Bartosz Saramak

Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej[1]

Potencjał i ograniczenia białego wywiadu

Każda z klasycznych dyscyplin wywiadowczych ma swoje cechy charakterystyczne, potencjał oraz ograniczenia. Podobnie jest również z białym wywiadem, który ma własną, bardzo wyraźną specyfikę. Jedną z istotniejszych cech białego wywiadu jest możliwość dostarczenia niezwykle szerokiego tła problemu i zbudowanie odpowiedniego kontekstu do dalszej jego analizy. Informacje dostarczane przez środki masowego przekazu zapewniają ogólną wiedzę, która, co ważne, jest podana w przystępnej i odpowiednio przygotowanej formie. Pozwala to na bardzo szybkie i sprawne zapoznanie się z kontekstem społecznym, kulturowym, historycznym oraz religijnym analizowanej sytuacji, co z kolei znacznie zwiększa szansę na uzyskanie prawidłowej i pełniejszej odpowiedzi podczas dalszych działań wywiadowczych prowadzonych innymi środkami. Odnosi się to szczególnie do kwestii formułowania zapytań kierowanych do pionów operacyjnych. Dzięki wstępnej analizie informacji z otwartych źródeł jest bowiem możliwe pełniejsze i dokładniejsze sprecyzowanie ich zakresu i charakteru. Niejednokrotnie zdarza się, że informacje zawarte w otwartych źródłach okazują się na tyle szczegółowe i pewne, że podejmowanie kosztowniejszych metod ich uzyskania w ogóle nie jest potrzebne. Biały wywiad pozwala także na zweryfikowanie informacji zebranych wcześniej przy wykorzystaniu innych dyscyplin, co niewątpliwie w sposób korzystny wpływa na jakość ostatecznego materiału wywiadowczego[2]. Weryfikacja taka pozwala często na wyłapywanie błędów zespołu zbierającego informacje, a czasem nawet na obnażenie jego niekompetencji lub wykrycie świadomej lub nieświadomej (zastosowanej przez obce wywiady) manipulacji i dezinformacji[3]. W tym właśnie kontekście można przeanalizować zarówno podstawowe zalety, jak i ograniczenia białego wywiadu.

Potencjał i zalety

Zalety wykorzystania otwartych źródeł informacji w działalności wywiadowczej zostały już wcześniej nakreślone, ale aby w pełni zrozumieć potencjał, jaki w sobie kryją, warto przeanalizować je dokładnej. S.C. Mercado, jeden z najbardziej znanych

[1] Fragment pracy magisterskiej, która zajęła I miejsce w konkursie Szefa ABW *na najlepszą pracę licencjacką/magisterską z dziedziny bezpieczeństwa wewnętrznego państwa* (edycja 2013/2014), rozdział I pt. *Pojecie i charakterystyka białego wywiadu* (podrozdziały 3.1–3.3) i rozdział IV pt. *Wybrane obszary wykorzystania otwartych źródeł informacji* (podrozdział 3) wraz z podsumowaniem. Redakcja dokonała niezbędnych zmian numeracji tytułów i przypisów (przyp. red.).

[2] *Open Source Intelligence, Headquarters*, s. 2-2 [online], http://www.fas.org/irp/doddir/army/atp2-22-9.pdf [dostęp: 28 VII 2013].

[3] Z. Siemiątkowski, *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009, s. 35.

amerykańskich specjalistów zajmujących się omawianą tematyką, stwierdził, że podstawowymi zaletami czy wręcz przewagami, jakie wywiad jawnoźródłowy ma nad pozostałymi dyscyplinami wywiadowczymi, są szybkość i łatwość pozyskiwania informacji, ich ilość, różnorodność, jakość i przejrzystość, a także niewielkie koszty ich analizy[4].

Szybkość, z jaką można sięgnąć po informacje z otwartych źródeł, jest rzeczywiście oszałamiająca. Głównym tego powodem jest przede wszystkim rewolucja w zakresie technologii informacyjnej oraz powstanie i upowszechnienie się sieci Internet. Komputer, podstawowe oprogramowanie i szerokopasmowe łącze internetowe to narzędzia, które pozwalają w czasie rzeczywistym śledzić i analizować wydarzenia rozgrywające się nawet po drugiej stronie kuli ziemskiej. Tempo pracy współczesnych dziennikarzy powoduje, że niejednokrotnie zdobywają oni bieżące informacje znacznie szybciej niż służby wywiadowcze. Materiały mogą się ukazywać prawie natychmiast po ich sporządzeniu. Pracy koncernów medialnych nie spowalnia procedura związana ze ściśle przestrzeganym obiegiem informacji i w przeciwieństwie do służb państwowych, mogą one działać w zasadzie bez żadnych ograniczeń[5]. Dlatego też często najważniejsze decyzje w państwie są podejmowane nie na podstawie raportów wywiadowczych, ale informacji przekazywanych przez media (fenomen ten został nazwany „efektem CNN-u"). Nie ma jednak powodu, aby funkcjonariusze wywiadu ścigali się z reporterami. Z tego właśnie względu ciągły monitoring mediów jest tak ważny i przydatny. Pozwala zaoszczędzić zasoby, które dużo pożyteczniej można wykorzystać na prowadzenie długoterminowych analiz[6].

