Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej:
historia, praktyka, perspektywy

Uniwersytet Warszawski
Wydział Dziennikarstwa i Nauk Politycznych

Bartosz Saramak

Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy

Warszawa 2015

Recenzja:
dr hab. Zbigniew Siemiątkowski (UW)

Redakcja językowa:
Alicja Siemianowska

Redaktor prowadzący:
Jarosław Szczepański

Projekt okładki:
Anna Koźbiel

ISBN: 978-83-63183-94-3

Arkuszy wydawniczych: 7,5

Wydawca:
Wydział Dziennikarstwa i Nauk Politycznych
Uniwersytet Warszawski
ul. Krakowskie Przedmieście 3
00–927 Warszawa
tel./fax 48 22 55 22 952
www.wydawnictwo.wdinp.uw.edu.pl

Druk i oprawa: Zakład Graficzny UW. Zam. 1026/2015

Spis treści

Table of Contents

Wstęp

Wywiad od zarania dziejów kojarzył się ze snuciem intryg, zdobywaniem tajnych współpracowników i wykradaniem sekretnych informacji. Świat szpiegów, zarówno tych działających na rzecz służb państwowych, jak i prywatnych korporacji, zawsze otoczony był silną aurą tajemniczości. W naturalny sposób objęła ona również sztukę pozyskiwania informacji, która nierozerwalnie łączona jest z różnymi formami ryzykownych i skomplikowanych, a co za tym idzie widowiskowych, metod pracy operacyjnej. Zakładanie podsłuchów, skryta obserwacja, niepostrzeżone przechwytywanie korespondencji czy trudne werbunki to obraz pracy wywiadowczej najmocniej utrwalony w kinie czy literaturze szpiegowskiej. W rzeczywistości jednak sztuka zdobywania informacji wygląda dużo prozaiczniej: staranna lektura prasy, branżowych czasopism, fachowej literatury, wnikliwa analiza radiowych doniesień czy publicznych wystąpień. Właśnie tak postrzegać należy wywiadowcze rzemiosło, które już od ponad wieku opiera się przede wszystkim na wyszukiwaniu i analizie jawnych i ogólnie dostępnych informacji, w sposób niezrównany budujących kontekst ważnych aktualnie kwestii. Mimo iż biały wywiad, jak zwykło się nazywać tę właśnie metodę pracy wywiadowczej, nie jest zbyt spektakularnym obszarem działalności wywiadowczej, to jednak dzięki niemu, w sposób mniej lub bardziej świadomy, pozyskiwana jest lwia część materiałów będąca punktem wyjścia do dalszych analiz, decyzji i działań. Nie ulega wątpliwości, że problem wykorzystania otwartych źródeł informacji w działalności wywiadowczej stanowi zagadnienie dosyć istotne, zarówno z punktu widzenia instytucji i służb odpowiedzialnych za bezpieczeństwo państwa, jak i korporacji oraz firm prywatnych działających w tym obszarze. Warto również zauważyć, że na niebagatelny wzrost jego znaczenia wpłynęła bardzo dynamicznie postępująca rewolucja w dziedzinie technologii informacyjnych, w szczególności powstanie i rozwój internetu. Najlepszym tego dowodem jest zauważalny wzrost zainteresowania naukowców problematyką, szeroko rozumianego, wykorzystania otwartych

źródeł informacji. Uznać to należy za ważny symptom, gdyż tematyka ta jest stosunkowo skomplikowana, a zapotrzebowanie na rzeczowe, naukowe analizy ogromne. Na szczęście, z roku na rok liczba tego typu opracowań, do których zalicza się, m.in. również poniższa praca, rośnie.

Na podjęcie szerszej analizy problemu wykorzystania otwartych źródeł informacji w działalności wywiadowczej wpłynęło kilka czynników. Jednym z najważniejszych z nich był brak kompleksowego opracowania tej kwestii w polskiej literaturze. Dostępne publikacje ograniczają się zazwyczaj do bardzo fragmentarycznego ujęcia problemu. Brakuje natomiast analizy zestawiającej ze sobą rozmaite sposoby i filozofie wykorzystania metody białego wywiadu w poszczególnych obszarach działalności wywiadowczej. W efekcie specyfika i wyjątkowy charakter białego wywiadu wymyka się świadomości przeciętnego czytelnika. Inną przesłanką do podjęcia badań na omawiany temat była chęć dokładnego poznania i zaprezentowania specyfiki wykorzystania otwartych źródeł w różnych instytucjach i środowiskach. Brak kompleksowych analiz porównawczych w polskiej literaturze przedmiotu wydaje się bowiem poważną przeszkodą w dyskusji nad kierunkami oraz zakresem wykorzystania metody białego wywiadu w instytucjach państwowych, a także możliwości szerszej współpracy w tym względzie w najbliższej przyszłości. Poniższa praca jest więc próbą, chociaż częściowego, uzupełnienia tej luki badawczej. Niemniej ważnym powodem pochylenia się nad problemem jest, jak już zauważono wcześniej, jego waga. Trudno wyobrazić sobie, aby jakikolwiek podmiot specjalizujący się w pozyskiwaniu informacji mógł w dzisiejszych czasach pozwolić sobie na zignorowanie potencjału kryjącego się w wykorzystaniu otwartych źródeł informacji. W dobie internetu i nieustanie postępującej cyfryzacji stały się one wręcz fundamentem działalności wywiadowczej, nie tylko podmiotów prywatnych, ale również służb i instytucji państwowych. Fakt ten potwierdza status samodzielnej dyscypliny wywiadowczej, jaki biały wywiad uzyskał już wiele lat temu w zachodnich służbach specjalnych.

Podstawowym celem poniższej monografii jest więc przedstawienie specyfiki wykorzystania otwartych źródeł informacji w działalności wywiadowczej przy jednoczesnym ukazaniu zarówno ich zalet i potencjału, jak i ograniczeń oraz wad. Ponadto ambicją autora było dokonanie przeglądu najważniejszych z nich oraz zaprezentowanie wybranych, najbardziej newralgicznych obszarów, w których metoda białego wywiadu może być w sposób najpełniejszy użyta. Hipotezę badawczą pracy stanowi założenie, że w wyniku postępującej rewolucji w dziedzinie technologii informacyjnych rola i skala wykorzystania otwartych źródeł informacji systematycznie wzrasta. W celu falsyfikacji owej hipotezy należy zadać szereg, bardziej szczegółowych pytań badawczych. Po pierwsze – niezbędne wydaje się zde-

finiowanie pojęć takich, jak „otwarte źródła informacji" i „„biały wywiad" oraz nakreślenie specyfiki jego wykorzystania. Po drugie – konieczne wydaje się wskazanie ram białego wywiadu, rozumianego jako odrębna i samodzielna dyscyplina wywiadowcza, przy jednoczesnym pochyleniu się nad jego potencjałem, ograniczeniami oraz rysującymi się w przyszłości perspektywami i wyzwaniami. Po trzecie – nieodzowne jest prześledzenie ewolucji, jaką na przestrzeni lat przeszła metoda białego wywiadu, zarówno na świecie jak i Polsce. Po czwarte – nakreślić należy typologię, według której podzielić można współczesne, otwarte źródła informacji. Po piąte – trzeba postawić pytanie, jakie miejsce wśród nich zajmuje internet i jak rysują się perspektywy jego użycia w celach wywiadowczych. Po szóste – zapytać należy, w jakich obszarach – zarówno w sektorze publicznym, jak i prywatnym – wykorzystanie metody białego wywiadu wydaje się najbardziej celowe i pożądane. Po siódme wreszcie – bezwzględnie pochylić się trzeba nad zagrożeniami, jakie powoduje wdrożenie omawianej metody w procesie planowania i przygotowywania zamachów terrorystycznych.

W monografii wykorzystanych zostało kilka metod badawczych, zarówno pierwszego jak i drugiego rzędu. W trakcie badań nad problemem genezy oraz ewolucji białego wywiadu, użyta została przede wszystkim metoda historyczna polegająca na poszukiwaniu i badaniu genezy zjawisk, które przyczyniły się do wytworzenia metodyki pozyskiwania informacji ze źródeł jawnych, opisywanej w dalszej części pracy. To właśnie dzięki niej możliwe było odnalezienie wielu związków przyczynowo-skutkowych między zdarzeniami z przeszłości a sytuacją teraźniejszą. Nie mniej pomocne, zwłaszcza w dalszym stadium badań, okazały się także inne metody. Pierwszą z nich jest metoda analizy instytucjonalno-prawnej polegająca na studiowaniu aktów normatywnych tworzonych przez instytucje państwowe, określające ramy jawności i dostępności informacji oraz regulujące funkcjonowanie służb i organów administracji publicznej wykorzystujących metodę białego wywiadu. Niemałe znaczenie dla odpowiedzi na postawione pytania badawcze miały również metody porównawcza oraz systemowa, które zastosowane razem, dały możliwość wskazania podobieństw oraz różnic między zachodzącymi procesami, instytucjami i systemami. Pozwoliły one na zestawienie rozwiązań stosowanych w sektorze publicznym oraz prywatnym, a także porównanie rozwiązań organizacyjnych funkcjonujących w Polsce i w wybranych państwach. Z kolei metodą drugiego rzędu, umożliwiającą ostateczne usystematyzowanie wniosków, wskazanie trendów, a także ocenę wybranych służb i instytucji wykorzystujących otwarte źródła informacji, była metoda problemowa.

Ze względu na ogromną liczbę otwartych źródeł informacji konieczne okazało się zawężenie analizy do kilku najbardziej przydatnych lub

najciekawszych z nich. Podobny problem zaistniał w przypadku doboru podmiotów wykorzystujących metodę białego wywiadu. Ich wybór dokonany został w sposób maksymalnie przekrojowy i umożliwiający pokazanie uniwersalności oraz interdyscyplinarności omawianej metody. Dlatego też poniższa monografia ma przede wszystkim przeglądowy i porządkujący charakter. Tak więc, mimo iż w celu zilustrowania procesu pozyskiwania informacji ze źródeł otwartych, przedstawionych zostało wiele szczegółowych technik i narzędzi, to poniższego opracowania nie należy traktować jako podręcznika do nauki zasad wywiadu jawnoźródłowego, a jedynie swego rodzaju wprowadzenie ułatwiające zrozumienie jego specyfiki.

Rozdział pierwszy poniższej monografii ma trzy zadania. Po pierwsze – zawiera pewną siatkę pojęciową, niezbędną do dalszych rozważań. To właśnie w nim zostało wyjaśnione pojęcie oraz specyfika otwartych źródeł informacji oraz białego wywiadu. Po drugie – charakteryzuje biały wywiad jako odrębną i samodzielną dyscyplinę wywiadowczą. Po trzecie – przedstawia zalety i potencjał oraz wady i ograniczenia, które nierozerwalnie wiążą się z wykorzystaniem otwartych źródeł informacji w działalności wywiadowczej, jednocześnie nakreślając nowe wyzwania i perspektywy ich użycia. Drugi rozdział koncentruje się na przedstawieniu historii białego wywiadu, prezentując szereg czynników determinujących jego powstanie oraz wpływających na jego ewolucję. W tej części pracy ukazana została niezwykle bogata i różnorodna tradycja wykorzystywania otwartych źródeł informacji, zarówno przez państwowe służby specjalne, jak i podmioty prywatne. Szczególną uwagę poświęcono zarysowaniu historii rozwoju białego wywiadu w Polsce, począwszy od II Rzeczpospolitej, przez okres Polski Ludowej, a kończąc na czasach współczesnych. Rozdział trzeci stanowi natomiast analizę poszczególnych źródeł informacji. Scharakteryzowane zostały zarówno źródła tradycyjne, takie jak prasa, szara literatura, radio i telewizja oraz ogólnie dostępne rejestry i dokumenty, jak i te bardziej współczesne – geoinformacja oraz internet. W szczególności to ostatnie źródło, czy ściślej mówiąc metaźródło informacji, zostało poddane wnikliwej analizie, ukazującej jego wręcz niewyobrażalny potencjał wywiadowczy. W ostatnim, czwartym rozdziale, przedstawione zostały wybrane obszary wykorzystania otwartych źródeł informacji. W sektorze prywatnym – działalność wywiadowni gospodarczych, międzynarodowych korporacji świadczących usługi wywiadu strategicznego czy w końcu niezależnych infobrokerów. W sektorze publicznym – działalność służb specjalnych, policji oraz wybranych struktur administracji rządowej. Zamknięcie analizy stanowi natomiast charakterystyka roli, jaką metoda białego wywiadu odgrywa w działalności terrorystycznej.

Oceniając obecny stan badań nad metodą białego wywiadu, należy wyraźnie stwierdzić, że zdecydowanie brakuje na tym polu polskojęzycznych

monografii, ujmujących temat w sposób przekrojowy i pełny. Pewnymi wyjątkami są: publikacja Krzysztofa Liedela i Tomasza Serafina[1] oraz praca zbiorowa pod redakcją Wojciecha Filipkowskiego i Wiesława Mądrzejowskiego, która zawiera dwanaście opracowań dotyczących omawianej problematyki[2]. Ponadto wyróżnić można kilka niezwykle wartościowych artykułów autorów takich jak Krzysztof Radwaniak[3], Piotr Niemczyk[4] czy też Błażej Stromczyński i Paweł Waszkiewicz[5]. Zupełnie inaczej sytuacja prezentuje się w przypadku anglojęzycznej literatury przedmiotu. Liczba wyjątkowo dobrej jakości monografii oraz różnego rodzaju obszernych opracowań jest tak duża, że nie sposób dokonać jej wyczerpującego przeglądu. Oprócz licznych anglojęzycznych publikacji monograficznych oraz artykułów naukowych, niezwykle pomocne w pisaniu niniejszej pracy okazały się również podręczniki i poradniki tworzone na wewnętrzne potrzeby Sojuszu Północnoatlantyckiego oraz armii Stanów Zjednoczonych. Podkreślić należy również fakt dużej dostępności źródeł obcojęzycznych w internecie, co niewątpliwie znacząco ułatwiło stworzenie poniższego opracowania.

---

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

[2] *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki,* W. Filipowski, W. Mądrzejowski (red.), Warszawa 2012.

[3] K. Radwaniak, P.J. Wrzosek, *Biały wywiad w Policji – pozyskiwanie i analiza informacji ze źródeł otwartych* [w:] J. Konieczny (red.), *Analiza informacji w służbach policyjnych i specjalnych*, Warszawa 2012; K. Radwaniak *Biały wywiad w policji – narzędzie rozpoznawania zagrożeń terrorystycznych*, „Studia prawnicze. Rozprawy i Materiały" 2012, nr 2 (11).

[4] P. Niemczyk, *BAI*, „Przegląd Bezpieczeństwa Wewnętrznego" Wydanie Specjalne, 6 kwietnia 2010; P. Niemczyk, *Wywiadownie gospodarcze jako źródło informacji „białego wywiadu"*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9 (5).

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

Rozdział I

Pojęcie i charakterystyka białego wywiadu

1. Pojęcie otwartych źródeł informacji i białego wywiadu

Pozornie zdefiniowanie pojęć takich, jak „biały wywiad" czy „otwarte źródła informacji", nie powinno stanowić problemu. Zwłaszcza to pierwsze wyrażenie jest znane i długo już używane – zarówno w żargonie polskich służb specjalnych, jak i literaturze ich dotyczącej. Ogólnie rzecz ujmując, „biały wywiad" to działalność polegająca na zdobywaniu informacji ze źródeł jawnych i ogólnie dostępnych. O ile owa metoda była i jest powszechnie znana i wykorzystywana na całym świecie, o tyle samo pojęcie „białego wywiadu" jest czysto polskim pomysłem. Za granicą (przede wszystkim na Zachodzie) zwykło się raczej używać amerykańskiego akronimu OSINT (od ang. *Open Source INTelligence*), którego rozwinięcie można przetłumaczyć jako „wywiad ze źródeł otwartych" lub też „wywiad jawnoźródłowy". Należy jednak pamiętać, iż akronim ten jest znacznie młodszy niż polskie pojęcie „białego wywiadu". Wcześniej w literaturze anglojęzycznej używano raczej określenia „wywiad jawny" (ang. *overt intelligence*). Według Allena Dullesa, legendarnego szefa amerykańskiego wywiadu w okresie zimnej wojny, „w wywiadzie zagranicznym pozyskiwanie informacji przebiega na różne sposoby, nie wszystkie z nich są jednak tajemnicze czy sekretne. Jest to szczególnie prawdziwe w odniesieniu do wywiadu jawnego, w którym informacje pochodzą z gazet, książek, naukowych i technicznych czasopism, oficjalnych sprawozdań z obrad rządu czy z radia i telewizji. Nawet powieść lub przedstawienie może zawierać przydatne informacje o stanie społeczeństwa [tłum. własne – B.S.][6]".

Większość badaczy słusznie stawia znak równości między szeroko rozumianym wywiadem ze źródeł otwartych (czyli OSINT-em) a „białym wywiadem".

---

[6] A.W. Dulles, *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World*, Washington 2006, s. 49.

Według J. Lareckiego jest to metoda pracy wywiadowczej, polegająca na studiowaniu i analizie zagranicznych materiałów publikowanych oficjalnie lub ogólnie dostępnych. Należą do nich głównie prasa codzienna i periodyczna (polityczna, techniczna, biznesowa), dokumentacja i sprawozdania z działalności i zamierzeń rządów (oświadczenia premiera i ministrów), partii rządzących i opozycyjnych, specjalistycznych kongresów oraz prac parlamentarnych (np. wystąpień i interpelacji posłów, stenogramów z prac komisji sejmowych), ponadto wnioski patentowe, audycje radiowe i telewizyjne, internet, otwarte bazy danych, geoinformacja i wiele innych ogólnodostępnych źródeł. Ta forma wywiadu zwana jest również wywiadem bezagenturalnym, publicznym, jawnym, pasywnym bądź monitoringiem jawnych źródeł informacji[7].

1.1. Odcienie wywiadu

Nie jest to jednak podejście jedyne. Analizując anglojęzyczną siatkę pojęciową dotyczącą omawianego zagadnienia, można stwierdzić, że polski „biały wywiad" i amerykański OSINT to pojęcia bardzo zbliżone, ale jednak nietożsame. W żargonie polskich służb specjalnych wywiad „biały" to przeciwieństwo, jak się łatwo domyślić, „czarnego wywiadu" – a więc twardego wywiadu operacyjnego – który informacje zdobywa niejawnie, wykorzystując przy tym środki takie, jak agentura, podsłuchy, kontrola korespondencji, przechwytywanie sygnałów radiowych itp.[8] Pojęcia „czarny wywiad" używa się również w odniesieniu do najbardziej utajonej sfery działań wywiadowczych, czyli skrytego pozyskiwania chronionych informacji[9]. Wyróżnikiem „białego wywiadu" wydaje się więc brak konieczności naruszania czyjejś prywatności czy łamania prawa chroniącego poufne bądź tajne informacje. Właśnie w tym duchu metoda ta definiowana jest w środowisku polskich służb specjalnych. Według B. Sienkiewicza bowiem, głównym celem komórek odpowiedzialnych za „biały wywiad" jest „zajmowanie się legalnym zdobywaniem informacji z przestrzeni publicznej i przetwarzaniem ich w sposób dający pionom operacyjnym możliwość reakcji w sytuacjach tego

---

[7] J. Larecki, *Wielki leksykon służb specjalnych świata: organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny*, Warszawa 2007, s. 749-750.

[8] T.A. Aleksandrowicz, *Biały wywiad w walce z terroryzmem* [w:] K. Liedel, P. Piasecka (red.), *Rola mediów w przeciwdziałanie terroryzmowi,* Warszawa 2009, s. 81.

[9] K. Radwaniak, P.J. Wrzosek, *Biały wywiad w Policji – pozyskiwanie i analiza informacji ze źródeł otwartych* [w:] J. Konieczny (red.), *Analiza informacji w służbach policyjnych i specjalnych*, Warszawa 2012, s. 113.

wymagających[10]". Praktyka wywiadowcza pokazuje jednak, że między „czystą bielą" a „czystą czernią" występuje bardzo szerokie spektrum szarości.

W kontekście „legalności" podejmowanych działań kluczowym czynnikiem jest podmiot, który zbieraniem informacji się zajmuje, oraz zakres uprawnień mu przysługujących. Granica między środkami postrzeganymi jako operacyjne a całą resztą instrumentarium wywiadowczego jest bowiem stosunkowo płynna. Warto zauważyć, że szczególnie w polskich warunkach, gdzie tzw. czynności operacyjno-rozpoznawcze nie są zdefiniowane w sposób uniwersalny i każda ze służb stosuje je na podstawie odrębnych przepisów, wyznaczenie granic wspomnianego wcześniej „czarnego wywiadu" nie jest możliwe.

Sprawę dodatkowo komplikuje kwestia prowadzenia działań wywiadowczych przez podmioty prywatne, nieposiadające uprawnień takich jak służby państwowe. Powstaje więc pytanie, czy wszystkie działania zmierzające do uzyskania informacji, które zgodnie z prawem są podejmowane przez podmioty niepaństwowe, można uznać za „biały wywiad". Nie do końca. Byłoby to niewątpliwe sporym nadużyciem, gdyż w dużym stopniu metody stosowane przez wywiadownie gospodarcze czy firmy detektywistyczne wykraczają poza pozyskiwanie i analizę materiałów jawnych i ogólnie dostępnych[11].

To właśnie obszar tzw. „szarego wywiadu". Pojęcie to, używane raczej w języku potocznym, dotyczy głównie sektora prywatnego, którego pracownicy nie są państwowymi funkcjonariuszami i nie dysponują szerokimi uprawnieniami śledczymi. W tym kontekście „szary wywiad" można rozumieć jako pewną grupę metod pracy operacyjnej (patrząc z perspektywy organów państwowych), których wykorzystanie jest zgodne z obowiązującym prawem (a więc podjąć je może każda osoba prywatna), ale wymaga dodatkowych środków (czy to finansowych, czy też ludzkich). Wymienić tu można wywiad środowiskowy (co oznacza, że osoba zbierająca informacje korzysta z pomocy osób trzecich), analizę kryminalistyczną (badanie odcisków palców, testy DNA, informatyka śledcza) czy obserwację osób i miejsc. Zastrzec trzeba jednak, że perspektywa ta dotyczy przede wszystkim firm detektywistycznych i metodyki przez nie stosowanej[12]. Wyżej opisane działania są oczywiście często podejmowane przez służby specjalne i policyjne. W tym wypadku definiowane są jednak po prostu jako czynności

---

[10] B. Sienkiewicz, *Historia pewnego złudzenia*, „Przegląd Bezpieczeństwa Wewnętrznego" Wydanie Specjalne, 6 kwietnia 2010, s. 52.

[11] Szerzej zob.: E. Jawers, *Agent, handlarz, prawnik, szpieg: Tajemniczy świat korporacyjnego szpiegostwa*, Kraków 2010.

[12] *Techniki wywiadowcze - biały, czarny i szary wywiad* [w:] http://www.detektyw.edu.pl/techniki-wywiadowcze-bialy-czarny-i-szary-wywiad [dostęp: 11 lipca 2014].

operacyjno-rozpoznawcze, a nie „szary wywiad". W przypadku wywiadowni gospodarczych, często sięgających po te metody, możliwe jest zdobycie wielu niezbędnych danych, takich jak np. informacje o niejawnych powiązaniach kapitałowych i personalnych pomiędzy przedsiębiorstwami, składnikach majątku niepodlegających ujawnieniu w dokumentach urzędowych czy o rzeczywistej polityce działania i osobach faktycznie podejmujących decyzje[13]. W polskiej literaturze tego typu wiedza definiowana jest jako tzw. „szare informacje" (czyli takie, które pochodzą z tzw. źródeł półotwartych). Są to informacje, których nie można zdobyć w sposób bezpośredni, lecz drogą okrężną poprzez sieć kontaktów nieformalnych[14]. W tym kontekście można uznać, że traktowany łącznie obszar „białego" i „szarego" wywiadu to ta część pracy wywiadowczej, którą wykonać można, nie posiadając żadnych specjalnych uprawnień, zastrzeżonych dla funkcjonariuszy służb państwowych.

Jak więc widać, granice białego wywiadu trudno uznać za ostre. Tezę tę potwierdzają dodatkowo inne niejasności związane z analizą omawianej metody w kategoriach „legalności". Nie zawsze bowiem przepisy prawa w sposób jasny i oczywisty definiują, co uznać można za informację ogólnodostępną, a co za treści prywatne i zastrzeżone. Ponadto sprawę dodatkowo komplikuje fakt, że regulacje dotyczące tej materii bardzo różnią się w poszczególnych krajach, co w dobie internetu i cyfrowej eksterytorialności ma niemałe znaczenie. Dobrą tego ilustracją są ciągłe kontrowersje związane z wykorzystywaniem dokumentów poufnych – ujawnionych i upublicznionych na stronach internetowych, takich jak np. WikiLeaks.org. Ponadto warto również zauważyć, że służby państwowe odpowiedzialne za bezpieczeństwo korzystają z różnego rodzaju publikacji i materiałów objętych prawem autorskim na specjalnych, innych niż ogólne, warunkach. W Polsce kwestia ta regulowana jest przez ustawę o prawie autorskim i prawach pokrewnych[15]. Fakt ten powoduje, że służby specjalne i policyjne przetwarzają owe informacje na innych zasadach niż podmioty niepubliczne wykorzystujące metodę białego wywiadu. Nie dziwi więc fakt, iż wielu badaczy uznaje tę dyscyplinę wywiadowczą za swoistą „szarą strefę" (ang. *grey zone*), wskazując jednocześnie, iż samo tylko kryterium legalności nie do końca jest w stanie zarysować wyraźną granicę, za którą kończy się biały wywiad[16].

---

[13] K. Turaliński, *Wywiad gospodarczy i polityczny. Metodyka, taktyka i źródła pozyskiwania informacji*, Radom 2011, s. 28.

[14] M. Kwięciński, *Wywiad gospodarczy w zarządzaniu przedsiębiorstwem*, Warszawa-Kraków 1999, s. 57.

[15] Ustawa z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych* (Dz.U. 1994 nr 24 poz. 83), art. 33^2.

[16] G. Hribar, I. Podbregar, T. Ivanuša, *OSINT: A "Grey Zone"?,* "International Journal of Intelligence and CounterIntelligence" 2014, vol. 27, issue 3, s. 542-544.

Nie mniejszy problem stanowi również precyzyjne i jednoznaczne zdefiniowanie „dostępności", „otwartości czy „jawności" informacji. Zarówno dostępność, otwartość, jak i jawność są pojęciami na tyle nieostrymi, że wyznaczenie ich jasnej granicy tylko z pozoru wydaje się proste. Każda informacja ma swoje źródło – otwarte bądź zamknięte. Otwarte tzn. dostępne dla nieorganicznej, bliżej nieokreślonej grupy osób, z którego korzystać można w pełni legalnie. Źródło zamknięte natomiast charakteryzuje się ograniczonym dostępem i brakiem możliwości dowolnego i nieskrępowanego wykorzystania. W oparciu o charakter informacji (rozumianej jako proste stwierdzenie faktu bądź opis jakiegoś zjawiska[17]) instytucje państwowe czy firmy prywatne wypracowują własne metody ich pozyskiwania, gromadzenia, przetwarzania, analizy i formułowania konkretnych wniosków. Tak więc analizując informacje, np. pod kątem ich znaczenia dla bezpieczeństwa i ładu publicznego, można przyjąć, że te pochodzące z miejsca publicznego są pochodzenia otwartego. Czy taką informacją można jednak dowolnie dysponować? Nie, gdyż osoby przebywające w miejscu publicznym korzystają z prawnej ochrony własnego wizerunku. Monitoring wizyjny umożliwia co prawda utrwalenie obrazu z miejsc publicznych i użycie jego zapisu do dalszej analizy, ale tylko i wyłącznie przez osoby do tego uprawnione (np. funkcjonariuszy policji czy służb specjalnych). Nie ma więc mowy o powszechnej dostępności do takiego zapisu czy jego publikacji. Dlatego też nie można tego typu źródła określić jako otwartego[18].

1.2. Open Source Intelligence, czyli amerykański OSINT

Ogromny wkład w rozwój wywiadu ze źródeł jawnych miały amerykańskie służby specjalne. Nic więc dziwnego, że to właśnie Amerykanie stworzyli najpełniejszą siatkę pojęciową dotyczącą tego zagadnienia, która swoje odzwierciedlenie znalazła w licznych publikacjach Sojuszu Północnoatlantyckiego. Mowa tu o trzech rozbudowanych podręcznikach („NATO Open Source Intelligence Handbook" z 2001 roku oraz „NATO Open Source Intelligence Reader" i „NATO Intelligence Exploitation of the Internet" z 2002 roku[19]). Ponadto jako istotne ich uzupełnienie traktować należy instrukcję amerykań-

[17] T.R. Aleksandrowicz, *Analiza informacji w administracji i biznesie*, Warszawa 1999, s. 25.

[18] K. Radwaniak, P.J. Wrzosek, *Biały wywiad w Policji…*, s. 121.

[19] Szerzej zob.: *NATO Open Source Intelligence Handbook,* Norfolk November 2001 oraz *NATO Open Source Intelligence Reader,* Brussels February 2002 [w:] http://www.oss.net [dostęp: 17 sierpnia 2014], a także: *NATO Intelligence Exploitation of the Internet*, Brussels October 2002 [w:] http://www2.gwu.edu [dostęp: 17 sierpnia 2014].

skiego Departamentu Armii z 2005 roku pt. „Open Source Intelligence”[20]. Opracowania te stały się podstawą do stworzenia własnych metod i technik pozyskiwania informacji ze źródeł otwartych w większości wojskowych służb specjalnych krajów należących do sojuszu. Ponadto za ich pośrednictwem do opracowań naukowych dotyczących omawianej tematyki (zarówno w Polsce, jak i za granicą), trafiło wiele pojęć i skrótów związanych z wywiadem jawnoźródłowym oraz analizą informacji.

Bazowym pojęciem przytoczonym w tym opracowaniu są dane jawne (ang. *open source data* – OSD), czyli surowe, nieopracowane dane pochodzące z drukowanych, radiowych lub telewizyjnych nośników informacji. Może być to więc zdjęcie, zapis elektroniczny, mapa satelitarna czy prywatny list. Za nieco bardziej złożone uznano informacje pochodzące ze źródeł jawnych (ang. *open source information* – OSINF), ale obejmujące dane, które zostały już zgrupowane i wstępnie przygotowywane przez poddanie ich pewnym zabiegom edytorskim (są to np. książki, artykuły i publikacje prasowe czy raporty). Dzięki temu, że dane zawarte w tych informacjach zostały poddane już filtrowaniu i wartościowaniu przez autora, możliwa jest ich prezentacja decydentowi[21].

Najistotniejsze pojęcie, czyli wywiad ze źródeł otwartych, czy też – według niektórych tłumaczeń – wywiad jawnoźródłowy[22] (ang. *open source intelligence* – OSINT), a więc odpowiednik polskiego pojęcia „biały wywiad”, zostało zdefiniowane jako zaplanowane poszukiwanie, selekcjonowanie, wnioskowanie i dystrybucja informacji do określonej grupy odbiorczej (np. sztabu lub innych decydentów), zgodnie ze zgłoszonym wcześniej, ściśle określonym zapotrzebowaniem (ang. *request for information* – RFI). Z założenia w wywiadzie jawnoźródłowym stosuje się zweryfikowane metody pracy wywiadowczej, co pozwala na wytworzenie tzw. jawnoźródłowego materiału wywiadowczego. Metodyka ta nie jest jednak odgórnie i sztywno narzucona. Nawet wspominane wcześniej opracowania NATO są pod tym względem raczej zbiorem luźnych zaleceń, budującym nie tyle same procedury, ile ich wspólne ramy. Metodykę postępowania z danymi i informacjami ze źródeł jawnych każda służba policyjna czy wywiadowcza wypracowuje we własnym zakresie i na bazie własnych doświadczeń. Z kolei wywiad jawnoźródłowy rozumiany jako wynik prac wywiadowczych to opracowanie analityczne

[20] Obecnie obowiązuje uaktualniona wersja z czerwca 2012 roku, zob.: *Open Source Intelligence,* ATP 2-22.9, Headquarters, Department of the Army, Washington 2012 [w:] http://deep-web.org/wp-content/uploads/2012/09/atp2-22-9.pdf [dostęp: 17 sierpnia 2014].

[21] *NATO Open Source Intelligence Handbook…,* s. 2.

[22] Pojęcie to zostało zaproponowane w pierwszej polskiej monografii poświęconej otwartym źródłom informacji. Szerzej zob.: K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011.

(czy też produkt analityczny), zawierające konkretne wnioski, wynikające z analizy wyłącznie danych i informacji ze źródeł otwartych[23].

Zweryfikowany wywiad jawnoźródłowy (ang. *validated open source intelligence* – OSINT-V) jest natomiast określany jako informacja, która w bardzo wysokim stopniu uzyskała potwierdzenie w wyniku weryfikacji polegającej na użyciu innych metod pracy wywiadowczej (także objętych tajemnicą, np. wykorzystaniu agentury) przez funkcjonariuszy posiadających dostęp do informacji niejawnych; ewentualnie jeśli informacja ta pochodzi ze źródła, którego autentyczność i wiarygodność jest oczywista (np. relacje telewizyjne lub radiowe na żywo)[24]. OSINT-V może więc powstać jako produkt analityczny uwzględniający informacje niejawne (a więc już nie jawnoźródłowe) lub jako produkt analityczny wyłącznie na bazie informacji ze źródeł otwartych (ale uzyskanych wieloma kanałami). Wskazywane są powiązania między danymi i informacjami, prowadzona jest ich wspólna, krzyżowa analiza, zaś wnioski z nich płynące są syntezowane.

W tym miejscu warto podkreślić różnicę dostrzeganą przez niektórych polskich badaczy między klasycznie rozumianym polskim pojęciem białego wywiadu a definicjami amerykańskimi. W polskich służbach istnieje wieloletnia praktyka, aby informacje pochodzące ze źródeł jawnych weryfikować i łączyć już na wstępnym etapie analizy z informacjami objętymi tajemnicą (zdobytymi np. drogą operacyjną). W takim przypadku ostateczny produkt analizy nie może być wykorzystany w sposób otwarty i staje się informacją niejawną. W tym kontekście pojęcie białego wywiadu, którym posługują się polskie służby, jest zdecydowanie bardziej odpowiednikiem akronimu OSINT-V (a nie OSINT, który jako produkt może być dystrybuowany bez żadnych ograniczeń)[25].

Definicje natowskie kładą więc nacisk na ścisłe sprofilowanie informacji pod kątem otrzymanego wcześniej zapotrzebowania oraz odpowiednią ich weryfikację. W tym miejscu warto przytoczyć również nieco inną definicję wywiadu jawnoźródłowego, zawartą w jednym z opracowań Departamentu Armii Stanów Zjednoczonych. Rozumiany on jest jako pozyskiwanie informacji (publicznie dostępnych, o które każdy może legalnie poprosić, kupić je lub zdobyć w wyniku obserwacji) o dużym znaczeniu, systematycznie gromadzonych w bazach danych, przetwarzanych i analizowanych. Opracowany materiał stanowi zaś odpowiedź na zapytanie wywiadowcze o określonych wymaganiach. Jako źródło otwarte zdefiniowano osobę lub inny podmiot

---

[23] *NATO Open Source Intelligence Handbook…,* s. 2.

[24] Ibidem, s. 3.

[25] K. Radwaniak, P.J. Wrzosek, *Biały wywiad w Policji….,* s. 116-118.

dostarczający informacji nieobjętych ochroną prywatności lub niechronionej przed upublicznieniem. Za informacje ogólnodostępne (publiczne) uznane zostały dane, fakty albo materiały opublikowane, wyemitowane publicznie lub otrzymane po wystosowaniu zapytania do osoby publicznej lub urzędu, a także legalnie zebrane w wyniku obserwacji na spotkaniu otwartym dla społeczeństwa[26].

1.3. Wywiad jawnoźródłowy w ujęciu polskim

Podsumowując zebrane powyżej zagraniczne przykłady definiowania zjawiska, można stwierdzić, że wywiad ze źródeł jawnych stanowi wyodrębnioną dyscyplinę pracy wywiadowczej. Jego cechą szczególną jest zaś odmienna od pozostałych specyfika źródeł informacji (otwartość, dostępność, jawność), które, co ważne, są zbierane, selekcjonowane i dystrybułowane zgodnie z założeniami określonymi wcześniej przez składający zapytanie podmiot (decydenta). Z czasem zaprezentowane powyżej amerykańskie podejście (a co za tym idzie również wypracowane wraz z nim pojęcia, skróty i terminy) zaczęło przenikać również do polskich opracowań, dotyczących służb specjalnych oraz analizy informacji. W zasadzie można przyjąć, że określenia takie jak „wywiad jawnoźródłowy" (dosłowne tłumaczenie amerykańskiego zwrotu *Open Source Intelligence*), czy po prostu samodzielnie używany akronim OSINT, zaczęły stopniowo wypierać polskie sformułowanie „biały wywiad"[27]. W tym kontekście warto przytoczyć recepcję wyżej wymienionej terminologii w najnowszej polskiej literaturze przedmiotu.

Podstawowym pojęciem, również w polskim piśmiennictwie, są „dane jawnoźródłowe", które przyjęło się rozumieć jako określone, istotne parametry przedstawione w najprostszej formie, pochodzące z pierwotnych lub wtórnych źródeł informacji, nieobjętych klauzulą poufności, a które jako takie nie pozwalają jednak na wnioskowanie. Można je podzielić na „dane wymierne" oraz „dane opisowe". Pierwsze z nich prezentują określoną wartość lub nazywają obiekty, miejsca, osoby czy zjawiska. Natomiast „dane opisowe" przedstawiają jakość danych wymiernych, ich cechy i własności, a także czynności bezpośrednio związane z aktywnością podmiotów wyrażonych przez te dane. Z kolei „informację jawnoźródłową" definiuje

[26] *Open Source Intelligence,* Headquarters, Department of the Army, US Army Field Manual Interim FMI 2-22.9, Washington 2006, s. 2-1 [w:] http://www.fas.org/irp/doddir/army/atp2-22-9.pdf [dostęp: 28 lipca 2014].

[27] 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:] L.K. Paprzycki, Z. Rau (red.), *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu,* Warszawa 2009, s. 279.

się w polskiej literaturze przedmiotu jako ciąg danych, które pochodzą z jednego bądź większej liczby źródeł jawnych, a który to ciąg podlega procesowi oceny z uwzględnieniem ich zawartości oraz czasu publikacji. Informacja jawnoźródłowa stanowi jeden z elementów tzw. materiału wywiadowczego. Jej wykorzystanie zależy jednak od wyniku weryfikacji jej wartości, czyli określenia jakości oraz poziomu wiarygodności. Ewaluacja wartości informacji pochodzącej ze źródeł jawnych wygląda identycznie jak ocena informacji pozyskanych innymi metodami. Wartość informacji jest uwarunkowana faktem, czy mówi ona o miejscu i czasie zdarzenia, podmiotach, przyczynach i skutkach, a także czy opisuje przebieg wydarzeń, zachowanie oraz cechy charakterystyczne obiektów i osób. Innymi słowy, im pełniejsza jest informacja, im więcej komponentów zawiera, tym lepiej[28].

Natomiast „źródło otwarte" rozumiane jest jako podmiot lub przedmiot, który posiada specyficzne walory umożliwiające generowanie informacji w postaci pozwalającej na ich legalne (ale także etyczne) utrwalanie, przetwarzanie, przesyłanie oraz gromadzenie. Źródła informacji dzielą się na pierwotne i wtórne. Często zdarza się, że informacja ze źródła pierwotnego posiada ograniczenia dotyczące jej rozpowszechniania – jest poufna lub prywatna (źródło nie jest więc otwarte). Jednak gdy pozyskuje się ją za pośrednictwem źródła wtórnego (już ogólnodostępnego – np. prasowej relacji), dostępność informacji nie stanowi już problemu. Podobna sytuacja ma miejsce w przypadku dziennikarzy, którzy w terenie mają bezpośredni kontakt z osobami obserwującymi lub uczestniczącymi w jakichś wydarzeniach. Ich przekaz może różnić się od ostatecznej wersji, zmienionej w redakcji i opublikowanej. W tym wypadku źródłem wtórnym będzie konkretne medium zatrudniające dziennikarzy, które może wpływać na kształt lub też kontekst informacji docierających do odbiorcy. Podział źródeł na pierwotne i wtórne ważny jest również w kontekście ewaluacji informacji. W wyniku zainteresowania tematem innych mediów (a więc potencjalnych źródeł) przekaz może zostać wzbogacony o zdobyte niezależnie informacje, zaś wiarygodność doniesień dodatkowo zweryfikowana. Źródła pierwotne są dużo wartościowsze z punktu widzenia analizy, jednak zazwyczaj dotarcie do nich jest trudniejsze (a czasem wręcz niemożliwe), niż ma to miejsce w przypadku źródeł wtórnych. Droga do tych drugich jest znacznie łatwiejsza, ale czasami (zwłaszcza kiedy występują w nadmiarze) potrafią one znacząco skomplikować pracę analityczną, tworząc tzw. szum informacyjny. Dzieje się tak, gdyż tylko pozornie przyrost liczby informacji ułatwia właściwe rozpoznanie problemu. W praktyce jednak niezbędne jest wykorzystanie modelu selekcji (ekstrakcji) informacji, który pozwala nie tylko

[28] K. Liedel, T. Serafin, *Otwarte źródła informacji…,* s. 51.

na wyodrębnienie poszukiwanych słów i zwrotów, ale również odrzucenie danych powtarzających się[29].

Odwołując się do polskiej literatury przedmiotu, można stwierdzić, że wywiad jawnoźródłowy stanowi jedną z dyscyplin wywiadowczych, polegającą na zaplanowanym (w niektórych przypadkach tematycznym i incydentalnym) pozyskiwaniu informacji ze źródeł otwartych, ich selekcjonowaniu, zestawianiu, digitalizacji, tłumaczeniu i transkrypcji, analizowaniu, zestawianiu i wnioskowaniu na ich podstawie oraz gromadzeniu i dystrybucji do wcześniej ustalonej grupy odbiorców w określonej uprzednio zwizualizowanej formie. Głównym celem wywiadu jawnoźródłowego jest dostarczenie informacji lub bezpośrednio danych wykorzystywanych podczas tworzenia analiz wywiadowczych, przewidywania zagrożeń i prognozowania rozwoju sytuacji operacyjnej. Poprzez zastosowanie sprawdzonych metod pracy wywiadowczej możliwe jest opracowanie materiału, który ułatwia poszukiwanie relacji zachodzących pomiędzy informacjami dotyczącymi ludzi i zdarzeń pozostających w zainteresowaniu służb. Jest to więc bardzo istotna forma uzupełniania innych dyscyplin wywiadowczych. Efekty działalności tego rodzaju, po usystematyzowaniu, zmniejszają zapotrzebowanie na informacje niejawne, zdobyte w wyniku działań operacyjnych, co wydatnie zmniejsza koszty oraz ryzyko pozyskania określonej wiedzy. Dzięki uwzględnieniu kontekstu politycznego, społecznego, ekonomicznego i militarnego możliwa jest głębsza analiza, a groźba wyciągnięcia błędnych wniosków i wysnucia mylnej diagnozy znacząco spada[30].

