Krzysztof Radwaniak
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego

Biały wywiad w policji – narzędzie rozpoznawania zagrożeń terrorystycznych

Wprowadzenie

Policja, jako formacja powołana do ochrony bezpieczeństwa ludzi oraz utrzymywania bezpieczeństwa i porządku publicznego, swoją misję realizuje przede wszystkim przez ochronę życia i zdrowia ludzi oraz ich mienia przed bezprawnymi zamachami naruszającymi te dobra[1], a akt terrorystyczny do tej grupy niewątpliwie należy. Na szczeblu krajowym i w kontaktach międzynarodowych policja, a w szczególności wyspecjalizowane jednostki organizacyjne Komendy Głównej Policji, takie jak Biuro Operacji Antyterrorystycznych, Centralne Biuro Śledcze, Główny Sztab Policji czy Biuro Prewencji, realizują zadania związane z przeciwdziałaniem i zwalczaniem zagrożeń terrorystycznych przede wszystkim na poziomie taktycznym, współdziałają też z innymi podmiotami na poziomie strategicznym i operacyjnym[2].

Policja prowadzi działania defensywne i ofensywne. Działania defensywne są działaniami obronnymi i noszą nazwę działań antyterrorystycznych, natomiast działania ofensywne, czyli bezpośrednie akcje siłowe wyspecjalizowanych służb, mające na celu likwidację zagrożeń terrorystycznych, noszą nazwę działań kontrterrorystycznych[3]. Najogólniej ujmując, reaktywne działania policji mają miejsce po uzyskaniu informacji o zagrożeniu, natomiast działania proaktywne skupiają się na zapobieganiu wystąpienia zdarzeń ter-

[1] Ustawa o policji z 6 kwietnia 1990 r., Dz.U. 1990 Nr 30 poz. 179, z późn. zm., art. 1.
[2] www.msw.gov.pl/portal/pl/85/8478/Zagrozenia_terrorystyczne.html [14.10.2012].
[3] K. Dębiński, *Przeciwterroryzm – rola i zadania polskiej policji w działaniach antyterrorystycznych*, [w:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu*, red. L. Paprzycki, Z. Rau, Warszawa 2009, s. 262, 263.

rorystycznych. W ocenie K. Liedla[4], podejście proaktywne jest lepszą opcją, gdyż zmniejsza ryzyko wystąpienia aktu terrorystycznego, a tym samym strat w ludziach i mieniu. W ustawie o policji brak bezpośredniego odniesienia działań tej formacji do terroryzmu, a jednak (choćby intuicyjnie) trudno wyobrazić sobie jej pasywność wobec tego rodzaju zagrożeń. Czym zatem jest terroryzm? Słowo „terror" pochodzi od łacińskiego wyrazu *terrere* – straszyć, wywoływać przerażenie. Zatem akt terrorystyczny ma na celu właśnie wzbudzenie niepokoju, ma bezwzględny charakter i jest obliczony na możliwie największy wpływ społeczeństwo. Przemoc stosowana jest dla osiągnięcia celów politycznych, religijnych bądź ideologicznych. Popełniane przestępstwo ma często symboliczny charakter, jest zamierzone na efekt wykraczający poza bezpośrednie ofiary[5]. Przytoczone powyżej źródłosłów i definicja nie są oczywiście jedynymi w literaturze[6]. Niemniej przybliżenie pojęcia i zjawiska terroryzmu na tak ogólnym poziomie prowokuje zadanie ważnego pytania: dlaczego pomimo nieostrego ujęcia w przepisach, w oparciu o które pracuje policja, terroryzm jest zauważalny i pozostaje w jej szczególnym zainteresowaniu?

Definicja terroryzmu ewaluuje wraz z dynamiką procesów społecznych, zmienne bywają role ich uczestników. Często wczorajsi „terroryści", po osiągnięciu władzy stają się „mężami stanu", a upadli władcy podlegają surowej ocenie, nie tylko moralnej, ale i karnej. Policja jako organ państwowy powołany do „ochrony bezpieczeństwa ludzi oraz do utrzymywania bezpieczeństwa i porządku publicznego"[7], unika z zasady zaangażowania politycznego, skupiając się w głównej mierze na przeciwdziałaniu przestępczości. Biorąc pod uwagę poszczególne cechy terroryzmu, tj. popełnianie poważnych przestępstw kryminalnych, takich jak morderstwo, uszkodzenie ciała, mienia znacznej wartości itp. oraz motywacji, na podstawie których zostały one dokonane, np. chęć zastraszenia społeczności w celu wywołania zmian na scenie politycznej, jawi się jej zharmonizowana definicja[8]. Zatem w konwencjonal-

[4] K. Liedel, *Zarządzanie informacją w walce z terroryzmem*, Warszawa 2010, s. 58–59.

[5] F. Boltz Jr., K. J. Dudonis, D. P. Schulz, *The Cuterterrorism: Handbook Tactics, Procedures, and Techniques*, London–New York–Singapore 2005, s. 3, 4.

[6] Zob.: B. Hoffman, *Oblicza terroryzmu*, Warszawa 1999. Autor pochodzenie słowa „terroryzm" wywodzi z okresu rewolucji francuskiej, kiedy system *regime de la terreur*, miał pozytywne konotacje, jako instrument zarządzania w na nowo budowanym, w założeniu – lepszym – społeczeństwie. Miał na celu zastraszanie kontrrewolucjonistów i ogólnie mówiąc pozostałych „wrogów ludu".

[7] Ustawa o policji…, art. 1, ust. 1–2, pkt. 1–4.

[8] Decyzja ramowa Rady 2002/475/WSiSW z 13 czerwca 2002 r. w sprawie zwalczania terroryzmu, www.europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33168_pl.htm [19.10.2012].

nym ujęciu, na poziomie ogólności użytecznym dla dalszych rozważań można przyjąć, że terror, to metoda akcji przestępczej, przez którą sprawcy dążą do narzucenia przy pomocy strachu swej dominacji społeczeństwu lub państwu, aby zachować, przekształcić lub zniszczyć więzi porządku prawnego.

