołaja Kopernika w Toruniu.

Wprowadzenie

Wiedza od zawsze była ważnym elementem w działaniu służb bezpieczeństwa. Rozwój technik informatycznych oraz nieustanna współpraca międzynarodowa spowodowały, że gromadzenie i wykorzystywanie wiedzy stało się kluczowym warunkiem skutecznego zwalczania przestępczości. Ponieważ pozyskiwanie wiedzy nie jest jednak celem samym w sobie, aby faktycznie mogła ona służyć realizacji zadań stawianych służbom, należy ją odpowiednio przetworzyć i zanalizować[1].

Otwarte źródła najczęściej wykorzystywane przez służby policyjne to prasa, radio, telewizja, ogólnie dostępne rejestry, zasoby Internetu oraz dokumenty, które w świetle obowiązującego prawa przedsiębiorstwa zobowiązane są udostępniać[2]. Informacje, które pochodzą ze tego typu źródeł, to około 80% możliwych do zgromadzenia danych wywiadowczych. Niskie koszty ich pozyskiwania, brak inwazyjności i ryzyka, a także wszechstronny zakres dostępnych treści sprawiają, że biały wywiad oraz nowe rozwiązania wywiadu jawnoźródłowego stają się filarem współczesnego bezpieczeństwa państwa[3].

Dane jawne – konteksty terminologiczne

W polskim ustawodawstwie brak regulacji precyzujących pojęcia takie, jak *biały wywiad*, *wywiad źródeł jawnych* (ang. *Open Source INTelligence OSINT*, dalej: OSINT) czy też *otwarte źródła informacji*. Dlatego przedstawiciele doktryny formułują własne definicje[4]. I tak na przykład Krzysztof

---

[1] J. Konieczny, *Wstęp*, [w:] *Analiza informacji w służbach policyjnych i specjalnych*, pod red. J. Koniecznego, Warszawa 2012, s. IX.

[2] K. Radwaniak, P. J. Wrzosek, *Biały wywiad w Policji – pozyskiwanie i analiza informacji ze źródeł otwartych*, [w:] *Analiza informacji*..., s. 121.

[3] A. Ziółkowska, *Biały wywiad w bezpieczeństwie państwa* [online]. Bezpieczenstwowbiznesie.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://bezpieczenstwowbiznesie.pl/index.php/wywiad-gospodarczy/geopolityka/269-bialy-wywiad-w-bezpieczenstwie-panstwa.

[4] B. Sromczyńki, P. Waszkiewicz, *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5, s. 148.

Liedel i Tomasz Serafin proponują, by *informacją jawnoźródłową* określać „ciąg danych, które pochodzą z jednego lub więcej jawnych źródeł, które to dane podlegają procesowi ewaluacji z uwzględnieniem czasu publikacji informacji oraz ich zawartości”[5]. Podobną optykę przyjmuje Krzysztof Mroziewicz, który definiuje *biały wywiad* jako „analizę informacji z legalnie dostępnych źródeł”[6] i jednocześnie „najbezpieczniejszą i najbardziej przyjazną formę zdobywania tajemnic”[7].

W odróżnieniu od źródeł polskich bardziej precyzyjne wyjaśnienie terminu *Open Source Intelligence* przynoszą źródła obcojęzyczne, np. dokument NATO pt. „Open Source Intelligence Reader” z 2002 r. Czytamy w nim, że „OSINT to wynik przeprowadzenia pewnych czynności w stosunku do informacji. Są one specjalnie poszukiwane, porównywane ze sobą co do treści i wybierane są te najważniejsze dla odbiorcy procesu”[8]. Wspomniany dokument odwołuje się do wytycznych dyrektora amerykańskiej Centralnej Agencji Wywiadowczej (ang. Central Intelligence Agency, dalej: CIA) wydanych 1 marca 1994 r. pod nazwą *Director of Central Intelligence Directive*[9]. Na ich łamach zwraca się uwagę na publiczną dostępność danych i wskazuje, że mianem *otwartych danych* może *de facto* zostać określona każda informacja, o ile użyta jest w kontekście jawnym, bez narażania źródeł, metod wywiadowczych i państwa[10].