2. Biały wywiad jako dyscyplina wywiadowcza

Bez wahania można postawić tezę, iż biały wywiad już dawno stał się autonomiczną i niezależną dyscypliną wywiadowczą, zarówno w obszarze wywiadu, jak i rozpoznania wojskowego. Fakt ten potwierdza większość typologii podziału dyscyplin wywiadowczych ze względu na źródło pochodzenia informacji. Odwołując się do metodologii Sojuszu Północnoatlantyckiego, w przypadku rozpoznania wojskowego, wyróżnić można: rozpoznanie z ogólnodostępnych źródeł (ang. *Open Source Intelligence* – OSINT), rozpoznanie osobowe (ang. *Human Intelligence* – HUMINT), rozpoznanie akustyczne (ang. *Acoustic Intelligence* – ACINT), rozpoznanie obrazowe (ang. *Imagery Intelligence* – IMINT), rozpoznanie pomiarowo-badawcze (ang. *Measurement and Signature Intelligence* – MASINT), rozpoznanie

[29] Ibidem, s. 52.
[30] Ibidem, s. 54-55.

radiotechniczne (ang. *Radar Intelligence* – RADINT) i rozpoznanie radioelektroniczne (ang. *Signal Intelligence* – SIGINT). To ostatnie dodatkowo dzieli się na rozpoznanie radiowe (ang. *Communication Intelligence* – COMINT) oraz na rozpoznanie radiolokacyjne (ang. *Electronic Intelligence* – ELINT). Podział ten jest stosowany przez wszystkie państwa członkowskie NATO[31]. Warto podkreślić, iż w przypadku gdy obiektem rozpoznania jest państwo wysoko rozwinięte, uznaje się, że nawet do 95 proc. informacji może pochodzić ze źródeł ogólnodostępnych[32].

Zaprezentowana powyżej typologia natowska to nieco bardziej uszczegółowiona wersja klasycznego amerykańskiego podziału całokształtu działalności wywiadowczej na pięć obszarów. I tak obok wywiadu jawnoźródłowego (OSINT) wymienić można wywiad agenturalny (HUMINT), wywiad z kanałów łączności (SIGINT), wywiad ze środków obrazowych (IMINT) oraz wywiad środkami pomiarów i identyfikacji (MASINT). Ostatnie trzy dyscypliny określa się niekiedy mianem wywiadu technicznego (TECHINT). Każdy z tych obszarów (co widać w podziale zastosowanym przez Sojusz Północnoatlantycki) można z kolei podzielić na szereg podgrup, zależnie od użytych środków łączności, pomiaru i identyfikacji[33]. Z podobnym podziałem spotkać się można również w polskiej literaturze przedmiotu[34].

Wartość i rola wykorzystania otwartych źródeł informacji bywa oceniana różnie. Większość zachodnich ekspertów zajmujących się omawianą tematyką określa udział informacji pochodzących z wywiadu jawnoźródłowego na ponad 80 proc. całości materiału wywiadowczego zdobytego za pomocą wszystkich dyscyplin wywiadowczych. Wartość ta nie jest stała i zależy od bardzo wielu czynników, takich jak otwartość społeczeństwa, zakres tematyczny poszukiwanych informacji czy poziom, na którym są zbierane. Należy przyznać, że współcześnie informacje pochodzące ze źródeł otwartych zazwyczaj stanowią lwią część końcowego raportu wywiadowczego, na jaki zostało zgłoszone zapotrzebowanie, w niektórych wypadkach stanowiąc aż 95 proc. całości materiału[35].

Warto również zauważyć, że podział między poszczególnymi dyscyplinami nie jest ostry. Tyczy się to przede wszystkim obszaru określanego

---

[31] *Rozpoznanie wojskowe,* SGWP 1531/2001 (jawne), Warszawa 2001, s. 12.

[32] R. Jagiełło, *Wybrane aspekty wojskowego rozpoznania osobowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9 (5), s. 236.

[33] R.M. Clark, *Perspectives on Intelligence Collection,* "The Intelligencer: Journal of U.S. Intelligence Studies", vol. 20, no. 2 (Fall/Winter 2013), s. 47-48.

[34] M. Minkina, *Wywiad w państwie współczesnym*, Warszawa 2011, s. 181.

[35] S.D. Gibson, *Exploring the Role and Value of Open Source Intelligence* [w:] *Open Source Intelligence in Twenty-First Century*, Ch. Hobbes, D. Sailsbury (eds.), New York 2014, s. 9-11.

mianem OSINT. Poniższa analiza poszczególnych otwartych źródeł informacji pokaże bowiem, że w wielu przypadkach wyraźnie nakładają się one na obszary wszystkich pozostałych dyscyplin wywiadowczych. Dzieje się tak, gdyż wywiad jawnoźródłowy to dyscyplina niezwykle synkretyczna, dająca możliwość korzystania zarówno ze źródeł osobowych (np. poprzez analizę ekspercką), obrazowych (np. poprzez wykorzystanie ogólnie dostępnych zdjęć i map), jawnych raportów pomiarowych (np. pochodzących z morskich systemów automatycznej identyfikacji) jak i w końcu z olbrzymiej ilości danych elektronicznych pochodzących z ogólnie dostępnych kanałów łączności (np. z internetu). Obszary, które jeszcze kilka lat temu wydawały się zamknięte i zarezerwowane dla służb specjalnych i wojska, dziś w dużej mierze stały się szeroko dostępne[36].

Ponadto warto podkreślić, że obecnie całościowa analiza danych, pozyskanych ze wszystkich możliwych źródeł (ang. *all-source intelligence*) jest najważniejszym zadaniem nowoczesnego wywiadu[37]. W tym kontekście biały wywiad zawsze daje początek oraz tworzy ramy każdej „mozaiki wywiadowczej" wypełnianej później informacjami zdobytymi innymi sposobami[38]. Powoduje to, że granica między białym wywiadem a pozostałymi dyscyplinami wywiadowczymi zaciera się jeszcze bardziej.

Starając się scharakteryzować wywiad jawnoźródłowy jako jedną z dyscyplin wywiadowczych, nie należy zapominać jednak, iż rzemiosło zdobywania i analizowania informacji można pojmować również w nieco szerszym wymiarze. Wywiad jako taki (a więc nie tylko ten określany mianem „białego") może być definiowany na wielu różnych płaszczyznach. Po pierwsze, co zostało już zasygnalizowane wcześniej, jako pewien zbiór metod pozwalających na zdobywanie informacji. Po drugie, jako instytucja (np. rodzaj tajnej służby), której głównym zadaniem jest zdobywanie oraz analiza informacji żywotnie ważnych z punktu widzenia państwa (bądź firmy, korporacji czy innej organizacji pozarządowej). Po trzecie, jako swego rodzaju sztuka, której celem jest poznanie zamiarów przeciwnika, jego sposobu myślenia, przewidzenie reakcji obcych podmiotów na prowadzoną przez nas politykę czy też nawet próba pokierowania tą reakcją[39].

Jeśli przeanalizujemy pojęcie białego wywiadu na płaszczyźnie sztuki, okaże się, że można podchodzić do niego, wyznając co najmniej kilka,

---

[36] A.N. Liaropolus, *A (R)evolution in Intelligence Affairs? In Search of a New Paradigm,* "RIEAS: Research Paper", No. 100, (June 2006), s. 15.

[37] M. Herman, *Potęga wywiadu,* Warszawa 2002, s. 94.

[38] *NATO Open Source Intelligence Reader,* Brussels 2002, s. 10.

[39] Z. Siemiątkowski, *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009, s. 32.

niekiedy sprzecznych filozofii. Zależą one od wielu czynników. Najistotniejsze z nich to ustrój danego państwa, podejście do wykorzystywania nowych technologii (w szczególności tych informatycznych) czy też kształt i relacje pomiędzy poszczególnymi służbami specjalnymi oraz innymi organami administracji państwowej (jeśli mówimy o wykorzystaniu wywiadu jawnoźródłowego w sektorze publicznym).

Do wywiadu rozumianego jako sztuka pozyskiwania informacji można podchodzić na co najmniej kilka sposobów, co uwarunkowane jest odmienną filozofią, jaka wykształciła się w różnych systemach politycznych. O ile bowiem w państwach demokratycznych otwarte źródła informacji zawsze były w mniejszym lub w większym stopniu wykorzystywane przez służby specjalne oraz policję, o tyle w reżimach totalitarnych oraz autorytarnych traktowano je z dużą rezerwą. U podstaw tej różnicy leży podejście do problemu zachowania tajemnicy państwowej oraz towarzysząca mu głęboko zakorzeniona „kultura tajności". W państwach totalitarnych owa kultura przeobrażała się niekiedy wręcz w swoistą „manię tajności". Powodowało to, że każda informacja, mająca chociażby minimalny wpływ na bezpieczeństwo państwa niemal automatycznie zyskiwała status niejawnej. Takie podejście w oczywisty sposób wpływa na sposób wartościowania przez urzędników i funkcjonariuszy państwowych poszczególnych źródeł informacji. Te pochodzące ze źródeł jawnych i ogólnie dostępnych w naturalny sposób były uznawane za materiał niezbyt wartościowy i mniej pewny. Znaczniej bardziej cenione są informacje zdobyte drogą operacyjną, a więc płynące od agentury, z podsłuchów i obserwacji. Takie podejście potęguje przekonanie, że z ogólnie dostępnych źródeł pochodzić może jedynie wroga dezinformacja (media postrzegano przede wszystkim jako źródło propagandy, a nie potencjalnie użytecznych informacji). Natomiast prawdziwie wartościowe i przydatne dane pozyskiwane mogą być jedynie z „pierwszej ręki". Problem ten nie ominął również polskich służb specjalnych, w których jeszcze długi czas po transformacji ustrojowej w 1989 roku panował swoisty „kult pracy operacyjnej", zaś do informacji dostarczanych przez piony analityczne, korzystające z metod białego wywiadu, podchodzono z bardzo dużą nieufnością[40].

Ten ostatni problem bynajmniej nie dotyka tylko i wyłącznie służb wywiadowczych państw totalitarnych i autorytarnych. Również w państwach demokratycznych występują ostre spory pomiędzy pionami analitycznymi i operacyjnymi. Jest bowiem oczywiste, że informacje zdobyte drogą operacyjną częstokroć bywają okupione poświęceniem znacznie większej ilości sił i środków (co wiąże się ze specyfiką pracy w terenie, w szczególności za

[40] I. Janke, *Tajni potrzebują ciszy*, „Życie", 21 grudnia 1996 [w:] http://j59.tripod.com/zycie.html [dostęp: 19 czerwca 2014].

granicą). Mniejsze koszty pozyskania informacji ze źródeł ogólnodostępnych nie oznaczają jednak, że praca analityczna należy do łatwych i niewymagających. Praktyka pokazuje, że jest zupełnie odwrotnie – osoby zajmujące się nią muszą cechować się dużą inteligencją, pilnością i dokładnością oraz, co równie ważne, przejawiać zacięcie bliższe pracownikom naukowym niż oficerom operacyjnym. Mimo że działalność ta rzadko ukazywana jest przez autorów powieści i filmów sensacyjnych, to właśnie ona decyduje o istocie i wartości wywiadu[41].

Niemniej jednak we współczesnych państwach demokratycznych, gdzie istnieje szeroki dostęp do informacji publicznej, świadomość ogromnych możliwości, jakie niesie ze sobą zastosowanie metody białego wywiadu, jest na zupełnie innym poziomie. Dzieje się tak, gdyż transparentność to jedna z podstawowych zasad demokracji – naród bowiem, jako suweren, posiada niezbywalne prawo do kontroli rządu i całej administracji. Państwa demokratyczne mają więc w naturalny sposób mniej sekretów niż reżimy autorytarne czy totalitarne[42]. Nie oznacza to jednak, że nie mają ich wcale, zwłaszcza kiedy pod uwagę bierze się przede wszystkim służby wywiadowcze i aparat bezpieczeństwa państwa. Wszystkie instytucje z tego sektora niejako ze swej natury oparte są na swego rodzaju „kulturze tajności". Nie jest to nic dziwnego, zważywszy na liczne obwarowania prawne dotyczące pracy z informacjami niejawnymi – zarówno w Polsce, jak i za granicą. Problemem jest natomiast fakt, iż czasem nawet w państwach demokratycznych dochodzi do swoistego paraliżu, polegającego na daleko posuniętej nieufności wobec innych służb oraz organów administracji, która znacząco utrudnia efektywną i szybką wymianę oraz dystrybucję informacji. Jako najbardziej jaskrawy przykład takiego stanu można przytoczyć sytuację panującą w amerykańskim systemie bezpieczeństwa narodowego na krótko przed wydarzeniami z 11 września 2001 roku. Niechęć do dzielenia się owocami pracy wywiadowczej i mało efektywny system dystrybucji poufnych informacji doprowadził do spektakularnej klęski. Wielu amerykańskich badaczy uważa, że obok konieczności zmiany kultury organizacyjnej, jednym ze skuteczniejszych środków zaradczych może okazać się szersze wykorzystanie otwartych źródeł informacji[43]. Szybkość i łatwość pozyskania informacji oraz brak ograniczeń w ich dystrybucji wydaje się w tym kontekście niezwykle przekonywającym argumentem.

---

[41] Z. Siemiątkowski, *Wywiad a władza…,* s. 35.

[42] R. Godson, *Dirty Tricks or Trump Cards. U.S. Covert Action & Counterintelligence*, New Jersey 2008, s. 118.

[43] H. Bean, *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence*, Santa Barbara–Denver–Oxford 2011, s. 15-16.

Można więc zaryzykować tezę, że podejście do zagadnienia białego wywiadu determinuje dwie filozofie całokształtu sposobu pozyskiwania informacji w służbach specjalnych i policyjnych. Pierwsza z nich, dominująca głównie w państwach niedemokratycznych (zwłaszcza w XX wieku) głosi, że w pierwszej kolejności korzystać należy z metod operacyjnych (czyli tzw. czarnego wywiadu), gdyż – po pierwsze – są one najpewniejsze, a po drugie – można je bez większych konsekwencji stosować w sposób nieograniczony (co daje służbom i instytucjom państwowym zdecydowaną przewagę). Druga filozofia, przyjmowana co do zasady we współczesnych państwach demokratycznych, zakłada, że wykorzystanie metod operacyjnych (a co za tym idzie ingerencja w prawa i wolności obywatelskie) to ostateczność, skutkująca dodatkowymi działaniami kontrolnymi ze strony organów sądowych i prokuratorskich. W pierwszej kolejności sięgać należy bowiem do metodyki wypracowanej w ramach wywiadu jawnoźródłowego, a dopiero gdy to konieczne – uciekać się do zastosowania specjalnych uprawnień, dających służbom państwowym możliwość władczego wkroczenia w życie obywateli. Bez wątpienia ta druga filozofia obecnie dominuje w świecie demokratycznym, czego skutkiem jest wzrost zainteresowania efektywnie prowadzonym białym wywiadem[44].

Owa dychotomia charakterystyczna była zwłaszcza dla okresu zimnowojennego. Współcześnie znaczenie otwartych źródeł informacji wzrosło również ze względu na związek, który zachodzi pomiędzy mediami a terroryzmem. Obecnie praktycznie każda walka w warunkach konfliktu asymetrycznego zmusza słabszą stronę do nagłaśniania działań zarówno własnych, jak i przeciwnika. Zainteresowanie społeczności międzynarodowej nawet regionalnymi problemami nadaje im wymiar globalny, a upublicznienie na szeroką skalę prowadzonej walki ogniskuje wokół stron zainteresowanie i tym samym generuje poparcie[45]. W oczywisty sposób powoduje to ogromny wzrost ilości informacji ważnych z punktu widzenia wywiadu we wszystkich mediach. Analiza informacji pochodzących z otwartych źródeł stała się niezwykle ważnym elementem współczesnych strategii antyterrorystycznych, ale także okazała się bardzo przydatna przy zdobywaniu informacji o wszelkich podmiotach niepaństwowych. Dlatego też biały wywiad staje się dziś jednym z najdynamiczniej rozwijanych narzędzi w rękach służb specjalnych[46].

---

[44] S. Gibson, *Open Source Intelligence: An Intelligence Lifeline*, „RUSI" 2004, no. 1 (149), s. 16-21.

[45] J. Tomasiewicz, *Środki komunikacji w strategii oporu niekierowanego* [w:] K. Liedel, S. Mocek (red.), *Terroryzm w medialnym obrazie świata*, Warszawa 2010, s. 100.

[46] 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. 91.

Najwięksi entuzjaści wykorzystania otwartych źródeł informacji w działalności wywiadowczej uczynili z białego wywiadu wręcz swego rodzaju radykalną filozofię. Najlepszym tego przykładem mogą być liczne publikacje amerykańskiego znawcy problematyki wywiadu jawnoźródłowego R.D. Steele, który postuluje nie tylko całkowite zerwanie z kulturą tajności panującą w służbach, ale również nakreśla wizję obywatelskiego wywiadu opartego właśnie na otwartych źródłach informacji. Efektem tych zmian miałaby być głęboka przemiana społeczno-polityczna oraz budowa nowoczesnego społeczeństwa informacyjnego[47]. Warto zauważyć, że podobna koncepcja upowszechnienia wiedzy z zakresu pozyskiwania i analizy informacji ze źródeł jawnych pojawiła się również na gruncie włoskim[48].

Nie należy zapominać również o krajach Dalekiego Wschodu, gdzie podejście do zdobywania informacji zawsze znacząco różniło się od paradygmatu dominującego w świecie zachodnim. W szczególności warte uwagi jest podejście chińskie, w którym biały wywiad niejednokrotnie odgrywał decydującą rolę. Ze względu na fakt, iż system zdobywania informacji (w szczególności tych o charakterze naukowo-technicznym) ze źródeł otwartych był nieustannie rozwijany w Chinach już od połowy lat '50-tych, obecnie ta dyscyplina wywiadowcza uważana jest za najważniejszą. Zdaniem niektórych amerykańskich teoretyków wywiadu, Chińczycy posiadają najlepiej przygotowanych i wyszkolonych profesjonalistów z zakresu wywiadu jawnoźródłowego na świecie[49].

3. Potencjał i ograniczenia białego wywiadu

Każda z wymienionych wcześniej dyscyplin wywiadowczych ma swoje charakterystyczne cechy, potencjał oraz ograniczenia. Podobnie jest również z białym wywiadem, określonym przez bardzo wyraźną specyfikę. Niewątpliwie jedną z istotniejszych cech białego wywiadu jest konieczność uwzględniania szerokiego tła problemu i budowania odpowiedniego kontekstu do dalszej analizy danych. Informacje dostarczane przez środki masowego przekazu zapewniają ogólną wiedzę, która, co ważne, podana jest w przystępnej i odpowiednio zsyntezowanej formie. Pozwala to na bardzo szybkie i sprawne zapoznanie się z kontekstem społecznym, kulturowym,

---

[47] Szerzej zob.: R.D. Steele, *The Open-Source Everything Manifesto: Transparency, Truth, and Trust*, Berkeley 2012.

[48] A. Politi, *The Citizen as "Intelligence Minuteman",* "International Journal of Intelligence and CounterIntelligence" 2003, vol. 16, no. 1, s. 34-38.

[49] W.C. Hannas, J. Mulvenon, A.B. Puglisi, *Chinese industrial espionage: Technology acquisition and military modernization*, London-New York 2013, s. 44.

historycznym czy religijnym zaistniałej sytuacji, co z kolei znacząco podnosi szansę na uzyskanie prawidłowej i pełniejszej odpowiedzi w czasie dalszych działań wywiadowczych, prowadzonych innymi środkami. Odnosi się to w szczególności do kwestii formułowania zapytań kierowanych do pionów operacyjnych. Dzięki wstępnej analizie informacji ze źródeł otwartych możliwe jest bowiem dużo pełniejsze i dokładniejsze sprecyzowanie ich zakresu i charakteru. Niejednokrotnie zdarza się również, że informacje zawarte w źródłach otwartych okazują się na tyle szczegółowe i pewne, że uciekanie się do innych, kosztowniejszych metod ich uzyskania w ogóle nie jest potrzebne. Biały wywiad pozwala także weryfikować informacje zebrane wcześniej za pomocą innych dyscyplin, co niewątpliwie w sposób korzystny wpływa na jakość ostatecznego materiału wywiadowczego[50]. To ostatnie częstokrotnie pozwala na wyłapanie błędów aparatu zbierającego, a czasem nawet na obnażenie jego niekompetencji czy też wykrycie świadomej lub nieświadomej (podsuniętej przez obce wywiady) manipulacji i dezinformacji[51]. W tym właśnie kontekście można przeanalizować podstawowe zalety oraz ograniczenia białego wywiadu.

3.1. Potencjał i zalety

Zalety wykorzystania otwartych źródeł informacji w działalności wywiadowczej zostały już wcześniej częściowo nakreślone, ale aby w pełni zrozumieć potencjał, jaki się za nimi kryje, warto przeanalizować je głębiej. Jeden z najbardziej znanych amerykańskich specjalistów zajmujących się omawianą tematyką S.C. Mercado stwierdził, iż podstawowymi zaletami, czy wręcz przewagami, jakie wywiad jawnoźródłowy ma nad pozostałymi dyscyplinami wywiadowczymi, są szybkość pozyskiwania informacji, ich ilość, różnorodność, jakość i przejrzystość oraz łatwość i niewielkie koszty ich analizy[52].

Szybkość, z jaką można sięgnąć po informacje ze źródeł otwartych, jest rzeczywiście oszałamiająca. Głównym powodem takiego stanu rzeczy jest przede wszystkim rewolucja w zakresie technologii informacyjnych oraz powstanie i upowszechnienie się internetu. Komputer, podstawowe oprogramowanie i szerokopasmowe łącze internetowe to narzędzia, które

[50] *Open Source Intelligence, Headquarters*, Department of the Army, US Army Field Manual Interim FMI 2-22.9, Washington 2006, s. 2-2 [w:] http://www.fas.org/irp/doddir/army/atp2-22-9.pdf [dostęp: 28 lipca 2014].

[51] Z. Siemiątkowski, *Wywiad a władza…*, s. 35.

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

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 ukazywać się właściwie natychmiast po ich wytworzeniu. 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 formalnych ograniczeń[53]. Dlatego też często najważniejsze decyzje w państwie podejmowane są nie na podstawie raportów wywiadowczych, ale informacji przekazywanych przez media (fenomen ten nazwany został „efektem CNN-u"). Nie ma jednak sensu, 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 analiz długoterminowych[54].

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 więc 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 efektami swojej pracy, a czasem nawet do udzielania szybkiej pomocy w postaci konsultacji czy przeprowadzenia zleconej analizy. Dzięki informacjom zawartym w źródłach otwartych dotarcie do tych ludzi nie stanowi współcześnie żadnego problemu. Ponadto wielość i różnorodność komercyjnych baz danych i repozytoriów sprzyja wzajemnej konkurencji, a co za tym idzie dbałości o jakość i wiarygodność oferowanych danych[55].

Wydaje się, że to właśnie owa jakość informacji jest zaletą najczęściej poddawaną krytyce, choć istnieje wystarczająca liczba źródeł sprawdzonych i wielokrotnie zweryfikowanych (takich jak np. największe agencje prasowe,

---

[53] K. Leetaru, *The Scope of FBIS and BBC Open-Source Media Coverage, 1979–2008 (U)*, "Studies in Intelligence" vol. 54, no. 1 (March 2010), s. 18.

[54] Z. Siemiątkowski, *Wywiad a władza…*, s. 38-39.

[55] H. Minas, *Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century?,* "RIEAS: Research Paper", No. 139, (January 2010), s. 32-33.

koncerny medialne, uniwersytety czy wreszcie komercyjne bazy danych), aby bez narażania się na nadmierne ryzyko oprzeć się na informacjach z nich pochodzących. Warto równocześnie podkreślić, że dociekliwość dobrych dziennikarzy, wykorzystujących najnowocześniejszy sprzęt, częstokroć owocuje materiałem wyjątkowo wysokiej klasy, którego uzyskanie drogą operacyjną byłoby nieporównanie droższe i znacznie bardziej czasochłonne. Wydaje się więc, że stosunek jakości pozyskiwanych materiałów do kosztów z tym związanych to kolejna niepodważalna zaleta białego wywiadu. Pod tym względem metoda ta jawi się jako efektywna i wydajna. Cyfrowy charakter współczesnej informacji powoduje, że koszt tworzenia i utrzymania repozytoriów i baz danych czy korzystania z ich zasobów jest minimalny. Dlatego też większość informacji pozyskiwanych z przestrzeni publicznej jest zupełnie darmowa[56].

Cyfrowy charakter wiąże się z kolejną zaletą współczesnej informacji jawnoźródłowej. Łatwość jej przetwarzania oraz analizy wzrosła ogromnie. Klej i nożyczki zostały zastąpione przez oprogramowanie, w sposób automatyczny wspierające wyszukiwanie, selekcję i ekstrakcję informacji. Szybkość i wygoda analizy uległa więc znaczącej poprawie. Duże znaczenie ma tu także stosunkowa otwartość warsztatu, na którym opiera się współczesna sztuka wyszukiwania i analizy informacji. Dzieje się tak ze względu na bardzo szerokie wykorzystanie otwartych źródeł informacji poza sektorem publicznym. Owocuje to m.in. bogatą ofertą szkoleń i warsztatów skierowanych do funkcjonariuszy państwowych służb odpowiedzialnych za bezpieczeństwo, ale również researcherów, infobrokerów, specjalistów wywiadu, detektywów, dziennikarzy, naukowców czy analityków z sektora rządowego oraz prywatnego[57]. Taki stan rzeczy powoduje, że warsztat analityczny specjalistów z różnych sektorów przenika się i uzupełnia, dzięki czemu możliwa jest ciągła poprawa standardów i wprowadzanie coraz to nowych, doskonalszych technik i narzędzi pozwalających na sprawniejszą eksplorację kolejnych źródeł.

Z punktu widzenia służb wywiadowczych biały wywiad posiada jeszcze jedną zaletę nie do przecenienia. Ryzyko wykrycia przez kontrwywiad i konsekwencję z tym związane są znikome. Dlatego też metoda ta była tak szeroko wykorzystywana przez zachodnie służby wywiadowcze w państwach

---

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

[57] Przykładem mogą być szkolenia oferowane przez firmę *Mediaquest*, zob.: http://www.mediaquest.pl/osint/ [dostęp: 18 sierpnia 2014] czy też *Niemczyk i wspólnicy*, zob.: http://niwserwis.pl/artykuly/e-learning-kurs-bialy-wywiad-jako-metoda-pracy-detektywistycznej.html [dostęp: 18 sierpnia 2014].

totalitarnych. Przypadek kraju takiego, jak Korea Północna 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. Dlatego też możliwość oparcia się w takich warunkach na otwartych źródłach informacji wydaje się nie do przecenienia[58].

Kolejną zaletą, zwłaszcza w realiach współczesnej demokracji liberalnej, jaką daje wykorzystanie otwartych źródeł informacji, jest bardzo niska ingerencja w prawa człowieka i obywatela oraz prywatność postronnych osób[59]. Analizując problem z punktu widzenia służb państwowych odpowiedzialnych za bezpieczeństwo, nie sposób nie dostrzec dwóch ogromnych korzyści. Po pierwsze, niewielka „inwazyjność" różnych form białego wywiadu pozwala obyć się bez sądowej i prokuratorskiej kontroli, nieuniknionej w przypadku zastosowania bardziej złożonych metod pracy operacyjnej. Sprzyja więc szybkości pozyskiwania informacji, uprasza procedury z tym związane oraz angażuje mniej środków. Druga zaleta to ułatwienie budowy znacznie korzystniejszego społecznie wizerunku. Im rzadziej bowiem służby specjalne uciekają się do inwigilacji, wykorzystania agentury i innych środków „specjalnych", tym bardziej postrzegane są jako „mniej opresyjne" i przyjazne obywatelom. W tym kontekście biały wywiad uznać należy za metodę najbardziej sprzyjającą utrzymaniu takiego właśnie wizerunku.

Ostatnią z zalet godną podkreślenia jest możliwość zastosowania stosunkowo szerokiej dystrybucji raportów opracowanych przy wykorzystaniu białego wywiadu, co wynika z pominięcia procedur dotyczących ochrony informacji niejawnych. Już sam brak konieczności objęcia specjalną ochroną tajnego źródła znacząco upraszcza obieg i sposób przechowywania informacji. W tym kontekście dodatkową korzyścią jest nie tylko możliwość dużo szerszej wymiany informacji z służbami sojuszniczymi, ale również zastosowania tzw. outsourcingu i, tym samym, bieżącej współpracy z podmiotami prywatnymi zajmującymi się pozyskiwaniem informacji[60]. Elastyczność dysponowania materiałami opracowanymi na podstawie źródeł otwartych w bezpośredni sposób wpływa więc na znaczące obniżenie kosztów pracy wywiadowczej oraz wzrost jej efektywności poprzez zdecydowanie lepszą alokację sił i środków.

---

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

[59] G. Hribar, I. Podbregar, T. Ivanuša, *OSINT: A "Grey Zone"?...,* s. 539.

[60] H. Minas, *Can the Open Source Intelligence…,* s. 33-34.

3.2. Ograniczenia i wady

Mimo wielu niepodważalnych zalet biały wywiad ma także swoje ograniczenia oraz wady. Niektóre z nich wynikają bardziej z sygnalizowanych wcześniej uprzedzeń niż rzeczywistych ułomności omawianej dyscypliny. Przykładem takiego uprzedzenia może być chociażby zarzut mówiący o zakłócaniu „czystości" klasycznego cyklu wywiadowczego opartego na informacjach pochodzących ze źródeł niejawnych, każdorazowo głęboko i dokładnie weryfikowanych, zgodnie z arkanami sztuki wywiadowczej[61]. Nie da się ukryć, że biały wywiad ma również swoje rzeczywiste i wyraźnie dostrzegalne ograniczenia. Współcześnie najbardziej dotkliwa z jego wad wynika z nadmiaru informacji, który jest niewątpliwym problemem. To, co wydaje się największą zaletą otwartych źródeł informacji, a więc ich nieograniczona objętość i różnorodność, w praktyce może sprawić kłopot w trakcie prowadzenia analizy. Wyselekcjonowanie informacji wiarygodnych oraz oryginalnych danych wymaga nie tylko nie lada umiejętności, ale również zajmuje sporo czasu. Aby w pełni korzystać z możliwości, jakie daje biały wywiad, potrzeba sporo fachowej wiedzy i niemałego doświadczenia. Dodatkową niedogodnością jest konieczność nieustannego radzenia sobie ze zjawiskiem, ciągle narastającego, tzw. szumu informacyjnego, czyli nadmiaru danych, utrudniającego wyodrębnienie informacji prawdziwych i istotnych. Wraz z rozwojem mediów zjawisko to sukcesywnie przybiera na sile, by w dobie internetu stać się podstawnym problemem, z którym borykają się wszyscy specjaliści zajmujący się zdobywaniem i analizą informacji.

Wydaje się, że również 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[62]. Ponadto szybkość przyrostu danych wydaje się znacznie przewyższać wzrost możliwości programów przeznaczonych do ich analizy. Dlatego też wydaje się, że zjawisko szumu informacyjnego będzie z czasem wciąż narastać, a nie maleć.

Innym problemem wiążącym się z automatyzacją procesu wyszukiwania i analizy informacji jest kwestia sporej trudności ich weryfikacji. Bardzo trudno zweryfikować termin umieszczenia danej informacji w sieci, co utrudnia

---

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

[62] 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 (eds.), Lanham 2006, 275-276.

sprawdzenie ich wiarygodności oraz rzutuje na ich aktualność i przydatność[63]. 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. Owo zjawisko przez analityków nazywane jest tzw. „efektem echa" (ang. *echo effect*)[64].

Ponadto warto zauważyć, że mimo wszechstronności i uniwersalności białego wywiadu są obszary, gdzie okazuje się on zupełnie nieprzydatny. Zazwyczaj ma to miejsce na najniższym, taktycznym poziomie. Przykładem może być problem tropienia przywódców najgroźniejszych grup terrorystycznych. Mimo że chętnie wykorzystują oni internet do celów propagandowych, to robią to na tyle profesjonalnie, aby nie pozostawić tzw. „cyfrowych odcisków stóp" (ang. *digital footprint*), a większość czasu przebywają w miejscach odciętych całkowicie nie tylko od sieci, ale również 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[65].

Inną niezwykle ważną do przezwyciężenia trudnością jest bariera językowa. Problem ten towarzyszył białemu wywiadowi od samego początku. Dziś jednak, kiedy monitoring internetowych serwisów społecznościowych odgrywa coraz większą rolę, zaś angielski przestaje mieć uprzywilejowaną pozycję jako *lingua franca*, problem ten staje się coraz poważniejszy. Brak specjalistów biegle władających językami takimi, 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[66]. Niektórzy eksperci szacują, że aż 50 do 80 proc. informacji dotyczących obszaru zainteresowania wywiadowczego państw cywilizacji zachodniej nie jest publikowanych w języku angielskim[67]. Niewątpliwie fakt ten poważnie ogranicza rzeczywistą przydatność otwartych źródeł, nawet przy szerokim wykorzystaniu coraz doskonalszych

---

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

[64] *Open Source Intelligence (OSINT): Issues for Congress, CRS Report for Congress,* R.A. Best, A. Cumming, (eds.), Congressional Research Service, 5 December 2007, p. CRS-9 [w:] http://www.fas.org/sgp/crs/intel/ RL34270.pdf [dostęp: 19 sierpnia 2014].

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

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

[67] M.M. Lowenthal, *Open Source Intelligence: New Myths, New Realities*…, s. 277.

elektronicznych translatorów.

Ostatnią, ale wcale nie najmniej ważną ułomnością cechującą wywiad jawnoźródłowy, jest 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 dezinformacji, zabieg ten można zdefiniować jako swego rodzaju sztukę wprowadzania w błąd określonych grup społecznych, mający zawsze planowy i celowy charakter. Jest ona prowadzona w sposób systematyczny i fachowy za pomocą rozbudowanego instrumentarium, zaś jej podstawowym narzędziem są mass media. Dezinformacja obok podstępu, intoksykacji, wpływania oraz białej i czarnej propagandy jest podstawowym orężem prowadzenia wojny informacyjnej[68]. Implikuje to konieczność posiadania przez specjalistów zajmujących się białym wywiadem nie tylko dobrego warsztatu analitycznego, ale również ogromnej wiedzy ogólnej i dużego dystansu do każdego z analizowanych źródeł. Doskonałą ilustracją tego problemu mogą być niemałe kłopoty z prawidłową analizą silnie zideologizowanej prasy radzieckiej w trakcie zimnej wojny, prowadzoną przez amerykański wywiad[69].

3.3. Wyzwania i nowe perspektywy

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

W tym kontekście największe nadzieje pokładane są w daleko idącej automatyzacji procesu wywiadu jawnoźródłowego, na każdym z jego etapów. Według T. Serafina, przy analizie na poziomie strategicznym można wyróżnić ich osiem. Kolejno są to: planowanie, standaryzacja, pozyskiwanie, indeksowanie, tłumaczenie, analiza, wizualizacja oraz dystrybucja. Planowanie to nic innego jak określenie strategii i głównych kierunków działania oraz określenie zbioru źródeł. Przez standaryzację rozumieć należy

---

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

[69] R.W. Pringle, *The Limits of OSINT: Diagnosing the Soviet Media*, 1985-1989, "International Journal of Intelligence and CounterIntelligence" 2007, vol. 20, no. 2, s. 240-257.

określenie kryteriów dalszego wyszukiwania, digitalizację źródeł drukowanych oraz opracowanie wielojęzycznych zapytań. Samo pozyskiwanie informacji to z kolei ich wyszukiwanie i selekcja oraz ekstrakcja danych. Czwarty komponent, czyli indeksacja źródeł, to również tagowanie informacji i danych. Dalej następuje proces tłumaczenia i transkrypcji informacji, a następnie analiza i wnioskowanie. Jej owocem jest standaryzacja materiału wyjściowego i prezentacja wyników, czyli wizualizacja. Ostatnim etapem całego procesu jest dystrybucja, a więc dostarczenie materiału do określonych podmiotów w ustalonej formie i czasie. Każde z wyżej wymienionych działań można znacząco 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[70]. Wszystkie z wymienionych 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 znacząco podnieść zarówno wydajność, jak i wygodę pozyskiwania informacji ze źródeł otwartych.

Warto zauważyć, że już dzisiaj istnieje rozbudowane oprogramowanie analityczne przydatne w wykorzystywaniu otwartych źródeł informacji. Niektóre z takich programów komputerowych powstały specjalnie z myślą o służbach i instytucjach odpowiedzialnych za bezpieczeństwo[71]. Dają one możliwość zastosowania i łączenia m.in. analizy powiązań, analizy geograficznej, monitoringu, różnorodnych baz danych, raportów i dokumentów. W zamyśle twórców tego typu oprogramowanie ma zawczasu identyfikować i alarmować użytkowników o nowych zagrożeniach, osobach podejrzanych i innych anomaliach. Oprogramowanie tego typu umożliwia również legalne zbieranie informacji, analizę i zarządzanie nimi w czasie rzeczywistym, bez konieczności wcześniejszego badania ich zawartości metodami klasycznymi. Przynajmniej w teorii pozwala to nieco łatwiej sprostać wyzwaniom, takim jak olbrzymia ilość i różnorodność informacji ze źródeł otwartych, konieczność analizy zawartości tzw. „głębokiego internetu" (ang. *deep weeb*) czy też radzenia sobie z wielojęzycznością gwar i żargonów. Obecnie wykorzystanie

---

[70] T. Serafin, *Automatyzacja procesu wywiadu…,* s. 83.

[71] 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.

tego typu rozwiązań jest coraz poważniej rozważane m.in. przez polską policję. Ma to zapewniać wczesną identyfikację zagrożeń i działań o charakterze kryminalnym, które uprzednio mogłyby być przeoczone lub nieczytelne, oraz dać lepsze możliwości podejmowania działań proaktywnych (zamiast reagowania na skutki)[72].

Wiąże się to z kolejnym wyzwaniem, przed jakim stoi obecnie biały wywiad, czyli analizą „Big Data". Poprzez pojęcie „Big Data" rozumieć należy 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[73]. Takie zbiory charakteryzują się dużą ogólnością, dotyczą bowiem niezindywidualizowanych strumieni danych, takich jak np. długość odwiedzin na stronie internetowej czy też długość rozmowy telefonicznej, informacje odnośnie do innych produktów zamówionych przez klienta w sklepie internetowym (dzięki pobraniu informacji z tzw. plików cookies) czy też ilość polubień (lajków) na Facebooku. Są to więc informacje określane mianem metadanych (czyli danych opisujących inne dane). Choć są one 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 jednak, wykrycie związku przyczynowo-skutkowego nie jest najistotniejsze. 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 wcześniej analitycy nie mieli dostępu – możliwość badania niemal całej populacji, a nie tylko jej próbki (z natury obarczonej błędem doboru)[74]. Cechy te powodują, że analiza „Big Data" ma ogromny wpływ na szeroko pojęte bezpieczeństwo publiczne, gdyż daje spore możliwości, jeśli chodzi

---

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

[73] „Big Data" powszechnie opisuje się przy pomocy koncepcji 4V, czyli czterech charakterystycznych czynników, definiujących te zbiory informacji. Są to: *Volume* (ilość danych), *Variety* (różnorodność analizowanych danych i informacji), *Velocity* (przetwarzanie w czasie rzeczywistym) i wreszcie *Value* – czyli wartość, jaką możemy uzyskać z połączenia wszystkich poprzednio wymienionych czynników. Zob.: T. Słoniewski, *Od BI do „Big Data"* [w:] *Nowa twarz Business Intelligence*, R. Jesionek (red.), s. 8 [w:] http://it-manager.pl/wp-content/uploads/Nowa-twarz-BI1.pdf [29 czerwca 2014].

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

o lepsze przewidywanie i modelowanie zagrożeń takich, jak zorganizowana przestępczość czy terroryzm[75].

Prace nad wykorzystaniem analizy „Big Data" (w szczególności w obszarze serwisów społecznościowych) są prowadzone m.in. przez brytyjskie służby specjalne. W założeniu dzięki informacjom uzyskanym w trakcie automatycznej analizy mają być 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 stać się jednym z komponentów wywiadu jawnoźródłowego Sojuszu. Docelowo ma to wydatnie ułatwić wykrywanie wczesnych symptomów radykalizacji poglądów, zarówno w przypadku całych społeczności, jak i pojedynczych osób, a tym samym znacząco zwiększyć możliwości i zakres działania zespołów analitycznych[76].