Policja inicjuje lub włącza się w działania związane z przeciwdziałaniem zagrożeniom terrorystycznym przez działania prewencyjne, zasadniczo niejawną pracę, określaną jako operacyjną i przez fizyczną likwidację terroryzmu[9]. J. Szafrański w publikacji *Edukacja antyterrorystyczna* zwrócił uwagę na równie istotną płaszczyznę działań antyterrorystycznych, tj. reagowanie[10]. Warto w tym miejscu przybliżyć wskazane obszary działań związanych z zapobieganiem i zwalczaniem terroryzmu, ze szczególnym uwzględnieniem zadań policji:

- rozpoznanie, ukierunkowane na rozpoznanie potencjalnych zagrożeń, środowisk podatnych na werbunek, osób lub organizacji prowadzących lub wspierających działalność terrorystyczną, oraz wymiana tychże informacji z innymi służbami,
- działania prewencyjne, realizowane przez ochronę osób i obiektów wymagających szczególnej ochrony, działania zabezpieczające w trakcie patroli prewencyjnych w służbach patrolowych i obchodowych oraz przez odpowiednią politykę kryminalną państwa,
- fizyczne zwalczanie, aktywność policji w zakresie kontrterroryzmu, tj. zwalczanie wszelkich aktów terroryzmu realizowane przez wyspecjalizowane służby, w szczególności przez oddziały antyterrorystyczne,
- reagowanie, w sytuacji zaistnienia ataku terrorystycznego, realizowane przez wdrażanie określonej wiedzy lub procedur przez uczestników zdarzenia lub służby odpowiedzialne za jego likwidację. Powyższe działania są realizowane w ramach systemu zarządzania kryzysowego[11].

Fizyczne zwalczanie oraz reagowanie (najogólniej ujmując), związane jest z umiejętnością likwidowania zagrożeń przez wyspecjalizowane jednostki umiejscowione w strukturach konkretnych służb, jak również sprawnością działania i współdziałania w sytuacji kryzysowej, w tym zagrożenia terrorystycznego. Działania prewencyjne również związane są z uzyskaniem określonej wiedzy na temat potencjalnych ataków oraz wypracowania i realizacji procedur ochrony ważnych osób lub obiektów. Innymi słowy, są to działania wymagające rozpoznania zagrożeń, a miarą sprawności służb jest umiejętność przeciwdziałania zagrożeniom i likwidacji skutków po ich wystąpieniu. Jesz-

[9] K. Dębiński, *op. cit.*, s. 267–268.

[10] J. Szafrański, *Edukacja antyterrorystyczna*, [w:] *Zarządzanie kryzysowe wyzwaniem dla edukacji*, red. A. Urban, Szczytno 2007, s. 85.

[11] *Ibidem*, s. 85–86.

cze ściślejszy związek z rozpoznaniem ma odpowiednia polityka kryminalna, a w szczególności profilaktyka społeczna. Zagrożenie terrorystyczne jest zjawiskiem powszechnym, zatem edukacja antyterrorystyczna nie powinna ograniczać się jedynie do szkolenia funkcjonariuszy, ale również zwykłych obywateli. Przykładowo, informacje na temat zachowania osób, które planują dokonanie zamachu terrorystycznego, czy też dokonują werbunku do organizacji terrorystycznych, nie są umiejscowione w próżni. Wyszukanie tego rodzaju informacji i jej wykorzystanie daje szansę zapobieżenia zdarzeniu lub minimalizacji jego skutków. Z kolei wiedza każdego obywatela na temat rozpoznawania sytuacji mogących skutkować wystąpieniem określonych zagrożeń, czy też umiejętności zachowania się w środowiskach podatnych na propagandę terrorystów, może być nieoceniona. Rozpoznanie z kolei jest jednym z najistotniejszych elementów budowania wiedzy w służbach policyjnych i specjalnych, ma bezpośrednie przełożenie na prewencję, likwidację zagrożeń oraz reagowanie. Jak zauważył J. Konieczny[12], w dzisiejszych czasach niezwykle ważne jest budowanie wiedzy, która zapewnia określony potencjał, ale jeszcze istotniejsze jest jej należyte wykorzystanie. Mądrość organizacji w połączeniu z jej doświadczeniem powinna mieć źródło w wiedzy, której elementem budowania jest właśnie rozpoznanie. Objętość referatu nie pozwala na szczegółowy opis wszystkich płaszczyzn działań antyterrorystycznych. Aby dokonać wyboru najwłaściwszego obszaru aktywności policji, gdzie wykorzystuje się biały wywiad, przybliżenie rozpoznania i dalsze rozważania na temat analizy informacji pochodzących ze źródeł otwartych, wydają się ścieżką najbardziej wskazaną.

Biały wywiad w policji

Biały wywiad najogólniej ujmując, jest metodą pozyskiwania i analizy informacji pochodzących z otwartych, ogólnodostępnych źródeł[13]. Kojarzony jest najczęściej z działalnością służb wywiadowczych (cywilnych lub wojskowych), jako jedna z metod jej pracy. Typologia została opracowana w oparciu o rodzaje źródeł informacji, przyjmując nazewnictwo z połączenia skrótu nazwy źródła, którego ma dotyczyć (np. od angielskiego słowa *Human* – człowiek – HUM) oraz skrótu anglojęzycznej nazwy wywiadu (angielskie słowo *Intelligence* – wywiad – INT), czyli HUMINT. Oprócz wymienionej, w praktyce służb wojskowych i niektórych specjalnych wykształciły się ta-

[12] J. Konieczny, *Zagadnienia wprowadzające*, [w:] *Analiza informacji w służbach policyjnych i specjalnych*, red. J. Konieczny, Warszawa 2012, s. 2.