Współcześnie biały wywiad wydaje się mieć wręcz nieograniczone możliwości, jeśli chodzi o objętość źródeł i ich zakres tematyczny. Niewątpliwą i niepodważalną zaletą wykorzystania otwartych źródeł jest ilość oraz różnorodność informacji w nich zawarta. Cecha ta jest szczególnie przydatna, kiedy analiza ma na celu zbudowanie tła i przestawienie szerszego kontekstu (społecznego, ekonomicznego, historycznego, religijnego). Daje to możliwość wieloaspektowego pokazania problemu, co rzadko jest możliwe przy wykorzystaniu innych dyscyplin wywiadowczych. Ponadto potencjałem nie do przecenienia jest liczba dziennikarzy, blogerów, ekspertów i naukowców gotowych do dzielenia się wynikami swojej pracy, a czasem nawet do udzielania szybkiej pomocy w postaci konsultacji czy przeprowadzenia zleconej analizy. Dzięki informacjom zawartych w otwartych źródłach, dotarcie do tych ludzi nie jest żadnym problem. Ponadto wielość i różnorodność komercyjnych baz danych i repozytoriów sprzyja konkurencji, a co za tym idzie dbałości o jakość i wiarygodność oferowanych danych[7].

Wydaje się, że to właśnie jakość informacji jest zaletą, która jest najczęściej poddawana krytyce, choć istnieje wystarczająca liczba źródeł sprawdzonych i wielokrotnie zweryfikowanych (takich jak np. największe agencje prasowe, koncerny medialne, uniwersytety czy komercyjne bazy danych), aby bez narażania się na nadmierne ryzyko oprzeć się na informacjach z nich pochodzących. Warto równocześnie podkreślić, że dociekliwość dziennikarzy wykorzystujących najnowocześniejszy sprzęt często owo-

[4] S.C. Mercado, *Reexamining the Distinction Between Open Information and Secrets* [online], https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/Vol49no2/ reexamining_the_distinction_3.htm [dostęp: 17 VIII 2014].

[5] K. Leetaru, *The Scope of FBIS and BBC Open-Source Media Coverage, 1979–2008 (U)*, „Studies in Intelligence", 2010, nr 1, s. 18.

[6] Z. Siemiątkowski, *Wywiad a władza…,* s. 38–39.

[7] H. Minas, *Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century?,* „RIEAS: Research Paper", 2010, nr 139.

cuje materiałem wyjątkowo dobrej klasy, którego uzyskanie drogą operacyjną byłoby nieporównanie droższe i znacznie bardziej czasochłonne. Tak więc stosunek jakości zdobywanych materiałów do kosztów z tym związanych to kolejna niepodważalna zaleta białego wywiadu. Pod tym względem metoda ta jest postrzegana jako efektywna i wydajna. Cyfrowy charakter współczesnej informacji powoduje, że koszty tworzenia i utrzymania repozytoriów oraz baz danych, a także korzystanie z ich zasobów są minimalne. Dlatego też większość informacji pozyskiwanych z przestrzeni publicznej jest zupełnie darmowa[8].

Cyfrowy charakter jawnoźródłowej informacji wiąże się z kolejną jej zaletą, którą jest łatwość jej przetwarzania oraz przeanalizowania. Klej i nożyczki zostały zastąpione przez oprogramowanie, w sposób automatyczny wspierając wyszukiwanie, selekcję i ekstrakcję informacji. Podstawą współczesnej sztuki wyszukiwania i analizy informacji jest bardzo szerokie wykorzystanie otwartych źródeł informacji poza sektorem publicznym. Owocuje to m.in. bogatą ofertą szkoleń i warsztatów skierowanych nie tylko do funkcjonariuszy służb państwowych odpowiedzialnych za bezpieczeństwo, lecz także do researcherów, infobrokerów specjalistów wywiadu, detektywów, dziennikarzy, naukowców, analityków z sektora rządowego oraz prywatnego[9]. Powoduje to, że warsztat analityczny specjalistów z różnych sektorów przenika się i uzupełnia, dzięki czemu jest możliwa ciągła poprawa standardów i wprowadzanie coraz to nowych, doskonalszych narzędzi pozwalających na sprawniejszą eksplorację kolejnych źródeł.

Z punktu widzenia służb wywiadowczych biały wywiad posiada jeszcze jedną zaletę nie do przecenienia. Ryzyko wykrycia zbierania informacji przez kontrwywiad i konsekwencję z tym związane są znikome. Dlatego też metoda ta była szeroko wykorzystywana przez zachodnie służby wywiadowcze w państwach totalitarnych. Przypadek Korei Północnej pokazuje, że problem ten jest wciąż aktualny. Stworzenie i koordynacja nawet najszczuplejszej siatki opartej na tajnych współpracownikach w warunkach permanentnej kontroli i inwigilacji jest zadaniem niezwykle trudnym, czasochłonnym i kosztownym[10].