Warto dodać jednak, że obok sporych nadziei, analiza „Big Data" budzi również niemałe obawy, a jej implementacja na szeroką skalę może napotkać na pewne problemy natury zarówno technologicznej, jak i społecznej. Pierwszą trudnością, którą z czasem można jednak przezwyciężyć, są ogromne koszty budowy i ciągłej modernizacji infrastruktury teleinformatycznej, zdolnej z jednej strony przechowywać olbrzymie ilości danych, a z drugiej wydajnie analizować je w czasie rzeczywistym. Współcześnie na budowę tego typu centrów analitycznych, złożonych z potężnych systemów klastrów obliczeniowych oraz wysokowydajnych macierzy dyskowych, stać tylko najbogatsze kraje. Drugim, znacznie poważniejszym, społecznym problemem jest postawienie granicy, między danymi prywatnymi poszczególnych użytkowników sieci a informacjami upublicznionymi i dostępnymi dla wszystkich. W tym kontekście widać, że w cyberprzestrzeni granice pomiędzy dwoma dyscyplinami wywiadowczymi, jakimi są OSINT i SIGINT, ulegają systematycznemu zatarciu. Co istotne, wydaje się, iż ta tendencja rodzi coraz silniejszy niepokój społeczny. Wśród obrońców prawa do prywatności największe obawy budzi możliwość nieskrępowanego zestawiania informacji z różnych baz danych (przede wszystkim metadanych telekomunikacyjnych z zawartością profili w różnych serwisach społecznościowych) dokonywa-

---

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

[76] N. Couch, B. Robins, *Big Data for Defence and Security*, RUSI Occasional Paper, September 2013, s. 10-11 [w:] https://www.rusi.org/downloads/assets/RUSI_BIGDATA_Report_2013.pdf [dostęp: 26 sierpnia 2014].

nego w czasie rzeczywistym i to na masową skalę. Krzyżowe zastosowanie dwóch wyżej wymienionych dyscyplin wywiadowczych, wsparte wydajnymi narzędziami analitycznymi daje ogromne możliwości, ale jednocześnie nasuwa pytanie o celowość takich działań oraz sposób i zakres ich społecznej kontroli. Jak pokazują badania przeprowadzone przez naukowców z Massachusetts Institute of Technology, na podstawie analizy samych tylko metadanych telekomunikacyjnych (informacji o tym, kto z kim i kiedy się łączył oraz o lokalizacji) można z 80–90 proc. dokładnością przewidzieć zachowanie danej jednostki (np. gdzie znajdzie się ona w ciągu kolejnych 12 godzin). Do jeszcze ciekawszych wniosków doszli badacze z Uniwersytetu w Cambridge, kiedy porównali wyniki testów psychologicznych, przeprowadzonych wśród 58 tys. użytkowników Facebooka z analizą danych na ich temat, które były publicznie dostępne. Na podstawie tego, jakie treści badane osoby „polubiły" w internecie, można było ustalić ich pochodzenie rasowe, poziom inteligencji, orientację seksualną, uzależnienia czy poglądy polityczne z trafnością na poziomie 80–90 proc[77]. Trudno się więc dziwić, że tak precyzyjne możliwości zautomatyzowanego profilowania, coraz częściej prowokują dyskusję o skali i celowości systemu masowej inwigilacji, który można w niedalekiej przyszłości stworzyć, dzięki wykorzystaniu wyżej wymienionych metod.

***

W literaturze przedmiotu brakuje zgody co do jednoznacznego przebiegu granic, za którymi kończy się wywiad prowadzony z wykorzystaniem otwartych źródeł informacji a zaczynają inne dyscypliny wywiadowcze. Z kolei różnorodność podejść co do zakresu oraz form wykorzystania omawianej metody wywiadowczej implikuje bardzo obszerny zbiór określeń, którymi jest ona nazywana. Nie należy więc dziwić się, iż pojęcia takie, jak „wywiad jawny", „wywiad jawnoźródłowy", „OSINT" czy „biały wywiad" definiowane są w nieco inny sposób. Nie mniej jednak określeń tych można używać zamiennie, gdyż pomimo odmiennej proweniencji odnoszą się w gruncie rzeczy do jednej i tej samej metody pozyskiwania i analizy informacji ze źródeł ogólnodostępnych i jawnych. Odrębną kwestią pozostaje natomiast problem wyznaczenia granic między tym, co uznać można za dane publicznie dostępne i jawne, a tym, co uważane jest obecnie za obszar prywatności. Zagadnienie to jest szczególnie trudne do rozstrzygnięcia współcześnie – w dobie cyfrowego przetwarzania informacji oraz wszechobecnego wykorzystania internetu. Postawienie wyraźnej i jednoznacznej granicy pomiędzy poszcze-

[77] K. Szymielewicz, *Szpieg w pajęczynie,* „Polityka" 2014, nr 14 (2952), s. 69.

gólnymi źródłami informacji przy wykorzystaniu tylko i wyłącznie kryterium ich legalności, a następnie budowa w oparciu o to definicji omawianej metody wywiadowczej wydaje się z góry skazane na niepowodzenie.

Warto jednocześnie zauważyć, iż definicje powstałe na gruncie amerykańskiej teorii wywiadu wydają się być nieco szersze i odnoszą się raczej do poszczególnych źródeł niż do metod ich analizy. Z kolei w polskiej literaturze przedmiotu, przy definiowaniu pojęcia „wywiadu jawnoźródłowego", największy nacisk kładziony jest na sam proces pozyskiwania i analizy informacji. Jak więc widać, zbudowanie precyzyjnej i jednocześnie stosunkowo uniwersalnej definicji wydaje się zadaniem niezwykle trudnym. Wynika to przede wszystkim z odmiennej kultury organizacyjnej oraz różnic w zakresie wykorzystania omawianej metody. W innych kategoriach będzie ona pojmowana w państwowych służbach odpowiedzialnych za bezpieczeństwo, w innych w instytucjach administracji publicznej, a w jeszcze innych w sektorze prywatnym. W szczególności, jeśli dodatkowo weźmie się pod uwagę lokalną specyfikę i metodykę pracy wywiadowczej.

Tak czy inaczej wyżej wymienione pojęcia można, w większości przypadków, stosować wymiennie. Nie ma bowiem sensu tworzyć dla zagranicznego ujęcia tego samego problemu odrębnej kategorii pojęciowej. Różnice w pojmowaniu omawianej metody pracy wywiadowczej na gruncie polskim oraz w literaturze anglojęzycznej, choć zauważalne, nie są na tyle znaczące, aby uzasadnione było różnicowanie pojęć takich, jak „biały wywiad" i „OSINT" lub „wywiad jawnoźródłowy". Najogólniej rzecz biorąc, za powyższą metodę pracy wywiadowczej uznać należy ogół działań mających na celu pozyskanie określonych informacji ze wszelkich źródeł jawnych i ogólnie dostępnych, bez konieczności wykorzystania specjalnych uprawnień lub tworzenia legendy operacyjnej.

Nie ulega wątpliwości, że wywiad jawnoźródłowy (OSINT) uznać można za jedną z podstawowych i w pełni samodzielnych dyscyplin wywiadowczych. Co ważne, jest ona w chwili obecnej fundamentem każdej nowoczesnej służby wywiadowczej, zaś udział informacji zdobytych metodami białego wywiadu ocenia się nawet na ponad 80 proc. Jak więc widać, skala wykorzystania otwartych źródeł informacji w działalności wywiadowczej jest bez wątpienia znacząca. Co ważne, trend ten jest zauważalny nawet pomimo daleko posuniętej kultury tajności, panującej, co do zasady, we wszystkich służbach oraz instytucjach odpowiedzialnych za bezpieczeństwo państwa. Zakres wykorzystania białego wywiadu w poszczególnych państwach jest bardzo różny i uzależniony jest przede wszystkim od systemu politycznego oraz dominującej filozofii w zakresie prowadzenia działań wywiadowczych. W państwach o długiej tradycji demokratycznej, gdzie fundamentem funkcjonowania szeroko pojętej administracji publicznej jest zasada transpa-

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

Wraz z rewolucją w dziedzinie technologii informacyjnych oraz upowszechnieniem się internetu znacząco 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 utrudnia analizę łatwych do zdobycia i potencjalnie ważnych informacji. Pewnym ograniczeniem bywa również nieprzydatność informacji pochodzących ze źródeł jawnych, na najniższym taktycznym szczeblu, w trakcie realizacji antyterrorystycznych operacji specjalnych. Jak więc widać, mimo iż większość informacji da się uzyskać ze źródeł otwartych, to często najcenniejsze z nich zdobyć można, jedynie stosując metody pracy operacyjnej.

Pomimo wyżej wymienionych wad, potencjał, jaki tkwi obecnie w białym wywiadzie, jest bez wątpienia kolosalny. 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 pokładane są w tzw. analizie „Big Data", umożliwiającej bardzo skuteczne prognozowanie trendów społecznych oraz wskazywanie potencjalnych zagrożeń. Z drugiej strony, istnieją jednak liczne obawy, iż narzędzie to nie tyle posłuży do poprawy bezpieczeństwa, co raczej ułatwi budowę niekontrolowanego przez nikogo systemu masowej inwigilacji.

Rozdział II

Historia białego wywiadu

Historia wykorzystywania otwartych źródeł informacji w działalności wywiadowczej jest tak długa, jak stary jest sam wywiad. Wraz z upowszechnianiem się informacji drukowanej, a później radia, telewizji i w końcu internetu informacje ze źródeł ogólnodostępnych stanowiły coraz większą część analiz i raportów wywiadowczych. Już w wieku XIX powszechna stała się praktyka monitorowania prasy, co w wydatny sposób oszczędzało zarówno czas, jak i środki, których wymagałoby pozyskanie tych informacji za pośrednictwem agentury. Przypadki, w których udało się pozyskać niezwykle wartościowe i strategicznie przydatne informacje, bazując tylko i wyłącznie na analizie źródeł ogólnodostępnych, są bardzo liczne – nawet kiedy cofniemy się aż do okresu, w którym nowoczesny wywiad dopiero się kształtował. Za prekursorów białego wywiadu uznać można Brytyjczyków. Już w 1808 roku podczas konfrontacji z wojskami Napoleona w Hiszpanii i Portugalii generał Wellington zalecał swoim sztabowcom staranną lekturę prasy, gdzie opisywano sposób organizacji nowych formacji francuskiej piechoty[78]. W podobnym okresie (około roku 1830) również Pruscy i Rosyjscy sztabowcy zaczęli korzystać z analiz wywiadowczych dotyczących liczebności i rozmieszczenia obcych wojsk a powstałych w oparciu o źródła ogólnie dostępne[79]. Już wtedy dostrzegano potencjał kryjący się w możliwości szerokiego wykorzystania otwartych źródeł informacji. Departamenty wywiadu w wiktoriańskiej Anglii przeznaczały odrębne fundusze na ten właśnie cel, co można uznać za początki autonomizacji dyscypliny wywiadowczej, za jaką dziś uchodzi wywiad jawnoźródłowy[80]. Na przełomie XIX

[78] S.D. Gibson, *Exploring the Role and Value of Open Source Intelligence* [w:] *Open Source Intelligence in Twenty-First Century*, Ch. Hobbes, D. Sailsbury (eds.), New York 2014, s. 13.

[79] M. Herman, *Potęga wywiadu*, Warszawa 2002, s. 24.

[80] Ibidem, s. 87.

i XX wieku powstały również pierwsze komercyjne firmy zajmujące się analizą publicznie dostępnych materiałów i budową własnych baz danych dotyczących m.in. problematyki wojskowej. Najlepszym tego przykładem mogą być dokonania Brytyjczyka Fredericka Thomasa Jane'a i działalność opartego na nich później przedsiębiorstwa. W roku 1898 wydał on atlas pt. „All the World's Fighting Ships", zawierający szkice i opisy ponad 200 okrętów wojennych. Publikacja ta, cyklicznie aktualizowana i wydawana, stała się jednym z podstawowych źródeł informacji wielu wywiadów ówczesnych marynarek wojennych. Z kolei firma, której Jane dał początek, obecnie jest jednym z najbardziej znanych międzynarodowych dostarczycieli informacji na temat techniki wojskowej i obronności[81].

Warto również zauważyć, że druga połowa XIX w. wraz z rozwojem przemysłowym, przyniosła wzrost zapotrzebowania na profesjonalne informacje gospodarcze, a w konsekwencji – rozwój wywiadowni gospodarczych, początkowo zwanych biurami informacyjnymi. Instytucje te oparte były głównie na wykorzystaniu danych jawnych i ogólnie dostępnych. Pierwsze na świecie biuro informacyjne, pod taką właśnie nazwą (fr. *Le bureau des renseignements* – Biuro Informacyjne), świadczyło usługi śledcze i kredytowe. Założył je w 1833 roku w Paryżu znany awanturnik i zarazem były szef francuskiej policji kryminalnej – Eugene François Vidocq. Zauważyć należy, iż w tym samym czasie w Stanach Zjednoczonych bardzo prężnie rozwijała się profesja prywatnego detektywa. Było to zasługą Allana Pinkertona, byłego śledczego, który w 1850 roku utworzył Narodową Agencję Detektywistyczną, także szeroko korzystającą ze źródeł jawnych[82]. Przykłady te bardzo dobrze obrazują ścisły związek zachodzący między sektorem państwowym i prywatnym w dziedzinie białego wywiadu, towarzyszący tej dyscyplinie wywiadowczej w zasadzie od chwili jej narodzin. Chodzi tu zarówno o metodykę pracy jak i o ludzi, którzy z dużym powodzeniem wykorzystywali doświadczenie zdobyte na państwowych posadach w późniejszej działalności komercyjnej.

W tym okresie największym beneficjentem korzyści płynących z wykorzystania otwartych źródeł informacji były niewątpliwie państwowe struktury, odpowiedzialne za wywiad wojskowy. Dzięki szybko rozwijającym się mediom społeczeństwa stawały się bardziej otwarte, a coraz więcej informacji dotyczących potencjału militarnego przeciwnika dawało się zdobyć bez uciekania się do kosztownych metod pracy operacyjnej i ryzykowania

---

[81] P. Kelso, *A wealth of knowledge,* "The Guardian", 31 October 2001 [w:] http://www.theguardian.com/world/2001/oct/31/afghanistan.politicsphilosophyandsociety [dostęp: 23 sierpnia 2014].

[82] Szerzej zob.: E. Jawers, *Agent, handlarz, prawnik, szpieg: Tajemniczy świat korporacyjnego szpiegostwa*, Kraków 2010, s. 55-94.

skandali dyplomatycznych. Czasopisma i lokalnie wydawane gazety zawierające fragmentaryczne dane, po zestawieniu przez sprawnego rezydenta, umożliwiały ujawnienie schematu sił zbrojnych oraz potencjału i przeznaczenia poszczególnych oddziałów wrogiej armii. Informacje dotyczące historii wojskowości również dostarczały wiele przydatnej wiedzy, gdyż większość jednostek wojskowych rzadko zmieniała miejsce dyslokacji, przez dziesięciolecia użytkując te same koszary[83].

Podobnie jak w wojsku, biały wywiad jako metoda wywiadowcza zaczął być stosowany w policji wraz z rozwojem informacji drukowanej, zwłaszcza prasy. Policjantom (szczególnie wyższych szczebli kierowania) nieobca była lektura codziennej prasy. To właśnie gazety okazywały się najlepszym źródłem aktualnej informacji zarówno o przestępstwach, jak i potencjalnych zagrożeniach. Z publikowanych tekstów można było się sporo dowiedzieć nie tylko o aktywności kryminalnego półświatka, ale również na temat tendencji i nastrojów społecznych czy radykalnej działalności politycznej[84]. Biały wywiad traktowany był jednak tylko jako pewnego rodzaju dopełnienie informacji z innych źródeł, nie zaś metodycznie zaplanowany proces prowadzony przez wyselekcjonowaną grupę analityków. Nie ulega jednak wątpliwości, że mimo braku procedur i jednolitych metod analizy informacji, tego rodzaju działalność już przed II wojną światową była w pracy policji niezwykle ważna i pozwalała chociażby na ocenę materiałów zdobytych drogą operacyjną w dużo szerszym i głębszym kontekście (zwłaszcza społeczno-politycznym). Było to o tyle istotne, iż w tym okresie to właśnie policja pełniła w większości państw rolę wewnętrznej służby bezpieczeństwa (tak było również w Polsce), odpowiedzialnej za monitoring nastrojów społecznych czy też zwalczanie zagrożeń o charakterze terrorystycznym.

Znaczący wzrost intensywności wykorzystania jawnych źródeł informacji nastąpił tuż przed wybuchem II wojny światowej. To właśnie wtedy po raz pierwszy powstawać zaczęły wyspecjalizowane zespoły, których głównym zadaniem było zbieranie i analiza informacji ze źródeł otwartych. Na tym polu duże osiągnięcia mieli przede wszystkim Niemcy. To właśnie w Abwehrze, jako jednej z pierwszych służb wywiadowczych, wydzielono oddzielną komórkę organizacyjną zajmującą się tylko i wyłącznie białym wywiadem. Był to referat I P (niem. *Presseauswertung* – analiza prasy), znajdujący się w Wydziale I, odpowiedzialnym za wywiad zagraniczny.

---

[83] J. Keegan, *Wywiad w czasie wojny. Zdobywanie wiedzy o nieprzyjacielu od czasów napoleońskich do al-Kaidy*, Warszawa 2003, s. 267.

[84] K. Radwaniak, P.J. Wrzosek, *Biały wywiad w Policji – pozyskiwanie i analiza informacji ze źródeł otwartych* [w:] J. Konieczny (red.), *Analiza informacji w służbach policyjnych i specjalnych*, Warszawa 2012, s. 113.

Dziedziną, w której otwarte źródła były wyjątkowo przydatne, był wywiad ekonomiczny. Na tym odcinku Niemcy stworzyli sztab wojskowo-gospodarczy (niem. Amtsgruppe Wehrwirschaftsstab), odpowiadający za koordynację zbrojeń. Instytucja ta prowadziła samodzielne studia wywiadowcze państw potencjalnie nieprzyjacielskich, opierając się przede wszystkim na otwartych źródłach informacji. Do najistotniejszych z nich należały urzędowe statystyki państw obcych i opracowania statystyczne Trzeciej Rzeszy, obca literatura ekonomiczna i wydawnictwa prasowe (analizowano codziennie około 50 gazet i 100 periodyków zagranicznych, a także liczne biuletyny przemysłowe i ekonomiczne), wyniki badań niemieckich i zagranicznych instytutów naukowych (np. opracowania Instytutów Ekonomiki Światowej przy uniwersytetach w Hamburgu i Kilonii) czy też zasoby archiwalne niemieckich koncernów (m.in. I.G. Farben, Siemens, Deutche Bank, Reichskreditgesellschaft czy Metallgesellschaft)[85]. Firmy niemieckie były również intensywnie wykorzystywane do zbierania informacji za granicą. Dobrym tego przykładem jest działalność niemieckiej placówki wywiadu gospodarczego, funkcjonującej na terytorium Stanów Zjednoczonych. Powiązany z niemiecką firmą I.G. Farben, Max Ilinger otworzył przedsiębiorstwo o nazwie Chemnyco, będące w rzeczywistości przykryciem dla wyspecjalizowanego zespołu, zbierającego informacje pochodzące z branżowych periodyków na temat wykorzystania nowych technologii w amerykańskim przemyśle. Firma przeznaczała na zakup samych tylko czasopism technicznych 4 tysiące dolarów rocznie. Dzięki ich analizie Niemcy stworzyli mapy przemysłowe złóż naftowych, linii wybrzeży i rurociągów w Stanach. Firma co tydzień przesyłała do Rzeszy raporty, wzbogacone o wycinki prasowe na temat amerykańskiego przemysłu[86].

O ile wykorzystywanie informacji pochodzących ze źródeł otwartych stało się powszechną praktyką jeszcze przed wybuchem drugiej wojny światowej, o tyle prawdziwy przełom nastąpił w latach ’30 i ’40-tych. W 1939 roku w Wielkiej Brytanii w ramach BBC uruchomiony został dział Digest of Foreign Broadcasts (później przemianowany na Summary of World Broadcasts), szerzej jednak znany pod nazwą BBC Monitoring. Była to pierwsza działająca na globalną skalę komórka białego wywiadu, analizująca informacje pochodzące z prasy i radia, na potrzeby służb specjalnych oraz rządu. Skala monitoringu była jak na owe czasy ogromna, w połowie 1943 roku BBC monitorowała około 1,25 miliona słów dziennie[87]. Autonomiczne

---

[85] W. Kozaczuk, *Bitwa o tajemnice. Służby wywiadowcze Polski i Rzeszy Niemieckiej 1922-1939*, Warszawa 1999, s. 229-231.

[86] L. Korzeniowski, A. Pepłoński, *Wywiad gospodarczy. Historia i współczesność*, Kraków 2005, s. 43-44.

[87] F. Schaurer, J. Störger, *The Evolution of Open Source Intelligence (OSINT)*, "The Intelligencer: Journal of U.S. Intelligence Studies", vol. 19, no. 3, (Winter/Spring 2012), s. 53.

komórki, pozyskujące informacje ze źródeł jawnych (przede wszystkim z prasy), działały również poza granicami Zjednoczonego Królestwa, m.in. w Sztokholmie, gdzie w trakcie wojny pracowało aż sześćdziesiąt osób[88]. Brytyjczycy wykorzystywali również dziennikarzy na terenach okupowanych, którzy na miejscu analizowali prasę lokalną i na jej podstawie wysyłali meldunki o dyslokacji niemieckich wojsk[89].

W ślady Brytyjczyków bardzo szybko poszli Amerykanie. Jeszcze w grudniu 1939 roku pracę rozpoczęło uniwersyteckie Princeton Listening Center. Jego podstawowym zadaniem była transkrypcja, tłumaczenie i analiza radiowych audycji propagandowych nadawanych z Berlina, Londynu, Paryża, Rzymu i Moskwy. Do kwietnia 1941 roku w centrum opracowano ponad 15 milionów słów transkrypcji materiałów przetłumaczonych z języka angielskiego, niemieckiego, francuskiego, włoskiego. W dniu 26 lutego 1941 roku na polecenie prezydenta Roosevelta centrum zostało poddane reorganizacji i w jego miejsce utworzono Służbę Monitoringu Nadawców Zagranicznych (Foreign Broadcast Monitoring Service – FBMS), podlegającą Federalnej Komisji Komunikacji. Podstawowymi zadaniami służby były monitoring, tłumaczenie, transkrypcja i analiza informacji pochodzących z audycji radiowych państw Osi. Do końca 1942 roku służba osiągnęła sporą wydajność. Tłumaczonych było ponad 500 tysięcy słów dziennie pochodzących z 25 stacji radiowych, nadających w 15 językach[90]. Największym wyzwaniem, przed jakim stali zarówno Brytyjczycy, jak i Amerykanie, był problem braku odpowiednich kadr – ludzi z jednej strony sprawdzonych i pewnych, a z drugiej władających biegle egzotycznymi językami, takimi jak np. japoński czy chiński[91].

Amerykanie stale monitorowali i analizowali również prasę i książki ukazujące się w czasie wojny za granicą. Za ich dostarczanie odpowiedzialny był Międzyresortowy Komitet Nabywania Zagranicznych Publikacji (Interdepartmental Committee for the Acquisition of Foreign Publications – IDC). Pod koniec wojny do analizy kierowano astronomiczną liczbę 45 tysięcy stron tekstu tygodniowo. W celu łatwego dostępu stworzono potężne repozytorium i indeks wszystkich dostępnych pozycji. W chwili zakończenia wojny znajdowało się w nim 300 tys. fotografii, 350 tys. numerów czasopism, 50 tys. książek, ponad milion map i 300 tys. innych dokumentów[92].

---

[88] M. Herman, *Potęga wywiadu…*, s. 87.

[89] A. Wojciulik, *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków* [w:] W. Filipowski, W. Mądrzejowski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki,* Warszawa 2012, s. 49.

[90] K. Leetaru, *The Scope of FBIS and BBC Open-Source Media Coverage, 1979–2008 (U)*, "Studies in Intelligence" vol. 54, no. 1 (March 2010), s. 19.

[91] S.C. Mercado, *FBIS Against the Axis, 1941-1945*, "Studies in intelligence", FBMS, s. 33-43.

[92] A. Olcott, *Open Source Intelligence in a Networked World*, London-New York 2012, s. 16.

Niedługo po wojnie, w 1947 roku FBMS została na mocy National Security Act przemianowana na Foreign Broadcast Information Service (FBIS) i pod tą nazwą włączona w struktury świeżo powołanej Centralnej Agencji Wywiadowczej (CIA). Rok później, na podstawie porozumienia, obie agencje – amerykańska i brytyjska, zobowiązały się do współpracy i wymiany analiz będących owocem ich pracy. Nastąpił również podział zainteresowań wywiadowczych – BBC skupiła się na analizie materiałów z Azji Centralnej i ZSRR, FBIS na Ameryce Południowej oraz Dalekim Wschodzie. Wspólnie monitorowano Afrykę, Środkowy Wschód oraz Europę. Ponadto wprowadzono wspólne standardy analizy i edycji raportów[93].

Zaraz po zakończeniu II wojny światowej Amerykanie zintensyfikowali rozbudowę innych struktur zajmujących się białym wywiadem. Obok FBIS działającej prężnie przez cały okres zimnej wojny w ramach CIA powstał Wydział Dokumentacji Zagranicznej (Foreign Document Division – FDD). Komórka ta zajmowała się przede wszystkim analizą ogólnie dostępnych dokumentów oraz prasy zagranicznej[94]. Dużym wsparciem dla niej był również Obronny Wydział Badawczy (Defense Research Division – DRD), wchodzący w skład Biblioteki Kongresu. Początkowo zespół ten, powstały na wniosek Departamentu Lotnictwa i pierwotnie (od 1948 roku) funkcjonujący pod nazwą Air Studies Division, skoncentrowany był na analizie książek oraz zagranicznych periodyków dotyczących techniki lotniczej. Później jednak zakres prowadzonych analiz znacząco się rozszerzył i objął również problemy związane z bieżącą polityką międzynarodową. Zaowocowało to kolejną reorganizacją i zmianą nazwy. W 1970 roku strukturę przemianowano na Federalny Wydział Badawczy (Federal Research Division – FRD). Analitycy FRD byli odpowiedzialni m.in. za specjalistyczne tłumaczenia i analizę dostarczonych materiałów, pochodzących przede wszystkim z prasy oraz publikacji zagranicznych. Ponadto na podstawie zbiorów biblioteki tworzyli analizy kontekstowe oraz biogramy na potrzeby armii oraz CIA[95].

Już w latach pięćdziesiątych zachodnie służby specjalne zdawały sobie sprawę z potencjału, który kryje się w białym wywiadzie, zwłaszcza jeśli chodzi o gromadzenie informacji na temat państw bloku wschodniego. Zdaniem amerykańskiego teoretyka wywiadu H.H. Ransoma, w czasie pokoju służby wywiadowcze były w stanie zdobyć w ten sposób nawet do 80 proc. potrzebnych

---

[93] K. Leetaru, *The Scope of FBIS…,* s. 19-20.

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

[95] R.L. Worden, *Gathering Multidisciplinary Information for the Policy-Making Community* [w:] http://www.loc.gov/rr/frd/pdf-files/info_for_policymakers.pdf [dostęp: 15 sierpnia 2014].

informacji. Wraz z nasilaniem się zimnej wojny udział tajnych operacji systematycznie spadał na rzecz pozyskiwania informacji ze źródeł otwartych. Było to spowodowane z jednej strony coraz doskonalszym systemem bezpieczeństwa, a z drugiej coraz większym udziałem mediów (nawet w państwach bloku wschodniego) w życiu społecznym[96]. Mimo iż w państwach należących do sowieckiej orbity wpływów otwarte źródła wykorzystywano w dużo mniejszym stopniu (czego przyczyną było przejęcie radzieckiej filozofii podejścia do wywiadu), to zdarzały się jednak wyjątki. Najlepszym tego przykładem jest działalność wschodnioniemieckiego Ministerstwa Bezpieczeństwa Publicznego (Ministerium für Staatssicherheit – MfS, potocznie – *Stasi*), analizującego miesięcznie około tysiąca czasopism i stu książek pochodzących z RFN, a także dwanaście godzin dziennie audycji emitowanych przez radio i telewizję tego kraju[97]. W okresie zimnej wojny metoda białego wywiadu wykorzystywana była również z powodzeniem w wywiadzie wojskowym. Przykładem może być brytyjsko-argentyńska wojna o Falklandy, kiedy to wywiad brytyjski ze względu na brak innych źródeł w swoich analizach oparł się głównie na opracowaniach „Jane's Fighting Ships" oraz „Military Balans" wydawanych przez Instytut Studiów Strategicznych, a dostępnych w publicznych bibliotekach[98].

Potencjał kryjący się w możliwościach wykorzystania otwartych źródeł informacji do celów wywiadowczych został dostrzeżony nie tylko przez Europejczyków i Amerykanów. Krajem, który już od 1956 roku bardzo intensywnie pracował nad stworzeniem kompleksowego systemu umożliwiającego pozyskiwanie i analizę informacji ze źródeł jawnych, były komunistyczne Chiny. W 1958 do życia powołano Chiński Instytut Informacji Naukowo-Technicznej, będący centralną komórką odpowiedzialną za koordynację pozyskiwania, przetwarzania i dystrybucji zagranicznych materiałów pochodzących ze źródeł otwartych. Do roku 1966 Chińczykom udało się zbudować gigantyczną jak na owe czasy bazę danych o charakterze naukowo-technicznym. W jej skład wchodziło ponad 11 tys. różnych zagranicznych periodyków, 500 tys. raportów badawczych, publikacji rządowych, materiałów pokonferencyjnych i prac dyplomowych, ponad 5 milionów zagranicznych patentów oraz kilka milionów próbek produktów potencjalnie przydatnych z punktu widzenia chińskiego przemysłu. Wszystko z ponad 50 krajów[99]. System pozyskiwania, przetwarzania, tłumaczenia, analizy i dystrybucji

---

[96] H.H. Ranson, *Central intelligence and national security*, Cambridge 1958, s. 19.

[97] F. Schaurer, J. Ströger, *The Evolution …*, s. 53.

[98] J. Keegan, *Wywiad w czasie wojny…*, s. 267.

[99] W.C. Hannas, J. Mulvenon, A.B. Puglisi, *Chinese industrial espionage: Technology acquisition and military modernization*, London-New York 2013, s. 19-20.

zagranicznych materiałów o charakterze naukowo-technicznym (pochodzących przede wszystkim z otwartych źródeł informacji) był stale rozbudowywany i w 1989 roku tworzył już wielopodmiotową wspólnotę wywiadowczą. Dwa lata później powstał również podręcznik wywiadowczy, koncentrujący się głównie na metodach pozyskiwania informacji ze źródeł otwartych[100]. Podobne usystematyzowanie zachodniej metodyki wykorzystania otwartych źródeł informacji nastąpiło ponad dziesięć lat później, kiedy to Sojusz Północnoatlantycki wydał trzy wspominane wcześniej podręczniki.

1. Biały wywiad w II Rzeczpospolitej

Praca z otwartymi źródłami informacji nie była obca również polskiemu wywiadowi. Metodę tą stosowano zarówno na poziomie centralnym, jak i w ekspozyturach terenowych[101]. Biały wywiad miał się szczególnie dobrze na kierunku niemieckim, co z jednej strony było spowodowane chronicznym brakiem funduszy na działalność agenturalną, z drugiej dużą dostępnością źródeł jawnych (zwłaszcza w porównaniu ze ściśle cenzurowaną prasą sowiecką). Brak środków wydatnie stymulował więc maksymalne wykorzystanie źródeł jawnych. W Oddziale II nie było jednak wyodrębnionej komórki zajmującej się tylko i wyłącznie gromadzeniem i analizą informacji ze źródeł otwartych (tak jak to miało miejsce np. w niemieckiej Abwehrze). Oficerowie Dwójki odpowiedzialni za analizę prasy zagranicznej działali w ramach Referatu V, odpowiedzialnego za szyfry własne oraz korespondencję, znajdującego się w Wydziale Organizacyjnym. Warto przy tym pamiętać, że już wtedy wojna informacyjna stanowiła niemałe wyzwanie dla polskiego wywiadu[102]. Z kolei jako przykład szerokiego wykorzystania otwartych źródeł informacji, również w ekspozyturach zagranicznych, można przytoczyć działalność płk M. Wyżła-Śnieżyńskiego, *attaché* wojskowego w Czechosłowacji, tworzącego świetne raporty wywiadowcze, oparte przede wszystkim na analizie prasy i katalogów czechosłowackich firm zbrojeniowych[103].

---

[100] Dokument dostępny w języku angielskim, szerzej zob.: H. Zhongwen, W. Zongxiao, *Sources and Techniques of Obtaining National Defense Science and Technology Intelligence,* Beijing 1991 [w:] http://fas.org/irp/world/china/docs/sources.html [dostęp: 16 sierpnia 2014].

[101] K. Danielewicz, *Formy i metody pracy operacyjnej wywiadu polskiego w latach 1921-1939 na przykładzie Lwowskiej Ekspozytury Wewnętrznej nr 5 Oddziału II Sztabu Generalnego (Głównego)* [w:] P. Kołakowski, A. Popłoński (red.), *Wywiad wojskowy II Rzeczpospolitej,* Kraków 2011, s. 283.

[102] A. Żebrowski, *Oddział II Sztabu Generalnego (Głównego) Wojska Polskiego uczestnikiem wojny informacyjnej na kierunku Niemcy i Rosja* [w:] P. Kołakowski, A. Popłoński (red.), *Wywiad wojskowy II Rzeczpospolitej,* Kraków 2011, s. 357-388.

[103] A. Wojciulik, *Rola „białego wywiadu"…*, s. 48.

Ponadto warto zauważyć, że w okresie międzywojennym istniały również polskie firmy prywatne, zajmujące się wywiadem gospodarczym. Wśród nich wymienić można przedsiębiorstwa takie, jak Biuro Kredytowo-Informacyjne „Wywiad" Sp. z o.o. we Lwowie (w skład zarządu wchodzili przedstawiciele Związku Banków w Polsce) czy Międzynarodowe Biuro Informacyjne „Providentia" B. Abramowicza. Trzeba dodać, że prężny rozwój firm tego typu na ziemiach polskich miał miejsce jeszcze w czasie zaborów. Do bardziej znanych należało m.in. Biuro Handlowo-Informacyjne A. Rosenthala, założone w 1896 roku Biuro Informacyjno-Komisowe S. Klaczkina czy Wywiadownia Handlowa K. Piechockiego. Warto podkreślić, że przy zbieraniu informacji ich pracownicy korzystali przede wszystkim z ogólnodostępnych źródeł, takich jak rejestry handlowe, księgi hipoteczne, publikowane w prasie bilanse roczne czy kartoteki protestów wekslowych. Typowe raporty zawierały dane takie, jak data założenia firmy, jej skrócona historia czy zakres działalności. Ponadto określały jej strukturę prawną, majątek i aktualny stan interesów, charakteryzowały właściciela oraz oceniały jego zdolność kredytową. Częstokroć zawierały także informacje o różnych powiązaniach badanej spółki[104].

Prawdopodobnie bogate doświadczenia na tym polu sprawiły, że mimo braku wyspecjalizowanych komórek zajmujących się monitoringiem radia i prasy metoda białego wywiadu była szeroko wykorzystywana przez polskie służby specjalne właśnie w obszarze wywiadu gospodarczego. Dobrym dowodem na to może być powołanie do życia w grudniu 1932 roku Polskiej Agencji Informacji Handlowej (PAIH). Była to instytucja wywiadu gospodarczego, pozornie będąca prywatną firmą z siedzibą w Warszawie. Agencja została jednak utworzona z kredytów Ministerstwa Spraw Wojskowych (Biura Wojskowego Ministerstwa Przemysłu i Handlu) i podlegała Oddziałowi II Sztabu Głównego WP[105]. Zakres zadań PAIH, wykonywanych na zlecenie Oddziału II Sztabu Głównego WP, koncentrował się głównie na działaniach o charakterze profilaktycznym. Agencja prowadziła wywiady dotyczące zlecanych zagadnień, dostarczała informacji i opinii o przedsiębiorstwach działających na terytorium II Rzeczypospolitej, dostawcach i firmach mających kontakty z Wojskiem Polskim. W raportach PAIH oceniano ich lojalność wobec państwa polskiego, a także poziom ogólnej kompetencji (np. fachowość, odpowiedzialność finansową). Rozległa sieć informacyjna PAIH stwarzała także spore możliwości i ułatwienia dla wywiadu wojskowego, które wykraczały poza zagadnienia typowo ekonomiczne. Tyczyło się to

[104] *Historia wywiadu gospodarczego. Część 2.* [w:] http://www.paulo.pl/hwg2.html [dostęp: 30 sierpnia 2014].

[105] W. Kozaczuk, *Bitwa o tajemnice…*, s. 233.

przede wszystkim analizowania kwestii ujemnego wpływu różnych zjawisk gospodarczych i zachowań określonych przedsiębiorstw (zagranicznych oraz polskich) na interesy i funkcjonowanie polskiego przemysłu zbrojeniowego. W związku z tym PAIH na bieżąco sporządzała analizy tematyczne, w których prezentowała opis szkodliwego wpływu na obronność kraju wybranych operacji gospodarczych w sektorze przemysłu i handlu prywatnego, opartego na kapitale obcym. Zadania dla wywiadu wojskowego realizował głównie wydział „S" w PAIH, sporządzając okresowo szczegółowe studium kluczowych gałęzi gospodarki, przemysłu i handlu, analizując ich stan pod kątem interesów i potrzeb obronności kraju oraz samowystarczalności gospodarczej[106].

W latach 1934-1937 miała miejsce rozbudowa struktury PAIH, kiedy to utworzono filie terenowe w Katowicach, Łodzi, Gdyni, Poznaniu i Lwowie oraz znacznie powiększono terenową sieć informacyjną. Warto podkreślić, iż w 1937 roku rejestr współpracowników PAIH obejmował aż 4500 korespondentów terenowych i 200 wykwalifikowanych informatorów stałych, którzy zajmowali się opracowywaniem i wyjaśnianiem zagadnień specjalistycznych (branżowych). PAIH w okresie swojej działalności stworzyła wiele analiz na potrzeby instytucji centralnych i Oddziału II Sztabu Głównego WP. Ten ostatni w przypadku wątpliwości weryfikował wybrane raporty za pomocą własnych, niejawnych, źródeł wywiadowczych. Pod koniec 1937 roku opracowania przekazywane przez PAIH były oceniane stosunkowo wysoko (zyskując „dobre" lub „bardzo dobre" noty). Podejmowano próby wykorzystania działalności PAIH w zakresie wywiadu głębokiego na terenie Niemiec, ze szczególnym uwzględnieniem sektorów przemysłu niemieckiego mających kluczowe znaczenie dla obronności i sektora zbrojeniowego III Rzeszy. Jeszcze przed wybuchem wojny zdołano utworzyć jedną placówkę wywiadowczą, opartą na filii zagranicznej PAIH, wykorzystywano również niektóre placówki handlu zagranicznego w celu pozyskiwania informacji. Działalność PAIH w porównaniu ze skalą penetracji gospodarczej stosowanej głównie przez Niemcy w międzywojennej Polsce (różne instytucje wywiadu gospodarczego), była zauważalnie skromniejsza. Wynikało to z lepszej organizacji tego typu struktur, rozwijanych w Niemczech już od 1918 roku. Głównymi z nich były Sonderdienst Nuntia – przejęta przez Abwehrę w roku 1930 organizacja wywiadu ekonomicznego, czy Sicherheitsdienst I.G. Farben Leverkusen – wywiad gospodarczy koncernu IG Farben obejmujący swym zasięgiem ponad 11 największych zakładów przemysłowych i ich placówek zagranicznych[107].

---

[106] Ibidem, 234-236.

[107] Ibidem, 237-242.

Warto zauważyć, że niemałe zasługi na polu rozwoju białego wywiadu w Polsce miał marszałek Józef Piłsudski. Nakazał on w czerwcu 1934 roku utworzenie w Generalnym Inspektoracie Sił Zbrojnych tajnego Biura Studiów Strategicznych o nazwie Laboratorium. Jego głównym zadaniem było rozpoznanie narastającego zagrożenia wojennego ze strony obydwu wielkich sąsiadów Polski, poprzez analizę sytuacji wewnętrznej ZSRR i Niemiec. W zamyśle Piłsudskiego Biuro miało stać się ośrodkiem analitycznym, niezbędnym w planowaniu operacyjnym na szeroką skalę. Celem tej komórki było skoordynowanie i wzmocnienie różnych prac typu wywiadowczego oraz analiza informacji pochodzących ze źródeł takich jak radio czy prasa. Ponadto Laboratorium uzupełniało oraz kontrolowało prace Oddziału II Sztabu Głównego WP. Piłsudski uważał, iż Dwójka dostarczała wystarczająco dużo informacji potrzebnych do oceny położenia militarnego Niemiec i ZSRR, natomiast brakowało wiadomości o aktualnej sytuacji wewnętrznej, co szczególnie było widoczne w odniesieniu do państwa niemieckiego[108]. Strukturę tę można uznać za jedną z pierwszych wyspecjalizowanych komórek analitycznych, działających na potrzeby państwa polskiego, która swym kształtem, zakresem zainteresowań i metodami pracy była najbardziej zbliżona do struktur zajmujących się białym wywiadem w innych, wcześniej wymienionych państwach.

2. Biały wywiad w PRL-u

Również po wojnie służby komunistyczne w pewnym, ograniczonym, stopniu korzystały z metod wywiadu jednoźródłowego. Nie istniały co prawda odrębne instytucje korzystające tylko i wyłącznie z jawnych źródeł informacji, jednak w ramach Ministerstwa Spraw Wewnętrznych działało Biuro Studiów, a od sierpnia 1989 r. Departament Studiów i Analiz[109]. W tym okresie informacje pozyskiwane w ramach białego wywiadu były jedynie drobnym dodatkiem do materiałów uzyskiwanych drogą operacyjną. Taki stan rzeczy był jednak normą, zważywszy na filozofię i metodykę działania wszystkich służb specjalnych w bloku wschodnim w tamtym okresie. Praca analityczna i studyjna była rozproszona i tylko w niewielkim stopniu oparta na wykorzystaniu źródeł otwartych. Niemałe znaczenie miało samo nastawienie do pracy analitycznej jako takiej. Panowało bowiem powszechne przekonanie, że naprawdę wartościowe informacje można uzyskać tylko i wyłącznie

[108] P. Kołakowski, *„Laboratorium" Komórka Analityczna Józefa Piłsudzkiego*, „Słupskie Studia Historyczne" 2010, nr 16, s. 123 [w:] http://ssh.apsl.edu.pl/baza/wydawn/ssh016/kolakowski.pdf [dostęp: 23 lipca 2014].

[109] J. Larecki, *Wielki leksykon służb specjalnych…*, s. 369.

w drodze działań operacyjnych – im bardziej skomplikowanych i szerzej zakrojonych, tym lepiej. Do pracy analitycznej podchodzono z dużym dystansem, a sami analitycy mieli zazwyczaj status „funkcjonariuszy drugiej kategorii"[110]. Nie znaczy to jednak, że ze źródeł jawnych nie korzystano zupełnie. Robiono to jednak doraźnie i, co ważne, przede wszystkim w dziedzinie wywiadu zagranicznego. Funkcjonariusze wywiadu przebywający na placówkach zagranicznych byli zobowiązani do sporządzania rutynowych notatek, na podstawie informacji zawartych w prasie codziennej, branżowych czasopismach, książkach czy też w telewizji. Była to jedna z podstawowych metod diagnozowania nastrojów społecznych na Zachodzie. W ograniczony sposób otwarte źródła informacji wykorzystywano również w wojskowych służbach specjalnych, o czym może świadczyć m.in. pozycja „wydawnictwa krajowe i zagraniczne" w wykazie rzeczowych źródeł informacji[111].