[13] K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011, s. 57–74.

kie metody pracy wywiadowczej, jak SIGINT (*Signal Intelligence*) – wywiad sygnałowy, IMINT (*Imagery Intelligence*) – w oparciu o analizę zdjęć satelitarnych i lotniczych, MASINT (*Measurement and Signature Intelligence*) – realizowany za pomocą specjalistycznych czujników w oparciu o pomiary wszelkich obiektów i prowadzenie na tej podstawie ich identyfikacji oraz charakterystyki, czy wreszcie OSINT (*Open Source Intelligence*) – wywiad prowadzony w oparciu o źródła otwarte. Warto w tym miejscu przybliżyć kilka podstawowych pojęć białego wywiadu. W publikacji pt. *NATO Open Sources Intelligence Handbook* (2001 s. 2, 3) znajdują się następujące terminy:

- dane jawne (*open source data* – OSD) – surowe dane dostępne w otwartych źródłach,
- informacje z otwartych źródeł (*open source information* – OSINF) – dane wstępnie opracowane, zebrane w jeden dokument, poddane pewnym zabiegom edytorskim (np. książki, artykuły i inne publikacje prasowe, raporty, inne),
- biały wywiad (*open source intelligence* – OSINT) – metoda, ale również wynik pewnych czynności w stosunku do informacji z otwartych, jawnych źródeł. Tak rozumiany biały wywiad to opracowanie analityczne (produkt analityczny), zawierające konkretne wnioski wynikające z analizy wyłącznie informacji z otwartych źródeł,
- zweryfikowany, potwierdzony biały wywiad (*validated open source intelligence* – OSINT-V) – produkt o wysokim stopniu pewności, prawdopodobieństwa. Jest efektem pracy wyszkolonego analityka, zazwyczaj posiadającego dostęp do różnych, innych niż otwarte informacji lub baz danych (także objętych tajemnicą, niejawnych). OSINT-V jest uzasadniony tego rodzaju informacjami, ale może także być potwierdzony przez informacje ze źródeł otwartych, co do których nie ma wątpliwości, że są pewne, wiarygodne i wartościowe[14].

Opierając się na wnioskach K. Radwaniaka i P. J. Wrzoska, dotyczących białego wywiadu[15], na obecnym etapie rozważań można przyjąć, że w działaniach policji stosowany był i nadal praktykuje się biały wywiad. Przy obecnym, bardzo szerokim dostępie policjantów do otwartych źródeł (w dużej mierze internetowych), trudno sobie wyobrazić prowadzących rozpoznanie lub różnego rodzaju postępowania funkcjonariuszy, którzy unikaliby korzystania z ogólnodostępnych źródeł informacji.

[14] US Army, *NATO Open Sources Intelligence Handbook*, www.au.af.mil/au/awc/awcgate/nato/osint_reader.pdf [20.10.2012].

[15] K. Radwaniak, P. J. Wrzosek, *Biały wywiad w policji – pozyskiwanie i analiza informacji ze źródeł otwartych, Analiza informacji...*, s. 113–120.

Paradoksalnie, przy coraz szerszym dostępie do otwartych źródeł informacji, przy ustalaniu regulaminów komend sukcesywnie zmienia się lub usuwa zadania związane z białym wywiadem. Aby bliżej zobrazować ten proces, można porównać, przykładowo, zadania Wywiadu Kryminalnego ujęte w Regulaminach KGP z roku 2004 i 2010. W Regulaminie KGP z 2004, a dokładnie w załączniku nr 13 do Zarządzenia nr 366 Komendanta Głównego Policji z 20 kwietnia 2004 r. w sprawie regulaminu Komendy Głównej Policji, w pkt. 1 ppkt. 2 ujęto jedno ze szczegółowych zadań Wydziału: „pozyskiwanie i gromadzenie informacji przydatnych do rozpoznania osobowego, obiektowego i zagadnieniowego z ogólnie dostępnych, otwartych źródeł informacji"[16] [podkreślenie moje – K.R.]. Z kolei Zarządzenie nr 749 Komendanta Głównego Policji z 27 maja 2010 r. w sprawie regulaminu Komendy Głównej Policji, nie zawiera już podobnych zapisów. Najbardziej zbliżony do cytowanego powyżej zadania ujętego w załączniku nr 3, tj. pkt 1 ppkt 5, „określanie i identyfikacja, na podstawie prowadzonych analiz, czynników sprzyjających występowaniu przestępczości oraz metod jej zapobiegania"[17], wskazuje na wysoki stopień ogólności zadania oraz pominięcie kluczowych terminów dotyczących białego wywiadu. Odnosząc się do praktyki policyjnej i badań z tego zakresu można przyjąć, że biały wywiad jest stosowany, ale w formie ograniczonej, niemalże „intuicyjnie", bez wsparcia specjalistycznej wiedzy zawartej np. w piśmiennictwie krajowym i zagranicznym. Korzystanie z doświadczeń wywiadowczych innych służb, przy uwzględnieniu specyfiki pracy policji, z pewnością podniosłoby poziom jej pracy.

Edukacja antyterrorystyczna z uwzględnieniem białego wywiadu

Jak zostało wcześniej zaznaczone, zagrożenie terrorystyczne należy traktować jako powszechne, dlatego edukacja w tym zakresie powinna być udziałem całego społeczeństwa, nie tylko odpowiednich służb. Warto tu przybliżyć przeprowadzone przez J. Szafrańskiego badania dotyczące poziomu edukacji antyterrorystycznej w polskich szkołach policji. Z analizy programów szkoleniowych wynika, że policjanci – słuchacze szczególnie kursów podstawowych, mają w programie przedmioty dotyczące przeciwdziałania terroryzmowi, ale w liczbie godzin nieadekwatnej do treści koniecznych do przekazania[18]. Warto nadmienić, że są to zajęcia podające ogólne informacje o terroryzmie

[16] Zarządzenie nr 366 Komendanta Głównego Policji z 20 kwietnia 2004 r., Dz.U. KGP, nr 7.

[17] Zarządzenie nr 749 Komendanta Głównego Policji z 27 maja 2010 r., Dz.U. KGP, nr 6.