Poza wyjaśnieniem znaczenia terminu *otwarte dane*, w literaturze zagranicznej wytycza się także cztery zasadnicze etapy ich analizowania. Są to:

1) zebranie danych surowych (ang. *Open Source Data*, OSD), pochodzących z pierwotnego źródła (tj. publikacji drukowanych,

---

[5] K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011, s. 51.

[6] K. Mroziewicz, *Czas pluskiew*, Warszawa 2007, s. 334.

[7] Tamże.

[8] *NATO Open Source Inteligence Reader* [online]. Oss.net [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO OSINT Reader FINAL 11OCT02.pdf.

[9] *Director of Central Intelligence Directive* [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: https://fas.org/irp/offdocs/dcid212.htm.

[10] *Biały wywiad, czyli otwarte źródła informacji w działalności śledczej i wywiadowczej* [online]. Zawsze czujni.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://www.zawszeczujni.pl/2015/09/biay-wywiad-czyli-otwarte-zroda.html.

mediów, stron internetowych, fotografii) i przedstawienie ich w najprostszej formie,
2) poddanie analizie zebranych danych (ang. *Open Source Information*, OSINF), poddanie ich pewnym zabiegom edytorskim, zebranie ich w jeden dokument i przekazane osobom zarządzającym w celu dalszego rozpowszechnienia,
3) zaplanowane uzyskanie informacji, tzw. biały wywiad (ang. *Source Intelligence*, SINT) – przekazanie danych wyselekcjonowanej grupie odbiorców i zgodnie z zasadami określonymi przez składającego zapytanie (każda służba policyjna czy wywiadowcza wypracowuje we własnym zakresie metodykę postępowania z danymi i informacjami),
4) weryfikacja informacji, tzw. zweryfikowany, potwierdzony biały wywiad (ang. *Validated Open Source Inteligence*, OSINT-V) – potwierdzenie stopnia poziomu pewności informacji na podstawie różnych źródeł[11].

Rodzaje otwartych źródeł informacji wykorzystywane w pracy organów ścigania

Otwarte źródła informacji najczęściej wykorzystywane w pracy organów ścigania można podzielić na kilka kategorii:

1) media tradycyjne:
   - prasa drukowana (np. dzienniki, czasopisma branżowe, dokumenty rządowe),
   - telewizja informacyjna, rozgłośnie radiowe,
   - literatura (książki, publicystyka, analizy, śledztwa dziennikarskie),
2) Internet:
   - internetowe wydania gazet i czasopism,
   - blogi, mikroblogi,
   - portale społecznościowe,
   - strony wiki,
   - serwisy wideo,

[11] B. Sromczyńki, P. Waszkiewicz, dz. cyt., s. 149.

- serwisy fotograficzne,
- strony internetowe przedsiębiorców,
- rejestry domen WHOIS,
- mapy, zdjęcia satelitarne, zdjęcia lotnicze.

3) usługi komercyjne:
   - podmioty gospodarcze, które za opłatą przygotowują sprofilowane raporty i analizy,
   - wydawnictwa marketingowe,
4) szara literatura (ang. *grey literature*) – analizy, informacje będące do dyspozycji tylko poprzez wyspecjalizowane kanały, generowane przez środowiska akademickie, organizacje państwowe i pozarządowe,
5) bazy danych i katalogi[12].

Obserwując praktykę śledczą służb specjalnych, można zaryzykować stwierdzenie, że wykorzystywanie otwartych źródeł informacji, przede wszystkim zasobów Internetu, jest nieodłącznym elementem działań wykrywczych. Niestety, faktem jest, że działanie takie nie jest obce również zorganizowanym grupom przestępczym oraz ugrupowaniom terrorystycznym, które adaptują techniki charakterystyczne dla białego wywiadu i używają ich w swojej działalności[13].

Znaczenie metadanych w wywiadzie białym

Istotnym aspektem związanym z białym wywiadem są metadane, a więc informacje pozwalające zidentyfikować i opisać dany obiekt. Chociaż z ich znaczenia mało który użytkownik sieci zdaje sobie świadomie sprawę, warto zauważyć, że mogą one odegrać doniosłą rolę w działaniach operacyjnych służb specjalnych. Dla przykładu, każde zdjęcie zrobione apa-

[12] G. Dobrowolski, W. Filipkowski, M. Kisiel-Dorohnicki, W. Rakoczy, *Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu*, [w:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu*, pod red. L. K. Paprzyckiego, Z. Rau, Warszawa 2009, s. 281–282.