Pewnym wyjątkiem były jednak działania podjęte względem Radia Wolna Europa (RWE). Systematyczny nasłuch i monitoring audycji radiowych był standardem już przed II wojną światową. Ogromne zmiany na tym polu przyniosła jednak zimna wojna, kiedy to walka z audycjami nadawanymi przez RWE, stała się jednym z podstawowych zajęć służb bezpieczeństwa państw Układu Warszawskiego. Działania te implikowały jednocześnie konieczność stałego i systematycznego monitoringu wrogiego medium. Skala przedsięwzięcia była ogromna, gdyż całodobowym nasłuchem zajmowało się w Polsce kilkuset etatowych pracowników Służby Bezpieczeństwa. Co ciekawe, praca ta była uważana, zwłaszcza przez ludzi wywodzących się z komunistycznego aparatu władzy, za wyjątkowo deprawującą i niesprzyjającą kształtowaniu odpowiednich postaw podwładnych. Już w 1955 roku ostrzegano, że funkcjonariusze zajmujący się nasłuchem są stale i systematycznie nastawieni na oddziaływanie wrogiej propagandy, przez co stan moralno-polityczny pracowników Zarządu Wydzielonej Łączności Radiowej jest niezadowalający[112]. Cała operacja związana z nasłuchem RWE tylko częściowo nastawiona była na zdobycie i analizę informacji, trudno uznać ją więc za klasyczny element białego wywiadu. Nie ulega jednak wątpliwości, że pozyskiwane w ten sposób informacje były wykorzystywane

[110] Z. Siemiątkowski, *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009, s. 34.

[111] *Instrukcja o działalności kontrwywiadowczej w Siłach Zbrojnych PRL*, Warszawa 15 marca 1984, §59 [w:] B. Kapuściak (red.), *Instrukcje pracy kontrwywiadowczej Wojskowej Służby Wewnętrznej wraz z instrukcjami prowadzenia dokumentacji i ewidencji (1957-1990)*, INP, Kraków 2010, s. 308.

[112] P. Machcewicz, *Walka z Radiem Wolna Europa (1950-1975)* [w:] R. Terlecki (red.), *Aparat bezpieczeństwa wobec emigracji politycznej i Polonii*, Warszawa 2005, s. 18.

operacyjnie przez SB. Ponadto wyżej przytoczony problem bardzo dobrze obrazuje uprzedzenia natury ideologicznej, które skutecznie utrudniały wykorzystanie na szerszą skalę otwartych źródeł informacji w większości służb państw bloku wschodniego.

Biały wywiad był jednak szeroko wykorzystywany przez zachodnie służby specjalne operujące na terenie Polski. Szczególnie dużą wagę przykładali do tej metody Amerykanie oraz Brytyjczycy. Nastręczało to sporo problemów polskim służbom bezpieczeństwa, gdyż zbieranie informacji metodami jawnymi i legalnymi wymykało się ówczesnej definicji szpiegostwa. Niemniej jednak szerokie wykorzystanie otwartych źródeł informacji nie uszło uwadze polskiego kontrwywiadu. Ta metoda pozyskiwania informacji była niezwykle doceniana przez pracowników zachodnich placówek dyplomatycznych z racji jej łatwości i bezpieczeństwa oraz stosunkowo dużej efektywności. Znawcy tego okresu stawiają nawet tezę, iż biały wywiad był najczęstszą i najbardziej podstawową formą działalności wywiadowczej prowadzonej przez zachodnie służby w bloku wschodnim[113].

W większych ambasadach zatrudniano pracowników zajmujących się tylko i wyłącznie opracowywaniem serwisów informacyjnych. Zawierały one wyselekcjonowane i przetłumaczone wiadomości, cytaty, streszczenia i wychwycone komentarze. Szeroko i regularnie korzystano przy tym z oficjalnej prasy, ale także ze źródeł mniej znanych i słabiej nasyconych propagandą (m.in. opracowań dostępnych w bibliotekach publicznych – monografii czy roczników statystycznych). Cenne, gdyż szczegółowe dane można było znaleźć w lokalnych i zakładowych gazetach. Bardzo uważnie śledzono również media audiowizualne, nagrywając najciekawsze reportaże radiowe czy filmy kinowe (np. materiały wytwórni „Czołówka"). Analizowano także okazyjną, specjalistyczną literaturę (np. periodyk „Życie Partii"), a także wielogodzinne wystąpienia kolejnych I sekretarzy KC PZPR, starając się z nich wydobyć interesujące sygnały, tendencje i informacje. Ogromna liczba tych materiałów powodowała, że pracownicy placówek dyplomatycznych katalogowali interesujące tytuły, sporządzali wykazy i odsyłali zgromadzone zasoby do macierzystych central, czytając na miejscu tylko niewielki jego procent. Metoda białego wywiadu wykorzystywana była również bardziej bezpośrednio. Dyplomaci państw zachodnich uczęszczali bowiem na interesujące ich wykłady, prelekcje czy prezentacje, odbywające się na uczelniach czy w branżowych klubach (np. w Klubie Dziennikarza), a nawet na obrony prac doktorskich. Starali się też śledzić

[113] P. Pleskot, *Dyplomata, czyli szpieg. Działalność służb kontrwywiadowczych PRL wobec zachodnich placówek dyplomatycznych w Warszawie (1956-1989). Część pierwsza*, Warszawa 2013, s. 369.

nowości wydawnicze (zwłaszcza w dziedzinie techniki i ekonomii), kupowali skrypty w kioskach akademickich. Ponadto ambasady wykorzystywały możliwości prenumeraty, np. ataszaty wojskowe prenumerowały czasopisma specjalistyczne (takie, jak np. „Żołnierz Wolności", „Skrzydlata Polska", „Wojskowy Przegląd Techniczny", „Granica", „W Służbie Narodu" czy „Morze"). Na ich podstawie przygotowano raporty dla centrali wywiadowczych, czasem przesyłając całe numery do analizy. Regularność i pieczołowitość analizy potwierdza dodatkowo fakt, iż placówka amerykańska i brytyjska, działające w Warszawie, wspólnie przygotowywały codziennie biuletyn informacyjny w języku angielskim pt. „Press Summary". Zawierał on informacje z wszystkich działów – politycznego, ekonomicznego i społeczno-kulturalnego. Opracowywała go wspólna, wyodrębniona komórka, zajmująca się tłumaczeniem z polskiej prasy. Ponadto miała ona za zadanie przygotowywać konkretne, szczegółowe raporty na tematy zlecone przez obie ambasady[114].

Polskie służby doskonale zdawały sobie sprawę z „systematycznej analizy publikacji i wydawnictw wywiadowczego zainteresowania" oraz „wykorzystania różnych ośrodków informacyjnych i placówek naukowych", trafnie zauważając, iż granice między działalnością naukową a wywiadowczą ulegają coraz mocniejszemu zatarciu. Wiedziano również, że na Zachodzie na coraz szerszą skalę wykorzystywana jest zautomatyzowana analiza informacji dokonywana przy pomocy „elektronicznych maszyn cyfrowych"[115].

Warte odnotowania są również dokonania opozycji antykomunistycznej na polu pozyskiwania i analizy informacji ze źródeł jawnych. Do komórek zajmujących się taką działalnością można zaliczyć m.in. Serwis Informacyjny Solidarności założony w 1988 roku przez Piotra Niemczyka, późniejszego współtwórcę Biura Analiz i Informacji Urzędu Ochrony Państwa. Struktura ta zbierała informacje o strajkach i przekazywała je wszystkim zainteresowanym (m.in. Radiu Wolna Europa, Głosowi Ameryki czy BCC). Oprócz kontaktów z działaczami związkowymi autorzy opracowań wykorzystywali również w znacznym stopniu informacje z wydawanych oficjalnie, ale trudno dostępnych pism, takich jak np. „W Służbie Narodu" (faktycznego organu Służby Bezpieczeństwa)[116].

---

[114] Ibidem, s. 370-373.

[115] F. Bielak, *Służby wywiadowcze Republiki Federalnej Niemiec*, MON, Warszawa 1985, s. 158.

[116] P. Niemczyk, *BAI*, „Przegląd Bezpieczeństwa Wewnętrznego" Wydanie Specjalne, 6 kwietnia 2010, s. 60.

3. Wywiad ze źródeł otwartych po 1989 roku

Gigantyczną zmianą jakościową w podejściu do otwartych źródeł informacji było powołanie do życia Biura Analiz i Informacji (BAiI) w Urzędzie Ochrony Państwa, utworzonym w 1990 roku w miejsce zlikwidowanej Służby Bezpieczeństwa. Pomysłodawcą projektu był Bartłomiej Sienkiewicz, zainspirowany podobnym rozwiązaniem istniejącym w służbach francuskich. Nowa komórka miała dwa zadania. Po pierwsze – w legalny sposób zdobywać ogólnodostępne informacje i przetwarzać je w sposób dający pionom operacyjnym UOP możliwość szybkiej reakcji na wszelkie wykryte zagrożenia. Po drugie – Biuro miało pełnić rolę wewnętrznej kontroli jakości, wprowadzając jednocześnie nową filozofię pozyskiwania informacji – dopiero tam, gdzie kończyły się możliwości białego wywiadu, powinny zaczynać się kompetencje pionów operacyjnych[117]. Głównym źródłem informacji Biura była prasa lokalna, opisująca wiele różnych zdarzeń, które nie przebiły się do mediów centralnych. W skład BAiI wchodziły cztery działy merytoryczne. Pierwszy z nich zajmował się zagrożeniami dla bezpieczeństwa państwa i porządku konstytucyjnego. Drugi zagrożeniami ekonomicznymi (głównie nagminnymi w owym czasie nieprawidłowościami w procesie prywatyzacyjnym). Trzeci wydział miał za zadanie monitoring zagrożeń związanych z bezpieczeństwem i integralnością terytorialną państwa, a płynących ze strony mniejszości narodowych oraz różnego rodzaju związków wyznaniowych. Wydział czwarty, odpowiedzialny za merytoryczne zadania BAiI, opracowywał biuletyny okresowe. W jego skład wchodził Zespół Informacji Bieżącej, który pracował 24 godziny na dobę. Miał on za zadanie opracowywanie informacji dotyczących najważniejszych wydarzeń zarówno z kraju, jak i ze świata. Powstanie Biura zbiegło się w czasie z rewolucją w dziedzinie technologii infomacyjnych, co miało wyraźne odbicie w szybkiej ewolucji metod pracy komórki. Początkowo funkcjonariusze wertowali setki gazet i czasopism, a tworząc raporty i opracowania, posługiwali się głównie klejem i nożyczkami. Z czasem na biurkach pojawiły się komputery, a analitycy uzyskali dostęp do internetu i ogromnej ilości cyfrowych baz danych[118]. Nie ulega wątpliwości, że Biuro Analiz i Informacji było pierwszą nowoczesną komórką analityczną, zajmującą się wyłącznie białym wywiadem, w polskich służbach specjalnych. Doświadczenia zdobyte w trakcie jej organizacji oraz wypracowane metody pracy umożliwiły stworzenie sprawnie działających pionów analitycznych w wielu państwowych instytu-

[117] B. Sienkiewicz, *Historia pewnego złudzenia*, „Przegląd Bezpieczeństwa Wewnętrznego" Wydanie Specjalne, 6 kwietnia 2010, s. 52.

[118] P. Niemczyk, *BAI…,* s. 63-66.

cjach. Najlepszym tego przykładem jest powstanie i późniejsza działalność Ośrodka Studiów Wschodnich.

***

Historia białego wywiadu wydaje się bardzo bogata i tak długa, jak historia zinstytucjonalizowanego szpiegostwa. Za początek tej dyscypliny wywiadowczej uznać należy narodziny nowoczesnej prasy. Z kolei powstanie kolejnych mediów, takich jak radio, telewizja czy w końcu internet, znacząco przyśpieszyły jej rozwój, a także zdecydowanie poszerzyły zakres i skalę wykorzystania otwartych źródeł informacji w działalności wywiadowczej.

Pierwsze, specjalnie wydzielone komórki, zbierające informacje na potrzeby wywiadowcze metodą białego wywiadu, pojawiły się w okresie międzywojennym. Niewątpliwie krajami najszerzej wykorzystującymi omawianą dyscyplinę wywiadowczą były Wielka Brytania oraz Stany Zjednoczone. To właśnie w tych państwach jeszcze w trakcie trwania drugiej wojny zbudowano potężne struktury odpowiedzialne za systematyczny monitoring audycji zagranicznych stacji radiowych oraz prasy. Z otwartych źródeł informacji stosunkowo intensywnie korzystał również wywiad niemiecki. W trakcie zimnej wojny, wcześniej powstałe struktury były nieustannie rozbudowywane, zaś uzyskiwane przez nie informacje stanowiły znaczącą część urobku wywiadowczego. Wydaje się więc, że to właśnie monitoring mediów stał się fundamentem dzisiejszego, nowoczesnego wywiadu jawnoźródłowego. Warto odnotować również fakt niezwykle szerokiego i bardzo dobrze zorganizowanego wykorzystania otwartych źródeł informacji w Chińskiej Republice Ludowej. Kraj ten jako jeden z pierwszych stworzył rozbudowany system pozyskiwania i analizy informacji o charakterze naukowo-technicznym pochodzących ze źródeł jawnych.

Również w Polsce metoda białego wywiadu rozwijała się dobrze. Co prawda przed wybuchem drugiej wojny światowej polskie służby nie monitorowały radia i prasy w skali takiej jak Brytyjczycy, Niemcy czy Amerykanie, jednak wykorzystanie tych źródeł w trakcie działań polskiego wywiadu było raczej częstą praktyką. Tezę tę w szczególności potwierdza skala wykorzystania otwartych źródeł informacji w dziedzinie wywiadu gospodarczego, prowadzonego przez Polską Agencję Informacji Handlowej. Była to niewątpliwie największa i najsprawniej działająca instytucja w II RP, której funkcjonowanie oparte było przede wszystkim na szerokim wykorzystaniu technik białego wywiadu. W okresie powojennym, podobnie jak w całym bloku wschodnim, również w Polsce omawiana dyscyplina wywiadowcza została dosyć silnie zaniedbana. W tym właśnie okresie zaczęła być dostrzegalna poważna dysproporcja w zakresie monitoringu mediów po obu stronach

żelaznej kurtyny. O ile na Zachodzie był on prowadzony w sposób planowy i systematyczny, przede wszystkim na szczeblu centralnym, o tyle służby wywiadowcze państw bloku wschodniego sięgały do ogólnie dostępnych źródeł jedynie na najniższym szczeblu i to w sposób bardziej przypadkowy niż planowy.

Ten ostatni fakt odbił się niewątpliwie na nowo budowanych strukturach analitycznych służb specjalnych III RP. Trudne początki Biura Analiz i Informacji UOP dały zaczątek polskiej szkole analizy informacji oraz silny impuls do szerszego wykorzystania metody białego wywiadu w innych służbach i instytucjach państwowych. Niemiej jednak braki, zaniedbania okresu PRL-u, a przede wszystkim negatywne stereotypy, którymi przesiąknięci byli starzy funkcjonariusze SB, kontynuujący służbę w nowej rzeczywistości, na długie lata utrudniły budowę nowoczesnych i sprawnie działających struktur analitycznych wykorzystujących otwarte źródła informacji.

Rozdział III

Wybrane otwarte źródła informacji

1. Podział otwartych źródeł informacji

Podstawowym podziałem, którego dokonać można w celu uporządkowania otwartych źródeł informacji, jest wyodrębnienie dwóch grup – źródeł pierwotnych oraz wtórnych. Te pierwsze zawierają oryginalny opis obserwacji, spostrzeżeń czy badań, drugie zaś gromadzą, przetwarzają i prezentują informacje pochodzące ze źródeł pierwotnych. Im informacja mniej przetworzona, im bliżej źródła pierwotnego zostanie pozyskana, tym jest cenniejsza i łatwiejsza w ocenie. Okoliczności powstania informacji, warunki jej przechowywania i przekazywania rzadko są jednak w pełni znane, dlatego też jej ocena jest czasem niezwykle problematyczna. Częstokroć już samo precyzyjne ustalenie, gdzie informacja została wytworzona, bywa niemożliwe. To z kolei jest warunkiem koniecznym do ustalenia, czy mamy do czynienia ze źródłem pierwotnym czy wtórnym.

Informacje przypisać można również do konkretnych kanałów informacyjnych. Pierwszym takim kanałem jest środowisko naukowe i akademickie. Wyróżnić tu można różnego rodzaju programy szkoleniowe, wykłady, prace dyplomowe czy wyniki badań i analiz. Za drugi kanał można uznać administrację publiczną, organizacje międzynarodowe i pozarządowe. Podmioty te tworzą i udostępniają dokumenty, bazy danych oraz raporty i analizy o różnym charakterze. Trzecim kanałem są podmioty komercyjne i środki masowego przekazu. Produkują, nadają i publikują treści opisujące aktualne problemy o charakterze lokalnym, regionalnym i globalnym. Prowadzą autonomiczne bazy danych z własnymi materiałami. Kanał czwarty to biblioteki, dostarczające informacji zawartych w swoich zbiorach (książkach, czasopismach, starodrukach) oraz tworzące katalogi i bazy danych pomagające w ich wyszukiwaniu. Za kanał piąty uznać można osoby fizyczne, które

w różnej formie dostarczają informacji, niewystępujących jeszcze w sformalizowanych źródłach[119].

Podział źródeł informacji tylko z pozoru wydaje się prosty. Wynika to z faktu, że współcześnie poszczególne kategorie niezwykle silnie się przenikają. Szczególnie dobrze widoczne jest to w przypadku internetu, który w zasadzie zawiera w sobie niemal wszystkie pozostałe źródła informacji. Inną trudnością w stworzeniu kompletnej i w pełni jednoznacznej typologii otwartych źródeł są niezbyt wyraźne granice, za którymi kończy się biały wywiad. Biorąc jednak pod uwagę doświadczenia historyczne i przyjętą już metodykę, można wyróżnić takie grupy źródeł, jak prasa, literatura, radio i telewizja, ogólnodostępne rejestry, bazy danych, dokumenty, geoinformacja oraz internet. Trzeba jednak wyraźnie zaznaczyć, iż wymienione kategorie, jak już wyżej wspomniano, nie są w pełni rozłączne (przenikają się nawzajem). Spowodowane jest to przede wszystkim postępującą cyfryzacją, w wyniku której do cyberprzestrzeni przenoszone są coraz to nowe bazy danych oraz całe systemy przechowywania, przetwarzania i wymiany informacji.

2. Prasa

Prasa to potoczne określenie używane w stosunku do dzienników oraz różnego rodzaju czasopism o charakterze informacyjnym, wydawanych periodycznie (przynajmniej raz do roku), wyróżniających się stałym tytułem i kolejnym numerem. Niewątpliwie to właśnie narodziny prasy były jedną z najistotniejszych podwalin białego wywiadu. Już w XIX wieku służby państwowe, zajmujące się zbieraniem informacji, szeroko korzystały z owoców dziennikarskiej pracy. To właśnie w tym okresie rozpoczął się proces, którego finał obserwujemy dzisiaj – ze zdobywania informacji praca służb zaczęła przesuwać się w stronę ich selekcji, weryfikacji i oceny. Początkowo gwałtowny rozwój prasy spowodował nawet, że w połowie XIX nastąpił czasowy zanik państwowych struktur wywiadowczych (np. w krajach takich, jak Wielka Brytania, Francja czy Austria)[120]. Przyczyną był znaczący wzrost wydawanych tytułów, coraz większe nakłady i przede wszystkim nieustanne poszerzanie tematyki, z którą zapoznać się można było w prasie. Jak więc widać, już okresie kształtowania się pierwszych nowoczesnych struktur wywiadowczych, dziennikarstwo oraz otwarte źródła informacji stanowiły jeden z fundamentów wywiadu.

---

[119] K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011, s. 59.

[120] M. Herman, *Potęga wywiadu,* Warszawa 2002, s. 24.

To właśnie w owym czasie pojawiły się również pierwsze prywatne agencje prasowe, które znacząco przyczyniły się do rozwoju białego wywiadu. Są to instytucje działające do dzisiaj, a zajmujące się dostarczaniem materiału innym mediom (początkowo prasie, później radiu i telewizji, a obecnie również serwisom internetowym). Dzięki temu media te mogą zaoszczędzić na kosztach utrzymywania własnych korespondentów, zagranicznych i terenowych. Rozsiani po całym świecie przedstawiciele agencji są w stanie w ciągu kilku minut przygotować informację i wysłać ją natychmiast do centrali. Współcześnie istnieje wiele dużych, międzynarodowych agencji prasowych (np. Agencja Reutera założona w 1849 roku w Paryżu), pozyskujących ogromne ilości stosunkowo wiarygodnych i wstępnie zweryfikowanych informacji (co jest konieczne w czasach niezależnego dziennikarstwa doby internetu)[121]. Stały monitoring doniesień agencji prasowych to jeden z fundamentów metodyki pracy współczesnych struktur zajmujących się wywiadem jawnoźródłowym. Pierwsza polska instytucja tego typu to Polska Agencja Telegraficzna, powstała w grudniu 1918 roku. Dosyć szybko PAT stworzyła stałe placówki korespondentów za granicą, m.in. w Berlinie, Wiedniu, Paryżu, Rzymie, Królewcu i Moskwie, zaś informacje z nich płynące wydatnie wspomagały pracę Oddziału II SG. Polski wywiad nie ograniczył się jedynie do analizy informacji jawnie zdobytych przez PAT, ale szybko zainicjował stworzenie kolejnej struktury – Agencji Telegraficznej Express. Działalność ATE wykraczała jednak daleko poza ramy białego wywiadu, gdyż poza zdobywaniem informacji, zajmowała się również działaniami o charakterze propagandowym i dezinformacyjnym. Po wojnie w Polsce Ludowej państwowym monopolistą na tym polu stała się Polska Agencja Prasowa, działająca do dziś i do dziś będąca jednym z podstawowych źródeł informacji w analizie jednoźródłowej. Dziennie wysyła ona ponad 1000 depesz[122].

Jeśli chodzi o rozwój dziennikarstwa, szerokie wykorzystanie doniesień prasowych było możliwe ze względu na fakt, że od samego początku znaczna część informacji, pozostająca w sferze zainteresowania dziennikarzy oraz służb wywiadowczych i policji, była wspólna. Już pod koniec XIX wieku w gazetach pojawiały się sensacyjne nagłówki i tematy uważane często za tabu (a więc dotyczące skandali obyczajowych, brutalnych morderstw, gwałtów, wypadków, a nawet plotki dotykające osób publicznych). Był to

---

[121] M. Baranowska-Szczepańska, *Dziennikarstwo w pytaniach i odpowiedziach*, Poznań 2010, s. 29-30.

[122] *Historia PAP* [w:] http://www.pap.pl/palio/html.run?_Instance=cms_www.pap.pl&_PageID=1&s=oagencji.opis&dz=oagencji.papsa&_CheckSum=-1787247140 [dostęp: 20 lipca 2014]

świetny sposób na zdobywanie nowych czytelników. Podobnie zresztą jak nagłaśnianie i angażowanie się w trudne problemy społeczne, takie jak walka z korupcją, nepotyzmem i innymi nadużyciami w sferze publicznej. W tym kontekście bardzo ważne wydaje się wytworzenie specyficznej niszy, jaką stało się dziennikarstwo śledcze. Polega ono na ujawnianiu informacji istotnych dla opinii publicznej, a jednocześnie trudno dostępnych dla badaczy. Uprawiają je dziennikarze opisujący i wyjaśniający sprawy, które najczęściej powinny być przedmiotem dochodzenia policji i prokuratury (a czasem nawet służb specjalnych). Rzetelna publikacja, zawierająca wyniki takiego dziennikarskiego śledztwa, poprzedzona jest dogłębną weryfikacją uzyskanych informacji. Polega ona na zdobyciu i wykorzystaniu co najmniej kilku niezależnych od siebie źródeł informacji oraz użyciu technik zbliżonych do stosowanych przez instytucje posiadające uprawnienia śledcze[123]. Co ważne, rozwój dziennikarstwa śledczego miał bardzo duży wpływ na znaczące udoskonalanie metod białego wywiadu. Na przestrzeni lat dziennikarze śledczy stworzyli własny warsztat pracy oparty przede wszystkim na otwartych źródłach, tworząc ich typologie i zalecenia dotyczące ich analizy i weryfikacji informacji z nich pochodzących[124].

Warto zauważyć, że współcześnie dzięki tzw. sygnalistom (ang. *whistleblower*), prasa publikuje częstokroć również informacje niejawne, nierzadko mające duży wpływ na bezpieczeństwo na szczeblu państwowym czy międzynarodowym. Przykładem mogą być publikacje w brytyjskim dzienniku „The Guardian" z czerwca 2013, w których ujawniono program PRISM oraz kulisy pracy amerykańskiej NSA[125]. Tak dokładne informacje, których dostarczył E. Snowden, na temat tej służby nigdy wcześniej nie były publikowane. Przykład ten pokazuje dobitnie, jak potężnym pasem transmisyjnym może być prasa (czy też szerzej całe media), jeśli chodzi o ujawnianie najściślej strzeżonych tajemnic państwowych. Informacje tego typu są bezcenne nie tylko dla służb przeciwnika, ale w tym konkretnym przypadku, również m.in. dla terrorystów, którzy zostali uprzedzeni przed bardzo konkretnymi metodami inwigilacji elektronicznej.

Z puntu widzenia analizy źródeł jawnych przez służby i instytucje państwowe kluczowe znaczenie ma jednak prasa codzienna, branżowa oraz naukowa. To dzięki niej możliwe jest zbudowanie np. kompletnego obrazu

---

[123] K. Wolny-Zmorzyński, *Źródła informacji dla dziennikarza śledczego* [w:] M. Palczewski, M. Worsowicz (red.), *O dziennikarstwie śledczym: normy, zagrożenia, perspektywy,* Łódź 2009, s. 128-135.

[124] Szerzej zob.: D. Spark, *Dziennikarstwo śledcze: studium techniki*, Kraków 2007, s. 45-66.

[125] G. Greenwald, E. MacAskill, *NSA Prism program taps in to user data of Apple, Google and others,* "The Guardian", 7 czerwca 2013 [w:] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [dostęp: 20 lipca 2014].

danego sektora przemysłu, sytuacji danej mniejszości etnicznej w odległym państwie czy mechanizmów zmian w aparacie władzy sąsiedniego kraju. Analiza prasy pozwala więc na zbudowanie szerokiego kontekstu dla opracowywanego zagadnienia. Nic więc dziwnego, że przez wiele dziesięcioleci było to jedno z podstawowych zadań rezydentur wywiadu działających za granicą. Szczególnie intensywna praca analityczna ze źródłami prasowymi trwała w okresie zimnej wojny. Jak już wspomniano w poprzednim rozdziale, w tej dziedzinie prym wiedli Amerykanie oraz wywiady państw zachodnioeuropejskich. Jak wynika z materiałów zgromadzonych przez polską Służbę Bezpieczeństwa, gromadzeniem informacji jawnych zajmowały się przede wszystkim placówki dyplomatyczne państw zachodnich, znajdujące się w naszym kraju. Systematycznie prenumerowały one czasopisma oraz dokonywały hurtowych zakupów materiałów specjalistycznych, skupiając się głównie na publikacjach z zakresu wojskowości, ekonomii, kryptografii, samoobrony czy działalności organizacji paramilitarnych[126]. Z oczywistych względów tylko część pozyskanych w ten sposób danych jawnoźródłowych była analizowana na miejscu, reszta trafiała do wyspecjalizowanych ośrodków tłumaczeń oraz analiz za granicą. CIA oprócz ośrodka w Izraelu wykorzystywała krajowe placówki naukowe – np. Instytut Technologii w Massachusetts czy uniwersytety w Stanford i Michigan. Z podobnej współpracy korzystały służby brytyjskie (wykorzystujące uniwersytet w Manchesterze i bibliotekę Greenwich) oraz zachodnioniemieckie (współpracujące w zakresie białego wywiadu z Instytutem ds. Badań Rynków Wschodnich w Hamburgu)[127].

Współcześnie prasa także jest szeroko wykorzystywana przez służby specjalne, również te wojskowe. Dzięki branżowym periodykom (w przypadku polskiego rynku wydawniczego takim jak np. „Nowa Technika Wojskowa", „Armia" czy „Strzał") możliwy jest wygodny i sprawny monitoring trendów w dziedzinie najnowszych technologii wojskowych, efektów wykorzystania nowego sprzętu czy w końcu zmian organizacyjnych zachodzących w innych armiach. Co istotne, informacje te są przydatne nie tylko analitykom zajmującym się wąsko rozumianym naukowo-technicznym wywiadem wojskowym. Wiedza zdobyta dzięki monitoringowi prasy fachowej pozwala również na wyrobienie opinii na temat rynku zbrojeniowego, jego najnowszych produktów oraz aktualnych trendów, funkcjonariuszom odpo-

---

[126] Z. Więckiewicz, *Niektóre formy i metody działalności wywiadowczej. Publikacje i międzynarodowy ruch osobowy,* Departament Szkolenia i Doskonalenia Zawodowego MSW, Warszawa 1974, s. 18-19.

[127] W. Nowak, *Metody pracy kontrwywiadowczej*, Departament Szkolenia i Doskonalenia Zawodowego MSW, Warszawa 1985, s. 73-74.

wiedzialnym za osłonę antykorupcyjną i kontrwywiadowczą przetargów na sprzęt wojskowy. Ten element wywiadu jawnoźródłowego wydaje się więc współcześnie niezbędny do skutecznego przeciwdziałania nieprawidłowościom w szeroko pojętym obszarze zamówień publicznych, istotnych z punktu widzenia bezpieczeństwa państwa.

Z perspektywy działań o charakterze wywiadowczym oraz policyjnym prasa stanowi więc źródło informacji, które sklasyfikować można na dwóch poziomach. Po pierwsze, mogą być to informacje ogólne, przydatne do zbudowania tła istotnych wydarzeń oraz lepszego zrozumienia ich mechanizmów. Dostępność tego typu danych jest duża (również po polsku lub angielsku). Po wstępnym opracowaniu pozwalają one stworzyć ramy, w które wpisać można konkretne informacje, zdobyte drogą operacyjną bądź jawnie. To właśnie te konkretne, szczegółowe informacje stanowią drugi poziom klasyfikacji. Najprzydatniejszym źródłem wydaje się tutaj prasa lokalna[128]. Można szczegółowo przeczytać w niej o interesujących nas osobach, ich powiązaniach czy znaleźć relacje bezpośrednich świadków analizowanych wydarzeń. Dostępność tego typu tytułów jest już zdecydowanie mniejsza. Zazwyczaj brakuje wydań internetowych, więc konieczne jest nabycie egzemplarza papierowego. Jeśli jest to pozycja zagraniczna z odległego rejonu, jej zdobycie może stanowić znaczącą trudność i zauważalnie podnieść koszty oraz opóźnić analizę. Do tego kolejnym – często bardzo trudnym do pokonania problemem – jest język, w którym tekst został napisany. Jeśli jest on egzotyczny, konieczna jest pomoc tłumacza, co znowu zmniejsza szybkość i sprawność analizy.

Obok prasy lokalnej bardzo bogatym źródłem informacji na temat różnych społeczności i grup nieformalnych są tzw. fanziny (skrót od ang. *fan magizine*), czyli czasopisma tworzone przez amatorów, będących miłośnikami danej dziedziny. Fanziny wydawane są zarówno w wersji papierowej, jak i elektronicznej, rzadko jednak wychodzą poza wewnętrzny obieg danej grupy czy subkultury. Ten typ wymiany i rozpowszechniania informacji jest szczególnie popularny w środowisku kibiców piłki nożnej, zwłaszcza wśród ich najzagorzalszej części czyli tzw. ultrasów (łac. *ultra* – skrajny). Z założenia fanziny miały odgrywać rolę zamkniętych forów wymiany wiedzy i doświadczeń dotyczących działalności kibiców. W praktyce jednak zdobycie tego typu materiałów nie jest trudne. Można je bowiem po prostu nabyć lub też wymieniać się nimi. Co ważne, podobne pisma ukazują się również w innych subkulturach, o skrajnie odmiennym profilu – np. w środowisku wspinaczy górskich – dlatego mogą dostarczyć wartościowych informacji o wybranych grupach. Treść zawarta w fanzinach zawiera niezwykle cenną, często wręcz

[128] K. Liedel, T. Serafin, *Otwarte źródła informacji…,* s. 65.

unikatową, gdyż pozbawioną cenzury wiedzę na temat ludzi tworzących badane środowisko. Na jej podstawie bez trudu zbudować można mapę ich poglądów, wyznawanych wartości oraz przyjmowanych postaw[129].

Współcześnie analiza prasy, dzięki internetowi i mediom elektronicznym, diametralnie zmieniła kształt. W dobie wydań elektronicznych nabywanie i transport papierowych wydań czasopism przestały mieć sens (może z wyjątkiem niskonakładowej prasy lokalnej). Również tłumaczenie dzięki rozbudowanym narzędziom elektronicznym jest obecnie prostsze i, co najważniejsze, dużo szybsze i sprawniejsze. Łatwiejsze stało się też tworzenie oraz szybkie przeszukiwanie baz danych, dostępnych w przystępnej, elektronicznej formie. Same zaś bazy można zawęzić do najpotrzebniejszych informacji, gdyż prowadzenie archiwów w formie elektronicznej (do których można uzyskać szybki i stosunkowo anonimowy dostęp z zewnątrz) stało się domeną wydawców konkretnych tytułów. Zmiany w prasie, które przyniosła rewolucja informatyczna, nie są jednak bynajmniej tylko i wyłącznie pozytywne. Prasa jest bowiem coraz silniej wykorzystywana jako narzędzie walki informacyjnej, a dziennikarska niezależność systematycznie spada (doskonałą tego ilustracją może być kształt i rola systemu mediów w Federacji Rosyjskiej w okresie rządów Władimira Putina). W oczywisty sposób pociąga to za sobą również spadek obiektywizmu informacyjnego oraz zwiększenie się podatności prasy na różnego rodzaju akcję dezinformacyjne (prowadzone zarówno przez podmioty prywatne, jak i państwowe – np. obce służby specjalne).

3. Szara literatura

Obok prasy do ogromnie ważnych źródeł otwartych należy zaliczyć literaturę. Istotne są przede wszystkim publikacje książkowe (zwłaszcza te zawierające wiedzę specjalistyczną – np. opracowania naukowe). Częstokroć przydatne okazują się również pozycje biograficzne[130]. Dostęp do książek możliwy jest oczywiście poprzez księgarnie i biblioteki, jednak w ostatnich latach ogromną popularność zdobyły tzw. e-booki, czyli książki w formie elektronicznej. Ich pozyskanie jest niezmierne proste i szybkie, gdyż odbywa się przez internet. Inną zaletą jest też możliwość dużo sprawniejszej (bo częściowo zautomatyzowanej) analizy treści. Wraz z pojawieniem się książek w formie

[129] K. Radwaniak, P.J. Wrzosek, *Biały wywiad w Policji – pozyskiwanie i analiza informacji ze źródeł otwartych* [w:] J. Konieczny (red.), *Analiza informacji w służbach policyjnych i specjalnych*, Warszawa 2012, s. 122.

[130] Ibidem, s. 123.

elektronicznej bardzo popularne stało się zjawisko tzw. self-publishingu, czyli publikowanie własnych tekstów (częstokroć zawierających fachową i niezwykle przydatną wiedzę) w internecie, bezpośrednio przez autorów, jeszcze przed ich ukazaniem się w formie drukowanej. Ma to niemałe znaczenie, gdyż dostęp do takich pozycji jest znacznie łatwiejszy (o co dbają sami autorzy, w celu uzyskania większej liczby cytowań) oraz szybszy (gdyż znika długotrwały proces związany z przygotowaniem książki do druku).

Na szczególną uwagę zasługuje jednak tzw. szara literatura (ang. *grey literature)*. Tym mianem określa się potocznie trudno dostępne książki i opracowania, które najczęściej nie są objęte rejestracją bibliograficzną, a także dokumenty rządowe, akademickie, biznesowe i przemysłowe, pozostające poza komercyjnym obiegiem wydawniczo-księgarskim[131]. Tworzone są przez bardzo różne podmioty, m.in. instytucje rządowe wszystkich szczebli, ośrodki akademickie (instytuty, laboratoria), biblioteki, fundacje, ośrodki gospodarcze i przemysłowe, profesjonalne stowarzyszenia i federacje zawodowe, ośrodki badawcze, które statutowo nie prowadzą działalności wydawniczej. Adresatami i użytkownikami są określone instytucje lub konkretny ograniczony krąg osób, dla których stanowią one pierwotne źródła specjalistycznej informacji. Szara literatura z założenia kolportowana jest w niewielkiej liczbie egzemplarzy[132].

Wśród źródeł niepublikowanych można wskazać na co najmniej kilka kategorii szarej literatury. Po pierwsze – sprawozdania i raporty naukowe, techniczne, ekonomiczne, społeczne i inne, powstające w instytucjach publicznych i prywatnych. Po drugie – materiały pokonferencyjne niepublikowane i niedostępne za pośrednictwem handlowych sieci księgarskich. Po trzecie – różnego rodzaju normy, zalecenia techniczne, ekspertyzy oraz niektóre opracowania statystyczne. Po czwarte – tłumaczenia niepublikowane. Po piąte – artykuły specjalistyczne ukazujące się w czasopismach wydawanych w małych nakładach, udostępnianych nieodpłatnie lub o zasięgu lokalnym (nieobjęte rejestracją ISSN). Po szóste – dokumentacja techniczna, promocyjna i reklamowa[133]. Po siódme – dysertacje magisterskie i doktoranckie. Po ósme – materiały metodyczne i szkoleniowe przeznaczone do użytku wewnętrznego.

Szara literatura wydaje się istotnym źródłem informacji ze względu na kilka czynników. Po pierwsze – jest zazwyczaj bardzo aktualna; nieoficjalne dokumenty ukazują się z reguły szybciej niż formalne publikacje

---

[131] S. Cisek, *Szara literatura jako źródło informacji biznesowej. Zarys problematyki* [w:] http://ebib.oss.wroc.pl/2002/40/cisek.php#3 [dostęp: 21 lipca 2014].

[132] *Szara literatura – instrukcja* [w:] http:// ibin.us.edu.pl/cbn/szara_literatura.doc [dostęp: 21 lipca 2014].

[133] *Szara literatura* [w:] http://www.mini.pw.edu.pl/~dryzek/www/?S%B3ownik:Szara_literatura [dostęp: 21 lipca 2014].

(przykładem mogą być chociażby materiały konferencyjne rozdawane uczestnikom w trakcie obrad). Po drugie – kompletność informacji; wiadomości zawarte w „szarych publikacjach" są często bardziej szczegółowe niż te, które znajdą się w ewentualnych późniejszych oficjalnych publikacjach, np. w artykule naukowym z reguły nie opisuje się drobiazgowo wszystkich zastosowanych technik badawczych, faz eksperymentów itp., natomiast informacje takie mogą znaleźć się w sprawozdaniu z badań. Po trzecie i najważniejsze – w tego typu opracowaniach znaleźć można informacje najbardziej unikatowe. Znaczna część danych tam zawartych nigdy nie trafi do dokumentów publikowanych przez profesjonalnych wydawców[134].

Wydawać by się mogło, że szara literatura nie do końca przystaje do definicji informacji jawnoźródłowej zaprezentowanej w poprzednim rozdziale. Niemniej jednak dostęp do źródeł określanych mianem szarej literatury utrudniony jest tylko pozornie. W wielu krajach na świecie istnieją elektroniczne bazy danych (np. serwis OpenGrey.eu), w których gromadzone są opracowania właśnie tego typu. Dotarcie do nich, dzięki internetowym wyszukiwarkom, nie jest więc aż tak problematyczne, jak było to jeszcze kilka lat temu. Podobnie jest również w Polsce, gdzie od 2001 roku Ośrodek Przetwarzania Informacji we współpracy z bibliotekami i ośrodkami informacji przystąpił do organizowania Krajowego Systemu Informacji o Szarej Literaturze – POLSIGLE – poświęconego różnym rodzajom dokumentów niekonwencjonalnych i trudno dostępnych. System powstał z inspiracji Europejskiego Stowarzyszenia Użytkowników Szarej Literatury – EAGLE – jako narodowy system informacji o szarej literaturze współpracujący z europejskim systemem SIGLE. Jego uczestnikami, poza krajami Unii Europejskiej, są również m.in. Rosja, Stany Zjednoczone i Japonia. Zgodnie z przyjętą koncepcją, struktura organizacyjna polskiego systemu jest dwustopniowa. Obejmuje, po pierwsze, krajowy ośrodek POLSIGLE, odpowiedzialny za organizację, rozwój i eksploatację systemowej bazy danych oraz współpracę międzynarodową, którego rolę pełni Ośrodek Przetwarzania Informacji. Drugi poziom stanowią biblioteki i ośrodki informacji, realizujące zadania gromadzenia i ewidencjonowania oraz opracowywania, archiwizowania i udostępniania zbiorów szarej literatury, a także zasilania systemowej bazy danych[135].

System ów jest jedną z kluczowych części składowych serwisu internetowego Nauka Polska (http://nauka-polska.pl), dającego dostęp do szeregu baz danych zawierających opracowania, takie jak sprawozdania i raporty

[134] S. Cisek, *Szara literatura jako źródło informacji biznesowej. Zarys problematyki* [w:] http://ebib.oss.wroc.pl/2002/40/cisek.php#3 [dostęp: 21 lipca 2014].

[135] POLSIGLE [w:] http://nauka.opi.org.pl/polsigle/polsigle_opis.htm [dostęp: 22 lipca 2014].

z badań naukowych, materiały konferencyjne, informacje o instytucjach naukowych, pracach badawczo-rozwojowych, organizowanych targach, konferencjach i wystawach czy też spis nazwisk ludzi związanych z poszczególnymi dziedzinami nauki oraz informacje o ich dorobku naukowym[136].