Kolejną zaletą wykorzystania otwartych źródeł informacji, zwłaszcza w realiach współczesnej demokracji liberalnej, jest niewielka ingerencja w prywatność osób trzecich oraz w prawa człowieka i obywatela[11]. Analizując problem z punktu widzenia służb państwowych odpowiedzialnych za bezpieczeństwo, nie sposób nie dostrzec dwóch płynących z tego korzyści. Po pierwsze niewielka „inwazyjność" różnych form białego wywiadu pozwala obyć się bez sądowej i prokuratorskiej kontroli, nieuniknionej w przypadku zastosowania metod pracy operacyjnej. Druga korzyść to kreowanie korzystniejszego wizerunku w oczach społeczeństwa. Im rzadziej służby specjalne stosują inwigilację i inne środki specjalne oraz wykorzystują agenturę, tym bardziej są postrzegane jako „mniej opresyjne" i przyjazne obywatelom. W tym kontekście biały wywiad

[8] R.D. Steele, *Open Source Intelligence,* w: *Handbook of Intelligence Studies, L. K. Johnson* (red.), London–New York 2006, s. 136–137.

[9] Przykładem mogą być szkolenia oferowane przez firmę *Mediaquest*, zob. http://www.mediaquest.pl/osint/ [dostęp: 17 VIII 2014] czy *Niemczyk i wspólnicy*, [online], http://niwserwis.pl/artykuly/e-learning-kurs-bialy-wywiad-jako-metoda-pracy-detektywistycznej.html [dostęp: 17 VIII 2014].

[10] S.C. Mercado, Sailing the Sea of OSINT in the Information Age: A Venerable Source in a New Era [online], https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csistudies/studies/vol48no3/ article05.html [dostęp: 15 VIII 2014].

[11] G. Hribar, I. Podbregar, T. Ivanuša, *OSINT: A "Grey Zone"?,* „International Journal of Intelligence and CounterIntelligence" 2014, t. 27, wyd. 3, s. 539.

należy uznać za metodę najbardziej sprzyjającą utrzymaniu takiego właśnie wizerunku. Warto zauważyć, że obecnie jednym z najbardziej kluczowych źródeł informacji stały się internetowe portale społecznościowe (zwłaszcza Twitter i Facebook). Analitycy amerykańskiego Open Source Center działającego w strukturach CIA czytają codziennie nawet 5 mln wpisów z nich pochodzących. Na podstawie tak zdobytych danych sporządza się raporty dotyczące bieżących nastrojów społecznych w wielu miejscach na świecie oraz przygotowuje prognozy dotyczące nadchodzących wydarzeń[12].

Ostatnią zaletą godną podkreślenia jest możliwość stosunkowo szerokiej dystrybucji raportów opracowanych przy wykorzystaniu białego wywiadu, co wynika z pominięcia procedur dotyczących ochrony informacji niejawnych. Już sam fakt, że nie ma konieczności objęcia specjalną ochroną tajnego źródła, znacznie upraszcza obieg i sposób przechowywania informacji. Dodatkową korzyścią jest nie tylko możliwość dużo szerszej wymiany informacji z sojuszniczymi służbami, lecz także zastosowania tzw. *outsourcingu* i tym samym bieżącej współpracy z podmiotami prywatnymi zajmującymi się pozyskiwaniem informacji[13]. Elastyczność dysponowania materiałami opracowanymi na podstawie otwartych źródeł w bezpośredni sposób wpływa na obniżenie kosztów pracy wywiadowczej oraz powoduje wzrost jej efektywności przez zdecydowanie lepsze wykorzystanie sił i środków.

Ograniczenia i wady

Mimo wielu niepodważalnych zalet, biały wywiad ma także swoje ograniczenia oraz wady. Niektóre z nich są związane bardziej z sygnalizowanymi wcześniej uprzedzeniami niż rzeczywistymi ułomnościami omawianej dyscypliny. Przykładem takiego uprzedzenia może być chociażby zarzut zakłócania „czystości" klasycznego cyklu wywiadowczego, którego podstawą jest informacja pochodząca ze źródeł niejawnych, każdorazowo głęboko i dokładnie weryfikowana zgodnie z zasadami sztuki wywiadowczej[14]. Nie da się ukryć, że biały wywiad ma również swoje rzeczywiste i wyraźnie dostrzegalne ograniczenia. Współcześnie najbardziej dotkliwym problemem dla służb jest nadmiar informacji. To, co wydaje się największą zaletą otwartych źródeł informacji, a więc ich nieograniczona objętość i różnorodność, w praktyce może stanowić kłopot w procesie analizy. Wyselekcjonowanie informacji wiarygodnych oraz oryginalnych danych wymaga nie tylko nie lada umiejętności, lecz także zajmuje sporo czasu. Aby w pełni korzystać z możliwości, jakie daje biały wywiad, potrzeba fachowej wiedzy i niemałego doświadczenia. Dodatkową niedogodnością jest konieczność poradzenia sobie ze zjawiskiem, ciągle narastającego tzw. szumu informacyjnego, czyli nadmiaru

[12] „Mściwi bibliotekarze", jak żartobliwie nazywani są pracownicy OSC, podkreślają, że obecnie nieocenionym źródłem informacji, jeśli chodzi o śledzenie błyskawicznie rozwijających się wydarzeń, są właśnie serwisy społecznościowe. Jako przykład można przytoczyć zamieszki mające miejsce w Bangkoku w 2010 r. Informacje, których nie byli w stanie dostarczyć ani funkcjonariusze wywiadu ani dziennikarze, na bieżąco pojawiały się na Twitterze i Facebooku. Warto zaznaczyć, że źródła były szczegółowo weryfikowane, na podstawie doświadczeń z przeszłości zostali wytypowani najbardziej wiarygodni autorzy wpisów. W przypadku rozruchów w Bangkoku analitycy wykorzystywali relacje zaledwie 12–15 użytkowników Twittera. Analogiczny scenariusz powtarzał się również wielokrotnie podczas arabskiej wiosny. Zob. J. Przybylski, *Zaczytani agenci CIA*, „Rzeczpospolita" z 7 listopada 2011 [online], http://www.rp.pl/artykul/748071. html?print=tak&p=0 [dostęp: 5 VII 2014].