[18] J. Szafrański, *Edukacja antyterrorystyczna*, [w:] *Zarządzanie kryzysowe wyzwaniem dla edukacji*, red. A. Urban, Szczytno 2007, s. 87.

i ewentualnie (chociaż w wymiarze niedostatecznym) sposób postępowania policjanta na miejscu zdarzenia. Wiedza dotycząca sposobów rozpoznania osób, organizacji oraz innych zagrożeń terrorystycznych przekazywana jest w sposób nieusystematyzowany, natomiast zagadnienia dotyczące białego wywiadu, o ile w ogóle występują – są traktowane marginalnie. Na wyższym poziomie szkolenia programy przewidują zapoznanie słuchaczy z podstawową wiedzą na temat wywiadu jawnoźródłowego. Przykładowo, w programie szkolenia dla absolwentów szkół wyższych (SASW) w Wyższej Szkole Policji w Szczytnie, odbywają się wykłady dotyczące właśnie białego wywiadu. Uczelnia prowadzi również studia podyplomowe w zakresie kryminalistyki w procesie karnym, gdzie białemu wywiadowi poświęcono 13 godzin. Popularne i wydawałoby sie nośne twierdzenie, że „w dzisiejszym świecie nie chodzi już o to, czy wystąpi sytuacja kryzysowa czy nie, ale o to, kiedy, jakiego rodzaju i w jaki sposób", nie zawsze jednak trafia do słuchaczy – policjantów, którzy jako jedni z pierwszych mogą zetknąć się z atakiem terrorystycznym lub przez stosowanie określonej wiedzy takowemu zapobiec. Policjant często myśli „nic nie ma prawa się wydarzyć, a jeżeli już, to z pewnością gdzie indziej" lub „zagadnienie jest ciekawe, ale do walki z terroryzmem są inne służby". Następnie wracając do macierzystej jednostki ten sam funkcjonariusz często słyszy „mamy wiele innych ważniejszych spraw na głowie, dajmy sobie spokój z terroryzmem, weźmy się do pracy" itp. Oczywiście policja posiada opracowane procedury związane z osiąganiem gotowości do przeciwdziałania zagrożeniom terrorystycznym (pięciostopniowe – oznaczone kolorami, od zielonego do czerwonego, w zależności od stopnia zagrożenia)[19]. Takie procedury posiada każda jednostka organizacyjna policji, od komendy głównej począwszy, a na komisariatach skończywszy. Są to jednak dokumenty chronione klauzulami niejawności. Mając na względzie „wrażliwość" niektórych informacji utajnianie wydaje się słuszne pod kątem ich ochrony, lecz taka sytuacja nie sprzyja budowaniu wiedzy szeregowych policjantów na temat istoty zagrożeń terrorystycznych, zapobieganiu im, udziału w zwalczaniu, czy reagowaniu[20].

Dokumentacja często tworzona jest przez specjalistę w dziedzinie zarządzania kryzysowego, a użyta terminologia i procedury nie zawsze są zrozumiałe nawet do przełożonych. Ponadto katalog zadań policji z biegiem lat

[19] Zarządzenie nr pf 964 Komendanta Głównego Policji z 9 września 2004 r. w sprawie określenia sposobu osiągania gotowości policji do przeciwdziałania zagrożeniom terrorystycznym.

[20] Obecnie trwają prace nad przepisami dotyczącymi wprowadzenia nowego aktu prawnego w sprawie określenia sposobu osiągania gotowości policji do przeciwdziałania zagrożeniom terrorystycznym, ma to być dokument jawny. Tym samym powyższy akapit może stracić częściowo na aktualności, co jest zgodne z przedstawionymi przez autora postulatami.

systematycznie się poszerza, a nieubłagany „wyścig mierników ocennych"[21] sprawia, że z natury niezwykle istotne sprawy rozpoznawania i przeciwdziałania zagrożeniom terrorystycznych bywają traktowane jako drugorzędne. Tak zarysowany problem zaburzeń komunikacji i wymiany informacji o zagrożeniach w policji (a także poza jej struktury), nie napawa optymizmem. Aktywizacja antyterrorystyczna nie tylko funkcjonariuszy policji, ale każdego obywatela napotyka bariery organizacyjne i kulturowe. Panująca w służbach policyjnych „kultura tajności" w stosunku do równie umownie określanej „kultury otwartości"[22] sprawia, że poważaniem cieszą się informacje zdobyte przez pracę operacyjną (por. HUMINT), a opatrzenie dokumentów klauzulami niejawności ma w założeniu nadawać informacjom znaczenia. W praktyce często zdarza się, że np. dyżurni komend powiatowych otrzymują niejawne komunikaty, których treść jest zbliżona do wiadomości, które słyszeli poprzedniego dnia w środkach masowego przekazu. Taka sytuacja często rodzi niezrozumienie, a nawet skrywaną kpinę tam, gdzie powinna być najmniej wskazana. Tak naprawdę już po uzyskaniu informacji z otwartych źródeł, hipotetyczny policjant winien na nią odpowiednio zareagować, nie czekając na komunikaty z „centrali".

Tutaj pojawia się kolejna przeszkoda w komunikacji – nieumiejętność wychwycenia informacji o zagrożeniu, a jeśli już zostanie zauważona – brak wiedzy na temat możliwości jej wykorzystania. Nierzadko funkcjonariusze lub osoby cywilne, będące w posiadaniu ważnych informacji dla wsparcia rozpoznania często nie wiedzą, w jaki sposób mają je przekazać, zdarza się też, że informacja zostaje przekazana, ale zostaje przez służby zlekceważona[23]. Jaskrawym przykładem tego rodzaju sytuacji były wydarzenia z lipca 2011 r. w Norwegii. Anders Breivik wysadził w powietrze budynek rządowy w centrum Oslo, zabijając 7 osób i raniąc kolejnych 7, a następnie, po kilku godzinach zastrzelił 76 osób, w tym wielu nastolatków. Znamienne jest, że na 90 minut przed atakiem Breivik wysłał do ponad 1000 adresatów poczty elektronicznej swój manifest wraz z linkiem do nagrania wideo, w których zapowiadał atak (opisując szczegółowo jego przygotowanie), tłumaczył też swoje motywy[24]. Komunikat był na tyle jasny, a czasu na zapobieżenie tragedii tak dużo, że na obecnie mówi się o porażce norweskich władz, służb specjal-

[21] M. Otrębski, *Apolityczność policji – nakaz prawny czy zobowiązanie moralne władzy państwowej*, „Bezpieczeństwo. Teoria i Praktyka" 2008, nr specjalny.