4. Radio i telewizja

Pierwsza połowa XX wieku to niewątpliwie okres przełomu i czas burzliwego rozwoju możliwości środków masowego przekazu. Początkowo radio, a później telewizja stały się mediami, z którymi zetknąć się musiał każdy z obywateli państw rozwiniętych. Nic więc dziwnego, że ich monitoring okazał się jednym z ważniejszych elementów białego wywiadu. Głównym powodem, dla którego zarówno radio, jak i telewizja stały się na tym polu tak ważne, jest fakt, że są to formy przekazu będące nośnikami najbardziej aktualnych informacji. Zwłaszcza obecnie, kiedy programy emitowane są 24 godziny na dobę przez 7 dni w tygodniu. Współcześnie istnieją setki stacji nadawczych z tysiącami programów i audycji. Nic więc dziwnego, że już od dłuższego czasu na ich określenie używa się pojęcia mass media, co odzwierciedla nie tylko ich olbrzymi zasięg, ale również potężną siłę oddziaływania społecznego[137]. Chociażby z tej przyczyny ich stały monitoring przez służby i instytucje państwowe stał się faktem już wiele lat temu.

Przydatność radia i telewizji jako otwartych źródeł informacji stale rośnie. Dzieję się tak, gdyż udział programów informacyjnych i publicystycznych w stosunku do programów i audycji czysto rozrywkowych stale się zwiększa. Olbrzymie znaczenie miało pojawienie się kanałów wyłącznie informacyjnych, wyodrębnionych z ramówki doczasowych stacji (tyczy się to przede wszystkim telewizji). Kanały te w większości podzielić można na dwie grupy – skoncentrowane na podawaniu informacji o charakterze społeczno-politycznym oraz finansowo-politycznym. Jeśli chodzi o telewizję, to samo pojęcie kanałów informacyjnych jest stosunkowo nowe. Najczęściej opisuje się je jako wyspecjalizowane kanały telewizyjne, na których serwisy informacyjne i programy publicystyczne są nadawane przez całą dobę. Najnowsze wydarzenia są prezentowane systematycznie, a bloki informacyjne i publicystyka przeplatane są analizami sytuacji politycznej, społecznej i gospodarczej oraz filmami dokumentalnymi i reportażami. Kanały informacyjne podzielić można na publiczne oraz prywatne. Wśród tych pierwszych najbardziej wszechstronnym i najefektywniej zorganizowanym jest bez

[136] *Nauka Polska* [w:] http://nauka-polska.pl/index.shtml [dostęp: 22 lipca 2014].
[137] K. Radwaniak, P.J. Wrzosek, *Biały wywiad w Policji…*, s. 123.

wątpienia BBC (British Broadcasting Corporation – Brytyjska Korporacja Nadawcza), mająca, jak już wcześniej wspomniano, spore doświadczenie w monitoringu mediów na potrzeby brytyjskiego wywiadu. Kanał BBC World News dostępny jest na całym świecie, zaś BBC News na terenie Wielkiej Brytanii. Oba kanały charakteryzują się selekcją informacji (tzw. *gatekeeping*) dokonywaną na innych zasadach (przede wszystkim udziałem informacji regionalnych). Podobnie sytuacja wygląda w wypadku innych publicznych nadawców. Przykładowo polski kanał TVP Info kładzie nacisk na przekazywanie informacji ze swojego kraju (regionu). Identycznie sytuacja wygląda w przypadku stacji komercyjnych, finansowanych ze środków prywatnych. Największym kanałem tego typu jest CCN International oraz CNN przeznaczonym dla odbiorców amerykańskich. Ponadto wymienić warto kanały takie, jak Fox News Chanel, Sky News, Al-Arabija czy Al-Dżazira (działający również w wydaniu międzynarodowym – Al Jazeera English). W Polsce najpopularniejszymi komercyjnymi kanałami informacyjnymi są TVN24 oraz Polsat News[138]. Warto podkreślić, iż współcześnie każdy z tego typu kanałów dysponuje również bardzo rozbudowanym internetowym portalem informacyjnym, aktualizowanym na bieżąco. Dzięki temu możliwa jest nie tylko znacznie szybsza i pełniejsza analiza przekazu, ale również zdecydowanie łatwiejsze staje się wychwycenie różnic, z pozoru nieistotnych szczegółów oraz kontekstu, komunikatu – w szczególności takiego, który został wytworzony w ramach obcego kręgu kulturowego.

Warto zauważyć, że w kontekście stałego monitoringu międzynarodowych mediów niemałe znaczenie ma wykorzystanie potencjału największych krajowych nadawców. Współcześnie rozwiązanie takie wydaje się szczególnie interesujące w kontekście potencjalnych scenariuszy prowadzenia nowoczesnej wojny informacyjnej. Obecnie agencje informacyjne o charakterze globalnym gromadzą informacje pochodzące od innych światowych nadawców i z własnych źródeł, a następnie przetwarzają je i dystrybuują jako niezależne, przy czym zazwyczaj w formacie i kontekście wygodnym dla interesu własnego kraju. Dlatego też podmioty te z jednej strony mogą być wykorzystywane do skutecznego kreowania opinii, z drugiej zaś występować w roli potężnego narzędzia wywiadu jawnoźródłowego, zdolnego do nadawania komunikatów moderowanych i badania oddźwięku, jaki powstaje globalnie. Wydaje się to zagadnieniem o fundamentalnym znaczeniu, zwłaszcza w epoce globalizacji i w dziedzinie współczesnego wywiadu, działającego na szczeblu strategicznym[139].

---

[138] K. Liedel, T. Serafin, *Otwarte źródła informacji..*, s. 66-67.

[139] *Globalna telewizja informacyjna i wywiad jawnoźródłowy* [w:] http://obserwatorpolityczny.pl/?p=1655#comments [dostęp: 2 września 2014].

Analizując rolę radia i telewizji we współczesnym białym wywiadzie, warto pochylić się również nad rozwojem metodyki pracy dziennikarskiej służącej do zdobywania informacji przekazywanych za ich pośrednictwem. Coraz częściej są to bowiem metody i techniki zbliżone do stosowanych przez policję i służby specjalne w ramach pracy operacyjnej. Wykorzystanie chociażby ukrytej kamery czy prowokacji dziennikarskiej powoduje, że informacje zdobyte w ten sposób mogą być naprawdę cenne (nie tylko z punktu widzenia wywiadowczego, ale również procesowego). Dlatego też telewizja wydaje się bardzo przydatnym otwartym źródłem informacji, jeśli chodzi o wykorzystanie go w policji[140]. W tym kontekście warto zwrócić również uwagę na fakt, że oprócz wykorzystania radia i telewizji w charakterze otwartych źródeł informacji w trakcie analizy materiałów dotyczących konkretnych spraw czy nawet rutynowego ich monitoringu przez odpowiednie komórki, spełniają one jeszcze jedną istotną rolę (w szczególności w policji). Chodzi tu o „wychwytywanie" informacji na temat zdarzeń kryminalnych, przestępstw i różnego rodzaju zagrożeń dla bezpieczeństwa państwa na bieżąco, poza pracą o charakterze analitycznym – również w czasie pozasłużbowym. Uzyskane w ten sposób prawidłowo udokumentowane i szybko przekazane informacje mogą stanowić spory i przydatny wkład w całość procesu analitycznego[141].

5. Ogólnie dostępne rejestry i dokumenty

Jednym z fundamentów każdego współczesnego państwa demokratycznego jest prawo do szerokiego dostępu do informacji publicznej. Pozwala to na zapewnienie stosunkowo dużej transparentności poczynań administracji publicznej. Skutkiem tego każdy przeciętny obywatel z założenia ma możliwość wglądu do ogromnej liczby rejestrów, ewidencji oraz informatorów zawierających dane, częstokroć bardzo cenne z wywiadowczego punktu widzenia. Dzięki nim możliwa jest np. ocena kondycji finansowej interesującego nas przedsiębiorstwa czy ustalenie składu osobowego zarządu organizacji pozarządowej. Pozwala to na wskazanie oraz udowodnienie wielu powiązań personalnych i finansowych czy zgromadzenie danych umożliwiających zbudowanie gospodarczego tła analizowanego problemu.

Największym i najczęściej wykorzystywanym w Polsce tego typu zbiorem danych jest Krajowy Rejestr Sądowy (KRS). Składa się on z trzech osobnych

[140] K. Liedel, T. Serafin, *Otwarte źródła informacji*.., s. 66.

[141] K. Radwaniak, P. J. Wrzosek, *Biały wywiad w Policji*…, s. 123.

działów. Pierwszy z nich to rejestr przedsiębiorców (a więc różnego rodzaju spółek), drugi zawiera spis dłużników niewypłacalnych. Trzeci to rejestr stowarzyszeń, organizacji społecznych i zawodowych, publicznych zakładów opieki zdrowotnej oraz fundacji. Aby uzyskać szczegółowe dane o interesującym nas podmiocie (przez internet sprawdzić można tylko podstawowe informacje) należy zapoznać się z pełną dokumentacją znajdującą się w Sądzie Rejonowym terytorialnie właściwym ze względu na główną siedzibę podmiotu. Akta są udostępniane w czytelniach, po zamówieniu złożonym osobiście lub drogą telefoniczną. Zazwyczaj dokumenty dostępne są dzień po ich złożeniu. Zamówienia dokonuje się na podstawie nazwy poszukiwanego podmiotu i jego numeru KRS. Można go ustalić za pomocą internetowej wyszukiwarki Ministerstwa Sprawiedliwości (http://krs.ms.gov.pl), ponieważ w KRS zamieszczane jest wiele szczegółowych danych (a ich udostępnienie jest ustawowym obowiązkiem podmiotów tam figurujących), co stanowi cenny zasób wiedzy na temat podmiotów znajdujących się w zainteresowaniu służb lub wywiadowni gospodarczych. W praktyce analiza akt KRS i weryfikacja pozyskanych stamtąd danych stanowi podstawowy element białego wywiadu ukierunkowanego na informacje o charakterze ekonomicznym[142].

Kolejną ważną bazą, udostępnianą przez wójtów, burmistrzów i prezydentów miast, jest Ewidencja Działalności Gospodarczej (EDG). Zawiera ona wiele informacji na temat osób prowadzących działalność gospodarczą (w tym również na podstawie koncesji i zezwoleń). W EDG możemy znaleźć dane zawierające m.in.: imię i nazwisko przedsiębiorcy, dane firmy, którą prowadzi (a także firm, które prowadził w przeszłości), numer PESEL, datę urodzenia, adres zamieszkania i siedziby oddziałów (byłych i aktualnych), datę rejestracji (i wyrejestrowania) działalności czy przedmiot działalności. Zazwyczaj dane te udostępniane są również na stronach internetowych miast i gmin, a zaimplementowana wyszukiwarka ułatwia ich znalezienie. Warto również dodać, że w formie elektronicznej (https://www.ceidg.gov.pl) istnieje również Centralna Ewidencja Informacji o Działalności Gospodarczej, prowadzona przez Ministerstwo Gospodarki.

Rejestr REGON (akronim od Rejestr Gospodarki Narodowej) prowadzony przez Główny Urząd Statystyczny jest kolejną bardzo istotną otwartą bazą informacji. Figurują w niej wszystkie osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej, osoby fizyczne prowadzące działalność gospodarczą, a także wszystkie jednostki lokalne tych podmiotów. Znajomość numeru REGON lub NIP (Numer Identyfikacji Podatkowej) pozwala

[142] K. Turaliński, *Wywiad gospodarczy i polityczny. Metodyka, taktyka i źródła pozyskiwania informacji*, Radom 2011, s. 63-69.

uzyskać informacje dzięki internetowej wyszukiwarce (http://stat.gov.pl/regon). Oba numery są jawne, zaś firmy, osoby fizyczne i prawne, a także inne podmioty, często umieszczają je na swoich stronach internetowych.

Innym przydatnym otwartym źródłem są księgi wieczyste (KW), prowadzone w celu ustalenia stanu prawnego nieruchomości. Dzięki digitalizacji danych możliwy jest wgląd do ich treści za pośrednictwem witryny internetowej Ministerstwa Sprawiedliwości (http://ekw.ms.gov.pl). Wcześniej konieczna była wizyta we właściwym terytorialnie Sądzie Rejonowym. Aby jednak korzystać z tej bazy, konieczna jest znajomość numeru KW. Można go ustalić we właściwym terytorialnie Starostwie Powiatowym (w wydziale właściwym rzeczowo dla zagadnień geodezji, kartografii i katastru), podając adres nieruchomości. Dzięki temu możliwy staje się wgląd do dokładnych akt gruntów lub budynków. Numer ten nie podlega ochronie prawnej i udostępniany jest wszystkim zainteresowanym. Wgląd do ksiąg wieczystych nie wymaga również wskazywania interesu prawnego ani żadnych dodatkowych zezwoleń. Podobnie jak w przypadku dostępu do wszelkich innych akt sądowych jest też bezpłatny. Księga wieczysta podzielona jest na kilka działów, a każdemu z nich przyporządkowane są inne wpisy tematyczne. Można znaleźć tam informacje na temat aktualnych i poprzednich właścicieli nieruchomości, ograniczeń w rozporządzaniu nieruchomością, praw i roszczeń, a także obciążeń hipotecznych[143].

Wartym uwagi jest również Monitor Sądowy i Gospodarczy (MSiG), będący ogólnopolskim dziennikiem urzędowym, w którym publikuje się obwieszczenia i ogłoszenia wymagane przez Kodeks postępowania cywilnego, Kodeks spółek handlowych, ustawę o Krajowym Rejestrze Sądowym oraz inne przepisy. Warto zauważyć, że każdy wpis do rejestru przedsiębiorców musi być ogłoszony w MSiG. Korzystanie z bazy danych możliwe jest przez internet za pośrednictwem wyszukiwarki znajdującej się na stronie Ministerstwa Sprawiedliwości (http://pdi.ms.gov.pl). Dostęp do publikatora wymaga jednak rejestracji. W oparciu o dane pochodzące z MSiG działa wiele serwisów o charakterze prawno-gospodarczym (np. Legalis – http://www.legalis.pl).

Oprócz wyżej wymienionych publicznych baz danych istnieje jeszcze wiele prywatnych serwisów ułatwiających pozyskiwanie informacji ze źródeł otwartych. Takie wyspecjalizowane podmioty odpłatnie pośredniczą w uzyskiwaniach odpisów – w imieniu zleceniodawcy realizując zamówienia i dostarczając dokumenty pod wskazany adres. Jednym z takich serwisów jest np. http://www.krs-odpisy.pl. Można zamówić tam odpisy informacji

[143] K. Turaliński, *Wywiad gospodarczy i polityczny. Metodyka, taktyka i źródła pozyskiwania informacji*, Radom 2011, s. 71-72.

m.in. z KRS, EDG, KW, Rejestru Dłużników Niewypłacalnych czy też Rejestru Zastawów[144].

Warto dodać, że dostęp do dokumentów publicznych możliwy jest za pomocą wyżej wymienionych baz i rejestrów, ale również na zasadach określonych przez ustawę o dostępie o informacji publicznej[145]. Prawo do informacji publicznej pozwala na wgląd do dokumentów urzędowych, korzystanie z już przetworzonych przez administrację danych oraz dostęp do posiedzeń kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów[146]. Wbrew pozorom liczba podmiotów zobligowanych do udostępniania informacji publicznej nie jest wcale mała i nie ogranicza się jedynie do organów władzy publicznej. Obejmuje ona również organy samorządów gospodarczych i zawodowych, podmioty reprezentujące Skarb Państwa oraz państwowe i samorządowe osoby prawne (lub jednostki organizacyjne), a także wszelkie podmioty, które wykonują zadania publiczne lub dysponują majątkiem publicznym. Jak więc widać, w grupie tej znajduje się sporo komercyjnych firm i przedsiębiorstw kooperujących w mniejszym lub większym stopniu z administracją państwową. Oprócz tego, do udostępniania informacji publicznej zobligowane są również organizacje związkowe oraz organizacje reprezentujące pracodawców[147]. Informację uzyskać można, składając pisemne zapytanie w wybranym urzędzie, wysyłając je drogą e-mailową lub też korzystając ze specjalnego urzędowego publikatora teleinformatycznego – Biuletynu Informacji Publicznej (BIP). Jest to niezwykle przydatne narzędzie wyszukiwania informacji publicznych, gdyż tworzy ujednolicony system stron internetowych, zbudowanych wedle jednego schematu. Ułatwia to wydatnie dostęp do konkretnych danych (np. struktury organizacyjnej, danych personalnych kierownictwa czy danych adresowych). Istnieje również główna strona, na której udostępniane są adresy stron BIP podmiotów zobowiązanych do prowadzenia Biuletynu oraz podstawowe dane teleadresowe tych podmiotów. Dostęp do informacji o instytucjach jest możliwy przez spis podmiotów, mapę oraz moduł wyszukujący[148].

W kontekście dostępu do informacji publicznej wspomnieć należy również o dokumentach gromadzonych w czasie przetargów. Dostęp do nich sankcjonuje Prawo zamówień publicznych[149]. Podlegają one udostępnieniu

---

[144] K. Radwaniak, P.J. Wrzosek, *Biały wywiad w Policji…*, s. 126.

[145] Ustawa z dnia 6 września 2001 r. *o dostępie do informacji publicznej* (Dz.U. 2001 nr 112 poz. 1198).

[146] Ibidem, art. 3.

[147] Ibidem, art. 4, pkt. 1.

[148] *Biuletyn Informacji Publicznej* [w:] http://www.bip.gov.pl [dostęp: 14 lipca 2014].

[149] Ustawa z dnia 29 stycznia 2004 r. *Prawo zamówień publicznych* (Dz.U. 2004 nr 19 poz. 177), art. 25.

na zasadach dostępu do informacji publicznej. Osoba występująca o wgląd w akta ma prawo wskazać miejsce, gdzie chce to uczynić, poprosić o wysłanie kopii pocztą, faksem lub też e-mailem. Co ważne, wiele istotnych i bardzo szczegółowych informacji jest podawanych przez zamawiającego już na etapie samego ogłoszenia. Są one zawarte w dokumencie pt. „Specyfikacja istotnych warunków zamówienia", który jest zawsze w formie elektronicznej umieszczony na stronie podmiotu zamawiającego. Warto dodać, że od osoby zainteresowanej dokumentacją przetargową nie można żądać interesu prawnego, z powodu którego chciałaby się zapoznać ze wskazanymi informacjami. Oczywiście wgląd do dokumentów nie jest nieograniczony, gdyż jawność niektórych umów może być wyłączona na podstawie przepisów o ochronie informacji niejawnej lub też na podstawie innych tajemnic (np. przedsiębiorstwa, bankowej, handlowej czy notarialnej) ustawowo chronionych[150]. Podkreślić należy również fakt, że zarówno w tym przypadku, jak i w ogóle, nieudostępnienie informacji publicznej nieobjętej tajemnicą grozi sankcjami karnymi (w tym do roku pozbawienia wolności)[151]. Pokazuje to, jak w demokratycznym państwie prawa silna (przynajmniej w teorii) jest pozycja obywatela i jak duże są możliwości nieskrępowanego pozyskiwania informacji od instytucji państwowych.

Inną ważną bazą informacji publicznej są systemy Orka oraz Orka 2 zawierające bazę interpelacji, zapytań, pytań i oświadczeń poselskich. Częstokroć poruszane tam tematy mają ogromne znaczenie dla bezpieczeństwa i obronności państwa. Dostęp do obydwu archiwów można uzyskać poprzez oficjalną stronę internetową Sejmu RP[152]. Z witryny tej można pobrać również wiele wysokiej jakości analiz i opracowań sporządzanych przez Biuro Analiz Sejmowych[153].

Największą, najbardziej uniwersalną i przejrzystą platformą do eksploatacji danych publicznych z wielu różnych otwartych źródeł, jest jednak powstałe w 2014 roku Centralne Repozytorium Informacji Publicznej (https://danepubliczne.gov.pl). W założeniu twórców Centralne Repozytorium ma stać się otwartym narzędziem informatycznym, ułatwiającym dostęp i powszechne wykorzystanie tzw. elementów zasobu informacyjnego jednostek administracji publicznej (a więc m.in. ich raportów, sprawozdań, prezentacji czy faktur). Z perspektywy użytkownika platforma ma umożliwiać proste

[150] K. Radwaniak, P.J. Wrzosek, *Biały wywiad w Policji…*, s. 128.

[151] Ustawa z dnia 6 września 2001 r. *o dostępie do informacji publicznej* (Dz.U. 2001 nr 112 poz. 1198), art. 23.

[152] *Archiwum* [w:] http://www.sejm.gov.pl/Sejm7.nsf/page/achiwum [dostęp: 14 lipca 2014].

[153] *Publikacje Biura Analiz Sejmowych* [w:] http://www.sejm.gov.pl/Sejm7.nsf/publikacjeBAS.xsp [dostęp: 14 lipca 2014].

i intuicyjne dotarcie z jednego miejsca do zasobów informacyjnych pochodzących od wielu różnych instytucji. Dzięki ujednoliconemu standardowi metadanych[154] możliwa jest również szybka i wydajna analiza zawartych tam informacji przy użyciu oprogramowania analitycznego oraz bezpośrednie wykorzystanie ich do budowy aplikacji mobilnych. Każdy użytkownik może przeszukiwać zasoby informacyjne wedle kryterium podmiotowego, po kategoriach lub słowach kluczowych oraz przy użyciu wyszukiwarki. Po wyszukaniu ma on dostęp do metadanych oraz linków powiązanych z zasobami i jednostkami informacji publicznej. Użytkownik może także założyć konto w CRIP, jeśli chce tworzyć swoje indywidualne zestawienia zasobów informacyjnych lub mieć dostęp do swojej historii wyszukiwań. Korzystanie z Centralnego Repozytorium jest możliwe także przez interfejs programistyczny (API), który został udostępniony z myślą o profesjonalistach – twórcach aplikacji i usług[155]. CRIP daje więc ogromne możliwości, jeśli chodzi o prowadzanie w pełni zautomatyzowanego wywiadu jawnoźródłowego.

Warto zauważyć, że niemałym ułatwieniem w przeszywaniu ogólnodostępnych rejestrów znaczenia mają portale obywatelskie, których głównym celem jest ułatwienie społecznej kontroli nad administracją publiczną. W polskich warunkach najlepszym przykładem tego typu witryny może być mojePaństwo.pl, będące otwartym zestawem aplikacji (ang. *open source software)*[156]. Ze względu na bardzo dużą liczbę funkcjonalności jest on świetnym narzędziem do przeszukiwania publicznych raportów i sprawozdań (np. raportów NIK, oświadczeń majątkowych posłów i senatorów czy rejestru ich korzyści). Co ważne, portal bardzo dobrze współpracuje z wyszukiwarką Google, przez co już z jej poziomu możliwe jest wyszukanie wielu przydatnych informacji (chociażby dotyczących podmiotów figurujących w KRS). Ponadto serwis wyposażony jest w proste narzędzia analityczne, pozwalające m.in. na automatyczną wizualizację wyszukanych powiązań osobowych i kapitałowych.

6. Geoinformacja

Geoinformacja to dziedzina geografii zajmująca się zbieraniem, pozyskiwaniem, gromadzeniem, przetwarzaniem, przesyłaniem, analizą, interpretacją danych geoprzestrzenych (a więc informacji o położeniu, geometrycznych

[154] Rozporządzenie Rady Ministrów z dnia 12 marca 2014 r. *w sprawie Centralnego Repozytorium Informacji Publicznej* (Dz.U. 2014 poz. 361), § 6.

[155] P. Kozłowski, *CRIP – wszystkie dane publiczne w jednym miejscu* [w:] http://datablog.pl/2014/05/21/crip-dane-publiczne-jednym-miejscu [dostęp: 29 sierpnia 2014].

[156] *O portalu* [w:] http://mojepanstwo.pl/oportalu [dostęp: 22 sierpnia 2014].

własnościach i przestrzennych relacjach obiektów zlokalizowanych na ziemi). Jako, że dane te są w znacznej większości bezpłatnie udostępniane, korzystanie z opracowań geoinformacyjnych może być jedną z ważniejszych technik białego wywiadu. Podstawowym narzędziem geoinformacyjnym jest System Informacji Geograficznej (ang. *Geographic Information System – GIS*). Jest to system informacyjny służący do wprowadzania, gromadzenia, przetwarzania oraz wizualizacji danych geograficznych, którego jedną z funkcji jest wspomaganie procesu decyzyjnego. Każdy system GIS składa się z bazy danych geograficznych, sprzętu komputerowego, oprogramowania oraz twórców i użytkowników. Szeroką grupę zastosowań GIS stanowi wszelkiego typu ewidencja – gruntów, budynków (wszelkiego rodzaju zasobów). Szczegółowe informacje tego typu wykorzystują urbaniści, geodeci, konstruktorzy. Zastosowanie warstwowej organizacji map umożliwia łatwą modyfikację jedynie wybranych obiektów, bez konieczności przerysowywania całej mapy. Komputerowa ewidencja własności gruntów z powodzeniem może zastąpić tradycyjną, prowadzoną za pomocą rejestrów i map geodezyjnych (katastralnych). Inną grupę zastosowań stanowi wykorzystanie GIS do przetwarzania informacji o lokalizacji wszelkiego rodzaju zjawisk, zwłaszcza tych cechujących się znaczną zmiennością w czasie. W tej grupie zastosowań mieści się analiza danych o charakterze statystycznym, takich jak np. zagrożenie przestępczością, występowanie chorób czy struktura użytkowania gruntów. Systemy te mogą również być bardzo wygodnym narzędziem do przetwarzania danych o infrastrukturze technicznej terenu (m.in. o sieciach wodociągowych, gazowniczych, energetycznych czy liniach komunikacyjnych)[157]. Dane z omawianych systemów zazwyczaj udostępniane są na zasadzie komercyjnej, niemniej jednak dzięki organizacjom takim jak Open Source Geospatial Fundation możliwe jest również darmowe ich wykorzystanie. Fundacja ta wspiera i tworzy bowiem wysokiej jakości otwarte oprogramowanie GIS[158].

Oprócz zaawansowanych narzędzi, jakie daje GIS, istnieje też wiele portali udostępniających mapy oraz zdjęcia satelitarne. W polskiej cyberprzestrzeni największym i najprzydatniejszym z nich jest bez wątpienia Geoportal powstały w roku 2005, kiedy Główny Urząd Geodezji i Kartografii rozpoczął realizację projektu GEOPORTAL.GOV.PL. W wyniku prac stworzono stronę internetową pozwalającą na dostęp do wielu geograficznych baz danych. Jako że informacja przestrzenna była wykorzystywana niemal we wszystkich sektorach gospodarki – m.in. w rolnictwie, leśnictwie, budownictwie, a także w administracji państwowej oraz działalności podmiotów prywatnych,

[157] K. Liedel, T. Serafin, *Otwarte źródła informacji…*, s. 69-71.
[158] *OSGeo* [w:] http://www.osgeo.org [dostęp: 15 lipca 2014].

zdecydowano się na dalszy rozwój projektu. Obecnie dostępna jest już druga, rozbudowana wersja witryny – Geoportal 2. Powstała ona w wyniku kolejnego etapu projektu zrealizowanego w 2009 roku i dała dostęp online do aktualnej i dokładnej informacji przestrzennej, obejmującej dane o środowisku geograficznym, obiektach i zjawiskach w całej przestrzeni geograficznej[159].

Innymi przydatnymi serwisami, dającymi dostęp do map i zdjęć satelitarnych, są m.in. maps.google.pl, bing.com/maps czy targeo.pl. Zwłaszcza ten ostatni serwis jest niezwykle przydatny w szybkim lokalizowaniu budynków, gdyż zawiera mapy z trójwymiarowym obrysem obiektów. Ponadto wyjątkowo przydatną usługą, zwłaszcza podczas doraźnego planowania operacyjnego, jest Google Street, udostępniająca zdjęcia ulic wykonywanych z pespektywy samochodu. Zbiór fotografii jest ogromny, gdyż zawiera większość metropolii i miast na świecie. Niezwykle przydatnym źródłem informacji, zwłaszcza w kontekście rozpoznania wojskowego, są również serwisy internetowe udostępniające mapy z naniesionymi aktualnymi pozycjami wojsk. Przyjmują one zarówno formę stron internetowych, jak i aplikacji zintegrowanych z serwisami społecznościowymi takimi, jak np. Facebook, Twitter czy VK[160].

W tym kontekście wymieć należy również bardzo przydatną usługę online, jaką jest Wigle.net. Jej zadaniem jest konsolidacja informacji o lokalizacji sieci bezprzewodowych na całym świecie oraz ich zapisywanie w centralnej bazie danych. Serwis umożliwia wyszukiwanie sieci Wi-Fi na podstawie współrzędnych geograficznych, adresu lub nazwy sieci. Usługę można bardzo efektywnie wykorzystać podczas lokalizowania konkretnych osób. Serwis znalazł szerokie zastosowanie w pracy tzw. *skip tracerów* (tj. poszukiwaczy dłużników, którzy uchylają się od spłaty należności, a miejsce ich pobytu jest trudne do ustalenia).

7. Internet

Bez wątpienia internet jest najbardziej unikatowym źródłem informacji. W zasadzie powinien być on rozpatrywany w tym względzie na dwóch płaszczyznach. Po pierwsze – jako swoiste metaźródło informacji nie tylko opisujące i porządkujące źródła wymienione wcześniej, lecz także zawierające

[159] *Informacje ogólne* [w:] http://geoportal.gov.pl/web/guest/o-geoportalu/informacje-o--projekcie/informacje-ogolne [dostęp: 15 lipca 2014].

[160] Dobrym przykładem może być rosyjski portal *Military Maps* (http://militarymaps.info), dedykowany wojnie na Ukrainie – *Liveuamap* (http://liveuamap.com), czy też aplikacja *Soviet Military Maps Free* (https://play.google.com/store/apps/details?id=com.atlogis.sovietmaps.free&hl=pl).

w sobie informacje z nich pochodzące (będąc tym samym gigantycznym repozytorium). W tym sensie internet to swego rodzaju cyfrowy pas transmisyjny między nowoczesnymi mediami a ich odbiorcami. Mamy więc internetowe wydania prasowe, elektroniczne wersje książek i dokumentów, internetowe stacje telewizyjne i radiowe czy portale geoinformacyjne. Po drugie – internet to potężne źródło informacji samo w sobie. Serwisy społecznościowe, blogi czy wreszcie obszar głębokiego internetu to niewyobrażalna ilość danych, którą, co ważne, przy odpowiedniej wiedzy i środkach można przeszukiwać w sposób (w coraz większym stopniu) zautomatyzowany. Ciągły rozwój technologii cyfrowych powoduje, że internet nieustannie ewoluuje, rozrasta się i daje niemal nieograniczone możliwości transmisji, przechowywania i wyszukiwania danych. Coraz większa liczba funkcjonalności sprawia, że informacje, które można ściągnąć z sieci, stają się znacznie bardziej aktualne, kompletne i multidyscyplinarne.

Mimo że internet dla młodszych pokoleń wydaje się rzeczą naturalną, a obsługa narzędzi umożliwiających jego eksplorację intuicyjna, to dotarcie do niektórych danych nie jest łatwe. Zwłaszcza dla zwykłych użytkowników, niemających większej wiedzy na temat budowy i zasad działania sieci. Dzieje się tak, gdyż internet podzielić można zasadniczo na dwa obszary. Pierwszy z nich, objętościowo znacznie mniejszy, to zbiór ogólnodostępnych stron internetowych, forów, witryn i portali, których adresy są zindeksowane i osiągalne za pośrednictwem popularnych wyszukiwarek internetowych. Drugi obszar to tak zwany głęboki internet[161], a więc cała reszta danych znajdująca się w globalnej sieci, niedostępnych jednak z poziomu zwykłej przeglądarki internetowej ze względu na brak ich indeksacji (informacji o ich istnieniu będącej w posiadaniu wyszukiwarek). Eksploracja zarówno jednego, jak i drugiego obszaru jest niezwykle przydatna dla wywiadu jawnoźródłowego.

W odniesieniu do zaawansowanego przeszukiwania treści sieci używa się w literaturze informatycznej określenia tzw. kopanie w danych (ang. *data mining*), zaś algorytmy ich wyszukiwania są przedmiotem wielu opracowań

[161] Głęboki internet (ang. *Deep Web*) – nazywany również ukrytym lub niewidzialnym internetem, to potoczne określenie zasobów internetu, które są bardzo słabo albo wcale indeksowane przez wyszukiwarki internetowe. Są to przede wszystkim bazy danych o dynamicznie zmieniającej się zawartości (na którą wpływ bezpośredni mają ich użytkownicy), a także prywatne witryny (fora, serwisy aukcyjne itp.) o dynamicznej zawartości. Dostęp do części z nich uzyskać można wyłącznie po wcześniejszej rejestracji w bazie użytkowników bądź wniesieniu określonych opłat. Co ważne, 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* [w:] http://www.lib.berkeley.edu/TeachingLib/Guides/Internet//InvisibleWeb.html [dostęp: 23 lipca 2014].

naukowych. Przyczyną takiego stanu rzeczy jest brak wiedzy internautów o zasobach oraz technikach ich wyszukiwania, cenzura internetu wprowadzana przez niektóre państwa, komercjalizacja internetu oraz negatywne skutki możliwości indywidualizacji przez użytkownika dostarczanych mu treści. Aby w pełni korzystać z danych zawartych w sieci, trzeba dobrze opanować techniki zaawansowanego wyszukiwania informacji. Wymaga to zastosowania tzw. strategii *Via The Web* polegającej na użytkowaniu różnych narzędzi wyszukiwaczowych[162] i to w sposób zaawansowany (tzn. poprzez ciągłe wykorzystywanie operatorów logicznych oraz tzw. instrukcji wyszukiwarki), co pozwala na dotarcie do ukrytego internetu poprzez wielowarstwowe i wieloetapowe przeszukiwanie sieci[163]. W tym kontekście warto zwrócić uwagę, że nawet techniki wykorzystania opcji wyszukiwania zaawansowanego w niezwykle popularnych i w pełni darmowych wyszukiwarkach doczekały się odrębnych i stosunkowo obszernych poradników, właśnie w zakresie prowadzenia białego wywiadu[164]. Wśród najbardziej znanych i najczęściej używanych wyszukiwarek wymienić należy takie, jak amerykańskie Google i Bing, chińskie Baidu czy rosyjski Yandex, a także silniki klastrowe takie jak Carrot2 czy iSeek. Ponadto warto zauważyć, iż istnieje wiele narzędzi przygotowanych z myślą o specjalistach zajmujących się białym wywiadem. Jak już wspomniano wcześniej, są to rozbudowane aplikacje wspomagające wyszukiwanie, katalogowanie, weryfikowanie i łączenie informacji pochodzących z internetu, w tym również z jego ukrytej, nieindeksowanej części[165]. Co ciekawe, tego typu instrumentarium jest częstokroć tworzone i udostępniane przez samych infobrokerów[166].

Nie da się jednak ukryć, że nawet bez stosowania zaawansowanych technik wyszukiwania oraz specjalistycznych aplikacji analitycznych za pośred-

---

[162] Przykładem takich rozwiązań są m.in. wyszukiwarki ludzi takie, jak np. 123people.com, namechk.com, UserSherlock.com czy Pipl.com pozwalające na szybkie wyszukiwanie nazwiska, adresów e-mail czy loginów w różnych, rozproszonych bazach danych. Na podobnej zasadzie działają również wyszukiwarki WHOIS (domen).

[163] D. Mider, *Partycypacja polityczna w Internecie*, Warszawa 2008, s. 195-196.

[164] M. Bazzell, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*, January 2014, s. 1-26.

[165] J. Gill, *OpenMIND – precyzyjne narzędzie pozyskiwania informacji wywiadowczych z otwartych źródeł,* „Ochrona Mienia i Informacji" 2012, nr 1, s. 65-66.

[166] Przykładem może być m.in. Oryon Environment, czyli rozbudowany zestaw aplikacji (stworzonych głównie w oparciu o język programowania Python) wspomagający procesy gromadzenia i analizy informacji z otwartych źródeł. Naczelnym elementem pakietu jest przeglądarka Oryon Browser, która została wyposażona w wyselekcjonowane dodatki oraz linki do różnorodnych narzędzi wyszukiwania i wszechstronnego rekonesansu. Szerzej zob.: *Oryon Environment: Open Source Intelligence (OSINT) Framework* [w:] http://miis.pl/osint-oryon-env [dostęp: 16 września 2014].

nictwem internetu można zdobyć olbrzymią ilość przydatnych informacji. Jak już wspomniano powyżej, większość wymienionych rejestrów i ewidencji posiada własne wyszukiwarki, pozwalające na dostęp w trybie online do zdigitalizowanej części (a przynajmniej do jej większości) dokumentów. Do tego dodać należy blogi, słowniki, encyklopedie internetowe, różnego rodzaju komercyjne repozytoria czy serwisy społecznościowe.

Z punktu widzenia podmiotów wywiadowczych niezwykle wartościową kategorią źródeł internetowych są właśnie serwisy społecznościowe. Z uwagi na wyjątkowo bogaty i różnorodny zasób danych sztuka pozyskiwania z nich informacji doczekała się już własnej nazwy. W literaturze anglojęzycznej tego typu działalność określana jest jako SOCMINT (od ang. *Social Media Intelligence*)[167], co bez wątpienia uznać można za jedną z subdyscyplin wywiadu jawnoźródłowego. Istnieje kilka rodzajów serwisów społecznościowych. Pierwszą i zdecydowanie najważniejszą grupą są portale towarzyskie. Służą one przede wszystkim do nawiązywaniu kontaktów (również tych międzynarodowych) i komunikacji zwrotnej. Wśród nich, największym i dającym najpełniejszą wiedzę o jego użytkownikach oraz ich powiązaniach jest Facebook (https://www.facebook.com). Co prawda, analiza informacji zawartych w profilach użytkowników nosi znamiona pracy operacyjnej (aby osiągnąć maksymalną skuteczność, dobrze jest mieć na takim portalu własny profil, stworzony np. przy użyciu legendy). Nie jest to jednak bezwzględnie koniecznie, gdyż istnieje wiele narzędzi zawierających skrypty, które z poziomu źródła strony (na której znajduje się rozpracowywany profil) są w stanie wydobyć niemal wszystkie przydatne dane[168]. Warto jednocześnie dodać, że Facebook nieustannie rozwija własny silnik wyszukujący oparty na mechanizmach tzw. analizy „Big Data" (czyli tzw. Facebook Graph Search), dlatego też zastosowanie natywnej wyszukiwarki tego serwisu kryje w sobie naprawdę olbrzymi potencjał. Niemniej jednak, pamiętać trzeba o różnej i ciągle zmieniającej się popularności poszczególnych serwisów społecznościowych. O ile bowiem na obszarze Europy czy USA najpopularniejszym serwisem jest właśnie Facebook, to np. w Rosji znacznie większym zainteresowaniem cieszy się portal VK (https://vk.com – ros. *ВКонтакте*). Portale społecznościowe są niezwykle przydatnym źródłem informacji nie tylko z punktu widzenia cywilnych służb specjalnych oraz policji. Ze względu na fakt, iż przekrój ich użytkowników jest bardzo różny, można wśród

---

[167] D. Omand, C. Miller, J. Bartlett, *Towards the Discipline of Social Media Intelligence* [w:] *Open Source Intelligence in Twenty-First Century*, Ch. Hobbes, D. Sailsbury (eds.), New York 2014, s. 24-26.

[168] Szerzej zob.: *Custom Search Tools* [w:] http://www.inteltechniques.com/links.html [dostęp: 16 sierpnia 2014].

nich znaleźć także żołnierzy w służbie czynnej. Umieszczane przez nich zdjęcia i wpisy umożliwiają nie tylko bardzo precyzyjne potwierdzenie obecności konkretnych jednostek w danym regionie, ale ustalenie również ich morale czy rodzaju aktualnie wykorzystywanego sprzętu i wyposażenia[169]. Niezwykle pomocne w takich przypadkach są tzw. metadane zawarte w plikach graficznych. Na ich postawie można zazwyczaj ustalić dokładną pozycję geograficzną i datę czy też nazwę i model urządzenia, jakim zostało zrobione zdjęcie.

Kolejną grupą są serwisy networkingowe, np. Goldenline (http://www.goldenline.pl) czy LinkedIn (https://pl.linkedin.com), których celem jest umożliwienie kontaktów biznesowych oraz uczestnictwa w grupach tematycznych lub branżowych. Wyróżnić można również portale nastawione na publiczne udostępnianie konkretnych treści. Najpopularniejszym z nich jest YouTube.com, zawierający filmy umieszczane przez użytkowników z całego świata. Obok tych o charakterze szkoleniowym bądź będących zapisem branżowych spotkań i konferencji, wiele nagrań ma ogromną wartość dowodową i dokumentalną. Nierzadko ich analiza zwieńczona była ustaleniem lokalizacji poszukiwanych terrorystów czy też źródła pochodzenia broni wykorzystywanej w danym konflikcie. Na portalu YouTobe.com, opiera się w dużej mierze kolejna grupa ważnych z punktu wywiadowczego witryn, czyli serwisów dziennikarstwa obywatelskiego. Istotą ich funkcjonowania jest praca dziennikarzy-amatorów, tworzących niczym nieskrępowane i niecenzurowane materiały filmowe, relacje fotograficzne czy felietony i komentarze społeczno-polityczne. Przykładami takich stron są Wikinews (http://pl.wikinews.org) czy Wiadomości 24 (http://www.wiadomosci24.pl). Inną istotną grupą stron są fora dyskusyjne. Szczególnie wartościowe informacje znaleźć można na tych branżowych, gdzie swe uwagi wymieniają zazwyczaj wysokiej klasy specjaliści w jakieś dziedzinie, np. broni palnej (http://bron.iweb.pl). Istotny jest też fakt, że grupują one internautów o określonych poglądach i zainteresowaniach skoncentrowanych wokół poszczególnych tematów. Wśród przydatnych witryn należy wymienić również blogi oraz mikroblogi, czyli miejsca, w których użytkownicy internetu zamieszczają swoje przemyślenia lub dzielą się z innymi częstokroć bardzo niszową wiedzą (jako

[169] Dobrym tego przykładem może być sytuacja z lipca 2014 roku, kiedy to rosyjscy żołnierze, mimo zapewnień Kremla o ich neutralności, na portalu VK.com i Instagram, zamieszczali wpisy i zdjęcia potwierdzające swój udział w walkach na wschodniej Ukrainie. Zob.: *Rosyjscy żołnierze chwalą się bombardowaniem Ukrainy* [w:] http://www.defence24.pl/news_rosyjscy-zolnierze-chwala-sie-bombardowaniem-ukrainy [dostęp: 16 sierpnia 2014], zob. też: *Wojsko rosyjskie było na Ukrainie w czasie katastrofy boeinga. Dowód? Selfie żołnierza* [w:] http://wiadomosci.gazeta.pl/wiadomosci/1,114871,16407705,Wojsko_rosyjskie_bylo_na_Ukrainie_w_czasie_katastrofy.html [dostęp: 16 sierpnia 2014].

przykłady polskich witryn blogerskich można wymienić: www.blogger.com czy http://www.salon24.pl). Dużo istotniejsze z punktu widzenia wywiadowczego są jednak tzw. mikroblogi. Najpopularniejszym serwisem mikroblogerskim jest obecnie Twitter (https://twitter.com). Zarejestrowany użytkownik może wysyłać i odczytywać tak zwane tweety, czyli krótkie wiadomości tekstowe (maks. 140 znaków) oraz zdjęcia. Serwis jest obsługiwany również na urządzeniach mobilnych, a jego monitoring pozwala nie tylko na śledzenie wypowiedzi wybranych osób (w tym również najważniejszych polityków czy dziennikarzy), ale również na rejestrowanie w czasie rzeczywistym zmian nastrojów społecznych (co pozwala na zbudowanie swoistego systemu wczesnego ostrzegania). W ostatnich latach w trakcie różnego rodzaju zamieszek, ale również walk zbrojnych, Twitter wielokrotnie stawał się źródłem najświeższych informacji[170].