[13] E. Wójcik, *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej* [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://m.wspia.eu/file/21440/44-WÓJCIK.pdf; B. Saramak, *„Biały wywiad" w służbie terroryzmu*, [w:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, pod red. K. Liedela, P. Piaseckiej, T. R. Aleksandrowicza, Warszawa 2014, s. 182–196.

ratem cyfrowym czy też smartfonem wyposażone w metadane – a więc informacje opisujące urządzenie, którym wykonano zdjęcie oraz warunki, w jakich to nastąpiło – może stać się elementem identyfikacji i weryfikacji danych. Fotografie wyposażone w informacje takie, jak data i czas wykonania, ustawienia kamery, lokalizacja czy miniatura oryginalnego kadru, umieszczane np. w portalach społecznościowych (dane takie zachowują i udostępniają m.in. serwisy Twitter i Instagram), mogą znacznie ułatwiać organom ścigania odszukiwanie osób zaginionych czy podejrzanych lub doprowadzać do osób je publikujących[14]. Wystarczy mieć bowiem zainstalowaną wtyczkę do przeglądarki Mozilla Firefox – Exif Viewer, by pozyskać wszystkie wyżej wymienione informacje. Dowodem skuteczności wykorzystywania w działalności śledczej metadanych zintegrowanych z fotografiami jest przypadek El Chapo – przywódcy meksykańskiego kartelu narkotykowego, poszukiwanego kilka miesięcy przez policję. Niefrasobliwość jego syna, który w serwisie Twitter opublikował zdjęcia wyposażone w metadane geolokalizacyjne, doprowadziła do ujawnienia miejsca przebywania, a następnie ujęcia przestępcy[15]. Podobny przypadek miał miejsce z wykorzystaniem fotografii zamieszczonych w serwisie Instagram. Kiedy jeden z żołnierzy wojsk rosyjskich udostępnił w nim zdjęcia z wnętrza opancerzonego transportera, metadane lokalizacyjne ujawniły obecność wojsk rosyjskich na terenie Ukrainy, co ostatecznie obnażyło nieprawdziwość oficjalnych deklaracji władz rosyjskich w tym temacie[16].

Nieco innego przykładu możliwości wykorzystywania metadanych dostarcza użytkowanie serwisu Stolen Camera Finder[17], który ułatwia odnajdywanie zgubionego czy też skradzionego telefonu. Wystarczy wgrać jakiekolwiek zdjęcie ze swojego urządzenia, podać datę zagubienia/kradzieży, a serwis będzie przeszukiwał Internet pod kątem zdjęć wyko-

---

[14] *Zanim wgrasz wakacyjne zdjęcia do sieci…*[online]. Niebezpiecznik.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: https://niebezpiecznik.pl/post/zanim-wgrasz-wakacyjne-zdjecia-do-sieci/; *Biały wywiad, czyli otwarte źródła…*

[15] Więcej na ten temat: [Adam], *Syn narkotykowego bossa przez pomyłkę ujawnia na Twitterze lokalizację ojca* [online]. Zaufana Trzecia Strona [dostęp 31 marca 2017]. Dostępny w World Wide Web: https://zaufanatrzeciastrona.pl/post/syn-narkotykowego-bossa-przez-pomylke-ujawnia-na-twitterze-lokalizacje-ojca/.

[16] *Zanim wgrasz wakacyjne zdjęcia do sieci…*

[17] *Stolen Camera Finder* [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://www.stolencamerafinder.com/.

nanych urządzeniem po wskazanej dacie. Jeśli znajdzie jakieś informacje, to z dużym prawdopodobieństwem będą to dane zawarte w profilu społecznościowym należącym do znalazcy (albo złodzieja, albo osoby, która odkupiła lub znalazła sprzęt)[18].

Warto nadmienić, że poza plikami ze zintegrowanymi metadanymi dużą ilości tego typu informacji dostarczają także blogi czy serwisy aukcyjne. Często zdarza się bowiem, że aby skomentować dany post czy artykuł lub zakupić jakiś przedmiot, konieczne jest podanie danych osobowych. Ich ujawnienie i połączenie z konkretnym adresem IP może stanowić ważny punkt startowy do wszczęcia stosownych procedur śledczych: poszukiwawczych, przeszukiwawczych i identyfikacyjnych[19].