[22] H. Bean, *No More Secrets. Open Source Information and the Reshaping of US Intelligence*, Santa Barbara–Denver–Oxford 2011, rozdz. 3: *A Discourse-Centered Perspective on Open Source Developments*.

[23] *Ibidem*, rozdz. 6: *Open Source as a Resource for Citizen Participation in National Security Affairs*.

[24] J. Gill, *Open Mind – precyzyjne narzędzie pozyskiwania informacji wywiadowczych z otwartych źródeł*, „Policja 997" 2011, nr 11, s. 38.

nych, a także moralnej odpowiedzialności zwykłych obywateli. Można tylko przypuszczać, że przypadek norweskiego terrorysty, opisywany powyżej sposób prezentacji poglądów nie był jedyny. Sytuacja taka mogła mieć miejsce w sieciach społecznościowych, np. skupiających środowiska ultraprawicowe, co zapewne również nie zostało dostrzeżone lub po prostu zlekceważone. Należy zatem przyjąć, że takich i podobnych informacji jest i będzie w otwartych źródłach wiele. Dlatego właśnie biały wywiad jako narzędzie rozpoznawania zagrożeń terrorystycznych wart jest docenienia i popularyzacji.

Możliwości wykorzystania białego wywiadu

Pomimo przedstawionych wyżej przeszkód w stosowaniu białego wywiadu, narzędzie to nie jest policjantom obce[25]. Potwierdzeniem tej tezy są ciekawe badania przeprowadzone przez Wojciecha Filipkowskiego, a dotyczące wiedzy funkcjonariuszy policji na temat pozyskiwania i analizy informacji ze źródeł otwartych[26]. Badania zostały przeprowadzone na grupie 263 respondentów, biorących udział w różnego rodzaju szkoleniach i kursach policyjnych. Na pytanie, „czy ankietowany brał udział w szkoleniu specjalistycznym z zakresu zbierania i analizowania informacji pochodzących ze źródeł otwartych", aż 251 osób odpowiedziało przecząco, a tylko 3 miało takie doświadczenie (9 w ogóle nie udzieliło odpowiedzi). Respondenci generalnie mieli wiedzę na temat podstawowych źródeł białego wywiadu, a przeszło połowa z nich (61,45%) w swojej pracy pozyskiwała informacje z tych źródeł. Ponadto ankietowani upatrywali w większym stopniu miejsca białego wywiadu w pracy operacyjnej (42,76%), a tylko 6,90% w postępowaniu przygotowawczym. Warto przy tym zauważyć że najliczniejsza grupa respondentów (48,28) była zdania, że wykorzystanie informacji z otwartych źródeł ma takie samo znaczenie w pracy operacyjnej, jak w postępowaniach przygotowawczych. Trzeba jednak zaznaczyć, że policjanci odpowiadający na to i inne pytania nie zawsze mieli szerszą wiedzę na temat rozumienia białego wywiadu, a także jego usystematyzowanej formy OSINT oraz cyklu wywiadowczego. Niemniej można wyciągnąć wniosek, że prawie połowa ankietowanych widzi korzyści wywiadu jawnoźródłowego na obu etapach wykrywania i ścigania sprawców przestępstw. Wyniki przedstawionych badań są zbieżne z wnioskami P. Chlebowicza, który badając biały wywiad w świetle szeroko pojętej kryminalistyki, umieścił wywiad jawnoźródłowy w obszarze pracy operacyjno-rozpoznawczej

[25] K. Radwaniak, P. J. Wrzosek, *op. cit.*, s. 138–149.

[26] W. Filipkowski, *Wykorzystanie otwartych źródeł informacji. Wyniki badań ankietowych*, [w:] *Biały wywiad, otwarte źródła informacji – wokół teorii i praktyki*, red. W. Filipkowski, W. Mądrzejowski, Warszawa 2012.

z akcentem na czynności rozpoznawcze pod kątem zapewnienia okresowego lub stałego dostępu do informacji, a następnie ich opracowywania i wykorzystania w określonych prawem celach[27]. W ramach swoich badań W. Filipkowski poruszył wiele innych ważnych zagadnień dotyczących białego wywiadu, w opinii autora trafionych i istotnych dla zdiagnozowania wykorzystania w policji, a także wskazania możliwości i barier. Warto też przytoczyć jeszcze jeden wniosek z badań. Otóż na podstawie udzielonych odpowiedzi można postawić tezę, że policjanci widzą potrzebę wykorzystania białego wywiadu praktycznie na każdym szczeblu organizacyjnym policji. Pogląd ten skłania do postrzegania białego wywiadu nie jako ekskluzywnego zajęcia wąskiej grupy analityków w centralnych jednostkach policji, ale jako przydatnego narzędzia pracy policjantów liniowych.

Traktując rozpoznanie jako niezwykle ważny element przeciwdziałania zagrożeniom, w tym terrorystycznym, zasadna będzie analiza obecne uwarunkowania obiegu informacji o zagrożeniach, z zaznaczeniem wykorzystania otwartych źródeł informacji. Obecnie w policji rzadko spotyka się model analizy informacji OSINT (dla przypomnienia, analizie podawane są jedynie informacje pochodzące ze źródeł otwartych, dlatego wnioski z tego rodzaju analizy mogą być wykorzystywane bez ograniczeń prawnych). Narzędziem najbardziej zbliżonym do tradycyjnego białego wywiadu jest wywiad kryminalny, a szczególnie analiza kryminalna. Wywiad kryminalny jest narzędziem pomocniczym w realizacji przez policjantów określonych czynności służbowych, zawiera wiele cech systemowego postępowania z informacją kryminalną i wpisuje się w filozofię wywiadu jawnoźródłowego[28]. Odsyłając czytelnika do bardziej szczegółowych opracowań na ten temat warto jednak (przynajmniej na poziomie praktycznym i w pewnym stopniu ogólności) przybliżyć funkcjonowanie wywiadu kryminalnego w policji. W tego rodzaju podejściu do informacji spotyka się pojęcie cyklu wywiadowczego, na który składają się: pozyskiwanie, ocena, gromadzenie i przetwarzanie informacji, dokonywanie ocen i analiza oraz ukierunkowanie działań (por. Bronicki 2007: 99). Cykl ten jest zbliżony do innych tego rodzaju modeli w pokrewnych służbach. Informacje do analizy są pozyskiwane z wszelkich dostępnych źródeł informacji, w tym właśnie ze źródeł otwartych[29]. Szczególnym narzędziem wywiadu kryminalnego jest System Informacji Operacyjnych (SIO). Wszelkie infor-