[13] H. Minas, *Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century?*, „RIEAS: Research Paper" 2010, nr 139, s. 33–34.

[14] M. Minkina, *Wywiad w państwie współczesnym*, Warszawa 2011, s. 195.

informacji utrudniającego wyodrębnienie wiadomości prawdziwych i istotnych. Wraz z rozwojem mediów zjawisko to sukcesywnie przybiera na sile, aby w dobie internetu stać się podstawnym problem, z którym borykają się wszyscy specjaliści zajmujący się białym wywiadem.

Ciągły i niezwykle dynamiczny postęp w dziedzinie automatycznego wyszukiwania i analizy treści nie jest w stanie przezwyciężyć problemu nadmiaru informacji. Mimo wielkich nadziei pokładanych w samouczących się inteligentnych algorytmach, umożliwiających kontekstowe tłumaczenie tekstu, wizja całkowicie „bezosobowego" wywiadu jawnoźródłowego wciąż wydaje się jedynie odległą pieśnią przyszłości[15]. Ponadto szybkość przyrostu danych znacznie przewyższa wzrost możliwości programów przeznaczonych do ich analizy. Dlatego też prawdopodobnie zjawisko określane jako szum informacyjny będzie z czasem narastać.

Innym problem wiążącym się z automatyzacją procesu wyszukiwania i analizy informacji jest trudność ich weryfikacji. Niełatwo zweryfikować datę umieszczenia informacji w sieci, co komplikuje sprawdzenie ich wiarygodności oraz rzutuje na aktualność i przydatność[16]. Informacje, które pojawiają się w internecie, są wielokrotnie kopiowane, zazwyczaj bez podania pierwotnego źródła. Stuprocentowa weryfikacja tego, gdzie i w jakiej formie pojawiły się one po raz pierwszy, jest więc niemożliwa. Zjawisko to przez analityków nazywane jest „efektem echa" (ang. *echo effect*)[17].

Ponadto warto zauważyć, że mimo wszechstronności i uniwersalności białego wywiadu, są obszary, gdzie okazuje się on zupełnie nieprzydatny. Przykładem może być tropienia przywódców najgroźniejszych grup terrorystycznych. Mimo że chętnie wykorzystują oni internet do celów propagandowych, to robią to na tyle profesjonalnie, aby nie pozostawić „cyfrowych odcisków stóp" (ang. *digital footprint*), a większość czasu przebywają w miejscach odciętych całkowicie nie tylko od sieci, lecz także bez jakichkolwiek ewentualnych świadków. W takich przypadkach jedynie osobowe źródła informacji pozwalają na zdobycie potrzebnej wiedzy. Przykładem takiego scenariusza było m.in. ustalenie miejsca pobytu Osamy bin Ladena ukrywającego się na pograniczu afgańsko-pakistańskim[18].

Inną trudnością jest bariera językowa. Problem ten towarzyszył białemu wywiadu od samego początku. Obecnie, kiedy monitoring internetowych serwisów społecznościowych odgrywa coraz większą rolę, a język angielski przestaje mieć uprzywilejowaną pozycję jako *lingua franca*, problem ten staje się coraz poważniejszy. Brak specjalistów biegle władających takimi językami, jak chiński, arabski, hindu, farsi czy pasztu, poważnie ogranicza efektywność zbierania i analizy informacji pochodzących z najbardziej zapalnych części globu, a dzięki internetowi dostępnych niemal na wyciągniecie ręki[19]. Niektórzy eksperci szacują, że od 50 do 80 proc. informacji będących w zainteresowaniu wywiadów państw zachodniej cywilizacji nie jest publikowanych

[15] M.M. Lowenthal, *Open Source Intelligence: New Myths, New Realities,* w: *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, R.Z. George, R.D. Kline (red.), Lanham 2006, 275–276.

[16] M. Minkina, *Wywiad w państwie…,* s. 195.

[17] *Open Source Intelligence (OSINT): Issues for Congress, CRS Report for Congress,* R.A. Best, A. Cumming, (red.), Congressional Research Service, 5 December 2007, p. CRS-9, http://www.fas.org/sgp/crs/intel/RL34270.pdf [dostęp: 17 VIII 2014].

[18] Ch. Pallaris, *Open Source Intelligence: A Strategic Enabler of National Security*, „*CSS* Analyses in *Security Policy",* Vol. 3, No. 32 (April 2008), s. 2.

[19] S.C. Mercado, Sailing the Sea of OSINT in the Information Age…

w języku angielskim[20]. Niewątpliwie fakt ten poważnie ogranicza rzeczywistą przydatność otwartych źródeł, nawet przy szerokim wykorzystaniu coraz doskonalszych elektronicznych translatorów.