Inną grupą serwisów wartych uwagi z punku widzenia pozyskiwania informacji są encyklopedie internetowe oraz repozytoria (miejsca uporządkowanego przechowywania dokumentów)[171]. W tej kategorii najpopularniejszym serwisem jest bez wątpienia Wikipedia[172] (http://pl.wikipedia.org) oraz połączone z nią WikiLeaks (http://wikileaks.org). Godnym wymienienia są również repozytoria takie, jak np. NewspaperARCHIVE.com, posiadający bazę ponad 2 miliardów zdygitalizowanych artykułów prasowych, czy The Wayback Machine (http://archive.org/web), gdzie dostępnych jest ponad 400 miliardów zarchiwizowanych, na przestrzeni lat, wersji stron internetowych z całego świata. Warto również wspomnieć o istnieniu serwisów umożliwiających dzielenie się opracowaniami naukowymi na każdy temat. Wśród najpopularniejszych z nich wymienić trzeba chociażby Academia.edu, gdzie znaleźć można liczne, w tym niezwykle profesjonalne, artykuły i poradniki

[170] Duże znaczenie Twittera potwierdzają m.in. wydarzenia tzw. Arabskiej Wiosny, kiedy to posłużył on do koordynacji działań powstańczych skierowanych przeciwko bliskowschodnim reżimom. Obecnie stały monitoring tego serwisu i wykorzystanie informacji z niego płynących w analizie bieżącej wydaje się koniecznością, także w przypadku wszystkich nowoczesnych służb wywiadowczych. Szerzej zob.: J. Rovner, *Intelligence in the Twitter Age*, „International Journal of Intelligence and CounterIntelligence" 2013, no. 26, vol. 2, s. 260-271.

[171] M. Karciarz, M. Dutko, *Informacja w Internecie*, Warszawa 2010, s. 16-17.

[172] Wikipedia to serwis niezwykle przydatny, w szczególności jeśli chodzi o budowanie szybkiego kontekstu analizowanego zagadnienia. Dzięki ciągłej aktualizacji i dużemu zaangażowaniu autorów, stanowi on cenne i uniwersalne źródło informacji. Nie należy jednak zapominać o największym mankamencie tego serwisu, czyli ogromnej podatności na działania dezinformacyjne. Doskonałym przykładem może być sytuacja z 29 lipca 2014 roku, kiedy to zmieniono dane dotyczące pułapu maksymalnego samolotu Su-25, w celu uwiarygodnienia lansowanej przez Kreml hipotezy o zestrzeleniu malezyjskiego Boeinga (lot MH-17) przez ukraińską maszynę tego typu. Zob.: http://www.defence24.pl/news_kreml-o-katastrofie-mh17-nagly-wzrost-pulapu-su-25-w-wikipedii [dostęp: 17 sierpnia 2014].

związane z zagadnieniami dotyczącymi bezpieczeństwa. Pod tym względem bardzo przydatnymi witrynami są portale umożliwiające użytkownikom umieszczanie w spersonalizowanych katalogach różnego rodzaju plików. W polskim internecie przykładem jednego z bardziej znanych może być Chomikuj.pl, w którym zamieszczane są także liczne niecenzurowane materiały instruktażowe z zakresu bezpieczeństwa i wojskowości.

Także wymieniony wcześniej serwis WikiLeaks (ang. *leak* – „przeciek") może stanowić niezwykle cenne, z wywiadowczego punktu widzenia, źródło informacji. Witryna ta umożliwia publikowanie w sposób anonimowy dokumentów rządowych i korporacyjnych przez informatorów chcących zasygnalizować działania niezgodne z prawem. Operatorzy tej witryny twierdzą, iż niemożliwe jest wyśledzenie, skąd pochodzą wpisy, w związku z czym ich autorzy nie ponoszą ryzyka związanego z ujawnianiem takich informacji. W serwisie znaleźć więc można wiele upublicznionych dokumentów objętych klauzulą tajności[173]. Za najgłośniejsze publikacje uznać można te z roku 2010, kiedy to na WikiLeaks opublikowano blisko 100 tys. wojskowych dokumentów, dotyczących wojny w Afganistanie, zawierających raporty z walk i incydentów z udziałem wojsk koalicji w całym kraju i ukazujących realne straty cywilne, nieznane dotąd opinii publicznej. Wśród raportów znalazły się szczegółowe sprawozdania z takich incydentów, jak polski ostrzał wioski Nangar Khel czy niemieckie bombardowanie w Kunduz[174]. Do końca 2010 opublikowano również prawie 392 tys. dokumentów o wojnie w Iraku oraz zamieszczono ponad 250 tys. depesz dyplomatycznych z amerykańskich ambasad na całym świecie[175].

Ciekawym źródłem informacji są również serwisy bezpośrednio dedykowane wywiadowi jawnoźródłowemu. Można znaleźć na nich wiele przydatnych porad i uwag na temat warsztatu pracy analityka pracującego na źródłach otwartych, ale również sporo linków do potencjalnie interesujących nas witryn. Dobrym tego przykładem jest m.in. osintinsight.com – jedno z największych repozytoriów źródeł informacji oraz narzędzi dochodzeniowych online. Istnieją również branżowe bazy tego typu. Dostęp do nich jest jednak płatny i wymaga rejestracji. Świetnym przykładem jest serwis

---

[173] *WikiLeaks: About* [w:] http://www.wikileaks.org/wiki/WikiLeaks:About [dostęp: 10 sierpnia 2014].

[174] E. Schmitt, H.Cooper, *Leak May Hurt Efforts to Build War Support* [w:] http://www.nytimes.com/2010/07/28/ world/asia/28wikileaks.html?_r=3&hp& [dostęp: 10 sierpnia 2014].

[175] Warto zaznaczyć, że sposób funkcjonowania WikiLeaks budzi cały czas ogromne kontrowersje. Twórcom serwisu zarzucono wspieranie terroryzmu. Jego redaktor naczelny, Julian Assange, jest ścigany listem gończym. Zob.: Ch. McGreal, *Is WikiLeaks hi-tech terrorism or hype? Washington can't decide,* "The Guardian", 5 February 2011 [w:] http://www.theguardian.com/media/2011/feb/05/wikileaks-hi-tech-terrorism-hype [dostęp: 29 sierpnia 2014].

CI CENTRE (http://www.cicentre.com), który oferuje ogromny zasób informacji również na temat kontrwywiadu czy organizacji terrorystycznych, w tym stosowanych przez nich metod i technik działania.

Niezwykle bogate i przydatne z punktu widzenia wywiadu wojskowego są również regionalne portale informacyjne. Mimo że weryfikacja zawartych w nich informacji bywa trudna lub czasem nawet niemożliwa, to ich aktualność jest nie do przecenienia. Dobrym na to dowodem może być bardzo szerokie wykorzystanie tego typu źródeł w trakcie misji stabilizacyjnej prowadzonej przez NATO w Afganistanie. Wiedza pozyskiwana w ten sposób była skutecznie wykorzystywana nie tylko do lepszego poznania kontekstu społeczno-kulturowego i lokalnego systemu klanowo-plemiennego, ale również w trakcie planowania i przygotowania konkretnych operacji na szczeblu taktycznym. Oczywiście sporym wyzwaniem w tym przypadku okazała się konieczność biegłej znajomości języków takich jak paszto czy farsi[176]. Poza lokalnymi serwisami informacyjnymi niezwykle przydatne w budowaniu wiedzy kontekstowej na temat danego obszaru są portale krajowe i blogi, które swoją tematyką obejmują dany region. Zazwyczaj są one tworzone przez pasjonatów, świetnie znających opisywaną kulturę, lokalny język oraz nierzadko utrzymujących bliskie kontakty z miejscową prasą. Doskonałym przykładem takiego blogera, będącego jednocześnie wybitnym specjalistą z zakresu białego wywiadu, może być postać Brytyjczyka Eliota Higginsa[177]. Dzięki informacjom zdobytym poprzez wnikliwą analizę mediów społecznościowych, serwisów geoinformacyjnych oraz nagrań z YouToube, rozwikłał on m.in. zagadki takie, jak użycie broni chemicznej w trakcie wojny domowej w Syrii czy zestrzelenie malezyjskiego Boeinga 777 lotu nr MH-17 nad Ukrainą w 2014 roku, zaś wynikami tych śledztw podzielił się na swoim blogu (www.bellingcat.com).

Ponadto stosunkowo istotnym elementem cyberprzestrzeni, szczególnie z punktu widzenia pracy policji, są serwisy aukcyjne (w polskim internecie najpopularniejszymi z nich są m.in. http://allegro.pl) oraz ogłoszeniowe (np. http://olx.pl, http://otoMoto.pl, http://www.gumtree.pl). Witryny tego typu ważne są zwłaszcza w kontekście tropienia przestępstw przeciwko mieniu, gdyż są cennym źródłem informacji kryminalnych[178]. Można wręcz zaryzykować tezę, iż współcześnie to właśnie stały monitoring różnego rodzaju

---

[176] T. Serafin, A. Hejduk, *Wywiad jawnoźródłowy w walce z terroryzmem na pograniczu afgańsko-pakistańskim*, „Ochrona Mienia i Informacji" 2012, nr 1, s. 68-72.

[177] M. Rachid-Chehab, *Eliot Higgins. Człowiek, który przyłapał Putina* [w:] http://wyborcza.pl/magazyn/1,143016,17300814,Eliot_Higgins__Czlowiek__ktory_przylapal_Putina.html [dostęp: 2 lutego 2015].

[178] K. Radwaniak, P.J. Wrzosek, *Biały wywiad w Policji…*, s. 137.

serwisów aukcyjnych stanowi jedną z podstawowych metod walki z paserstwem. Oczywiście, tego typu działania mogą podlegać daleko idącej automatyzacji, dzięki usługom takim jak np. ScraperBandit.com, pozwalającym na skanowanie wybranych fragmentów sieci (np. serwisów aukcyjnych, forów internetowych czy grup dyskusyjnych) pod kątem wybranych fraz (np. hasła „dopalacze").

Wymienione powyżej portale i serwisy dają ogromne możliwości w zdobywaniu każdego rodzaju informacji. Prawdziwą kopalnią wiedzy jest jednak wspomniany już wcześniej głęboki internet. Już według szacunków z 2007 roku dysproporcja pomiędzy nim a powszechnie używaną częścią sieci była ogromna. W ukrytym internecie znajdowało się ok. 550 miliardów stron, zaś w powierzchniowej jego części – zaledwie 1 miliard. Warto jednocześnie zaznaczyć, że powiększanie się głębokiego internetu jest szybsze niż jego powierzchni. Nawet podstawowe umiejętności dają ogromne możliwości – szacuje się bowiem, że 97,4 proc. informacji w ukrytym internecie dostępne jest publicznie bez haseł i dodatkowych opłat, a tylko 1,6 proc. z częściowymi ograniczeniami, zaś 1,1 proc. po zarejestrowaniu[179]. Oznacza to, że przy zastosowaniu odpowiedniego oprogramowania oraz technik wyszukiwania informacji możliwe jest dotarcie do informacji niedostępnych dla standardowego użytkownika. Warto również dodać, że dane pochodzące z głębokiego internetu mogą być niezwykle cenne z puntu widzenia wywiadowczego.

Omawiając głęboki internet, nie sposób pominąć problemu anonimowego poruszania się po nim oraz dostępu do treści nielegalnych. Istnieje kilka sposobów pozwalających na takie działanie, jednak niewątpliwie najprostszym i najpopularniejszym sposobem jest wykorzystanie sieci TOR (skrót od ang. *The Onion Router*). Jest to wirtualna sieć komputerowa implementująca trasowanie cebulowe[180] drugiej generacji. Zapobiega ona analizie ruchu sieciowego i w konsekwencji zapewnia użytkownikom prawie anonimowy dostęp do zasobów internetu. Działa od 2004 roku. Na podobnej zasadzie działają sieci I2P, Freenet, GNUnet czy MUTE. Analogicznie do

[179] D. Mider, *Partycypacja…,* s. 196-197.

[180] Trasowanie cebulowe (ang. *onion routing*) technika służąca anonimowej komunikacji w sieci komputerowej. Polega ona na wielokrotnym szyfrowaniu wiadomości, a następnie przesyłaniu jej przez szereg węzłów zwanych routerami cebulowymi (ang. *onion routers*). Każdy z nich usuwa warstwę szyfrowania w celu uzyskania informacji o dalszym trasowaniu i przesyła dane do następnego routera. Takie działanie zapobiega ujawnieniu węzłom pośredniczącym pochodzenia, odbiorcy oraz treści wiadomości. Począwszy od 2008 roku sieć Tor dominuje w wykorzystywaniu tej technologii. Technologię opracowali i wprowadzili specjaliści związani z amerykańską marynarką wojenną, mając na celu stworzenie narzędzia umożliwiającego anonimową łączność poprzez internet. Zob.: Ł. Kaniewski, *Drugie dno Internetu*, „Focus", nr (220) 1/2014, s. 25.

nich TOR może być wykorzystywany w celu ominięcia mechanizmów filtrowania treści, cenzury i innych ograniczeń komunikacyjnych. Tym samym jest to świetne narzędzie do zbierania informacji unikatowych, niedostępnych z poziomu zwykłej wyszukiwarki internetowej.

Korzystanie z TOR-a pozwala na anonimowe przeglądanie i umieszczanie w sieci dowolnych treści. Szczególnie ciekawie prezentują się fora dyskusyjne, na których swoje poglądy, nawet te niezgodne z prawem, może wygłosić każdy. Można więc znaleźć zarówno wątki dotyczące polityki, jak również technik dokonywania przestępstw i pozyskiwania broni czy narkotyków. Co ważne, większość stron w tym ciemnym obszarze głębokiego internetu prowadzona jest w języku angielskim, ale ze względu na liczbę użytkowników pochodzących z naszego kraju język polski zaliczany jest do czołówki. Ułatwia to zapoznanie się ze specyfiką TOR-a, ale również usprawnia wyszukiwanie stron oraz forów. Co i tak nie jest proste, gdyż w przestrzeni tej nie funkcjonuje Google. Dotychczas sieć TOR nie posiadała wyszukiwarki porównywalnej do tej stworzonej w Kalifornii, jednakże istnieją rozwiązania i witryny, które pomagają w znalezieniu interesujących nas informacji (np. Torgle, Torch, The Abyss). Korzystanie z sieci TOR nie jest skomplikowane. Wystarczy ściągnąć specjalne oprogramowanie z oficjalnej strony projektu (www.torproject.org). Kolejnym krokiem jest odwiedzenie witryny The Hidden Wiki, która z powodzeniem wprowadzi początkującego użytkownika w świat głębokiego internetu. Co ważne, znaleźć tam można linki do popularnych stron w anonimowej części głębokiej sieci, jak również dowiedzieć się, czym charakteryzuje się ten obszar. Użytkownicy TOR-a mogą korzystać z hostingu (tzn. przechowywania plików), założyć adres oraz dokonywać zakupów za pomocą Bitcoins (czyli specjalnej wirtualnej waluty stworzonej w 2009 roku). Strony ukryte za TOR-em pozwalają zapoznać się z gigantyczną ilością ciekawych i niecenzurowanych artykułów oraz multimediów. W zasadzie, przy odpowiednim nakładzie pracy oraz dostatecznym poziomie umiejętności, możliwe jest odnalezienie informacji na każdy temat. Penetrowanie ukrytego internetu za pomocą TOR-a przypomina popularną wśród infobrokerów technikę „zbierania jagód", czyli wgłębianie się w pewien temat, przy czym odwiedzenie danej strony determinuje naszą kolejną decyzję o wejściu do kolejnego portalu[181]. Daje to więc niemal nieograniczone możliwości w zdobywaniu przez nikogo niekontrolowanej i niecenzurowanej wiedzy.

[181] J. Daniel, *Tor: Ciemna strona Głębokiego Internetu* [w:] http://tdint.pl/jan-daniel/tor-ciemna-strona-glebokiego-internetu [dostęp: 16 lipca 2014].

8. Inne źródła

Oprócz wyżej wymienionych, najbardziej oczywistych i najpopularniejszych źródeł, w literaturze przedmiotu doszukać się można jeszcze innych kategorii. Nie są to jednak źródła typowo otwarte lub też pokrywają się częściowo z omówionymi już obszarami, więc ich wymienienie bezpośrednio w przedstawionej powyżej typologii byłoby metodologicznym nadużyciem. Można do nich zaliczyć m.in. grupy eksperckie czy też inżynierię odwrotną.

Intersującą techniką pozyskiwania informacji, zaliczaną niekiedy do białego wywiadu, jest tzw. inżynieria odwrotna (ang. *reverse engineering*), czyli proces badania produktu (urządzenia, programu komputerowego) w celu ustalenia, jak on dokładnie działa, a także w jaki sposób i jakim kosztem został wykonany. Samo pozyskanie produktu odbywa się zazwyczaj zgodnie z prawem, jednak analiza zawartości może naruszać już prawa autorskie lub patenty. W przypadku technologii informatycznych wejście w posiadanie nielicencjonowanego oprogramowania niekoniecznie wyklucza jego ogólnodostępny charakter. Dzieję się tak w wyniku daleko posuniętego piractwa komputerowego. Technika inżynierii odwrotnej może być wykorzystana także przy analizie różnego rodzaju urządzeń technicznych, pozyskanych zgodnie z prawem za granicą. Zdobyta w ten sposób wiedza może zostać wykorzystana we własnym przemyśle. Przykłady tego typu działań są szczególnie liczne, jeśli chodzi o przypadki nielicencjonowanego kopiowania broni czy prostszych urządzeń technicznych, niewymagających dokładnej dokumentacji produkcyjnej. Technika ta jest niezwykle przydatna, w szczególności na polu wywiadu naukowo-technicznego.

Niektórzy autorzy do otwartych źródeł informacji zaliczają również systemy eksperckie, których owocem są opracowania, raporty i różnego rodzaju analizy przywoływane już wcześniej przy okazji omawiania szarej literatury oraz informacji publicznej. Kategorie te wymieniane przez wybranych specjalistów jako odrębne otwarte źródło informacji[182]. Nie ulega wątpliwości, że planowa i systematyczna współpraca służb specjalnych z niezależnymi ekspertami, pracującymi na otwartych źródłach informacji, kryje w sobie, zwłaszcza w dzisiejszych czasach, olbrzymi potencjał. W ten sposób znacząco da się poprawić zdolności analityczne służb, w szczególności jeśli można oprzeć się na konsultantach posiadających bogate, unikalne doświadczenie (np. zdobyte w trakcie wieloletniego pobytu poza granicami kraju, a przekładające się na znakomitą

[182] K. Liedel, T. Serafin, *Otwarte źródła informacji…*, s. 72.

znajomość nie tylko danego języka, ale także podłoża kulturowego, społecznego czy politycznego badanego problemu)[183].

W tym kontekście za odrębne źródło informacji można uznać również raporty, opracowania i innego rodzaju materiały tworzone na zamówienie wszelkiego rodzaju komercyjnych podmiotów, fundacji oraz stowarzyszeń, zajmujących się szeroko pojętą analizą informacji. Przykładami instytucji tego typu, wymienianych najczęściej w anglojęzycznej literaturze przedmiotu, są m.in. Factiva, Lexis-Nexis, Dialog, Economist Intelligence Unit czy też Oxford Analytica[184].

***

Stworzenie pełnej i zarazem całkowicie rozłącznej typologii wszystkich współczesnych otwartych źródeł informacji wydaje się niewykonalne. Jest to spowodowane, niezwykłą dynamiką zmian, wywołaną rewolucją w dziedzinie technologii cyfrowych. Niektóre źródła zyskują cyfrowy charakter i w mniejszym lub większym stopniu są przenoszone do internetu, inne tracą na znaczeniu lub znacząco zmieniają swój charakter, kształt i specyfikę. Nie ulega jednak żadnej wątpliwości, iż współcześnie najistotniejszym z nich stał się właśnie internet. Co więcej, wraz z coraz szybszym rozwojem technologii informatycznych jego waga w procesie wymiany i wyszukiwania informacji stale rośnie. Niemniej jednak jest to źródło problematyczne. Aby w pełni korzystać z jego dobrodziejstw (zwłaszcza z głębokiego internetu) konieczne jest posiadanie specjalistycznej wiedzy na temat technik jego przeszukiwania. Dzięki takim umiejętnościom każdy analityk zyskuje możliwość działania z nieporównywalnie większą wydajnością i skutecznością, gdyż wkładając w wyszukiwanie danych minimalny wysiłek, niewymagający nawet odchodzenia od komputera, może uzyskać niezwykle cenne i unikatowe informacje. Warto również zwrócić uwagę na fakt, że zasoby zawarte w cyberprzestrzeni nieustannie się rozrastają, zaś technologie wspomagające ich przetwarzanie są ustawicznie udoskonalane, dlatego też potencjał, który tkwi w internecie rozumianym jako źródło informacji wydaje się w zasadzie nieograniczony.

Mimo dobrodziejstw, które niesie ze sobą internet, do znacznej części informacji uzyskanych za jego pośrednictwem należy podchodzić zawsze z pewną rezerwą. W przeciwieństwie bowiem do tradycyjnych otwartych

[183] G. Hribar, I. Podbregar, T. Ivanuša, *OSINT: A "Grey Zone"?,* "International Journal of Intelligence and CounterIntelligence" 2014, vol. 27, issue 3, s. 532-533.

[184] H. Minas, *Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century?,* "RIEAS: Research Paper", No. 139 (January 2010), s. 12-13.

źródeł, informacjom pochodzącym z forów internetowych czy blogów częstokroć brakuje nawet wstępnej i elementarnej weryfikacji oraz redakcji, czego powiedzieć nie można o prasie, literaturze czy radiu i telewizji. Dlatego też źródła tradycyjne nadal wydają się niezwykle przydatne z punktu widzenia wywiadowczego, zaś obecna dwoistość ich natury (tradycyjna i cyfrowa) czyni ich analizę wygodniejszą i skuteczniejszą.

Trzeba podkreślić, że rewolucja w dziedzinie technologii cyfrowych ostatecznie rozwiązała także problem gromadzenia informacji w niewystarczająco pojemnych i rozproszonych archiwach. Dziś niemal wszystko trafia do sieci i już tam zostaje – wystarczy więc posiadać jedynie wiedzę i odpowiednie narzędzie, aby odnaleźć poszukiwane dane. Problem odległości i fizycznych ograniczeń przesyłanych informacji w dobie, kiedy na jednym pendrivie można pomieścić tyle informacji, ile jeszcze kilkanaście lat temu trzeba by transportować paroma wagonami kolejowymi, przestał więc mieć jakiekolwiek znaczenie.

Niemały wpływ na znaczące powiększenie się liczby otwartych źródeł informacji ma również coraz silniej promowana w administracji publicznej kultura jawności i otwartości. Zasadą jest, że dane publiczne powinny być udostępniane wszystkim zainteresowanym, zaś nakaz transparentności stał się fundamentem większości współczesnych państw demokratycznych. Dzięki tym zasadom oraz powszechnemu systemowi edukacji skala wykorzystania wszystkich powyżej wymienionych otwartych źródeł informacji wzrosła znacząco.

Rozdział IV

Wybrane obszary wykorzystania otwartych źródeł informacji

1. Biały wywiad w sektorze prywatnym

Jak już wspomniano wcześniej, zorganizowane i planowe wykorzystanie metody białego wywiadu w sektorze prywatnym sięga pierwszej połowy XIX wieku. Firmy prywatne, w przeciwieństwie do służb i instytucji państwowych, nigdy nie dysponowały specjalnymi uprawnieniami w zakresie pozyskiwania informacji. Właśnie ten czynnik spowodował, że każde przedsiębiorstwo chcące działać w granicach prawa, było zmuszone respektować zasadę traktowania jako podstawy opisanych wcześniej otwartych i ogólnie dostępnych źródeł informacji. Istnienie firm zajmujących się komercyjnym pozyskiwaniem i analizą informacji nie jest więc rzeczą nową. Niemniej jednak w ciągu ostatnich dwóch dekad na całym świecie obserwować można niezwykle dynamiczny rozwój tego sektora. Jest to spowodowane przynajmniej kilkoma czynnikami, z których za najważniejsze uznać można rewolucję w dziedzinie technologii informacyjnych, postępujący proces globalizacji oraz znaczący wzrost znaczenia zagrożeń asymetrycznych (takich jak np. międzynarodowy terroryzm).

W takich okolicznościach trudno dziwić się więc postępującej prywatyzacji działalności wywiadowczej, w której z kolei wyodrębnić można zasadniczo dwa zjawiska. Po pierwsze – rozwój prywatnych usług wywiadowczych, czyli tzw. outsoursing wywiadowczy. Po drugie – rozwój autonomicznych struktur wywiadu biznesowego w korporacjach transnarodowych oraz większych przedsiębiorstwach[185]. Wśród firm specjalizujących się w komercyjnym pozyskiwaniu informacji wyróżnić można przynajmniej kilka gałęzi wywiadu działającego na potrzeby sektora prywatnego. Do pierwszej i najbardziej rozbudowanej z nich zaliczyć można wywiad, który

[185] M. Ciecierski, *Wywiad biznesowy w korporacjach transnarodowych. Teoria i praktyka*, Toruń 2009, s. 26.

określić można mianem gospodarczego, konkurencyjnego czy też biznesowego (ang. *competitor intelligence, competitive intelligence, marketing intelligence*). Podmioty działające w tym obszarze ukierunkowane są głównie na zbieranie informacji o konkretnych spółkach i przedsiębiorstwach będących konkurencją bądź przyszłym partnerem dla zleceniodawcy. W Polsce firmy należące do tego segmentu nazywane są zazwyczaj wywiadowniami gospodarczymi, zaś podstawowymi źródłami, z jakich czerpią informacje, są ogólnodostępne rejestry i bazy danych. W tym kontekście trzeba zauważyć, że niezwykle dynamicznie rozwijającą się niszą w tym obszarze jest tzw. analityka biznesowa (ang. *business intelligence*). W tym wypadku trudno mówić jednak o pełnym zastosowaniu metody białego wywiadu, gdyż jest to raczej narzędzie menadżerów i specjalistów zajmujących się analizami ilościowymi i strategią przedsiębiorstw. Co prawda, informacje gromadzone w tzw. hurtowniach danych (ang. *data warehouse*) pochodzą również w części ze źródeł otwartych, jednak nie jest to regułą. Tego typu systemy wspierania decyzji kadry zarządzającej są zazwyczaj oparte na rozbudowanych informatycznych narzędziach zarządzania wiedzą, eksploracji danych oraz aplikacjach analitycznych, służących do wielowarstwowej analizy, interpretacji oraz zautomatyzowanej wymiany informacji (ang. *OnLine Analytical Processing* – OLAP)[186]. Za gałąź wywiadu komercyjnego, w której wykorzystanie klasycznie rozumianych otwartych źródeł informacji jest znacznie szersze, można bez wątpienia uznać działalność międzynarodowych firm specjalizujących się w tworzeniu analiz wywiadowczych na poziomie strategicznym. To właśnie z podmiotami tego typu współpracuje obecnie wiele rządowych służb wywiadowczych, zaś na ich potencjale opiera się w znacznej mierze wywiadowczy outsoursing, na najwyższym, strategicznym poziomie. Analizując obszar komercyjnego wykorzystania metody białego wywiadu, należy zwrócić także uwagę na oficjalne wyodrębnienie się kategorii tzw. infobrokeringu, a więc segmentu usług mających swój rodowód w bibliotekoznawstwie, a polegających na wyszukiwaniu, ocenie, selekcji, analizie i udostępnianiu informacji na zlecenie.

1.1. Wywiadownie gospodarcze

Analizując wykorzystanie białego wywiadu poza sektorem publicznym, niewątpliwie należy zacząć właśnie od wywiadowni gospodarczych. Po pierwsze – dlatego że z zasady czerpią dane ze źródeł otwartych, po drugie – ze względu na fakt, iż same w sobie stanowią jedno z podstawowych i najbardziej efektywnych źródeł informacji. Sam wywiad gospodarczy zdefiniować

[186] J. Surma, *Business Intelligence*, Warszawa 2009, s. 12-13.

można jako działalność polegającą na uzyskiwaniu, przetwarzaniu i udostępnianiu informacji dotyczących sytuacji prawnej, kadrowej, handlowej, finansowej i ekonomicznej przedsiębiorstw na zlecenie innych podmiotów gospodarczych w celu szacowania ryzyka współpracy, zdobywania przewagi konkurencyjnej i unikania strat lub odzyskiwania należności. Co ważne, wywiad gospodarczy należy odróżnić od szpiegostwa, przez które rozumie się próbę uzyskania dostępu do tajnych informacji przy użyciu prawnie niedozwolonych środków. Co do zasady wywiadownie gospodarcze korzystają bowiem z jawnych źródeł informacji oraz legalnych metod ich pozyskiwania (przestrzegając prawa i etyki zawodowej)[187].

Jak już wspomniano, wyspecjalizowane instytucje zajmujące się wywiadem gospodarczym potocznie zwane są w Polsce wywiadowniami gospodarczymi (ang. *consumer reporting agency* lub *credit reference agency*). Ich działalność opiera się głównie na odpłatnym pozyskiwaniu informacji dotyczących sytuacji gospodarczej przedsiębiorstw oraz sprawdzaniu wiarygodności i wypłacalności partnera w interesach. Wywiadownia gospodarcza na zlecenie przygotowuje raporty gospodarcze (handlowe, o płynności finansowej firm), których celem jest zminimalizowanie ryzyka związanego ze współpracą z niesolidnym przedsiębiorcą. Raporty gospodarcze mogą zawierać również analizę danych firmy na tle branży, powiązania tej firmy z innymi podmiotami lub osobami, a także wskaźnik prawdopodobieństwa upadku czy indeks zdolności płatniczej. Wywiadownie gospodarcze pozyskują dane przede wszystkim z rejestrów sądowych, ewidencji dotyczących przedsiębiorców, publikatorów urzędowych, periodyków oraz katalogów branżowych[188]. Innymi, często wykorzystywanymi typami źródeł, są ankiety wysyłane do wypełnienia przedsiębiorcom oraz dane z kwerendy wycinków prasowych i publikacji internetowych. Niektóre wywiadownie w ramach tzw. poszerzonych raportów oferują także przeprowadzenie wizji lokalnych czy nawet usługi detektywistyczne, niemniej jednak są to działania daleko odbiegające od standardowych[189].

Na rynku, zarówno polskim, jak i międzynarodowym, działa co najmniej kilkadziesiąt wywiadowni, które oferują zróżnicowany poziom oraz katalog usług. Najbardziej rozpowszechnione są wywiadownie internetowe, oferujące raporty opłacane przelewem lub tzw. mikropłatnościami przez telefon komórkowy. Ich cena waha się od kilku do kilkudziesięciu złotych, co zazwyczaj

---

[187] L. Korzeniowski, A. Pepłoński, *Wywiad gospodarczy. Historia i współczesność*, Kraków 2005, s. 85-89.

[188] Ibidem, s. 200-212.

[189] P. Niemczyk, *Wywiadownie gospodarcze jako źródło informacji „białego wywiadu"*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9 (5), s. 149.

ma związek z jakością analizy. Dlatego też staranność, aktualność i kompletność tego typu opracowań bywa bardzo różna. Jeżeli więc poszukiwane informacje mają służyć rozwiązaniu poważnego problemu, to warto poszukać sprawdzonej wywiadowni. Na polskim rynku ugruntowaną pozycję mają w zasadzie trzy firmy. Największy zasięg ma międzynarodowa korporacja pochodzenia amerykańskiego. Dwie pozostałe powstały w Europie i mają niemieckie oraz francuskie korzenie. Jedną z najważniejszych zalet tych przedsiębiorstw jest to, że gromadząc informacje w sposób permanentny i globalny, mają w swoich bazach danych rekordy o dziesiątkach milionów firm i mogą te informacje udostępniać online lub też (w przypadku raportów aktualizowanych na zamówienie) w kilkudniowym terminie. Jest to czynnik, który powoduje, że usługi wywiadowni gospodarczych mogą być z dużym powodzeniem wykorzystywane przez państwowe służby i instytucje zajmujące się bezpieczeństwem. Dzięki temu możliwe jest zaoszczędzenie czasu i pracy wielu funkcjonariuszy. Tak więc raporty wywiadowni są szczególnie przydatne w sytuacjach, gdy analitycy działają pod presją czasu, zaś terminy oddania raportów nie pozwalają na samodzielne zebranie informacji. Przy takim scenariuszu w ten sposób dostarczony materiał może trafnie wskazać punkty wyjścia do dalszych poszukiwań[190].

Ponadto warto podkreślić, że wiele firm, zwłaszcza międzynarodowych, doceniając szczególne znaczenie informacji gospodarczej w zarządzaniu przedsiębiorstwem, posiada w swoich strukturach własne komórki wywiadu gospodarczego, choć często nie są tak wprost nazywane. Najczęściej umieszcza się je w działach marketingu, badań i rozwoju, informacji zarządczej lub strategicznej, prawnych, sprzedaży, public relations i oczywiście – bezpieczeństwa korporacyjnego[191]. Na przestrzeni lat wywiad gospodarczy bardzo się rozwinął i z prymitywnej formy zdobywania pojedynczych informacji przekształcił się obecnie w wyrafinowany proces zaawansowanych analiz, skomplikowanych metod i technik, przeprowadzany przez zespoły wyselekcjonowanych specjalistów, skupionych w koncernach bądź mniejszych firmach. Polski rynek usług wywiadu gospodarczego, według danych na 2013 r., wyceniany był na około 100 mln zł. Ponadto w ostatnim czasie pojawiło się także kilka znaczących portali internetowych, oferujących usługi w omawianym zakresie, co jest niewątpliwie owocem coraz wyższego stopnia digitalizacji informacji gospodarczych[192].

---

[190] Ibidem, s. 148.

[191] *Historia wywiadu gospodarczego. Część 2.* [w:] http://www.paulo.pl/hwg2.html [dostęp: 30 sierpnia 2014].

[192] T. Starzyk, *Wywiadownie gospodarcze stosują biały wywiad*, „Gazeta Finansowa Online", 27 sierpnia 2012 [w:] http://www.gf24.pl/9344/wywiadownie-gospodarcze-stosuja-bialy-wywiad [dostęp: 4 sierpnia 2014].

1.2. Wywiad strategiczny w sektorze prywatnym

Obok wywiadowni gospodarczych na rynku działają również dużo bardziej rozbudowane prywatne agencje wywiadowcze (ang. *global information companies*), zajmujące się pozyskiwaniem i analizą informacji o charakterze strategicznym. Największe z nich posiadają narzędzia i środki umożliwiające działanie na skalę globalną. Taki zasięg powoduje, iż firmy te coraz częściej stają się partnerami dla rządowych agencji wywiadowczych i administracji poszczególnych państw. Korporacje tego typu z punktu widzenia omawianego zagadnienia można postrzegać dwojako. Z jednej strony niemal całość informacji przez nie pozyskiwana pochodzi ze źródeł otwartych (oczywiście z wyłączeniem ich własnych systemów MASINT i SIGINT). Z drugiej zaś ich komercyjnie oferowane analizy są jednym z istotniejszych źródeł dla instytucji państwowych.

Przykładem takiej agencji jest założony w 1959 roku koncern IHS, zatrudniający ponad 8 tys. ludzi (w tym 2 tys. tzw. „reporterów") w 31 krajach i świadczący usługi wywiadowcze oraz doradcze w dziedzinach takich, jak np. obronność, energetyka, komunikacja czy finanse[193]. Jedną z jego głównych i najlepiej rozpoznawalnych marek jest wspominana już wcześniej brytyjska Jane's Information Group, której początki sięgają roku 1898. To właśnie ta firma jest obecnie jednym z najbardziej znanych, prywatnych przedsiębiorstw zajmujących się białym wywiadem w dziedzinach szczególnie istotnych dla bezpieczeństwa większości współczesnych państw. Prowadzi ona również bardzo rozległą działalność wydawniczą, zaś oferowane tytuły stanowią jedno z podstawowych źródeł informacji wśród wielu służb specjalnych na świecie[194]. Inną globalnie działającą korporacją o podobnym profilu jest amerykański Stratfor, założony w 1996 w USA przez George'a Friedmana. Firma zajmuje się opracowywaniem różnego rodzaju analiz i raportów na potrzeby klientów prywatnych, a także niektórych agend rządu Stanów Zjednoczonych (w tym także dla CIA). Najwyżej cenionym produktem agencji jest raport dzienny (ang. *daily intelligence briefing*), stanowiący niekiedy jedno z podstawowych źródeł informacji o zagrożeniach bezpieczeństwa światowego[195]. Stratfor często bywa nazywany

---

[193] *About IHS* [w:] http://www.ihs.com/about/index.aspx [dostęp: 30 sierpnia 2014].

[194] Wśród nich są również służby polskie, tygodnik „Jane's Defence Weekly" to jedno z powszechniej używanych źródeł informacji w Centrum Analiz ABW. Zob.: B. Święczkowski, *Wykorzystanie tzw. białego wywiadu w działalności analityczno-informacyjnej Agencji Bezpieczeństwa Wewnętrznego* [w:] W. Filipowski, W. Mądrzejowski (red.) *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki,* Warszawa 2012, s. 174.

[195] *About Stratfor* [w:] http://www.stratfor.com/about#axzz3AUlNMJxT [dostęp: 30 sierpnia 2014].

cieniem CIA, co dosyć dobrze obrazuje skalę, zakres i możliwości działania tej firmy.

Potencjał ten jest szeroko wykorzystywany przez rządy wielu państw. Fakt tzw. outosourcingu usług wywiadowczych nie jest zjawiskiem nowym i wpisuje się dosyć mocno w globalny trend gwałtownego rozwoju sektora usług militarnych i bezpieczeństwa. Jeszcze w okresie zimnej wojny w celu wsparcia rządowych agencji wywiadowczych w USA do systemu bezpieczeństwa narodowego włączono wiele korporacji z sektora prywatnego. Na polu monitorowania łączności zagranicznej czy dostarczania technologii do interpretacji danych wykorzystano m.in. możliwości potentatów takich jak IBM. Obecnie prywatne przedsiębiorstwa wywiadowcze wykorzystywane są do realizacji bardzo wielu zadań wywiadowczych – od gromadzenia informacji pochodzących z wywiadu satelitarnego, przez usługi analityczne i dystrybucję informacji, do różnych instytucji państwowych[196].

Współcześnie tylko nieliczne służby wywiadowcze są w stanie utrzymywać własne systemy wywiadu elektronicznego i satelitarnego, w szczególności takie, które są w stanie działać w skali globalnej. Reszta zmuszona jest do wzajemnej współpracy (zwłaszcza w ramach organizacji międzynarodowych takich, jak np. NATO) oraz korzystania z danych dostarczanych przez firmy prywatne. Taki system pozyskiwania informacji to w dzisiejszych czasach ekonomiczna konieczność, wymuszona niezwykle dynamicznie postępującym rozwojem nowoczesnych technologii cyfrowych oraz gigantycznymi kosztami nieustannych modernizacji posiadanego sprzętu oraz systemów. Za tym postępem technologicznym nie nadążają jednak, zazwyczaj skąpe, budżety służb wywiadowczych mniejszych krajów. Pełne korzystanie z najnowszych zdobyczy techniki w dziedzinie wywiadu wymaga więc siłą rzeczy szerokiej współpracy między sektorem prywatnym i administracją państwową. Dodatkową tego zaletą jest znacznie większa elastyczność i szybkość pozyskiwania informacji w nieobjętych państwowymi procedurami, prywatnych agencjach wywiadowczych[197].

1.3. Infobrokering

Analizując problem coraz szerszego wykorzystania otwartych źródeł informacji, nie sposób nie dostrzec wyodrębnienia się nowego obszaru usług komercyjnych, kojarzących się do tej pory z informacją naukową oraz bibliotekoznawstwem. To właśnie na gruncie tych nauk narodziła się idea

[196] M. Ciecierski, *Wywiad biznesowy…*, s. 27.

[197] H. Bean, *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence*, Santa Barbara–Denver–Oxford 2011, s. 147-149.

infobrokeringu. Pojęcie infobrokeringu (czy też – infobrokerstwa) ma ścisły związek z gwałtownym przyrostem ilości informacji, a przede wszystkim ze wzrostem dostępności źródeł cyfrowych. Infobroker (od ang. *information brokering*, istnieją również inne anglojęzyczne nazwy tej profesji takie, jak np. *Knowledge broker, Data dealer, Independent information professional, Researcher*)[198] to nic innego jak specjalista w dziedzinie białego wywiadu. Z kolei według polskiego *Krajowego standardu kompetencji zawodowych* broker informacji (researcher) to zawód o charakterze usługowym, polegający na wyszukiwaniu, ocenie, selekcji, analizie i udostępnianiu informacji na zlecenie. Pełni on rolę pośrednika pomiędzy poszukującymi informacji a zasobami informacyjnymi (tj. mediami, bibliotekami, zasobami internetowymi itp.). Dostarczone przez brokera informacje muszą odnosić się do przedmiotu zlecenia i cechować się wysoką jakością, popartą wiarygodnymi źródłami[199]. Co ważne, informacja ta musi być pozyskana legalnie i może pochodzić tylko i wyłącznie ze źródła jawnego (choć niekoniecznie łatwego w eksploracji)[200]. W profesji tej występować może specjalizacja w zależności od rodzaju dostarczanej informacji, np. broker informacji biznesowej lub informacji prawniczej. Brokerzy informacji coraz częściej pracują w różnego rodzaju instytucjach, fundacjach, stowarzyszeniach i prywatnych przedsiębiorstwach, gdzie informacja odgrywa ważną rolę, mimo że firmy te nie są określone jako infobrokerskie. Informacje dostarczane przez brokera są wykorzystywane bezpośrednio przez zamawiającego lub mogą być poddawane dalszemu opracowaniu. Wedle wytycznych ministerialnych wykonywanie tego zawodu wymaga spostrzegawczości oraz umiejętności analizy i syntezy pozyskanych danych. Infobrokera powinna cechować więc dokładność, rzetelność, dbałość o szczegóły oraz posiadanie wiedzy z zakresu sposobów pozyskiwania informacji oraz umiejętności jej wartościowania[201]. Co interesujące, wedle powyższych zaleceń, zawód brokera informacji może wykonywać osoba, która ukończyła studia wyższe drugiego stopnia z zakresu informacji naukowej i bibliotekoznawstwa lub pokrewne kierunki. Istnieje również możliwość ukończenia studiów podyplomowych (kierunek: broker informacji, infobrokering, zarządzanie informacją lub pokrewne).