[27] P. Chlebowicz, *„Biały wywiad" z perspektywy kryminalistyki*, [w:] *Biały wywiad...*, s. 61–63.

[28] K. Radwaniak, P.J.Wrzosek *Biały wywiad...*, s. 140–144.

[29] Wytyczne nr 1/09 dyrektora Biura Wywiadu Kryminalnego KGP z 29 lipca 2009 r. w sprawie szczegółowego sposobu wykonywania przez funkcjonariuszy i pracowników jednostek oraz komórek organizacyjnych policji, czynności służbowych związanych z przetwarzaniem informacji w Systemie Informacji Operacyjnych, § 7 pkt 2.

macje, w tym pochodzące ze źródeł otwartych, wprowadzane są do systemu danych przy użyciu Systemu Meldunku Informacyjnego (SMI), za pomocą wystandaryzowanego formularza. Informacje powinny mieć przydatność wykrywczą, dowodową lub identyfikacyjną, o dowolnym stopniu wiarygodności bez względu na ich źródło[30]. Generalnie ujmując, każdy policjant może pozyskać informację z otwartego źródła, wykorzystać ją zgodnie z przepisami, a gdy uzna, że dana informacja jest na tyle cenna, że powinna zastać przekazana do szerszego wykorzystania, ma możliwość przekazania jej do systemu za pomocą meldunku informacyjnego[31]. Impulsem do gromadzenia informacji jest spostrzeżenie, że z pozoru mało użyteczna informacja, w połączeniu z innymi informacjami lub użyta w innym kontekście może zupełnie zmienić swój charakter i przynieść korzyści w procesie wykrywczym.

Zdaniem autora, postępowanie z informacjami o zagrożeniu terrorystycznym, w tym pochodzące ze źródeł otwartych mogą mieć podobny obieg, jak pozostałe informacje w SIO, gdzie w określonych zbiorach i podzbiorach gromadzone są wszelkie informacje odpowiadające wskazanym kryteriom. Tego rodzaju zgromadzenie w jednym miejscu wszelkich tematycznych informacji daje możliwość ich usystematyzowania i szerszej analizy. Przy braku w jednostkach terenowych i nadrzędnych stanowisk, które przypisane byłyby głównie do realizacji białego wywiadu, takie postępowanie z informacją z otwartego źródła wydaje się najbardziej optymalne.

Analiza informacji, w tym jawno-źródłowej, może być wykonywana na każdym poziomie decyzyjnym. Za T. Aleksandrowiczem[32] można powiedzieć, że analiza jest tworzeniem przy pomocy intelektu swoistej wartości dodanej, wychodząc poza dostępne fakty, informacje. Innymi słowy, np. pozyskane przez policjanta z otwartych źródeł informacje mogą być przez niego odpowiednio zinterpretowane i wykorzystane w procesie wykrywczym lub po prostu zapomniane. Aby uniknąć błędu zaniedbania, ten sam funkcjonariusz ma możliwość przekazania informacji do Wywiadu Kryminalnego, gdzie zostają zgromadzone i mogą zostać poddane analizie przez specjalistów. Oczywiście opis możliwości postępowania z informacją jawnoźródłową nie jest kompletny. Jak zostało wcześniej zauważone, w tej właśnie formacji występują prawne i techniczne możliwości analizy jawnoźródłowej prowadzonej indywidualnie przez funkcjonariuszy, a także w ramach cyklu wywiadowczego.

Warto się jednak zastanowić, czy jest to „górna granica" możliwości białego wywiadu w policji. Zapoznając się z ofertami producentów nowoczesnych

[30] *Ibidem*.

[31] *Ibidem*.

[32] T. Aleksandrowicz, *Analiza informacji w administracji i biznesie*, Warszawa 1999, s. 26.

technologii i oprogramowań do analizy informacji rysuje się nowe widzenie przedmiotu badań. Przykładem może być produkt szwajcarskiej firmy 3i-MIND[33], specjalizującej się w dziedzinie nowych rozwiązań w zakresie zarządzania ryzykiem dla organów ochrony porządku publicznego oraz agencji wywiadowczych.

W materiałach reklamowych firmy narzędzie przedstawione jest jako „kompletne, całościowe oprogramowanie obejmujące pełen zakres działalności służb i instytucji odpowiedzialnych za bezpieczeństwo". W jego ramach analizowane są informacje z analizy powiązań, analizy geograficznej, monitoringu, różnorodnych baz danych, raportów i dokumentów, wywiadu osobowego oraz właśnie białego wywiadu. Zaletą programu jest jego proaktywność. Ma on za zadanie identyfikowanie i alarmowanie użytkowników o nowych zagrożeniach, osobach podejrzanych i innych anomaliach. Zdaniem twórców produktu, gdyby został on w odpowiednim czasie zastosowany w Norwegii, być może nie doszłoby do masakry na wyspie Utoya[34]. Kolejnym oprogramowaniem komputerowym wspomnianej firmy, umożliwiającym legalne, pełne zbieranie informacji, analizę i zarządzanie informacjami ze źródeł otwartych w czasie realnym, bez konieczności wcześniejszego badania ich zawartości metodami klasycznymi, jest Open Mind. Wyzwaniem dla nowoczesnego OSINT-u jest bowiem:

- olbrzymia ilość i różnorodność informacji,
- zawartość „głębokiej sieci" (*deep weeb*),
- wielojęzyczność, gwary, żargony,
- nieustanne zmiany i aktualizacje
- ukrywanie tożsamości i sfer działania firm i organizacji.