Bibliotekarze ninja i media społecznościowe

Amerykańska agencja wywiadowcza CIA jest przykładem tego, jak biały wywiad działa w praktyce. Agencja prasowa Associated Press opublikowała raport, z którego wynika, że zlokalizowane w Wirginii Open Source Center skupia grupę analityków nazywanych „mściwymi bibliotekarzami" albo „bibliotekarzami ninja". Mianem tym określa się analityków, którzy mają za zadanie zdobyć informacje na podstawie powszechnie dostępnych źródeł, m.in. serwisów społecznościowych[20]. Serwisy te cieszą się zainteresowaniem, ponieważ w jednym miejscu gromadzą bardzo dużo informacji, które pochodzą bezpośrednio od użytkownika oraz jego znajomych. Informują o codziennych aktywnościach, sympatiach czy antypatiach, zainteresowaniach. Zawierają zdjęcia, filmy, informacje o znajomych użytkownika i miejscach, w których się znajduje, deklaracje udziału w wydarzeniach, a przede wszystkim informacje, czy jest on aktualnie dostępny online[21].

Na duże znaczenie wykorzystania mediów społecznościowych w pracy organów ścigania zwrócono uwagę w projekcie Comparative

---

[18] *Zanim wgrasz wakacyjne zdjęcia do sieci…*

[19] B. Sromczyński, P. Waszkiewicz, dz. cyt., s. 154.

[20] Ł. Michalik, Open *Source Center – sposób CIA na śledzenie Internetu* [online]. Gadzetomania.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://gadzetomania.pl/9480,open-source-center-sposob-cia-na-sledzenie-internetu.

[21] B. Sromczyński, P. Waszkiewicz, dz. cyt., s. 157.

Police Studies in the European Union (COMPOSITE) – realizowanym w strukturach 7 Programu Ramowego UE, w którego pracach uczestniczą przedstawiciele dziesięciu państw. W jego ramach dokonano m.in. wyodrębnienia dziewięciu obszarów wykorzystania mediów społecznościowych przez organy ścigania:

- media społecznościowe jako źródło informacji kryminalnej (ang. *Social Media as a Source of Criminal Information*),
- głos (aktywna obecność) w mediach społecznościowych (ang. *Having a Voice in Social Media*),
- przekazywanie informacji za pomocą mediów społecznościowych (ang. *Social Media to Push Information*),
- media społecznościowe jako dźwignia „mądrości tłumu" (ang. *Social Media to Leverage the Wisdom of the Crowd*),
- interakcje ze społeczeństwem za pomocą mediów społecznościowych (ang. *Social Media to Interact with the Public*),
- community policing poprzez media społecznościowe (ang. *Social Media for Community Policing*),
- ludzka twarz policji za pośrednictwem mediów społecznościowych (ang. *Social Media to Show the Human Side of Policing*),
- wsparcie policyjnej infrastruktury IT za pomocą mediów społecznościowych (ang. *Social Media to Support Police IT Infrastructure*),
- media społecznościowe wspierające efektywność policji (ang. *Social Media for Efficient Policing*)[22].

Wyżej zaprezentowana lista sposobów wykorzystywania przez służby śledcze informacji zawartych w mediach społecznościowych wyraźnie wskazuje, że portale społecznościowe mogą w tym zakresie pełnić trzy funkcje – informacyjną, dowodową i poszlakową[23].

Analiza informacji zamieszczanych na portalach społecznościowych pozwala ujawnić przedsięwzięcia zagrażające bezpieczeństwu przed popełnieniem wykroczenia. Zazwyczaj dotyczy to imprez masowych. Przykładowo, gdy organizatorzy tego rodzaju imprez poprzez ich promocję w mediach społecznościowych próbują zaprosić większą niż oficjalnie

[22] Tamże, s. 158.
[23] B. Sromczyńki, P. Waszkiewicz, dz. cyt., s. 158.

zgłoszona liczbę uczestników, policja – znajdując taką informację – może powiadomić organizatorów o złamaniu prawa i ze względów bezpieczeństwa podjąć stosowne działania prewencyjne lub w ostateczności – nie dopuścić do organizacji takich wydarzeń[24].