---

[198] A. Król, *Broker informacji – powstawanie nowego zawodu*, „Zagadnienia Naukoznawstwa" nr 1 (159), s. 73.

[199] *Broker informacji (researcher) (262204), Krajowy standard kompetencji zawodowych,* Centrum Rozwoju Zasobów Ludzkich Ministerstwa Pracy i Polityki Społecznej, Warszawa 2013, s. 6. [w:] http://nomad.pjwstk.edu.pl/AppData/Files/77_262204_broker_informacji_researcher.pdf [dostęp: 12 lipca 2014].

[200] A. Walczuk-Niewiadomska, G. Czapnik, Z. Gruszka, *Brokerstwo informacyjne w Polsce – przegląd publikacji*, „Acta Universitatis Lodziensis. Folia historica" 2013, nr 17, s. 217.

[201] *Broker informacji (researcher)…,* s. 6-7.

Jak więc widać, infobroker to nikt inny jak swego rodzaju „biały wywiadowca" działający z wolnej stopy i oferujący swoją wiedzę i doświadczenie podmiotom, którym potrzebna jest w danej chwili jakaś konkretna informacja. Co ważne, nie ma znaczenia zakres przedmiotowy skierowany do infobrokera – w przeciwieństwie do wywiadowni gospodarczych firmy infobrokerskie są dużo słabiej sprofilowanymi i wszechstronniejszymi strukturami. Nie bez znaczenia jest również rodowód tego zawodu, odwołujący się do bibliotekoznawstwa i z tej właśnie nauki czerpiący metody i techniki wieloetapowego pozyskiwania, weryfikacji oraz analizy informacji[202].

Symboliczną datę powstania tej profesji stanowi rok 1987, w którym powołano w USA stowarzyszenie AIIP – Association of Independent Information Professionals, zrzeszające obecnie brokerów informacji z całego świata[203]. W Polsce pierwsi infobrokerzy rozpoczęli działalność w latach '90-tych XX wieku, wtedy to nastąpiło szersze zainteresowanie tym zawodem i samą ideą komercyjnego zdobywania informacji[204]. Powstało kilkadziesiąt firm infobrokerskich, opracowano specjalistyczne serwisy internetowe, poszerzyła się oferta edukacyjna w omawianej dziedzinie, a także pojawiła się inicjatywa powołania polskiego Stowarzyszenia Brokerów Informacji[205].

Przy obecnym natłoku danych oraz wielości ich źródeł broker informacji często uznawany jest za zawód przyszłości – idealnego pośrednika między zasobami informacji a ludźmi i instytucjami, którzy ich potrzebują. O ile bowiem wyszukiwanie, nawet specjalistycznych danych, nie wydaje się trudne, o tyle ich prawidłowa ocena, selekcja oraz szybkie opracowanie w przystępny sposób wymaga już wszechstronnej wiedzy i bogatego warsztatu. Nic więc dziwnego, że z założenia infobroker posługuje się w swej profesji nowoczesnymi narzędziami informatycznymi oraz wszelkimi dostępnymi technologiami informacyjno-komunikacyjnymi. Informacja dostarczana przez brokerów informacji może mieć bardzo różny charakter – bibliograficzno-dokumentacyjny, analityczny, referencyjny, czy też statystyczny. Dlatego też zawód ten przyrównywany jest często do profesji menadżera zarządzającego wiedzą, dostarczającego potrzebnych informacji w czasie rzeczywistym, wspierającego procesy decyzyjne w organizacji[206].

---

[202] S. Cisek, *Broker informacji: istota zawodu*, [w:] http://eprints.rclis.org/bitstream/10760/10880/1/Cisek_ broker_informacji_istota.pdf [dostęp: 14 sierpnia 2014].

[203] *About AIIP* [w:] http://www.aiip.org/content/about-aiip [dostęp: 12 sierpnia 2014].

[204] J. Byrska, *Przyszłość należy do łowców informacji. Nowe multimedialne zawody*, „Gazeta Wyborcza", dod. „Komputery i Biuro" 1996, nr 38, s. 14.

[205] S. Cisek, *Infobrokering w praktyce: zasady wyszukiwania informacji w Internecie* [w:] http://eprints.rclis.org/18457/1/Cisek_infobrokering_internet.pdf [dostęp: 12 sierpnia 2014].

[206] *Infobrokering systemowy* [w:] http://www.studiapodyplomowe.eu/p2/index.php/kierunki/biznes-it/infobrokering-biznesowy [dostęp: 30 sierpnia 2014].

Omawiając sylwetkę infobrokera, warto również wspomnieć, o jeszcze jednej grupie specjalistów z tego obszaru, której rodowodu szukać należy nie tyleż w bibliotekoznawstwie, co w informatyce śledczej. Szybko ewoluujące technologie i szerokie spektrum zastosowań technik wywiadu jawnoźródłowego, zaowocowały wytworzeniem nowych, stosunkowo niedrogich w wykorzystaniu, metod gromadzenia oraz analizowania informacji. W tym kontekście na wyróżnienie zasługuje spory wkład do instrumentarium wywiadowcy specjalistów od informatyki (a w szczególności z zakresu bezpieczeństwa sieci oraz testów penetracyjnych). Dlatego metody i narzędzia rekonesansu oraz profilowania wykorzystywane do optymalizacji symulowanych ataków na sieci komputerowe, aplikacje internetowe lub działań socjotechnicznych, spełniają dziś komplementarne funkcje w procesie gromadzenia i ewaluacji danych jawnoźródłowych zarówno w działalności podmiotów państwowych jak i prywatnych[207].

2. Biały wywiad w sektorze publicznym

Obecnie otwarte źródła informacji są stosunkowo szeroko wykorzystywane we wszystkich instytucjach państwowych, nawet w strukturach niepełniących wąsko rozumianej funkcji wywiadowiczej. Dzieje się tak, gdyż dzięki rewolucji w dziedzinie technologii informacyjnych dostęp do znacznej liczby źródeł informacji, dających możliwość bezpośredniego wsparcia procesu decyzyjnego, stał się niezwykle prosty, szybki i wygodny. Głównymi beneficjentami zmian technologicznych stały się oczywiście podmioty nieposiadające specjalnych uprawnień w zakresie pozyskiwania informacji. Wśród nich wymienić można zarówno wszystkie urzędy administracji publicznej, jak i ściśle sprofilowane ośrodki analityczne. Niemniej jednak również instytucje takie, jak policja czy służby specjalnie, już wcześniej wykorzystujące metodę białego wywiadu, bardzo skorzystały na zmianach związanych z szerokim zastosowaniem nowych technologii w działalności wywiadowczej. Podobnie jak w przypadku sektora prywatnego, bez wahania postawić można tezę, iż rewolucja w dziedzinie technologii informacyjnych i pojawienie się internetu w znaczący sposób przedefiniowało podejście do białego wywiadu w sferze publicznej i spowodowało zauważalny wzrost wykorzystania otwartych źródeł informacji.

[207] M. Meller, *Open Source Intelligence* [w:] http://edu.opensourceintelligence.pl/0-wprowadzenie/1-open-source-intelligence [dostęp: 20 maja 2015].

2.1. Biały wywiad w służbach specjalnych

Służby specjalne, zwłaszcza te o profilu czysto wywiadowczym (informacyjnym), to instytucje korzystające ze wszystkich możliwych źródeł informacji, w tym również jawnych i ogólnodostępnych. Oczywiście wykorzystanie poszczególnych kategorii źródeł jest uzależnione w dużej mierze od specyfiki służby oraz zadań przez nią wykonywanych. Te, które zajmują się wywiadem (czy to cywilnym czy wojskowym), skupiają uwagę przede wszystkim na materiałach zawierających dane o wymiarze strategicznym (takie, jak np. informujące o sytuacji międzynarodowej, nastrojach społecznych w innych państwach czy nowych trendach w technice i strategii wojskowej oraz uzbrojeniu). Służby, których głównym zadaniem jest utrzymywanie szeroko pojętego bezpieczeństwa wewnątrz kraju, w otwartych źródłach informacji będą szukać głównie materiałów dotyczących obszaru wewnątrzpaństwowego (np. o nastrojach panujących wśród mniejszości etnicznych lub religijnych, doniesień o nieprawidłowościach w sferze publicznej czy aktywności ekstremistów). Ponadto każda ze służb wykorzystuje informacje ze źródeł otwartych, planując doraźną działalność operacyjną (np. korzystając z portali geoinformacyjnych czy opracowując uwiarygodniające legendy).

W polskim porządku prawnym nie funkcjonuje żadna oficjalna definicja pojęcia „służby specjalne". Formalnie za instytucje tego typu uznaje się pięć służb państwowych. Są to: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne[208]. Nie wszystkie z tych organów mieszczą się jednak w klasycznej definicji pojęcia, określającej służby specjalne jako zorganizowane przez państwo struktury, ukierunkowane na niejawne pozyskiwanie informacji istotnych z punktu widzenia bezpieczeństwa organizatora tej działalności (państwa) bądź przeciwdziałanie ich zdobywaniu przez podobne struktury, identyfikowane jako obce[209]. Nie każda ze służb, uznawana w Polsce za specjalną, zajmuje się tylko i wyłącznie pozyskiwaniem oraz ochroną informacji, dosyć wyraźnie wykraczając poza klasycznie rozumiany obszar wywiadu i kontrwywiadu. Takimi instytucjami są ABW oraz CBA, które metodami pracy oraz katalogiem uprawnień i zadań bliższe są bardziej organom policyjnym niż *stricte* wywiadowczym[210]. Fakt ten powoduje, że metodyka analizy oraz profil informacji zbieranych z otwartych źródeł informacji są w dużej mierze zbliżone to

[208] Ustawa z dnia 24 maja 2002 r. *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz. U. 2002 Nr 74 poz. 676) art. 11.

[209] S. Zalewski, *Służby Specjalne w państwie demokratycznym*, Warszawa 2005, s. 34.

[210] Z. Siemiątkowski, *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009, s. 32.

standardów panujących w polskiej policji. Inaczej jest w pozostałych trzech służbach, pozbawionych typowo policyjnych uprawnień dochodzeniowo-śledczych. Co ważne, brak owego instrumentarium, bardzo pomocnego w pracy typowo operacyjnej, pośrednio wymusza szersze i wnikliwsze wykorzystanie informacji pochodzących ze źródeł jawnych i ogólnodostępnych.

Organizacja komórek zajmujących się analizą informacji m.in. ze źródeł otwartych jest bardzo różna. W polskich służbach specjalnych nie występują odrębne, wyspecjalizowane zespoły analityczne, zajmujące się tylko i wyłącznie białym wywiadem. Najczęściej informacje, uzyskane na pewnym etapie analizy, weryfikowane są za pomocą zestawienia ich z zawartością niejawnych baz danych czy informacjami dotyczącymi danego zagadnienia uzyskanymi w drodze operacyjnej. Niemniej jednak znacząca część danych wykorzystywana przy analizie pochodzi właśnie ze źródeł otwartych. Większość amerykańskich specjalistów od spraw wywiadu ocenia, że ich odsetek wynosi średnio około 80 procent wszystkich wykorzystanych przy analizie informacji (w zależności od tematyki jest to od 40 do nawet 95 proc.)[211]. Sam odsetek funkcjonariuszy zajmujących się analizą informacji jest różny, w zależności od profilu służby, jej zadań oraz charakteru jej działania. W szeregach największych i najbardziej znanych zachodnich służb wywiadowczych liczba analityków jest znaczna[212]. Polskie służby wywiadowcze, mimo że zauważalnie mniej liczne od swoich zachodnich odpowiedników, również posiadają w swoich szeregach pewną liczbę specjalistów odpowiedzialnych za analizę informacji. Model organizacyjny struktur analitycznych nie jest w polskich służbach specjalnych jednolity. W Agencji Wywiadu strukturą odpowiedzialną za ten problem jest Biuro Informacji i Analiz[213]. Podobne struktury działają w ramach ABW (kiedyś Centrum Analiz, a obecnie Biuro Ewidencji i Analiz, czyli Biuro E)[214] oraz CBA (Departament Analiz)[215].

---

[211] A. Dupont, *Intelligence for the Twenty-First Century* [w:] W.K. Wark (ed.), *Twenty-First Century Intelligence,* London 2008, s. 26.

[212] Według danych z 2002 roku w Zarządzie Wywiadu amerykańskiej CIA pracowało ich ponad 1500, zaś w brytyjskiej SIS (potocznie znanej pod nazwą MI6) ok. 700-800. Dane te zapewne już dawno nie są aktualne, gdyż już od wielu lat, na całym świecie zauważalna jest ciągła i systematyczna rozbudowa pionów analitycznych, a w szczególności komórek odpowiedzialnych za analizę danych pochodzących ze źródeł elektronicznych. Zob.: M. Herman, *Potęga wywiadu,* Warszawa 2002, s. 49.

[213] Zarządzenie Nr 74 Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. *w sprawie nadania statutu Agencji Wywiadu* (M.P. 2011 nr 26 poz. 433), § 3 ust. 1.

[214] Zarządzenie Nr 73 Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. *w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego* (M.P. 2002 nr 26 poz. 432), § 3 ust. 1.

[215] Zarządzenie Prezesa Rady Ministrów z dnia 6 października 2010 r. *w sprawie nadania statutu Centralnemu Biuru Antykorupcyjnemu* (M.P. z 2010 r. Nr 76, poz. 953), § 3 ust. 1.

W obu tych służbach występuje więc jedna, centralna jednostka organizacyjna odpowiadająca za analizę informacji napływających z różnych ośrodków. Nieco inny model został wdrożony w wojskowych służbach specjalnych. W przypadku SKW taka centralna jednostka, czyli Zarząd Studiów i Analiz, została zlikwidowana w 2011 roku, zaś jej zadania są obecnie realizowane na poziomie poszczególnych Zarządów (m.in. Operacyjnego, Ochrony Ekonomicznych Interesów Sił Zbrojnych czy Ochrony Sił Zbrojnych). Zdaniem kierownictwa SKW, rozwiązanie takie umożliwiło usprawnienie, również w aspekcie czasowym, realizację czynności analityczno-informacyjnych, z możliwością bieżącego wytyczania kierunków dalszych działań w tym zakresie[216]. Jak więc widać, istnieją różne modele organizacji pracy analitycznej. Trudno jednak stwierdzić, który z nich jest optymalny. Dzieje się tak, gdyż zadania poszczególnych służb znacząco się różnią, co z kolei warunkuje wykorzystywanie odmiennych źródeł informacji, a także inny poziom ich analizy.

Warto jednak zauważyć, że w niektórych państwach w służbach specjalnych istnieją specjalne komórki analityczne zajmujące się tylko i wyłącznie pozyskiwaniem i analizą informacji pochodzących ze źródeł otwartych. Przykładem może być Open Source Center (OSC) działające od 2005 roku w strukturach amerykańskiej CIA. Warto podkreślić, że Centrum podległe jest bezpośrednio Dyrektorowi Wywiadu Narodowego (Director National Intelligence – DNI), co dowodzi jego dużego znaczenia. OSC wspomagane jest przez rozbudowany system elektroniczny umożliwiający sprawne gromadzenie, przetwarzanie, analizę i dystrybucję pozyskanych informacji – działający od 2006 roku Open Source Information System (OSIS)[217]. Na chwilę obecną jest to największa na świecie, specjalnie wydzielona struktura, przeznaczona do prowadzenia białego wywiadu w skali globalnej w sposób ciągły. Pracownicy OSC przez pełną dobę monitorują wiadomości publikowane w wychodzących na całym świecie gazetach, lokalnych stacjach radiowych i programach telewizyjnych czy blogach. Kluczowymi źródłami informacji są jednak portale społecznościowe (w szczególności Twitter i Facebook). Analitycy czytają codziennie nawet 5 milionów wpisów z nich pochodzących. Oznacza to konieczność biegłego posługiwania się językami takimi jak arabski, chiński, urdu czy farsi. Analizowana jest również bieżąca komunikacja, mająca miejsce np. w pokojach na internetowych czatach. Na podstawie tak zdobytych danych tworzone są raporty

[216] S. Hoc, *Analiza informacji kontrwywiadowczej* [w:] J. Konieczny (red.), *Analiza informacji w służbach policyjnych i specjalnych*, Warszawa 2012, s. 313.

[217] *Open Source Information System (OSIS)* [w:] http://www.globalsecurity.org/intell/systems/osis.htm [dostęp: 5 lipca 2014].

dotyczące bieżących nastrojów społecznych, w wielu miejscach na świecie oraz prognozy dotyczące nadchodzących wydarzeń[218].

W polskich służbach specjalnych nie istnieją obecnie niestety żadne struktury zbliżone do amerykańskiego OSC. Niemniej jednak dobrym przykładem wykorzystania otwartych źródeł informacji w służbach specjalnych jest działalność Agencji Bezpieczeństwa Wewnętrznego. Strukturą mającą największą styczność ze źródłami tego typu jest wymienione już wcześniej Biuro Ewidencji i Analiz. Podstawowym jego zadaniem jest uzyskiwanie i opracowywanie informacji pochodzących z jednostek kierunkowych (zarówno tych zdobytych operacyjnie, jak i drogą administracyjną). Co ważne jednak, struktura ta prowadzi również bardzo szeroki monitoring otwartych źródeł informacji, którego podstawowym celem jest rozpoznawanie charakteru i kierunków potencjalnych zagrożeń dla bezpieczeństwa państwa. Monitorowane są m.in. polskie i obcojęzyczne radykalne media (w tym również arabskie i kaukaskie), co pozwala na regularne opracowywanie raportów streszczających zawarte w nich treści, które mogą wskazywać na istnienie zagrożenia dla obywateli lub interesów Rzeczpospolitej[219].

Oprócz planowej i ciągłej działalności Biura Ewidencji i Analiz, informacje z otwartych źródeł informacji są szeroko wykorzystywane przez większość funkcjonariuszy Agencji. Wynika to z obowiązku uzyskiwania, przetwarzania i wykorzystywania informacji jawnych w trakcie realizowanych przez nich czynności, czy to operacyjnych czy też śledczych, związanych z tematyką ich pracy. Uwarunkowane jest to zarówno przepisami ustawy, jak i normami wewnętrznymi ABW. Wykorzystywana metodologia i zakres źródeł, na jakich funkcjonariusze się opierają, w dużej mierze zależy od kierunku działań i miejsca ich wykonywania. Inaczej będzie wyglądała analiza prowadzona przez oficerów z Departamentów Kontrwywiadu

---

[218] „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 przytoczyć można zamieszki mające miejsce w Bangkoku w 2010 roku. 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 wytypowani zostali najbardziej wiarygodni autorzy wpisów. W przypadku rozruchów w Bangkoku analitycy opierali się na relacjach zaledwie 12-15 użytkowników Twittera. Analogiczny scenariusz powtarzał się również wielokrotnie podczas arabskiej wiosny. Zob.: J. Przybylski, *Zaczytani agenci CIA*, „Rzeczpospolita", 7 listopada 2011 [w:] http://www.rp.pl/artykul/748071. html?print=tak&p=0 [dostęp: 5 lipca 2014].

[219] A. Makarski, *Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego. Geneza, zasady działania oraz doświadczenia po pierwszym roku funkcjonowania*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2 (2), s. 105-106.

czy Zwalczania Terroryzmu, a jeszcze inaczej Departamentu Bezpieczeństwa Ekonomicznego Państwa. Praktyka taka jest powszechna w zasadzie we wszystkich służbach, a także w policji. Warto zauważyć, że funkcjonariusze ABW poza wykorzystywaniem klasycznych otwartych źródeł informacji sięgają również po opracowania tworzone przez prywatne firmy wywiadowcze, udostępniane w formie biuletynów. Przykładem może być chociażby, bardzo znany amerykański „Jane's Defens Weekly". Z kolei w przypadku konieczności pozyskania informacji na temat działających w Polsce podmiotów gospodarczych, wykorzystywane są raporty rodzimych wywiadowni gospodarczych. Ponadto jawne informacje zbierane są również przy okazji udziału funkcjonariuszy w kongresach, konferencjach, prelekcjach i różnego rodzaju seminariach naukowych. Dobrym tego przykładem może być chociażby udział w Polskiej Platformie Bezpieczeństwa Wewnętrznego. Opracowywane przez ABW materiały mają formę raportów, informacji sygnalnych, analiz oraz biuletynów tematycznych i poświęcone są takim zjawiskom, jak szpiegostwo, terroryzm i ekstremizmy polityczne, zagrożenia dla podstaw ekonomicznych państwa czy też korupcja osób pełniących funkcje publiczne[220]. Warto również zaznaczyć, że funkcjonariusze Agencji przechodzą specjalne kursy z wykorzystania otwartych źródeł informacji, czego najlepszym przykładem mogą być prowadzone przez Centralny Ośrodek Szkolenia ABW w Emowie, szkolenia pt. „Biały wywiad – zbieranie informacji z otwartych baz danych"[221].

2.2. Zastosowanie białego wywiadu w policji

Jak pokazuje praktyka, zastosowanie otwartych źródeł informacji w policji również może przynieść niezwykle obiecujące rezultaty. W szczególności tyczy się to analizy kryminalnej prowadzonej przy wykorzystaniu informacji pochodzących z serwisów społecznościowych[222]. Tak zdobyte dane mogą skutecznie pełnić zarówno informacyjną, dowodową jak i poszlakową funkcję, co rodzi spore nadzieje na coraz szersze ich wykorzystanie przez organy ścigania[223].

---

[220] B. Święczkowski, *Wykorzystanie tzw. białego wywiadu…,* s. 172-176.

[221] P. Potejko, *10 lat Centralnego Ośrodka Szkolenia ABW w Emowie*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 3, s. 198.

[222] W tym kontekście niezwykle przydatną wiedzą wydają się doświadczenia zdobyte przez amerykańską policję. Szerzej zob.: *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities. Guidance and Recommendations*, February 2013 [w:] it.ojp.gov/docdownloader.aspx?ddid=1826 [dostęp: 31 sierpnia 2014].

[223] B. Stromczyński, P. Waszkiewicz, *Biały wywiad* w *praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prawo i Prokuratura" 2014, nr 5, s. 158-163.

Dlatego też w działaniach policji stosowana była i nadal jest metoda białego wywiadu. Przy obecnym, bardzo szerokim dostępie policjantów do otwartych źródeł (a w szczególności internetu), trudno sobie wyobrazić prowadzących rozpoznanie lub różnego rodzaju postępowania funkcjonariuszy, którzy unikaliby korzystania z ogólnodostępnych źródeł informacji[224].

Wykorzystywanie informacji ze źródeł otwartych w policji jest możliwe, a niekiedy nawet niezbędne, na niemal każdym z etapów pracy funkcjonariuszy. Już w ramach prowadzenia postępowania przygotowawczego (czyli np. przygotowania przesłuchań, okazań, konfrontacji i eksperymentów kryminalistycznych, inicjowania czynności sprawdzających czy chociażby budowania wiedzy o okolicznościach przestępstwa) oparcie się na instrumentach białego wywiadu wydaje się zasadne. W zależności od specyfiki sprawy, otwarte źródła informacji będą mniej lub bardziej przydatne. W przypadku gdy prowadzone jest np. postępowanie przygotowawcze z dziedziny przestępczości gospodarczej, pomocne mogą okazać się ogólnodostępne rejestry oraz raporty wywiadowni gospodarczych. Wiedza zdobyta na ich podstawie nie tylko przyda się w rozumieniu merytorycznych niuansów prowadzonego postępowania, ale również ułatwi i usprawni przeprowadzenie podstawowych czynności procesowych. Nawet w trakcie prowadzenia przesłuchania w oparciu o pozyskane informacje na temat kontekstu popełnionego przestępstwa, można budować wrażenie tzw. wszechwiedzy przesłuchującego. Jest to element taktyki kryminalistycznej prowadzenia przesłuchań, która pozwala uzyskać efekt zaskoczenia i pomaga w osiągnięciu lepszych rezultatów. Otwarte źródła informacji mogą przydać się również w inicjowaniu czy też pogłębianiu podjętych już czynności operacyjno-rozpoznawczych. Jak już wspomniano wcześniej, dzięki portalom społecznościowym i rejestrom, możliwe jest stosunkowo szybkie i łatwe pozyskanie informacji o podejrzanym. Da się ustalić jego wygląd, wiek, miejsce zamieszkania, kontakty, zainteresowania, stan majątkowy czy powiązania kapitałowe. W ten sam sposób możliwe jest również rozpoznanie środowisk kryminogennych takich, jak pseudokibice piłkarscy czy narkomani. Wewnętrzne fora internetowe czy fanziny mogą dostarczyć wielu informacji na temat struktury danego środowiska, jego kontaktów czy panujących w nim nastrojów[225]. Ponadto w pracy policyjnej metoda białego wywiadu może być wykorzystana również

---

[224] K. Radwaniak *Biały wywiad w policji – narzędzie rozpoznawania zagrożeń terrorystycznych*, „Studia prawnicze. Rozprawy i Materiały" 2012, nr 2 (11), s. 88.

[225] K. Radwaniak, P.J. Wrzosek, *Biały wywiad w Policji – pozyskiwanie i analiza informacji ze źródeł otwartych* [w:] J. Konieczny (red.), *Analiza informacji w służbach policyjnych i specjalnych*, Warszawa 2012, s. 138.

pod kątem identyfikacji potencjalnych lub słabo rozpoznawalnych zagrożeń, w klasycznej prewencji i prewencji kryminalnej czy w końcu dla celów organizacyjno-logistycznych[226].

Wachlarz zastosowań otwartych źródeł informacji w pracy policyjnej wydaje się bardzo szeroki. Mimo to możliwości, jakie daje obecnie elektronicznie wspomagany wywiad jawnoźródłowy, nie są przez polskich policjantów w pełni wykorzystywane. Odnosząc się bowiem do praktyki policyjnej i badań z tego zakresu, można zauważyć, że biały wywiad jest stosowany, ale w formie ograniczonej, niemalże „intuicyjnie", bez wykorzystania specjalistycznej wiedzy zawartej np. w piśmiennictwie krajowym i zagranicznym. Szersze oparcie się na doświadczeniach wywiadowczych innych służb (zarówno polskich, jak i zagranicznych) przy uwzględnieniu specyfiki pracy policji, z pewnością podniosłoby poziom i efektywność wykorzystania otwartych źródeł informacji[227].

2.3. Otwarte źródła informacji w administracji publicznej

Zmiany zachodzące we współczesnym świecie mają wpływ na wszystkie sfery życia społecznego, co przekłada się również na kształt i sposób działania współczesnej administracji publicznej. W jej strukturach, na każdym szczeblu, coraz istotniejszą rolę zaczyna odgrywać analiza informacji. Dziś każdy urzędnik działający w realiach nowoczesnego społeczeństwa informacyjnego, w mniejszym lub większym stopniu styka się z pracą analityczną. Z kolei analitycy pracujący w administracji w coraz większym stopniu są zmuszeni korzystać z wiedzy i rezultatów badań prowadzonych przez niezależne od rządu instytucje i organizacje. W tym kontekście zaczynają oni pełnić nowe funkcje; po pierwsze – organizatorów pracy takich instytucji (zamawiając opracowania i analizy na określony temat), po drugie – osób monitorujących ukazujące się opracowania, raporty i innego rodzaju materiały pochodzące ze źródeł otwartych oraz po trzecie – autorów sporządzających samodzielnie analizy w celu wsparcia nieustannie toczących się w administracji procesów decyzyjnych[228].

Jak więc widać, możliwości wykorzystania otwartych źródeł informacji w administracji publicznej wydają się obecnie bardzo szerokie.

---

[226] W. Mądrzejewski, *„Biały wywiad" w Policji* [w:] W. Filipowski, W. Mądrzejowski (red.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki,* Warszawa 2012, s. 128.

[227] K. Radwaniak, *Biały wywiad w policji – narzędzie rozpoznawania…*, s. 90.

[228] T.R. Aleksandrowicz, *Analityk informacji w administracji rządowej* [w:] K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Analiza informacji w zarządzaniu bezpieczeństwem,* Warszawa 2013, s. 26.

Dowodem na to mogą być liczne inicjatywy podejmowane w tym względzie za granicą, choćby austriackie pomysły na szerokie wykorzystanie monitoringu mediów (w szczególności ich internetowej części) w systemie zarządzania kryzysowego[229]. Pokazuje to, że skuteczne wykorzystanie informacji pochodzących z otwartych źródeł jest możliwe również na niższych szczeblach administracji państwowej. Niemniej jednak to na poziomie centralnym metoda białego wywiadu stosowana jest najczęściej, a dzieje się to zazwyczaj w wyspecjalizowanych ośrodkach analitycznych. Najlepszą i zdecydowanie najpełniejszą tego ilustracją może być rodzimy Ośrodek Studiów Wschodnich, będący rządową instytucją ekspercką, zajmującą się analizą sytuacji politycznej, gospodarczej i społecznej w krajach sąsiadujących z Polską. Na chwilę obecną bez wątpienia jest to w polskich warunkach podmiot państwowy, który w sposób najbardziej kompleksowy wykorzystuje metodę białego wywiadu na poziomie strategicznym.

Genezy powstania Ośrodka należy upatrywać w sytuacji geopolitycznej, w jakiej znalazła się Polska po przemianach 1989 roku. Brak rzetelnej wiedzy o sytuacji gospodarczej i społecznej w ZSRR, w Moskwie, w poszczególnych republikach związkowych i autonomicznych oraz w guberniach doskwierał zarówno polskiej administracji rządowej, jak i rodzimym przedsiębiorcom. Brak ten skutecznie ograniczał bowiem możliwości odbudowy polskiego eksportu. Dlatego też wiosną 1990 roku powstał projekt stworzenia banku informacji o ZSRR uzyskiwanych poprzez analizę gazet, wydawnictw urzędowych, programów radiowych i telewizyjnych. Autorem projektu był Marek Karp. Dzięki niemu w grudniu 1990 roku przy Ministerstwie Współpracy Gospodarczej z Zagranicą powołany został Ośrodek Studiów Wschodnich[230]. Początkowo jednym z podstawowych źródeł informacji była prasa z obszaru byłego ZSRR, cyklicznie przywożona pociągami i prywatnymi samochodami. Było to około 120 tytułów. Ponadto w trybie całodobowym prowadzono monitoring innych środków przekazu, takich jak agencje prasowe, stacje radiowe i telewizyjne. Biuletyn dzienny stanowił główny produkt Ośrodka dla odbiorów w administracji publicznej. Ponadto tworzono odpowiedzi na doraźnie formułowane zapotrzebowania. Zazwyczaj były to biogramy polityków, kalendaria wydarzeń czy charakterystyki podmiotów życia publicznego[231]. Połowa lat '90-tych to okres wielkich przemian

[229] G. Backfried, Ch. Schmidt, M. Pfeiffer, *Open Source Intelligence in Disaster Management* [w:] http://www.csis.pace.edu/~ctappert/dps/2012EISIC/data/4782a254.pdf [dostęp: 2 sierpnia 2014].

[230] *Historia z konsekwencjami – rozmawiają Krzysztof Kozłowski i Michał Komar*, Warszawa 2009, s. 274.

[231] J. Cichocki, J. Darczewska, B. Sienkiewicz, *Okręt koszykowa* [w:] J. Borkiewicz, J. Cichocki, K. Pełczyńska-Nałęcz (red.), *Okręt Koszykowa*, Warszawa 2007, s. 31.

w OSW. Na początku swojej działalności Ośrodek dzielił swoją działalność na opracowywanie informacji i ich analizę. Od 1995 roku instytucja przyjęła profil czysto analityczny. Druga połowa dekady stała się również czasem intensywnego rozwoju technologicznego, związanego z pojawieniem się internetu. Przełożyło się to na znaczące usprawnienie pracy OSW, a także rozpoczęło jego „otwieranie się" na innych odbiorców niż administracja państwowa. Wtedy to właśnie powstała pierwsza strona internetowa Ośrodka z materiałami dostępnymi dla wszystkich użytkowników, co było prawdziwym *novum* w tamtym okresie. Utrzymująca się niestabilna sytuacja na Bałkanach i rosnące znaczenie południowych sąsiadów Polski w kontekście rozszerzenia NATO spowodowały dołączenie w 1998 roku do obszaru zainteresowań OSW regionu Europy Środkowej i Bałkanów. W tym czasie znacznie silniej zaczęto analizować również problematykę dotyczącą energetyki. Z kolei wejście Polski do UE stworzyło potrzebę osadzenia analizy OSW także w kontekście polityki zachodniej, czego efektem było powołanie w roku 2005 zespołu niemieckiego. W 2012 roku zakres działania OSW rozszerzono o Turcję i obszar bałtycko-nordycki. W tym samym roku weszła w życie długo oczekiwana ustawa, regulująca umocowanie prawne Ośrodka i jednoznacznie definiująca jego zadania[232].

Obecnie do głównych zadań ustawowych OSW należy gromadzenie, opracowywanie oraz udostępnianie organom władzy publicznej informacji o istotnych wydarzeniach i procesach politycznych, społecznych i gospodarczych na obszarze Europy Środkowej, Europy Wschodniej, Rosji, Półwyspu Bałkańskiego oraz Kaukazu Południowego i Azji Centralnej, a w przypadkach uzasadnionych strategicznymi interesami politycznymi lub gospodarczymi RP również w innych rejonach. Ośrodek odpowiedzialny jest też za przygotowywanie analiz, ekspertyz i studiów prognostycznych dotyczących sytuacji politycznej, społecznej i gospodarczej oraz rozwoju stosunków międzynarodowych na tych obszarach. W zamyśle ustawodawcy OSW prowadzić ma stałą współpracę z polskimi i zagranicznymi instytucjami, ośrodkami nauki i osobami fizycznymi oraz promować polską myśl analityczną poza granicami kraju. Do ważnych zadań Ośrodka należy również inspirowanie, organizowanie i prowadzenie badań w zakresie problematyki wschodniej oraz przekazywanie ich wyników organom władzy publicznej, a także gromadzenie specjalistycznego księgozbioru i dokumentacji naukowej oraz organizowanie szkoleń. To ostatnie przejawia się m.in. w organizacji seminariów i konferencji, na których prezentowane są wyniki badań. Dzięki temu możliwe jest skuteczne upowszechnianie wiedzy o stanie i tendencjach zmian sytuacji politycznej, społecznej

[232] *Historia* [w:] http://www.osw.waw.pl/pl/historia [dostęp: 26 lipca 2014].

i gospodarczej oraz rozwoju stosunków międzynarodowych na badanych przez OSW obszarach[233].

Analizując ustawowe zadania OSW, można dojść do wniosku, iż instytucja będąca częścią administracji publicznej, która z założenia wykorzystuje jedynie otwarte źródła informacji, jest w stanie działać na bardzo wielu płaszczyznach. Ponadto liczni eksperci podkreślają, że jakość opracowań jest niezwykle wysoka. Ośrodek zaś zadziwia światowych znawców problematyki wschodniej trafnością i głębią swoich analiz[234]. Są one obecnie niebywale cennym źródłem informacji, zwłaszcza w obszarze bezpieczeństwa[235]. Po ponad 20 latach istnienia OSW przeszedł pełną drogę od niewielkiej organizacji, będącej wyobrażeniem o instytucji analitycznej, do liczącego prawie 70 osób profesjonalnego ośrodka badawczego. W tym czasie zmienił się zarówno sposób pracy, jak i jej zakres. Obecnie mapa zainteresowań analitycznych OSW obejmuje nie tylko polityczny Wschód powstały na gruzach ZSRR, ale i całą Europę Środkową, Bałkany, Niemcy i region nordycko-bałtycki oraz Turcję[236]. Niewątpliwie uznać należy, że szkoła pozyskiwania i analizy informacji, jaka powstała w OSW, miała niemały wpływ na metodykę wykorzystania białego wywiadu w polskich służbach specjalnych oraz innych instytucjach o profilu analitycznym.

3. Biały wywiad a terroryzm

Warto pamiętać, iż metoda białego wywiadu stosowana jest nie tylko przez służby specjalne, policję, administrację publiczną czy analityków z sektora prywatnego. Stanowi ona również podstawowe narzędzie wywiadowcze dla różnego rodzaju ugrupowań ekstremistycznych oraz terrorystów[237]. Szczególnie intensywnie wykorzystywanym przez nich otwartym źródłem informacji jest bez wątpienia internet. Cyberprzestrzeń stała

---

[233] Ustawa z dnia 15 lipca 2011 r. *o Ośrodku Studiów Wschodnich im. Marka Karpia* (Dz.U. 2011 nr 173 poz. 1029), art. 2.

[234] *Historia z konsekwencjami – rozmawiają Krzysztof Kozłowski i Michał Komar*, Warszawa 2009, s. 274.

[235] Świadczyć mogą o tym odrębne opracowania dotyczące chociażby problemów takich jak metodyka prowadzenia rosyjskiej wojny informacyjnej. Zob.: J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska - studium przypadku* [w:] http://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf [dostęp: 26 lipca 2014].

[236] *Historia* [w:] http://www.osw.waw.pl/pl/historia [dostęp: 26 lipca 2014].

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

się nie tylko polem walki, ale również obszarem działań dużo subtelniejszych, choć równie niebezpiecznych. Propaganda, dezinformacja, rekrutacja, komunikacja, zbieranie funduszy, planowanie oraz koordynacja działań w internecie, to zadania podejmowane przez większość współczesnych organizacji terrorystycznych. Oczywiście sieć to w pierwszej kolejności doskonałe miejsce do prezentowania swoich postulatów oraz dzielenia się relacjami z zamachów, czyli krótko mówiąc do walki psychologicznej opartej na różnych formach działań propagandowych i dezinformacyjnych. Podobnie jak z innymi mediami, terroryzm jest związany ściśle z internetem jako kanałem umożliwiającym dotarcie do niezwykle szerokiego audytorium[238]. Świetnym na to dowodem jest fakt, że między rokiem 1999 a 2009 liczba stron internetowych należących do terrorystów wzrosła ze stu do niemal pięciu tysięcy[239].

Jak już wspomniano wcześniej, internet rozrasta się w oszałamiającym tempie, co roku zyskując miliony nowych użytkowników. W tej nieprzebranej masie znajdują się również współcześni terroryści, którzy wykorzystują cyberprzestrzeń jako narzędzie umożliwiające łatwe i niezwykle efektywne zbieranie informacji potrzebnych do planowania poszczególnych zamachów. Przed rewolucją w dziedzinie technologii informacyjnych to państwo dysponujące rozbudowanym aparatem administracyjnym i wojskowym w dużej mierze reglamentowało dostęp do wiedzy. Książki, czasopisma czy nawet korespondencję można było cenzurować, zaś 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 posiadają wiele uprawnień umożliwiających, w razie potrzeby, szybkie i niepostrzeżone poszerzenie tego typu wiedzy. Niemniej jednak dysproporcja w dostępie do informacji nieustanie maleje, na czym korzystają przede wszystkim podmioty niepaństwowe, w tym również grupy terrorystyczne. Na szczególną penetrację narażone są współczesne państwa demokratyczne, gdzie występuje pełna transparentność życia publicznego. Z jednej strony pozwala to na sprawowanie przez ogół obywateli efektywnej kontroli społecznej nad aparatem władzy państwowej, z drugiej naraża tenże aparat na łatwą i niekontrolowaną penetrację przez ugrupowania terrorystyczne. Wiele z pozoru nieistotnych danych podanych na stronach internetowych urzędów państwowych, po wzbogaceniu ich o informacje z innych źródeł, daje

[238] B. Bolechów, *Terroryzm. Aktorzy, statyści, widownie,* Warszawa 2010, s. 225.

[239] R. Szymaniuk, *Cyberterroryzm – wcale nie wirtualne zagrożenie*, „Kwartalnik Bellona" nr 4/2009, s. 62.

znakomity materiał do przygotowania precyzyjnie wymierzonego ataku terrorystycznego. Mimo wielu bardzo złożonych metod kontroli treści internetu, ogromny problem stanowią nadal terroryści działający w pojedynkę, niemożliwi do zlokalizowana ze względu na brak jakichkolwiek podejrzanych powiązań. Są to tzw. samotne wilki (ang. *lone wolves*)[240], które bardzo często wykorzystują internet przede wszystkim jako źródło materiałów szkoleniowych oraz narzędzie do planowania zamachów, prawie w ogóle nie używając go w roli komunikatora. Łatwość w wykorzystaniu internetu w planowaniu zamachów spowodowana jest wchłonięciem przez to medium wielu innych źródeł, co pozwala zminimalizować kontakt ze światem zewnętrznym, a to ze względu na skrytość działalności terrorystycznej stanowi dosyć istotną zaletę. Z kolei, jak już wskazano wcześniej, przy zastosowaniu odpowiednich technik i narzędzi (np. klienta sieci TOR) możliwe jest stosunkowo bezpieczne i anonimowe korzystanie z zasobów sieci.