Open Mind, zdaniem twórców programu może przynieść pożytek w pokonaniu tychże barier w sposób legalny, jako narzędzie wspomagające biały wywiad. Ma zapewniać wczesną identyfikację zagrożeń i działań o charakterze kryminalnym, które uprzednio mogłyby być przeoczone lub nieczytelne. Daje możliwość podjęcia działań proaktywnych zamiast reagowania na skutki[35].

Warto w tym miejscu zastanowić się, czy przedstawiony przez J. Widackiego[36] postulat stosowania analizy informacji dla optymalizacji wykorzystania danych gromadzonych w toku zwalczania przestępczości, nie powinno

[33] 3i-MIND Technologies GmbH, Fortunagasse 28, 8001 Zurich, Switzerland, sales@3i-mind.com.

[34] J. Gill, *op. cit.*

[35] Posiłkując się materiałami firmy 3i-MIND autor nie podejmuje się próby reklamy, czy popularyzacji opisywanego oprogramowania. Zapewne niekompletna – skrótowa prezentacja informacji o produkcie ma na celu jedynie pokazanie nowych możliwości nowoczesnych technologii, ze szczególnym uwzględnieniem ich wykorzystania w rozpoznaniu zagrożeń.

[36] *Kryminalistyka*, red. J. Widacki, Warszawa 2008, s. 71, 72.

skłaniać właśnie do sięgnięcia po nowocześniejsze rozwiązania, zapewniające należyte miejsce białemu wywiadowi.

Podsumowanie

Pomimo braku wyraźnego zapisu dotyczącego zwalczania terroryzmu w ustawie o policji, formacja ta pełni ważną rolę w systemie przeciwdziałania zagrożeniom terrorystycznym. W tym celu policja prowadzi działania defensywne, noszące nazwę działań antyterrorystycznych oraz ofensywne, mające na celu bezpośrednią likwidację zagrożeń terrorystycznych, noszące nazwę działań kontrterrorystycznych. Policja realizuje oba zadania przez prewencję, zasadniczo niejawną pracę, określaną jako operacyjną i przez fizyczną likwidację terroryzmu, natomiast odnosząc się do poziomów działania, ukierunkowana jest na rozpoznanie, działania prewencyjne, fizyczne zwalczanie i reagowanie. Rozpoznanie spełnia kluczową rolę w kwestii przeciwdziałania terroryzmowi, dostarcza informacji i buduje wiedzę dając formacji potencjał. Jego wartość polega przede wszystkim na proaktywności, a tym samym zwiększa możliwości ochrony ludzi i ich mienia, pomaga też zidentyfikować zagrożenia i dopomóc w ich likwidacji. Jednym z narzędzi rozpoznania zagrożeń terrorystycznych jest biały wywiad oraz jego nowoczesna, usystematyzowana forma analityczna OSINT (*open source intelligence*). W policji nie wykształciła się odrębna, zbliżona do OSINT praktyka, niemniej jej elementy są znane i w niektórych przypadkach stosowane, aczkolwiek w sposób nieusystematyzowany. Policjanci coraz częściej i szerzej korzystają z otwartych źródeł informacji, a metody i techniki białego wywiadu są niejednokrotnie używane doraźnie zgodnie z kierunkami zainteresowania i w zakresie określonych potrzeb wynikających z prowadzonych lub planowanych działań. Pomimo niedoceniania możliwości białego wywiadu przez kierownictwo i szkolnictwo policyjne, liniowi funkcjonariusze są zainteresowani metodą i doskonaleniem zawodowym w tym kierunku. Przyjmując założenie, że cenna informacja może pochodzić zarówno od wyspecjalizowanego osobowego źródła wywiadowczego, jak i od zwykłego funkcjonariusza policji, należy przyjąć, że są to źródła równorzędne, gdyż jakość uzyskanej informacji jest najważniejsza. Funkcjonariusze, którzy korzystają służbowo lub prywatnie z otwartych źródeł powinni informacje w należyty sposób pozyskiwać, dokumentować i służbowo wykorzystywać. W zakresie rozpoznania jawnoźródłowego, wiadomości zostają poddane analizie i jeżeli dotyczą działalności terrorystycznej muszą być przekazane i wykorzystane w krajowym systemie przeciwdziałania terroryzmowi. W świetle obowiązujących przepisów nie

ma przeszkód w stosowaniu przez policjantów białego wywiadu, natomiast pozyskane informacje mogą być wykorzystane w czynnościach służbowych doraźnie lub gromadzone w bazach policyjnych bazach danych, a następnie wykorzystywane specjalistycznie.

Wywiad kryminalny i analiza kryminalna posiadają atrybuty zbliżone do tych właściwych także dla OSINT-u. Chociaż ten obszar zarządzania informacją w policji jest dobrze zorganizowany i wyraźnie usystematyzowany, warto się jednak zastanowić nad możliwościami rozwoju w dziedzinie wykorzystania nowoczesnych technologii i oprogramowań, które doceniają potencjał białego wywiadu. We współczesnej „erze informacji" pojemność otwartych źródeł jest wręcz nieograniczona. Logiczne zatem wydaje się rozwinięcie przez funkcjonariuszy umiejętności korzystania z informacji jawnoźródłowych, na przykład przez stosowanie białego wywiadu. Obieg informacji o zagrożeniach napotyka liczne bariery organizacyjne i kulturowe. Dominująca w służbach policyjnych i specjalnych, opozycyjna do kultury dzielenia się informacją, zwana umownie „kultura tajności" sprawia, że cenione są głównie informacje utajnione, pozyskane drogą operacyjną, ze szkodą dla jawnoźródłowych. Ponadto niedostateczna edukacja antyterrorystyczna wśród przedstawicieli służb policyjnych i specjalnych oraz zwykłych obywateli sprawiają, że język procedur może być niezrozumiały dla odbiorcy lub mogą nastąpić przeszkody w dotarciu istotnej informacji do osoby decyzyjnej. Dzisiejsza przestrzeń informacyjna nie jest przestrzenią braku, ale nadmiaru informacji. Dla przeciwdziałania zagrożeniom terrorystycznym kluczowe wydają się umiejętne zarządzanie wiedzą (zdobytą z uwzględnieniem źródeł otwartych) oraz optymalizacja jej wykorzystania.