Większość informacji pochodzących z portali społecznościowych może mieć charakter dowodowy. Czasami będzie to dowód na popełnienie konkretnego przestępstwa (jak np. przypadek Rodneya Knighta Jr., który po włamaniu do pewnego domu zalogował się na konto facebookowe syna właściciela domu i opublikował swoje zdjęcie ze skradzioną biżuterią i laptopem)[25], czasami – dowód poszlakowy (np. proces w sprawie śmierci sześciomiesięcznej Madzi z Sosnowca, w trakcie którego odtworzona została historia wyszukiwania w Internecie, dowodząca zainicjowania procesu wyszukiwania przez matkę dziewczynki haseł „zatrucie tlenkiem węgla" oraz „jak zabić bez śladów")[26].

Podsumowanie

Wiele osób ma wątpliwości, czy wykorzystywanie źródeł otwartych w pracy organów ścigania może być traktowane jako czynność operacyjno-rozpoznawcza i czy można traktować te informacje jako materiał dowodowy w sprawie. W Polsce wątpliwości te rozwiewa artykuł 14 Ustawy z dnia 6 kwietnia 1990 r. o Policji, w którym czytamy, że policja w celu rozpoznawania, zapobiegania i wykrywania przestępstw i wykroczeń obok czynności dochodzeniowo-śledczych i administracyjno-porządkowych ma prawo wykonywać czynności operacyjno-rozpoznawcze[27]. Czynności operacyjno-rozpoznawcze w przypadku pracy policji sprowa-

---

[24] S. Czubkowska, *Policja i urzędnicy śledzą cię na Facebooku* [online]. Wiadomosci.dziennik.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://wiadomosci.dziennik.pl/wydarzenia/artykuly/118564,policja-i-urzednicy-sledza-cie-na-facebooku.html.

[25] B. Sromczyńki, P. Waszkiewicz, dz. cyt., s. 162.

[26] *Hasło „zabić bez śladu" nie do obrony? Wyszukiwarka bezlitosna dla Katarzyny W*. [online]. Tvn24.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://www.tvn24.pl/wiadomosci-z-kraju,3/haslo-zabic-bez-sladu-nie-do-obrony-wyszukiwarka-bezlitosna-dla-katarzyny-w,324161.html.

[27] *Ustawa z dnia 6 kwietnia 1990 r. o Policji, tekst jednolity*, Dz.U. 2011, nr 7, poz. 58.

dzają się do ustalenia sprawców przestępstw oraz dowodów w procesie karnym czy też do rozpoznawania działalności przestępczej[28].

Mimo że nieograniczona objętość i różnorodność otwartych źródeł informacji są największą zaletą w procesie pozyskiwania informacji, to swoiste „bogactwo" może dla służb śledczych stanowić dotkliwy problem w procesie analizy. Wyselekcjonowanie informacji wiarygodnych zajmuje sporo czasu i wymaga specjalnych umiejętności. Aby maksymalnie wykorzystać możliwości białego wywiadu, potrzebna jest fachowa wiedza i duże doświadczenie. Kolejną kwestią jest ciągle przyrastająca ilość informacji oraz związany z tym szum informacyjny, który utrudnia, a niejednokrotnie wręcz uniemożliwia oddzielenie wiadomości prawdziwych i istotnych od fałszywych i błahych. Problemu tego nie rozwiązuje co gorsza dynamiczny postęp w dziedzinie automatycznego wyszukiwania i analizy treści. Wydaje się nawet, że automatyzacja procesów wyszukiwania informacji implikuje pewne problemy weryfikacji informacji. Nie jest bowiem łatwo zweryfikować datę umieszczonych w sieci informacji, ponieważ są one wielokrotnie kopiowane, często bez podania pierwotnego źródła, co bardzo komplikuje ocenę ich rzetelności. Takie zjawisko nazywane jest przez analityków „efektem echa".