Ostatnią, ale wcale nie mniej ważną wadą cechującą wywiad jawnoźródłowy, jest jego, stosunkowo duża, podatność na dezinformację. Manipulowanie przekazem medialnym i wpływanie na międzynarodową opinię publiczną to domena służb specjalnych tak stara, jak samo dziennikarstwo. Według V. Volkoffa, jednego z najbardziej znanych teoretyków wywiadu, dezinformacja to swego rodzaju sztuka wprowadzania w błąd określonych grup społecznych, mająca zawsze planowy i celowy charakter. Jest ona prowadzona w sposób systematyczny i fachowy za pomocą rozbudowanego instrumentarium, jej podstawowym narzędziem zaś są mass media. Dezinformacja oprócz podstępu, intoksykacji (wprowadzania w błąd – przyp. red.), wpływania oraz białej i czarnej propagandy jest podstawowym orężem prowadzenia wojny informacyjnej[21]. Implikuje to konieczność posiadania przez specjalistów zajmujących się białym wywiadem nie tylko dobrego warsztatu analitycznego, lecz także ogromnej wiedzy ogólnej i dużego dystansu do każdego z analizowanych źródeł. Doskonałą ilustracją tego problemu mogą być kłopoty, jakie z analizą silnie zideologizowanej prasy radzieckiej miał podczas zimnej wojny amerykański wywiad[22].

Wyzwania i nowe perspektywy

Niewątpliwie najbardziej przełomowym punktem w całej historii białego wywiadu była rewolucja w technologii informacyjnej oraz powstanie sieci Internet. Od tego właśnie momentu troskę o niedostatek informacji zastąpił problem ich nadmiaru. To właśnie z tą kwestią będą musieli poradzić sobie specjaliści od białego wywiadu. Obecnie problem ten wydaje się nierozwiązywalny, ciągły wzrost wydajności algorytmów wykorzystywanych do wyszukiwania i ilościowej analizy informacji daje jednak pewne podstawy do optymizmu.

Osoby zajmujące się białym wywiadem największe nadzieje pokładają w daleko idącej automatyzacji procesu wywiadu jawnoźródłowego na każdym jego etapie. Na poziomie strategicznym, według T. Serafina, można wyróżnić osiem etapów analizy. Są to: planowanie, standaryzacja, pozyskiwanie, indeksowanie, tłumaczenie, analiza, wirtualizacja oraz dystrybucja. Planowanie to nic innego jak określenie strategii i głównych kierunków działania oraz określenie zbioru źródeł. Przez standaryzację należy rozumieć określenie kryteriów dalszego wyszukiwania, digitalizację źródeł drukowanych oraz opracowanie wielojęzycznych zapytań. Samo pozyskiwanie informacji to z kolei wyszukiwanie i selekcja oraz ekstrakcja danych. Czwarty komponent, czyli indeksacja źródeł, to również tagowanie informacji i danych. Dalej następuje proces tłumaczenia i transkrypcji informacji, po którym dokonywana jest analiza i wnioskowanie, a następnie standaryzacja materiału wyjściowego i prezentacja wyników (wizualizacja). Ostatnim etapem całego procesu jest dystrybucja, czyli dostarczenie materiału do określonych podmiotów w ustalonej formie i określonym czasie. Każde z wyżej wymienionych

[20] M.M. Lowenthal, *Open Source Intelligence: New Myths, New Realities*, w: *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, R. Z. George, R. D. Kline (red.), Lanham 2006, s. 277.

[21] V. Volkoff, *Dezinformacja: Oręż wojny*, Warszawa 1991, s. 6–8.

[22] R.W. Pringle, *The Limits of OSINT: Diagnosing the Soviet Media*, 1985–1989, „International Journal of Intelligence and CounterIntelligence" 2007, nr 2, s. 240–257.

działań można usprawnić, stosując specjalistyczne oprogramowanie. Służy ono m.in. do tworzenia cyfrowych baz danych, rozpoznawania tekstu i mowy, biometrii, translacji, wyszukiwania, ekstrakcji, analizy powiązań, kryptografii czy skanowania i oceny wiarygodności witryn internetowych[23]. Wszystkie wymienione funkcjonalności można powiązać w jeden, kompletny analityczny system, dający możliwość daleko idącej automatyzacji całego procesu. Niewątpliwie jego wdrożenie w służbach i instytucjach wykorzystujących metodę białego wywiadu mogłoby znacznie zwiększyć zarówno wydajność, jak i wygodę pozyskiwania informacji z otwartych źródeł.

Warto zauważyć, że istnieje już rozbudowane oprogramowanie analityczne przydatne w wykorzystywaniu otwartych źródeł informacji. Niektóre programy komputerowe powstały specjalnie z myślą o służbach i instytucjach odpowiedzialnych za bezpieczeństwo[24]. Dają one możliwość zastosowania i łączenia m.in. analizy powiązań, analizy geograficznej, monitoringu, różnorodnych baz danych, raportów i dokumentów. W zamyśle twórców tego typu oprogramowań mają one z wyprzedzeniem identyfikować i alarmować użytkowników o nowych zagrożeniach, osobach podejrzanych i innych anomaliach. Programy te umożliwiają też legalne zbieranie informacji, analizę i zarządzanie nimi w czasie rzeczywistym, bez konieczności wcześniejszego badania ich zawartości metodami klasycznymi. Pozwala to, przynajmniej w teorii, na sprostanie wyzwaniom, takim jak olbrzymia ilość i różnorodność informacji z otwartych źródeł, konieczność analizy tzw. głębokiego internetu (ang. *deep weeb*)[25], a także tłumaczenia wielojęzyczności, gwar i żargonów. Obecnie wykorzystanie tego typu rozwiązań jest coraz poważniej rozważane m.in. przez polską policję. Zastosowanie tego rodzaju oprogramowań ma zapewniać wczesną identyfikację zagrożeń i działań o charakterze kryminalnym, które uprzednio mogły być przeoczone lub nieczytelne, oraz stworzy lepsze możliwości podejmowania działań proaktywnych (zamiast reagowania na skutki)[26].