Analizując zasoby internetu szczególnie przydatne w działalności terrorystycznej, wskazać należy co najmniej kilka obszarów sieci. Wśród portali internetowych, które wydają się szczególnie atrakcyjne z punktu widzenia organizacji terrorystycznych i ekstremistycznych, są serwisy społecznościowe, za pomocą których stosunkowo łatwo ustalić zapatrywania światopoglądowe właściciela konta. Powoduje to, że dosyć swobodnie można tworzyć listy, nie tylko osób, które warto zwerbować, ale również potencjalnych celów, przeznaczonych do zastraszania lub czasem nawet fizycznej eksterminacji. Podobnie sprawa ma się z serwisami networkingowymi, będącymi znakomitym narzędziem do nawiązania istotnych znajomości, dającymi możliwość łatwej infiltracji pewnych środowisk (np. pracowników ochrony odpowiedzialnych za strzeżenie infrastruktury krytycznej). Również branżowe fora dyskusyjne mogą dostarczyć potencjalnym terrorystom sporo przydatnych informacji. Szczególnie wartościowe są te dotyczące pirotechniki, materiałów wybuchowych czy broni palnej. Istotny jest też fakt, że grupują one internautów o określonych poglądach i zainteresowaniach wokół poszczególnych tematów, wśród których częstokroć znaleźć można wysokiej klasy specjalistów. Analiza treści tam zamieszczonych daje również możliwości aktywnego werbunku. Fora internetowe (zwłaszcza te będące częścią głębokiego internetu) to miejsca, gdzie możliwe jest pozyskanie niezwykle profesjonalnych materiałów szkoleniowych, tworzonych bezpośrednio na potrzeby ugrupowań terrorystycznych. Dobrym tego przykładem może być tzw. *Manchester Manual*, czyli publikacja przygotowana dla ekstre-

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

mistów islamskich działających w Wielkiej Brytanii[241]. Z punktu widzenia terrorystów bardzo wartościowym źródłem informacji są również portale udostępniające mapy oraz zdjęcia satelitarne. Daje to ogromne możliwości w planowaniu różnego rodzaju zamachów bombowych oraz incydentów typu *active shooter*. Dzięki możliwości zdalnego zapoznania się ze szczegółową topografią i usytuowaniem potencjalnych celów zamachowiec nie musi w ogóle narażać się na ryzyko zatrzymania lub nagrania przez monitoring przemysłowy. Nie trzeba więc robić zdjęć i szkiców, wystarczy wejść na odpowiednią stronę internetową. Takie planowanie akcji terrorystycznych przy wykorzystaniu danych satelitarnych miało miejsce już wielokrotnie. Przykładem może być tutaj sytuacja z 2006 roku, kiedy to w Bagdadzie wywiad brytyjski odnalazł na należących prawdopodobnie do terrorystów komputerach i nośnikach prawie 500 GB danych satelitarnych pobranych z Google Earth. Zdaniem Brytyjczyków, terroryści wykorzystali dane z tego systemu do ataku na wojska w Basrze[242]. Innym, niezwykle atrakcyjnym z punktu widzenia organizacji terrorystycznych, źródłem informacji są serwisy upubliczniające niejawne dokumenty dotyczące newralgicznych kwestii związanych z bezpieczeństwem państwa. Najbardziej znanym portalem tego typu jest Wikileaks.org. Jego administratorzy wielokrotnie oskarżani byli o łamanie tajemnicy państwowej. Jako przykład podać można publikację w 2010 roku listy instalacji (m.in. fabryk rurociągów, węzłów komunikacyjnych, portów, podmorskich kabli) na całym świecie, które Stany Zjednoczone uważają za kluczowe dla swojego bezpieczeństwa narodowego. Co ciekawe, na liście znalazło się wiele instalacji leżących poza granicami USA. Wymieniono również biegnący przez terytorium Polski ropociąg „Przyjaźń". Po wycieku w mediach szybko pojawiły się opinie, że jest to lista potencjalnych celów, którą mogliby wykorzystać terroryści[243]. Ponadto warto dodać, że na łamach omawianego serwisu opublikowano również listy przewodników i tłumaczy współpracujących z Amerykańską Armią w Iraku i Afganistanie, co uznać należy za informacje niezwykle cenne z punktu widzenia działających lokalnie organizacji terrorystycznych.

Można podać również wiele przykładów, kiedy istotne, cenne dla organizacji terrorystycznych, informacje wywiadowcze były ujawniane bezpośrednio przez administrację publiczną lub służby specjalne. Warto przywołać

---

[241] Z okrojoną i ocenzurowaną wersją podręcznika zapoznać się można na stronie amerykańskiego Departamentu Sprawiedliwości, zob.: *The Al Qaeda Manual*, Department of Justice [w:] http://www.justice.gov/ag/manualpart1_1.pdf [dostęp: 26 czerwca 2014].

[242] R. Szymaniuk, *Cyberterroryzm…*, s. 62.

[243] *List of facilities 'vital to US security' leaked*, 6 December 2010 [w:] http://www.bbc.co.uk/news/world-us-canada-11923766 [dostęp: 29 sierpnia 2014].

chociażby przypadek publikacji raportu z likwidacji Wojskowych Służb Informacyjnych. Jak wskazują niektórzy specjaliści, raport ujawnił wiele wrażliwych danych osobowych agentów, informacji dotyczących spenetrowanych przez polski wywiad firm oraz szczegółów operacji prowadzonej w Afganistanie. Co ważne, miało to miejsce w czasie, kiedy w tym kraju znajdował się kontyngent Wojska Polskiego prowadzący działania przeciwko islamskim terrorystom. Informacje zawarte w raporcie mogły okazać się bardzo przydatne dla wywiadu Al-Kaidy, stanowiącej głównego przeciwnika polskich żołnierzy. Dokument został bowiem opublikowany nie tylko w Monitorze Polskim, ale również w internecie (zarówno w oficjalnym cyfrowym publikatorze parlamentu – Internetowym Systemie Aktów Prawnych, jak i poza nim w wersji anglojęzycznej)[244]. Co ciekawe, informacje niezwykle przydatne w bieżącej działalności terrorystycznej publikowały na swoich stronach same służby specjalne. Przykładem może być tu strona internetowa Służby Kontrwywiadu Wojskowego, na której do 2012 roku skrupulatnie umieszczane były osiągnięcia dotyczące pracy kontrwywiadowczej w Afganistanie. Takie działanie służb budziło z kolei powszechne niezadowolenie i obawy polskich żołnierzy służących w kontyngencie, a odpowiedzialnych za realizację tych akcji. Bali się oni, że publikacja tego typu informacji w internecie może skutecznie prowokować talibów do organizacji nowych akcji odwetowych[245]. Obawy polskich żołnierzy były zdecydowanie na miejscu, gdyż terroryści już wcześniej pokazali, że są w stanie bardzo staranie monitorować, nie tylko oficjalne strony służb państw koalicji, ale również media społecznościowe. Dowodem tego był m.in. atak moździerzowy na amerykańską bazę w Iraku w 2007 roku. Nastąpił on zaraz po tym, jak żołnierze udostępnili zdjęcia (zawierające metadane ze współrzędnymi), z nowo przybyłym sprzętem, na Facebooku. Efektem aktu było zniszczenie lub ciężkie uszkodzenie czterech śmigłowców szturmowych AH-64 Apache[246].

***

Jak wynika z analizy wybranych obszarów wykorzystania otwartych źródeł informacji, biały wywiad przydatny jest na wszystkich szczeblach działalności wywiadowczej. Należy zauważyć również, że metoda ta pomocna

[244] A. Makowski, *Na rzecz obcego wywiadu*, „Wprost" 2014, nr 4 (1612), s. 16.

[245] Szerzej zob.: *Chore SKW* [w:] http://stowarzyszeniesowa.pl/wp-content/uploads/2013/02/Chore_SKW.pdf [dostęp: 26 sierpnia 2014].

[246] *Insurgents Destroyed US Helicopters Found in Online Photos*, 16 March 2012 [w:] http://www.livescience.com/19114-military-social-media-geotags.html [dostęp: 30 sierpnia 2014].

jest w eksploracji niemal każdego obszaru tematycznego, co wynika z tego, że rozwijała się ona równolegle na niwie różnych nauk, a nie tylko w ramach wąsko rozumianej teorii wywiadu. Dlatego też liczba i różnorodność podmiotów z niego korzystających jest tak wielka. W zależności od źródeł, na których opiera się analiza, możliwe jest skuteczne pozyskiwanie informacji zarówno na poziomie strategicznym, operacyjnym, jak i taktycznym. Dowodzi to ogromnej uniwersalności oraz interdyscyplinarności omawianej dyscypliny wywiadowczej.

Sam fakt szerokiego wykorzystania otwartych źródeł informacji w sektorze prywatnym nie dziwi. Niemniej jednak zjawiskiem, które rzuca się obecnie w oczy szczególnie wyraźnie, jest gwałtownie postępująca prywatyzacja działalności wywiadowczej. Obszary, w których państwa posiadały do tej pory niekwestionowany monopol na pozyskiwanie informacji, systematycznie się kurczą. Coraz częstszą praktyką staje się tzw. outsourcing wywiadowczy, czyli wykorzystanie usług podmiotów prywatnych przez państwową administrację oraz agencje wywiadowcze. Dotyczy to zarówno szczebla strategicznego, na którym działają potężne międzynarodowe korporacje, jak i poziomu lokalnego, na którym szczególnie aktywnie operują wywiadownie gospodarcze. Współpraca między prywatnym i państwowym sektorem wywiadowczym staje się z roku na rok coraz szersza, co z kolei przekłada się na intensywniejszy przepływ doświadczeń w zakresie wykorzystania otwartych źródeł informacji oraz wzrost ich ogólnego znaczenia. Znamienne dla naszych czasów wydaje się również wyodrębnienie zupełnie nowego zawodu, polegającego na wieloetapowym i wielowątkowym wyszukiwaniu oraz analizie informacji. Mowa tu o profesji infobrokera, będącej wręcz znakiem rozpoznawczym formującego się społeczeństwa informacyjnego.

Wykorzystanie metody białego wywiadu w służbach specjalnych oraz policji ma długą tradycję. W dobie postępującej rewolucji informatycznej stwarza ona jednak zupełnie nowe możliwości, dzięki czemu jej znaczenie systematycznie rośnie. Warto zauważyć, że mimo iż skala wykorzystania otwartych źródeł informacji w polskich służbach jest mniejsza niż na Zachodzie, to jednak ich potencjał jest coraz częściej dostrzegany. Rola analizy informacji rośnie również w administracji publicznej. Na polskim gruncie najbardziej znaną i najprężniej działającą strukturą analityczną, stosującą na szeroką skalę metodę białego wywiadu, jest Ośrodek Studiów Wschodnich im. Marka Karpia. Instytucja ta, opierając się wyłącznie na ogólnie dostępnych źródłach, od lat z dużym powodzeniem prowadzi analizę strategiczną tematycznie wychodzącą poza granice Europy Środkowo-Wschodniej.

Warto również zauważyć, że w chwili obecnej internet stał się podstawowym narzędziem do szybkiego i efektywnego zbierania informacji,

planowania oraz koordynacji działań terrorystycznych. Metoda białego wywiadu zajmuje szczególnie ważne miejsce w rzemiośle każdego współczesnego terrorysty, zaś dzięki jej dobremu opanowaniu możliwe staje się częściowe zniwelowanie przewagi w dostępie do informacji, jakie do niedawna służby specjalne i policja miały nad ugrupowaniami ekstremistycznymi. W tym kontekście zaznaczyć należy, że transparentność i szeroki dostęp do informacji publicznej to cechy konstytutywne każdego współczesnego państwa demokratycznego. Z jednej strony pozwala to wytworzyć niezwykle efektywną kontrolę społeczną nad poczynaniami władzy, z drugiej zaś ogromnie ułatwia zbieranie informacji i wybieranie celów najbardziej podatnych na atak terrorystyczny. Dylemat między wygodnym i prostym dostępem do informacji publicznej a bezpieczeństwem danych jest jednak nierozwiązywalny. Obostrzenie zasad owego dostępu wydaje się nie tylko bezcelowe (gdyż stoi to w sprzeczności z ideą budowy społeczeństwa obywatelskiego), ale również niebezpieczne (gdyż ułatwia mnożenie się patologii w sferze publicznej oraz prowadzi do rozmycia odpowiedzialności). Bezcelowe wydają się również wszelkie próby ograniczenia i cenzurowania zawartości internetu. Ze względu na dynamikę rozwoju sieci i liczbę jej użytkowników są to działania z góry skazane na niepowodzenie. Dlatego też zasadne wydaje się postawienie tezy, że wykorzystanie otwartych źródeł informacji (a w szczególności ich cyfrowej części) w działalności terrorystycznej będzie nasilać się w przyszłości. Co warto wziąć pod uwagę, jeśli chce się tej działalności skutecznie przeciwdziałać.

Wnioski

Biały wywiad nigdy nie należał do spektakularnych i widowiskowych obszarów pracy wywiadowczej, jednak jego wykorzystanie, bardzo często było tłem lub wstępem do głośnych i zakończonych sukcesem akcji – zarówno w przypadku służb specjalnych, policji, wielkich korporacji jak również zamachów terrorystycznych. Nic więc dziwnego, że spektrum możliwości wykorzystania otwartych źródeł wydaje się współcześnie tak szerokie. Wraz z postępującym rozwojem społeczeństwa informacyjnego metoda białego wywiadu coraz częściej wykorzystywana jest zarówno w służbach specjalnych, policji oraz instytucjach administracji publicznej, jak i w sektorze prywatnym. Korzystają z niej zarówno wywiadownie gospodarcze, działające na szczeblu lokalnym, jak i potężne międzynarodowe korporacje, zajmujące się wywiadem strategicznym. Sztuka pozyskiwania i analizy informacji ze źródeł jawnych i ogólnie dostępnych jest również szeroko uprawiana przez różnego rodzaju wolnych strzelców – infobrokerów czy też przez działające poza granicami prawa ugrupowania terrorystyczne. Ogólnie rzecz ujmując, biały wywiad zaczął być postrzegany jako interdyscyplinarne narzędzie do wytwarzania ustrukturyzowanej wiedzy, gotowej do wykorzystania w procesach decyzyjnych. Najważniejszą przyczyną takiego stanu rzeczy jest niewątpliwie nieustannie postępująca rewolucja w dziedzinie technologii informacyjnych.

Upowszechnienie się dostępu do internetu spowodowało, że państwo dysponujące rozbudowanym aparatem administracyjnym i wojskowym w sposób nieodwołalny utraciło monopol na reglamentację dostępu do wiedzy. Fakt ten wymusza szeroką współpracę między sektorem publicznym i państwowym. Bez niej bowiem wdrożenie nowoczesnych i wydajnych systemów wspomagających wyszukiwanie i analizę informacji wydaje się niemożliwe. Zastosowanie takich rozwiązań stało się obecnie absolutną koniecznością. Współcześnie to nadmiar informacji, a nie ich niedobór, jest największym wyzwaniem dla absolutnie każdej struktury wywiadow-

czej. To kolejny czynnik powodujący widoczny wzrost znaczenia oraz skali wykorzystania otwartych źródeł, bowiem właśnie informacje z nich pochodzące stanowią lwią część pozyskiwanego obecnie materiału wywiadowczego (wskaźnik ten w zależności od zakresu tematycznego waha się od 40 proc. do nawet 95 proc.). Dodatkowo podkreślić należy, że jest to dużo tańszy i prostszy, z powodów formalno-prawnych, sposób zdobywania informacji niż stosowanie typowych środków operacyjnych. Śmiało można więc stwierdzić, że biały wywiad stał się nie tylko odrębną i samodzielną, ale wręcz fundamentalną dyscypliną wywiadowczą.

Pochylając się nad historią białego wywiadu i jego ewolucji, nie sposób nie zauważyć zjawiska swoistego odwracania się filozofii pozyskiwania informacji w służbach specjalnych, co szczególnie wyraźnie widać w krajach należących do byłego bloku wschodniego, takich jak Polska. Kiedyś podstawą pracy wywiadowczej była agentura, dzięki której możliwe było pozyskanie większości potrzebnych informacji. Dobrze ulokowane źródła osobowe były w stanie dostarczyć niejednokrotnie cennych, często już wstępnie opracowanych informacji. Biały wywiad natomiast był traktowany zazwyczaj jako dodatek mający co najwyżej dostarczyć kontekstu do intensywnie prowadzonego rozpracowania operacyjnego. Współcześnie mamy do czynienia z odwróceniem tego trendu. Żadne z państw demokratycznych nie może pozwolić na bezkarne nadużywanie niejawnych, silnie ingerujących w prawa obywatelskie, metod pracy operacyjnej. Taki scenariusz zazwyczaj skutkuje szybkim spadkiem zaufania społecznego do przedstawicieli władzy i administracji państwowej. Dlatego też skryte metody pozyskiwania informacji stosowane są w sposób subsydiarny, tam gdzie metoda białego wywiadu zawodzi. Z kolei działalność operacyjna, w sferze czysto wywiadowczej (informacyjnej), częstokroć służy jedynie potwierdzeniu lub pogłębieniu uzyskanej już wcześniej wiedzy. Niewykluczone więc, że w przyszłości w służbach specjalnych nastąpi jeszcze silniejszy podział na działania o charakterze czysto informacyjnym (prowadzone przede wszystkim w oparciu o otwarte źródła informacji) oraz działania mające wywołać określony efekt (prowadzone głównie w oparciu o agenturę wpływu i szeroko rozumianą pracę operacyjną). Dowodem na realizację takiego scenariusza może być powstanie oraz działalność amerykańskiego Open Source Center, czyli potężnej międzyresortowej komórki odpowiedzialnej za prowadzenie białego wywiadu. Niewykluczone więc, że w przyszłości również w Polsce nastąpi wyodrębnienie podobnej instytucji o profilu czysto analitycznym, której zadaniem będzie tylko i wyłącznie działalność wywiadowcza w oparciu o jawne źródła informacji. Potwierdzeniem słuszności tych przypuszczeń wydaje się model funkcjonowania Ośrodka Studiów Wschodnich, który z kolejnymi latami poszerza zakres tematyczny swojej działalności, obecnie

daleko wykraczającej poza pierwotnie przyjęte ramy. Wysoka jakość analiz i opracowań tworzonych przez Ośrodek jest jaskrawym dowodem, iż w dzisiejszych czasach możliwe jest prowadzenie analizy strategicznej również bez wykorzystania utajnionych struktur wywiadowczych.

Porównując i zestawiając ze sobą poszczególne otwarte źródła informacji, dojść można w zasadzie do jednej, kluczowej konkluzji – wszechogarniającym metaźródłem informacji pozwalającym na zdobycie praktycznie pełnej wiedzy na niemal każdy temat stał się obecnie internet. Potencjał jego wykorzystania do celów wywiadowczych wydaje się w zasadzie nieograniczony. Niemniej jednak dużym wyzwaniem w jego skutecznej eksploracji jest stworzenie wydajnych a zarazem stosunkowo prostych w obsłudze narzędzi wspomagających automatyczną analizę informacji, w oceanie której toną obecnie analitycy. Bez takiego instrumentarium pokonanie przeciwności takich, jak zjawisko szumu informacyjnego czy barier językowych wydaje się zupełnie niemożliwe. Jednocześnie zauważyć należy, że w cyberprzestrzeni granice między wywiadem jawnoźródłowym a pozostałymi dyscyplinami wywiadowczymi bardzo silnie się zacierają. Już teraz jednoznaczne odseparowanie od siebie metod pozyskiwania i źródeł informacji przynależnych do OSINT-u lub SIGINT-u wydaje się bardzo problematyczne. Taki stan rzeczy budzi coraz silniejsze emocje wśród obrońców prawa do prywatności w cyberprzestrzeni. Największe obawy budzi kierunek rozwoju technologii związanych z tzw. analizą „Big Data", dzięki której możliwe staje się łączenie ze sobą bardzo różnorodnych baz danych (zarówno tych zawierających informacje ogólnodostępne, jak i tych poufnych). Nie dziwi więc coraz częściej pojawiające się pytanie o zasady wykorzystania tego typu metod oraz nadzór nad podmiotami je stosującymi.

Innym niełatwym wyzwaniem, będącym po części skutkiem ubocznym postępującej cyfryzacji, jest wykorzystanie otwartych źródeł informacji w działalności terrorystycznej. Łatwość i efektywność, z jaką można pozyskiwać dziś informacje za pośrednictwem internetu, powoduje, że metoda białego wywiadu w sposób nagminny wykorzystywana jest na etapie planowania i przygotowań do zamachów terrorystycznych. Pozwala ona potencjalnemu zamachowcowi cały czas pozostawać w cieniu, poza czujnym okiem służb specjalnych i policji. W szczególności dotyczy to tzw. samotnych wilków, którzy przy odpowiedniej dozie determinacji i ostrożności, dzięki internetowi są w stanie skutecznie zaplanować i przeprowadzić samodzielnie nawet bardzo złożony zamach terrorystyczny. Niestety dylemat między wygodnym i prostym dostępem do informacji publicznej a bezpieczeństwem danych wydaje się na chwilę obecną nierozwiązywalny. Dlatego też, państwowym służbom i instytucjom odpowiedzialnym za bezpieczeństwo, nie pozostaje nic innego jak pogodzić się z nieustannie topniejącą przewagą

w zakresie dostępu do informacji. Jedyną nadzieją wydaje się konsekwentne podnoszenie własnych zdolności analitycznych. Aby to osiągnąć, konieczne jest zarówno systematyczne zwiększanie kompetencji funkcjonariuszy odpowiedzialnych za analizę informacji oraz wprowadzanie nowych narzędzi usprawniających ten proces, ale również znacznie szersza współpraca zarówno ze środowiskami eksperckimi, jak i sektorem prywatnym.

Pomimo pewnych wad i ograniczeń wykorzystanie otwartych źródeł informacji w działalności wywiadowczej stwarza ogromny potencjał. Postępująca rewolucja informatyczna i powstawanie coraz to nowszych technologii, wspierających zautomatyzowane wyszukiwanie oraz analizę informacji, powoduje, że biały wywiad z roku na rok zyskiwać będzie na znaczeniu. Szczególnie duże nadzieje pokładane są w tzw. analizie „Big Data", umożliwiającej bardzo skuteczne prognozowanie trendów społecznych oraz wskazywanie potencjalnych zagrożeń. Warto również zauważyć, że w dorosłe życie wchodzi nowe pokolenie, od najmłodszych lat chłonące nowinki techniczne, będące owocami rewolucji w dziedzinie technologii informacyjnych. Ludzie ci znacznie bieglej poruszają się po internecie i w dużo wyższym niż poprzednie pokolenie stopniu wykorzystują jego możliwości w zakresie pozyskiwania informacji. Dlatego też poziom kompetencji cyfrowych nieustannie się podnosi, co niewątpliwie sprzyjać będzie jeszcze szybszemu rozwojowi białego wywiadu w najbliższych latach. Być może stoimy obecnie przed jednym z większych przełomów w historii wywiadu, w którym kluczową rolę odegrają połączone w odpowiednich proporcjach szeroko pojęte umiejętności analityczne oraz kompetencje cyfrowe.

Literatura

Źródła prawne

Ustawa z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych* (Dz.U. 1994 nr 24 poz. 83).

Ustawa z dnia 6 września 2001 r. *o dostępie do informacji publicznej* (Dz.U. 2001 nr 112 poz. 1198).

Ustawa z dnia 24 maja 2002 r. *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz. U. z 2002 r. Nr 74, poz. 676 ze zm.).

Ustawa z dnia 29 stycznia 2004 r. *Prawo zamówień publicznych* (Dz.U. 2004 nr 19 poz. 177).

Ustawa z dnia 9 czerwca 2006 r. *o Centralnym Biurze Antykorupcyjnym* (Dz.U. z 2006 r., Nr 104, poz. 708 ze zm.).

Ustawa z dnia 9 czerwca 2006 r. *o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (Dz.U. z 2006 r., Nr 104, poz. 709 ze zm.).

Ustawa z dnia 15 lipca 2011 r. *o Ośrodku Studiów Wschodnich im. Marka Karpia* (Dz.U. 2011 nr 173 poz. 1029).

Rozporządzenie Rady Ministrów z dnia 12 marca 2014 r. *w sprawie Centralnego Repozytorium Informacji Publicznej* (Dz.U. 2014 poz. 361).

Zarządzenie Nr 73 Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. *w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego* (M.P. z 2002 r., Nr 26, poz. 432).

Zarządzenie Nr 74 Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. *w sprawie nadania statutu Agencji Wywiadu* (M.P. z 2011 r., Nr 26, poz. 433).

Zarządzenie Nr 76 Prezesa Rady Ministrów z dnia 6 października 2010 r. *w sprawie nadania statutu Centralnemu Biuru Antykorupcyjnemu* (M.P. z 2010 r. Nr 76, poz. 953).

Leksykony i słowniki

Larecki J., *Wielki leksykon służb specjalnych świata: organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny*, Warszawa 2007.

Monografie i opracowania

Aleksandrowicz T.R., *Analiza informacji w administracji i biznesie*, Warszawa 1999.

Analiza informacji w służbach policyjnych i specjalnych, J. Konieczny (red.), Warszawa 2012.

Analiza informacji w zarządzaniu bezpieczeństwem, K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), Warszawa 2013.
Aparat bezpieczeństwa wobec emigracji politycznej i Polonii, R. Terlecki (red.), Warszawa 2005.
Baranowska-Szczepańsk M., *Dziennikarstwo w pytaniach i odpowiedziach*, Poznań 2010.
Bazzell M., *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*, January 2014.
Bean H., *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence*, Santa Barbara–Denver–Oxford 2011.
Bielak F., *Służby wywiadowcze Republiki Federalnej Niemiec*, Warszawa 1985.
Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki, W. Filipowski, W. Mądrzejowski (red.), Warszawa 2012.
Bolechów B., *Terroryzm. Aktorzy, statyści, widownie*, Warszawa 2010.
Borkiewicz J., Cichocki J., Pełczyńska-Nałęcz K., *Okręt Koszykowa*, Warszawa 2007.
Ciecierski M., *Wywiad biznesowy w korporacjach transnarodowych. Teoria i praktyka*, Toruń 2009.
Couch N., Robins B., *Big Data for Defence and Security*, "RUSI Occasional Paper", September 2013, https://www.rusi.org/downloads/assets/RUSI_BIGDATA_Report_2013.pdf
Dulles A.W., *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World*, Washington 2006.
Handbook of Intelligence Studies, L. K. Johnson (ed.), London-New York 2006.
Hannas W. C., Mulvenon J., A. Puglisi B., *Chinese industrial espionage: Technology acquisition and military modernization*, London-New York 2013.
Herman M., *Potęga wywiadu,* Warszawa 2002.
Historia z konsekwencjami – rozmawiają Krzysztof Kozłowski i Michał Komar, Warszawa 2009.
Intelligence and the National Security Strategist: Enduring Issues and Challenges, R.Z. George, R.D. Kline (eds.), Lanham 2006.
Instrukcje pracy kontrwywiadowczej Wojskowej Służby Wewnętrznej wraz z instrukcjami prowadzenia dokumentacji i ewidencji (1957-1990), B. Kapuściak (red.), Kraków 2010.
Jawers E., *Agent, handlarz, prawnik, szpieg: Tajemniczy świat korporacyjnego szpiegostwa*, Kraków 2010.
Keegan J., *Wywiad w czasie wojny. Zdobywanie wiedzy o nieprzyjacielu od czasów napoleońskich do al-Kaidy*, Warszawa 2003.
Korzeniowski L., Pepłoński A., *Wywiad gospodarczy. Historia i współczesność*, Kraków 2005.
Kozaczuk W., *Bitwa o tajemnice. Służby wywiadowcze Polski i Rzeszy Niemieckiej 1922-1939*, Warszawa 1999.
Godson R., *Dirty Tricks or Trump Cards. U.S. Covert Action & Counterintelligence*, New Jersey 2008
Kwięciński M., *Wywiad gospodarczy w zarządzaniu przedsiębiorstwem*, Warszawa-Kraków 1999.
Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011.
Mider D., *Partycypacja polityczna w Internecie*, Warszawa 2008.
Minkina M., *Wywiad w państwie współczesnym*, Warszawa 2011.
Nowa twarz Business Intelligence, R. Jesionek (red.), http://it-manager.pl/wp-content/uploads/Nowa-twarz-BI1.pdf
Nowak W., *Metody pracy kontrwywiadowczej*, Warszawa 1985.
O dziennikarstwie śledczym: normy, zagrożenia, perspektywy, M. Palczewski, M. Worsowicz (red.), Łódź 2009.

Olcott A., *Open Source Intelligence in a Networked World*, London-NewYork 2012.
Open Source Intelligence in Twenty-First Century, Ch. Hobbes, D. Sailsbury (eds.), New York 2014.
Pleskot P., *Dyplomata, czyli szpieg. Działalność służb kontrwywiadowczych PRL wobec zachodnich placówek dyplomatycznych w Warszawie (1956-1989). Część pierwsza*, Warszawa 2013.
Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu, Paprzycki L. K., Rau Z. (red.), Warszawa 2009.
Ranson H. H., *Central intelligence and national security*, Cambridge 1958.
Rola mediów w przeciwdziałanie terroryzmowi, K. Liedel, P. Piasecka (red.), Warszawa 2009.
Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji, K. Liedel, P. Piasecka, T. R. Aleksandrowicz (red.), Warszawa 2014.
Siemiątkowski Z., *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009.
Spark D., *Dziennikarstwo śledcze: studium techniki*, Kraków 2007.
Steele R. D., *The Open-Source Everything Manifesto: Transparency, Truth, and Trust*, Berkeley 2012.
Surma J., *Business Intelligence*, Warszawa 2009.
Terroryzm w medialnym obrazie świata, K. Liedel, S. Mocek (red.), Warszawa 2010.
Turaliński K., *Wywiad gospodarczy i polityczny. Metodyka, taktyka i źródła pozyskiwania informacji*, Radom 2011.
Twenty-First Century Intelligence, W.K. Wark (ed.), London 2008.
Volkoff V., *Dezinformacja: Oręż wojny*, Warszawa 1991.
Więckiewicz Z., *Niektóre formy i metody działalności wywiadowczej. Publikacje i międzynarodowy ruch osobowy,* Warszawa 1974.
Wywiad wojskowy II Rzeczpospolitej, Kołakowski P., Popłoński A. (red.), Kraków 2011.
Zalewski S., *Służby specjalne w państwie demokratycznym*, Warszawa 2005.
Zamach w Norwegii Nowy wymiar zagrożenia terroryzmem w Europie, K. Liedel, P. Piasecka, T. R. Aleksandrowicz (red.), Warszawa 2011.
Zhongwen H., Zongxiao W., *Sources and Techniques of Obtaining National Defense Science and Technology Intelligence,* Beijing 1991.

Artykuły

Backfried G., Schmidt Ch., Pfeiffer M., *Open Source Intelligence in Disaster Management*, http://www.csis.pace.edu/~ctappert/dps/2012EISIC/data/4782a254.pdf
Błoński M., *Twitter i „mściwi bibliotekarze" z Open Source Center*, 4 listopada 2011, http://kopalniawiedzy.pl/Open-Source-Center-CIA-bialy-wywiad-Twitter-Facebook,14232
Byrska J., *Przyszłość należy do łowców informacji. Nowe multimedialne zawody*, „Gazeta Wyborcza", dod. „Komputery i Biuro" 1996, nr 38.
Cisek S., *Broker informacji: istota zawodu*, http://eprints.rclis.org/bitstream/10760/10880/1/Cisek_broker_informacji_istota.pdf
Cisek S., *Szara literatura jako źródło informacji biznesowej. Zarys problematyki,* http://ebib.oss.wroc.pl/ 2002/40/cisek.php#3
Clark R.M., *Perspectives on Intelligence Collection,* "The Intelligencer: Journal of U.S. Intelligence Studies", vol. 20, no. 2 (Fall/Winter 2013).
Daniel J., *Tor: Ciemna strona Głębokiego Internetu*, http://tdint.pl/jan-daniel/tor-ciemna-strona-glebokiego-internetu

Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska - studium przypadku*, http://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf

Gibson S., *Open Source Intelligence: An Intelligence Lifeline*, *„RUSI" 2004*, no. 1 (149).

Gill J., *OpenMIND – precyzyjne narzędzie pozyskiwania informacji wywiadowczych z otwartych źródeł,* „Ochrona Mienia i Informacji" 2012, nr 1.

Greenwald G., MacAskill E., *NSA Prism program taps in to user data of Apple, Google and others,* "The Guardian", 7 czerwca 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Hribar G., Podbregar I., Ivanuša T., *OSINT: A "Grey Zone"?,* "International Journal of Intelligence and CounterIntelligence" 2014, vol. 27, issue 3.

Jagiełło R., *Wybrane aspekty wojskowego rozpoznania osobowego,* „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9 (5).

Janke I., *Tajni potrzebują ciszy,* „Życie", 21 grudnia 1996, http://j59.tripod.com/zycie.html

Kaniewski Ł., *Drugie dno Internetu*, „Focus" 2014, nr 1 (220).

Karciarz M., Dutko M., *Informacja w Internecie*, Warszawa 2010.

Kelso P., *A wealth of knowledge,* "The Guardian", 31 October 2001, http://www.theguardian.com/world/2001/oct/31/afghanistan.politicsphilosophyandsociety

Kołakowski P., *„Laboratorium" Komórka Analityczna Józefa Piłsudzkiego*, „Słupskie Studia Historyczne" 2010, nr 16.

Kozłowski P., *CRIP – wszystkie dane publiczne w jednym miejscu*, http://datablog.pl/2014/05/21/crip-dane-publiczne-jednym-miejscu

Król A., *Broker informacji – powstawanie nowego zawodu*, „Zagadnienia Naukoznawstwa" nr 1 (159).

Leetaru K., *The Scope of FBIS and BBC Open-Source Media Coverage, 1979–2008 (U)*, "Studies in Intelligence" vol. 54, no. 1 (March 2010).

Liaropolus A. N., *A (R)evolution in Intelligence Affairs? In Search of a New Paradigm,* "RIEAS: Research Paper", No. 100 (June 2006).

Makarski A., *Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego. Geneza, zasady działania oraz doświadczenia po pierwszym roku funkcjonowania* [w:] „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2 (2), s. 105-106.

Makowski A., *Na rzecz obcego wywiadu*, „Wprost" „Wprost" 2014, nr 4 (1612).

McGreal Ch., *Is WikiLeaks hi-tech terrorism or hype? Washington can't decide,* "The Guardian", 5 February 2011, http://www.theguardian.com/media/2011/feb/05/ wikileaks-hi-tech-terrorism-hype

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

Mercado S. C., *FBIS Against the Axis, 1941-1945*, "Studies in intelligence", no. 11 (Fall-Winter 2001).

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

Minas H., *Can the Open Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century?,* "RIEAS: Research Paper", No. 139, (January 2010).

Niemczyk P., *BAI*, „Przegląd Bezpieczeństwa Wewnętrznego" Wydanie Specjalne, 6 kwietnia 2010.

Niemczyk P., *Wywiadownie gospodarcze jako źródło informacji „białego wywiadu"*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9 (5).
Pallaris Ch., *Open Source Intelligence: A Strategic Enabler of National Security*, *"CSS* Analyses in *Security Policy",* Vol. 3, No. 32 (April 2008).
Politi A., *The Citizen as "Intelligence Minuteman",* "International Journal of Intelligence and CounterIntelligence" 2003, vol. 16, no. 1.
Potejko P., *10 lat Centralnego Ośrodka Szkolenia ABW w Emowie,* „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 3.
Pringle R. W., *The Limits of OSINT: Diagnosing the Soviet Media*, 1985-1989, "International Journal of Intelligence and CounterIntelligence" 2007, vol. 20, no. 2.
Przybylski J., *Zaczytani agenci CIA*, „Rzeczpospolita", 7 listopada 2011, http://www.rp.pl/artykul/748071. html?print=tak&p=0
Rachid-Chehab M., *Eliot Higgins. Człowiek, który przyłapał Putina*, http://wyborcza.pl/magazyn/1,143016,17300814,Eliot_Higgins__Czlowiek__ktory_przylapal_Putina.html
Radwaniak K., *Biały wywiad w policji – narzędzie rozpoznawania zagrożeń terrorystycznych*, „Studia prawnicze. Rozprawy i Materiały" 2012, nr 2 (11).
Rovner J., *Intelligence in the Twitter Age*, „International Journal of Intelligence and CounterIntelligence" 2013, no. 26, vol. 2.
Sajduk B., *Big data – polityczne i militarne aspekty rewolucji technologii informatycznych*, http://www.nowapolitologia.pl/politologia/stosunki-miedzynarodowe/big-data-polityczne-i-militarne-aspekty-rewolucji-technologii-informatycznych
Serafin T., Hejduk A., *Wywiad jawnoźródłowy w walce z terroryzmem na pograniczu afgańsko-pakistańskim*, „Ochrona Mienia i Informacji" 2012, nr 1.
Schaurer F., Störger J., *The Evolution of Open Source Intelligence (OSINT),* "The Intelligencer: Journal of U.S. Intelligence Studies", vol. 19, no. 3, (Winter/Spring 2012).
Sienkiewicz B., *Historia pewnego złudzenia*, „Przegląd Bezpieczeństwa Wewnętrznego" Wydanie Specjalne, 6 kwietnia 2010.
Starzyk T., *Wywiadownie gospodarcze stosują biały wywiad*, „Gazeta Finansowa Online", 27 sierpnia 2012, http://www.gf24.pl/9344/wywiadownie-gospodarcze-stosuja-bialy-wywiad
Stromczyński B., Waszkiewicz P., *Biały wywiad* w *praktyce pracy organów ścigania* na *przykładzie wykorzystania serwisów społecznościowych*, „Prawo i Prokuratura" 2014, nr 5.
Szymaniuk R., *Cyberterroryzm – wcale nie wirtualne zagrożenie*, „Kwartalnik Bellona" 2009 nr (4).
Szymielewicz K., *Szpieg w pajęczynie*, „Polityka" 2014, nr 14 (2952).
Techniki wywiadowcze – biały, czarny i szary wywiad, http://www.detektyw.edu.pl/techniki-wywiadowcze-bialy-czarny-i-szary-wywiad
Walczuk-Niewiadomska A., Czapnik G., Gruszka Z., *Brokerstwo informacyjne w Polsce – przegląd publikacji*, „Acta Universitatis Lodziensis. Folia historica" 2013, nr 17.
Worden R. L., *Gathering Multidisciplinary Information for the Policy-Making Community*, http://www.loc.gov/rr/frd/pdf-files/info_for_policymakers.pdf

Dokumenty

Broker informacji (researcher) (262204), Krajowy standard kompetencji zawodowych, Centrum Rozwoju Zasobów Ludzkich Ministerstwa Pracy i Polityki Społecznej, Warszawa 2013.
Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities. Guidance and Recommendations, February 2013.
Open Source Intelligence, FMI 2-22.9, Headquarters, Department of the Army, Washington 2006.

Open Source Intelligence, ATP 2-22.9, Headquarters, Department of the Army, Washington 2012.
Open Source Intelligence (OSINT): Issues for Congress, CRS Report for Congress, R.A. Best, A. Cumming (eds.), Congressional Research Service, Washington 2007.
Rozpoznanie wojskowe, SGWP 1531/2001 (jawne), Warszawa 2001.
NATO Open Source Intelligence Handbook, Norfolk, November 2001.
NATO Open Source Intelligence Reader, Brussels, February 2002.
NATO Intelligence Exploitation of the Internet, Brussels, October 2002.

Źródła internetowe

http://www.abw.gov.pl
http://www.skw.gov.pl
http://www.sejm.gov.pl
http://www.osw.waw.pl
http://krs.ms.gov.pl
https://www.ceidg.gov.pl
http://ekw.ms.gov.pl
http://pdi.ms.gov.pl
http://www.mediaquest.pl
http://edu.opensourceintelligence.pl
http://rynekinformacji.pl
http://niwserwis.pl
http://www.paulo.pl
http://nauka.opi.org.pl
http://nauka-polska.pl
http://www.pap.pl
http://geoportal.gov.pl
http://www.osgeo.org
http://www.bip.gov.pl
http://ibin.us.edu.pl
http://www.mini.pw.edu.pl
http://obserwatorpolityczny.pl
http://mojepanstwo.pl
http://stowarzyszeniesowa.pl
http://www.defence24.pl
https://panoptykon.org
http://www.phibetaiota.net
https://www.cia.gov
http://www.oss.net
http://www.justice.gov
http://www.lib.berkeley.edu
http://www.globalsecurity.org
http://www.inteltechniques.com
http://deep-web.org
http://www.wikileaks.org
http://www.stratfor.com
http://www.ihs.com
http://www.aiip.org
http://www.csis.pace.edu
http://www.bbc.co.uk
http://www.livescience.com
http://www.cicentre.com
http://osintinsight.com
http://books.google.com
http://bing.com/maps
http://www.academia.edu
http://newspaperarchive.com
https://www.bellingcat.com/about/
http://www.sas.com
http://fas.org
http://archive.org/web
https://wigle.net

Summary

The book provides an analysis of using publicly available sources in intelligence activities, with reference to history, practice and further perspectives. Also, it includes an overview of the most important present-day open sources as well as identifies certain trouble areas, in which the open source intelligence method can be used most effectively.

The primary objective of the analysis is to present the specifics of open sources intelligence (OSINT), while presenting both its advantages and potential, as well as its limitations and drawbacks. The book's aim is also to show the importance of the role that open source information has in the contemporary theory of intelligence, as well as the significance of the information technology revolution and the development of the Internet in OSINT's evolution.

The first chapter of the book focuses on three aspects. First of all, it contains a conceptual grid, necessary for further analysis, and gives an explanation of the concept of open sources and open source intelligence. Secondly, the chapter defines OSINT as a distinct intelligence discipline. Thirdly, it shows the advantages and potential as well as drawbacks and limitations of OSINT, which are always involved in intelligence collected from open sources, while outlining new challenges and perspectives of their use.

The second chapter focuses on the history of OSINT, identifying a number of factors which have determined its creation and have affected its evolution. This part of the book presents an extremely rich and varied tradition of using open source information, both by state security services, as well as private entities. Particular attention was paid to outlining the history of the development of OSINT in Poland, ranging from the Second Polish Republic, through the Polish People's Republic period, to modern times.

The third chapter is an analysis of various open sources of information; both traditional sources such as newspapers, grey literature, radio and television and generally available records and documents as well as more contemporary ones – geo-information and the Internet. In particular, the latter source, or more precisely this "meta-source" of information is analysed thoroughly, showing its almost unimaginable potential in intelligence activities.

The fourth and final chapter presents selected areas of the use of open source information; in the private sector – business information agencies, multinational corporations providing strategic intelligence services or finally, independent information brokers; in the public sector – activities of secret services, police and selected branches of public administration. The chapter ends with an analysis of the role that the open source intelligence method plays in terrorist activities.

The major conclusion drawn from the book is that the most important factor resulting in a significant increase in the role and scale of use of open sources in intelligence activities is the continually advancing revolution in information technology, in particular the creation and development of the Internet.