Chociaż biały wywiad wydaje się metodą uniwersalną, istnieją obszary, w których jest on całkowicie nieprzydatny. Za przykład może służyć proces tropienia przywódców grup terrorystycznych. Ich duże rozproszenie, nierzadko działalność w pojedynkę oraz wykorzystywanie wielu źródeł informacji (zwłaszcza Internetu) w roli narzędzia propagandy nie zaś komunikatora[29] znacznie obniża efektywność tej metody.

Problemem, jaki od samego początku towarzyszy białemu wywiadowi, jest bariera językowa. Brakuje specjalistów, którzy biegle władają takimi językami, jak chiński, arabski, hindu, farsi czy pasztu. Ogranicza to bardzo efektywność zbierania informacji pochodzących z różnych części świata.

Istotną wadą jest także dezinformacja, czyli manipulowanie przekazem medialnym i celowe wprowadzanie w błąd grup społecznych.

---

[28] E. Wójcik, dz. cyt., s. 435-436.

[29] M. Adamczuk, *Terroryzm indywidualny jako zagrożenie dla bezpieczeństwa europejskiego*, [w:] *Zamach w Norwegii. Nowy wymiar zagrożenia terroryzmem w Europie*, pod red. K. Liedela, P. Piaseckiej, T. R. Aleksandrowicza, Warszawa 2011, s. 44–46.

Oznacza to, że specjaliści zajmujący się białym wywiadem muszą posiadać dobry warsztat analityczny, ogromną wiedzę i duży dystans do każdego analizowanego źródła[30].

Osoby zajmujące się białym wywiadem wiążą duże oczekiwania z automatyzacją procesu wywiadu jawnoźródłowego, a więc tworzeniem i stosowaniem specjalistycznych baz danych, technik rozpoznawania tekstu i mowy, biometrii, translacji, analizy powiązań kryptografii czy skanowania i oceny wiarygodności witryn internetowych. Wdrożenie takiej automatyzacji postrzegane jest z jednej strony jako szansa na zwiększenie wydajności procesów pozyskiwania, analizy i zarządzania informacjami[31], z drugiej – poszerzenie możliwości podejmowania działań proaktywnych[32].

Mimo że początków białego wywiadu możemy doszukiwać się w okresie rozwoju prasy[33], w związku z rozwojem nowoczesnych technologii biały wywiad coraz częściej „przenosi się" do Internetu. I choć jest wykorzystywany przez służby śledcze, wielu jego funkcjonariuszy nie zdaje sobie sprawy, że realizuje właśnie tę formę wywiadu. Ponadto brak fachowej edukacji z wykorzystywania otwartych źródeł informacji ma wpływ na akcentowanie przekonania przez służby śledcze o wyższości informacji zdobytych drogą operacyjną nad tymi pozyskanymi za pomocą źródeł otwartych. Wprawdzie w policji nie wykształciła się osobna praktyka zbliżona do OSINT, jednak jej elementy są znane i czasami stosowane, ale w sposób nieusystematyzowany[34].

---

[30] B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej* [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://www.abw.gov.pl/download/1/1679/Saramak.pdf.

[31] T. Serafin, *Automatyzacja procesu wywiadu jawnoźródłowego w ramach działalności wywiadowczej i walki z terroryzmem*, [w:] *Analiza informacji w zarządzaniu bezpieczeństwem*, pod red. K. Liedela, P. Piaseckiej, T. R. Aleksandrowicza, Warszawa 2013, s. 83.

[32] K. Radaniak, *Biały wywiad w policji – narzędzie rozpoznawania zagrożeń terrorystycznych*, „Studia Prawnicze. Rozprawy i materiały" 2012, nr 2 (11), s. 96; B. Sarmak, *„Biały wywiad" w służbie terroryzmu*..., s 267.

[33] K. Radwaniak, P. J. Wrzosek, *Biały wywiad w Policji – pozyskiwanie i analiza informacji ze źródeł otwartych*, [w:] *Analiza informacji w służbach*..., s. 149.

[34] Tamże, s. 149.

Bibliografia

[Adam], *Syn narkotykowego bossa przez pomyłkę ujawnia na Twitterze lokalizację ojca* [online]. Zaufana Trzecia Strona [dostęp 31 marca 2017]. Dostępny w World Wide Web: https://zaufanatrzeciastrona.pl/post/syn-narkotykowego-bossa-przez-pomylke-ujawnia-na-twitterze-lokalizacje-ojca/.