Abstract
Open-source intelligence in police: a tool for identifying terrorist threats

The paper considers the identification of threats of terrorist nature by the police, with the emphasis on the potential of open-source intelligence in the area. Open-source intelligence is a tool that makes it possible to obtain and analyse correctly information from open sources, and primarily to acquire objective and reliable conclusions. Setting the research in the context of the national system of identifying, countering, and reacting to crime of terrorist nature, the author makes an attempt to answer the question how information obtained from open sources can contribute to developing knowledge of such threats. Moreover, the work contains an analysis of the vertical and horizontal information flow in the police, and accounts for the significance of information from open sources. A study of police regulations and other acts of law, referring to the position and tasks of the police in the system for countering and fighting terrorist threats, a review of Polish and foreign literature, and own observations from police practice provide convenient complementation of legal information. The author emphasises his observations on the so-called "culture of secrecy" predominant in the circulation of information in police and special forces today

and suggests an alternative solution, namely "share information" (*kultura wymiany informacji*). Presentation of the problem aims primarily at portraying both opportunities (new solutions) and limitations in the use of open source intelligence in police practice of identifying terrorist threats.

Literatura

Źródła

T. Aleksandrowicz, *Analiza informacji w administracji i biznesie,* Wyższa Szkoła Handlu i Prawa, Warszawa 1999.

Analiza informacji w służbach policyjnych i specjalnych, red. J. Konieczny, C.H. Beck, Warszawa 2012.

H. Bean, *No More Secrets. Open Source Information and the Reshaping of U.S. Intelligence*, Preager Security International, Santa Barbara–Denver–Oxford 2011.

F. Boltz Jr., K. J. Dudonis, D. P. Schulz, *The Cuterterrorism Handbook Tactics, Procedures, and Techniques,* Taylor & Francis Group Boca Raton, London–New York–Singapore 2005.

M. Bronicki, *Wywiad kryminalny w systemie komunikacji wewnętrznej policji*, [w:] *Znaczenie komunikacji i czynnika ludzkiego w funkcjonowaniu policji. Wybrane aspekty,* red. M. Trojak, Biuro Wydawnictw Prawniczych Polbod–Wyższa Szkoła Umiejętności Społecznych w Poznaniu, Poznań 2007.

P. Chlebowicz, *„Biały wywiad" z perspektywy kryminalistyki*, [w:] *Biały wywiad, otwarte źródła informacji – wokół teorii i praktyki*, red. W. Filipkowski, W. Mądrzejowski, C.K. Beck, Warszawa 2012.

K. Dębiński, *Przeciwterroryzm – rola i zadania polskiej policji w działaniach antyterrorystycznych*, [w:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu*, red. red. L. Paprzycki, Z. Rau, Wolter Kluwer, Warszawa 2009.

J. Gill, *Open Mind – precyzyjne narzędzie pozyskiwania informacji wywiadowczych z otwartych źródeł*, „Policja 997" 2011, nr 11, listopad.

W. Filipkowski, *Wykorzystanie otwartych źródeł informacji. Wyniki badań ankietowych*, [w:] *Biały wywiad, otwarte źródła informacji...*

B. Hoffman, *Oblicza terroryzmu*, Bertelsmann Media, Warszawa 1999.

Kryminalistyka, red. J. Widacki, C.H. Beck, Warszawa 2008.

K. Liedel, *Zarządzanie informacją w walce z terroryzmem*, Trio, Warszawa 2010.

K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011.

K. Radwaniak, P. J. Wrzosek, *Biały wywiad w policji – pozyskiwanie i analiza informacji ze źródeł otwartych*, [w:] *Analiza informacji w służbach policyjnych i specjalnych...*

R. D. Steele, *The New Craft of Intelligence Personal, Public & Political*, OSS International Press Oakton, Virginia 2002.

M. Otrębski, *Apolityczność policji. nakaz prawny czy zobowiązanie moralne władzy państwowej*, „Bezpieczeństwo. Teoria i Praktyka" 2008, numer specjalny.

J. Szafrański, *Edukacja antyterrorystyczna*, [w:] *Zarządzanie kryzysowe wyzwaniem dla edukacji*, red. A. Urban, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2008.

Akty prawne

Ustawa o policji z 6 kwietnia 1990 r., Dz.U. z 1990 r. Nr 30, poz. 179, z późn.zm.

Zarządzenie nr pf 964 Komendanta Głównego Policji z 9 września 2004 r. w sprawie określenia sposobu osiągania gotowości policji do przeciwdziałania zagrożeniom terrorystycznym.

Zarządzenie nr 366 Komendanta Głównego Policji z 20 kwietnia 2004 r., Dz.U. KGP, 21.05.2004.

Zarządzenie nr 749 Komendanta Głównego Policji z 27 maja 2010 r., Dz.U. KGP, 15.06.2012.

Wytyczne nr 1/09 Dyrektora Biura Wywiadu Kryminalnego KGP z 29 lipca 2009 r. w sprawie szczegółowego sposobu wykonywania przez funkcjonariuszy i pracowników jednostek oraz komórek organizacyjnych policji, czynności służbowych związanych z przetwarzaniem informacji w Systemie Informacji Operacyjnych.

Źródła internetowe

www.msw.gov.pl/portal/pl/85/8478/Zagrozenia_terrorystyczne.html [14.10.2012].

Decyzja ramowa Rady 2002/475/WSiSW z 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (z późniejszymi zmianami) [14.10.2012].

NATO Open Sources Intelligence Handbook, US Army 2001, www.au.af.mil/au/awc/awcgate/nato/osint_reader.pdf [20.10.2012].

www.europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33168_pl.htm [19.10.2012].