Kolejnym wyzwaniem, przed jakim stoi obecnie biały wywiad, jest analiza „Big Data". Przez pojęcie „Big Data" należy rozumieć zbiory informacji o dużej objętości, dużej zmienności lub dużej różnorodności, które wymagają nowych form przetwarzania w celu wspomagania procesu podejmowania decyzji, odkrywania nowych zjawisk oraz optymalizacji tych procesów[27]. Takie zbiory charakteryzują się dużą ogólnością, dotyczą

[23] T. Serafin, *Automatyzacja procesu wywiadu jawnoźródłowego w ramach działalności wywiadowczej i walki z terroryzmem,* w: K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Analiza informacji w zarządzaniu bezpieczeństwem*, Warszawa 2013, s. 83.

[24] Przykładem może być program *Open Mind*, czyli produkt szwajcarskiej firmy 3i-MIND specjalizującej się w dziedzinie nowych rozwiązań w zakresie zarządzania ryzykiem dla organów ochrony porządku publicznego oraz agencji wywiadowczych. Zob. J. Gill, *OpenMIND – precyzyjne narzędzie pozyskiwania informacji wywiadowczych z otwartych źródeł,* „Ochrona Mienia i Informacji" 2012, nr 1, s. 65–66.

[25] Głęboki Internet (ang. *Deep Web*) – nazywany również ukrytym lub niewidzialnym Internetem, to potoczne określenie zasobów sieci Internet, które są bardzo słabo albo w ogóle nie są indeksowane przez wyszukiwarki internetowe. Są to przede wszystkim bazy danych o dynamicznie zmieniającej się zawartości (na którą wpływ mają bezpośredni ich użytkownicy), a także prywatne witryny (fora, serwisy aukcyjne itp.) o dynamicznej zawartości. Dostęp do części z nich można uzyskać wyłącznie po wcześniejszej rejestracji w bazie użytkowników bądź po wniesieniu określonych opłat. Aby połączyć się z tego typu stroną, należy znać jej dokładny adres. Zob. *Invisible or Deep Web: What it is, How to find it, and Its inherent ambiguity* [online], http://www.lib.berkeley.edu/ TeachingLib/Guides/Internet//InvisibleWeb.html [dostęp: 23 XI 2013].

[26] K. Radaniak, *Biały wywiad w policji – narzędzie rozpoznawania zagrożeń terrorystycznych*, „Studia prawnicze. Rozprawy i Materiały" 2012, nr 2 (11), s. 96.

[27] „Big Data" powszechnie definiuje się za pomocą 4V, czyli czterech charakterystycznych czynników opisujących te zbiory informacji. Są to: *Volume* (ilość danych), *Variety* (różnorodność analizowanych danych i informacji), *Velocity* (przetwarzanie w czasie rzeczywistym) i *Value* – czyli wartość, jaką możemy uzyskać

bowiem niezindywidualizowanych strumieni danych, takich jak długość odwiedzin na stronie internetowej czy też długość rozmowy telefonicznej, informacje na temat produktów zamówionych przez klienta w sklepie internetowym (dzięki pobraniu informacji z tzw. plików *cookies*) czy też ilość lajków na Facebooku. Są to więc informacje określane jako „metadane" (czyli dane opisujące inne dane). Choć są zazwyczaj powiązane z konkretnymi osobami, w zamyśle nie są gromadzone w celu ich identyfikacji. Mają natomiast umożliwić ustalanie korelacji oraz prawdopodobieństwa występowania pewnych zjawisk. Co ważne, wykrycie związku przyczynowo-skutkowego nie jest najważniejsze. Podstawowym celem jest ustalenie prawdopodobieństwa wystąpienia pewnego zjawiska w przyszłości na podstawie analizy wcześniejszych przypadków. Warto jednak zauważyć, że na próbę, na podstawie której tworzy się prognozę, składa się olbrzymia ilość danych. Jest to coś, do czego analitycy wcześniej nie mieli dostępu – możliwość badania niemal całej populacji, a nie tylko jej próbki (z natury obarczonej błędem doboru próby)[28]. Cechy te powodują, że analiza „Big Data" ma ogromny wpływ na szeroko pojęte bezpieczeństwo publiczne, gdyż daje spore możliwości, jeśli chodzi o lepsze przewidywanie i modelowanie zagrożeń, takich jak zorganizowana przestępczość czy terroryzm[29].