Analiza informacji w służbach policyjnych i specjalnych, red. Jerzy Konieczny, Warszawa 2012.

Analiza informacji w zarządzaniu bezpieczeństwem, pod red. Krzysztofa Liedela, Pauliny Piaseckiej, Tomasza R. Aleksandrowicza, Warszawa 2013.

Biały wywiad, czyli otwarte źródła informacji w działalności śledczej i wywiadowczej [online]. Zawszeczujni.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://www.zawszeczujni.pl/2015/09/biay-wywiad-czyli-otwarte-zroda.html.

Czubkowska Sylwia, *Policja i urzędnicy śledzą cię na Facebooku* [online]. Wiadomosci.dziennik.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://wiadomosci.dziennik.pl/wydarzenia/artykuly/118564,policja-i-urzednicy-sledza-cie-na-facebooku.html.

Hasło „zabić bez śladu" nie do obrony? Wyszukiwarka bezlitosna dla Katarzyny W. [online]. Tvn24.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://www.tvn24.pl/wiadomosci-z-kraju,3/haslo-zabic-bez-sladu-nie-do-obrony-wyszukiwarka-bezlitosna-dla-katarzyny-w,324161.html.

Liedel Krzysztof, Serafin Tomasz, *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011.

Michalik Łukasz, *Open Source Center – sposób CIA na śledzenie Internetu* [online]. Gadzetomania.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://gadzetomania.pl/9480,open-source-center-sposob-cia-na-sledzenie-internetu.

Mroziewicz Krzysztof, *Czas pluskiew*, Warszawa 2007.

NATO Open Source Inteligence Reader [on-line]. Oss.net [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546 bf5c9f1ed/NATO OSINT Reader FINAL 11OCT02.pdf.

Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu, pod red. Lecha Krzysztofa Paprzyckiego, Zbigniewa Rau, Warszawa 2009.

Radwaniak Krzysztof, *Biały wywiad w policji – narzędzie rozpoznawania zagrożeń terrorystycznych*, „Studia Prawnicze. Rozprawy i materiały" 2012, nr 2 (11), s. 85–100.

Saramak Bartosz, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej* [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://*www.abw.gov.pl/download/ 1/1679/Saramak.pdf.*

Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji, pod red. Krzysztofa Liedela, Pauliny Piaseckiej, Tomasza R. Aleksandrowicza, Warszawa 2014.

Sromczyńki Błażej, Waszkiewicz Paweł, *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5, s. 146–170.

Ustawa z dnia 6 kwietnia 1990 r. o Policji, tekst jednolity, Dz.U. 2011, nr 7, poz. 58.

Wójcik Ewelina, *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej* [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: *http://m.wspia.eu/file/21440/44-WÓJCIK.pdf.*

Zamach w Norwegii Nowy wymiar zagrożenia terroryzmem w Europie, pod red. Krzysztofa Liedela, Pauliny Piaseckiej, Tomasza R. Aleksandrowicza, Warszawa 2011.

Zanim wgrasz wakacyjne zdjęcia do sieci...[online]. Niebezpiecznik.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: https://niebezpiecznik.pl/post/zanim-wgrasz-wakacyjne-zdjecia-do-sieci/.

Ziółkowska Agata, *Biały wywiad w bezpieczeństwie państwa* [online]. Bezpieczenstwowbiznesie.pl [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://bezpieczenstwowbiznesie.pl/index.php/wywiad-gospodarczy/geopolityka/269-bialy-wywiad-w-bezpieczenstwie-panstwa.

The Use of Open Source Information for Investigative Services

Abstract: The progressive increase in overt information resources and the ability to quickly and easily access them make more and more different entities use them in actions they take. Such a situation is observed, among others, in investigative services that use these resources prior to and during the execution of further intelligence activities conducted by other means. This article is an

attempt to describe the possibility of using open sources of information in the work of investigative services. It describes the essence and importance of overtly accessible information, the stages of its analysis and examples of its use by the prosecution services in Poland and abroad. The article also presents advantages and disadvantages of the so-called white interview and restrictions on the use of information open sources resulting from information resources increase and automation of information retrieval.

Keywords: analysis of information, investigative services, open sources of information, security services.