Prace nad wykorzystaniem analizy „Big Data" (szczególnie w obszarze serwisów społecznościach) są prowadzone m.in. przez brytyjskie służby specjalne. Dzięki informacjom uzyskanym podczas automatycznej analizy mają zostać stworzone podstawy systemu wczesnego ostrzegania przed niepokojami społecznymi za granicą. Podobne prace przy wsparciu naukowców prowadzi również Sztab Korpusu Sił Szybkiego Reagowania Dowództwa Sojuszniczych Sił Zbrojnych NATO (*NATO Allied Rapid Reaction Corps Headquarter*). Analiza „Big Data", oparta na systemie automatycznego wychwytywania zaburzeń wzorców zachowań społecznych, ma się stać jednym z komponentów wywiadu jawnoźródłowego Sojuszu. Docelowo ma to ułatwić wykrywanie wczesnych symptomów radykalizacji poglądów, zarówno w przypadku całych społeczności, jak i pojedynczych osób, a tym samym zwiększyć możliwości i zakres działania zespołów analitycznych[30]. (…)

Biały wywiad w służbie terroryzmu

Warto pamiętać, że metoda białego wywiadu jest stosowana nie tylko przez służby specjalne, policję, administrację publiczną czy analityków z sektora prywatnego, lecz także jest to podstawowe narzędzie wywiadowcze dla różnego rodzaju ugrupowań ekstremistycznych oraz terrorystów[31]. Szczególnie intensywnie wykorzystywanym przez nich otwartym źródłem informacji jest bez wątpienia internet. (…)

---

z połączenia wszystkich poprzednio wymienionych czynników. Zob. T. Słoniewski, *Od BI do „Big Data"*, w: *Nowa twarz Business Intelligence*, R. Jesionek (red.), s. 8. [online], http://it-manager.pl/wp-content/uploads/Nowa-twarz-BI1.pdf [29 VI 2014].

[28] B. Sajduk, *Big data – polityczne i militarne aspekty rewolucji technologii informatycznych* [online], http://www.nowapolitologia.pl/politologia/stosunki-miedzynarodowe/big-data-polityczne-i-militarne-aspekty-rewolucji-technologii-informatycznych [29 VI 2014].

[29] *Big data for public security,* s. 1 [online], http://www.sas.com/content/dam/SAS/en_us/doc/overviewbrochure/big-data-for-public-security-106812.pdf [29 VI 2014].

[30] N. Couch, B. Robins, *Big Data for Defence and Security*, s. 10–11 [online], https://www.rusi.org/downloads/assets/RUSI_BIGDATA_Report_2013.pdf [dostęp: 26 VIII 2014].

[31] Szerzej zob. B. Saramak, *„Biały wywiad" w służbie terroryzmu,* w: K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji,* Warszawa 2014, s. 182–196.

Jak już wspomniano, sieć Internet rozrasta się w oszałamiającym tempie, co roku zyskując miliony nowych użytkowników. Wśród nich znajdują się także współcześni terroryści, którzy wykorzystują cyberprzestrzeń jako narzędzie umożliwiające łatwe zbieranie informacji potrzebnych do planowania poszczególnych zamachów. Przed rewolucją informatyczną to państwo dysponujące rozbudowanym aparatem administracyjnym i wojskowym w dużej mierze reglamentowało dostęp do wiedzy. Książki, czasopisma czy nawet korespondencję można było cenzurować, a informacje dające przewagę – chronić. W dobie powszechnego dostępu do internetu ta przewaga gwałtownie topnieje. Oczywiście aparat państwowy nadal posiada monopol na przechowywanie oraz przetwarzanie najbardziej wrażliwych informacji o swoich obywatelach. Z kolei służby specjalne oraz policja mają wiele uprawnień umożliwiających w razie potrzeby szybkie i niepostrzeżone poszerzenie tego typu wiedzy. Niemniej jednak dysproporcja w dostępie do informacji nieustannie maleje, na czym korzystają przede wszystkim podmioty niepaństwowe, w tym również grupy terrorystyczne. Na szczególną penetrację narażone są współczesne państwa demokratyczne, w których występuje pełna transparentność życia publicznego. Z jeden strony pozwala to na sprawowanie przez ogół obywateli efektywnej kontroli społecznej nad aparatem władzy państwowej, z drugiej naraża ten aparat na łatwą i niekontrolowaną penetrację przez ugrupowania terrorystyczne. Wiele z pozoru nieistotnych danych znajdujących się na stronach internetowych urzędów państwowych, po wzbogaceniu ich o informacje z innych źródeł, daje wystarczający materiał do przygotowania precyzyjnie wymierzonego ataku terrorystycznego. Mimo wielu bardzo złożonych metod kontroli treści zawartych w internecie, ogromny problem nadal stanowią terroryści działający w pojedynkę, niemożliwi do namierzenia ze względu na brak jakichkolwiek podejrzanych powiązań, nazywani samotnymi wilkami (ang. *lone wolves*)[32]. Wykorzystują oni bardzo często internet jako źródło materiałów szkoleniowych oraz narzędzie do planowania zamachów, prawie w ogóle nie używając go w roli komunikatora. Łatwość używania internetu do planowania zamachów jest spowodowana wchłonięciem przez to medium wielu innych źródeł, pozwalając zminimalizować kontakt ze światem zewnętrznym, co ze względu na skrytość działalności terrorystycznej stanowi istotną zaletę. Przy zastosowaniu odpowiednich technik i narzędzi (np. klienta sieci TOR) możliwe jest stosunkowo bezpieczne i anonimowe korzystanie z zasobów sieci.(…)

Podsumowanie

Nie ulega wątpliwości, że wywiad jawnoźródłowy można uznać za jedną z podstawowych i w pełni samodzielnych dyscyplin wywiadowczych. Jest ona w chwili obecnej podstawą każdej nowoczesnej służby wywiadowczej, a udział informacji zdobytych metodami białego wywiadu ocenia się na ponad 80 proc. Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej jest więc ogromne i niepodważalne. Dzieje się to nawet pomimo daleko posuniętej kultury tajności panującej, co do zasady, we wszystkich służbach specjalnych. Zakres wykorzystania białego wywiadu w poszczególnych państwach jest bardzo różny i zależy przede wszystkich od systemu politycznego oraz tradycji w zakresie działań wywiadowczych. W państwach o długiej tradycji demokratycznej, w których fundamentem działania szeroko pojętej administracji publicznej jest

[32] M. Adamczuk, *Terroryzm indywidualny jako zagrożenie dla bezpieczeństwa europejskiego,* w: *Zamach w Norwegii Nowy wymiar zagrożenia terroryzmem w Europie*, K. Liedel, P. Piasecka, T. R. Aleksandrowicz (red.), Warszawa 2011, s. 44–46.

zasada transparentności, wykorzystywanie otwartych źródeł informacji zawsze było rzeczą normalną. Dużo wyraźniej dostrzegano tu również informacyjny, a nie tylko propagandowy, potencjał prasy, radia i telewizji. Z kolei w państwach, w których przez dłuższy czas funkcjonowały reżimy autorytarne lub totalitarne, zauważalne jest przywiązanie do znacznie szerszego wykorzystania metod pracy operacyjnej i mniejsze zaufanie do danych pochodzących z ogólnodostępnych źródeł. Było to spowodowane postrzeganiem zagranicznych mediów tylko i wyłącznie jako tuby propagandowej wroga, podającej informacje nieprawdziwe lub zmanipulowane. Wyjątkiem w tym dychotomicznym układzie wydają się Chiny, gdzie mimo reżimu komunistycznego, cały czas dostrzegano olbrzymi potencjał kryjący się w wykorzystaniu otwartych źródeł informacji, zwłaszcza w dziedzinie wywiadu naukowo-technicznego.

Wraz z rewolucją w dziedzinie technologii informacyjnych oraz upowszechnieniem się sieci Internet znacznie wzrósł także potencjał białego wywiadu. Do podstawowych jego zalet należy bez wątpienia zaliczyć szybkość pozyskiwania informacji, ich ilość, różnorodność, jakość i przejrzystość. Nie mniej istotna jest również łatwość, niewielkie koszty oraz znikome ryzyko związane z ich zdobywaniem. Z kolei do najpoważniejszych wad wywiadu jawnoźródłowego zaliczyć można spore trudności z przezwyciężeniem szumu informacyjnego, weryfikacją informacji pochodzących z nieautoryzowanych źródeł internetowych czy też dużą podatność na różnego typu dezinformację. Wyraźnym ograniczeniem jest również bariera językowa, która uniemożliwia analizę łatwych do zdobycia potencjalnie ważnych informacji. Pewnym ograniczeniem była również nieprzydatność informacji pochodzących z jawnych źródeł, na najniższym, taktycznym szczeblu, w trakcie realizacji antyterrorystycznych operacji specjalnych. Jak więc widać, mimo że większość informacji można uzyskać z otwartych źródeł, to często najcenniejsze z nich zdobyć można, jedynie stosując metody pracy operacyjnej.

Nie należy zapominać, że rozwój białego wywiadu stwarza również wiele wyzwań. Najpoważniejszym z nich wydaje się aktualnie problem szerokiego wykorzystania potencjału drzemiącego w omawianej metodzie przez organizacje terrorystyczne. Obecnie internet stał się podstawowym narzędziem do szybkiego i efektywnego zbierania informacji, planowania oraz koordynacji działań terrorystycznych. Metoda białego wywiadu zajmuje szczególne miejsce w rzemiośle każdego współczesnego terrorysty, dzięki zaś jej dobremu opanowaniu możliwe staje się częściowe zniwelowanie przewagi w dostępie do informacji, jakie do niedawna służby specjalne i policja miały nad ugrupowaniami ekstremistycznymi. Dlatego też zasadne wydaje się postawienie tezy, że wykorzystanie otwartych źródeł informacji (a szczególnie ich cyfrowej części) w działalności terrorystycznej będzie się nasilać w przyszłości. Co warto wziąć pod uwagę, jeśli chce się tej działalności skutecznie przeciwdziałać.

Pomimo wyżej wymienionych wad i ograniczeń, wykorzystanie otwartych źródeł informacji w działalności wywiadowczej stwarza niewątpliwie ogromy potencjał. Postępująca rewolucja informatyczna i powstawanie coraz to nowszych technologii wspierających zautomatyzowane wyszukiwanie oraz analizę informacji powoduje, że perspektywy wykorzystania otwartych źródeł informacji w działalności wywiadowczej są olbrzymie. W tym kontekście szczególnie duże nadzieje są pokładane w tzw. analizie „Big Data", umożliwiającej bardzo skuteczne prognozowanie trendów społecznych oraz wskazywanie potencjalnych zagrożeń. (…)