Marek Górka*

Działania informacyjne wywiadu w zakresie polityki bezpieczeństwa, w tym w wymiarze cyberprzestrzeni

Streszczenie

Ogromne zmiany i ciągły rozwój zastosowań technologii i komunikacji zmieniły sposób, w jaki postrzegany jest świat. Rewolucja informacyjna miała wpływ na gromadzenie danych wywiadowczych, ich przetwarzanie, analizę i rozpowszechnianie, a także na to, w jaki sposób decydenci mogą uzyskać dostęp do rzetelnych informacji w odpowiednim czasie, a także do źródeł, na których najprawdopodobniej będą polegać, gdy konkretna informacja jest potrzebna do podjęcia decyzji. Niniejszy artykuł próbuje opisać, przeanalizować i wyjaśnić naturę trwającej rewolucji informacyjnej, przedstawić jej główny wpływ na wywiad i politykę bezpieczeństwa oraz omówić znaczenia analizy wywiadowczej w kontekście realizowania działań podczas misji pokojowych.

Słowa kluczowe: polityka bezpieczeństwa, wywiad, kontrwywiad, cyberbezpieczeństwo, misje pokojowe, przetwarzanie informacji, komunikacja, rozwój technologiczny, polityka zagraniczna

* Dr Marek Górka, Wydział Humanistyczny, Politechnika Koszalińska, e-mail: marek_gorka@wp.pl.

Wstęp

Zależność między polityką a wywiadem od dawna uważana jest za kwestię o zasadniczym znaczeniu dla badań w zakresie polityki bezpieczeństwa. Rola służb wywiadowczych jako instytucji pozyskującej dane, jak i tworzącej wiedzę w ramach procesów politycznych nie została jeszcze szczegółowo przedyskutowana na forum akademickim. Wynika to przede wszystkim z poufnego charakteru informacji, który stanowi często podstawową barierę w budowaniu wiedzy na temat funkcjonowania tajnych służb. Drugim kluczowym problemem jest dynamicznie zmieniająca się rzeczywistość polityczno-gospodarcza, która sprawia, że trudno jest przewidzieć przyczyny, jak i konsekwencje określonych wydarzeń. Nie bez znaczenia jest także rewolucja technologiczna, która poprzez cyberprzestrzeń utworzyła alternatywną sferę rywalizacji międzynarodowej. Ponadto nowe narzędzia cyberkomunikacji sprawiły, że dotychczas znane zjawiska jak dezinformacja czy też wojna informacyjna nabrały nowego znaczenia dla politycznego otoczenia.

Przyczyną podjęcia się zagadnień związanych z wywiadem stały się pytania, które często pojawiają się w przestrzeni publicznej i dotyczą skuteczności tajnych służb w walce ze współczesnymi zagrożeniami. Obraz ewolucyjnego charakteru prowadzenia tajnych działań prowokuje także do refleksji o to, czy obecnie dominującą rolę odgrywają jeszcze ludzie, czy też metody i technologia? Innymi słowy, postęp technologiczny sprawia, że w działalności wywiadowczej może być zachwiana równowaga pomiędzy potencjałem ludzkim i potencjałem technicznym. Jednak to tylko człowiek widzi pewne zależności i podobieństwa między danymi, zjawiskami czy też wydarzeniami. I to właśnie on z pojedynczych elementów – jak puzzle – tworzy obraz zachodzących procesów i zjawisk. Bez odpowiedniej informacji, która daje możliwość realnego obrazu sytuacji, wszelkie podejmowane operacje będą działaniami na oślep, na skutek których ucierpią prawa i wolności obywatelskie.

Celem pracy jest udzielenie odpowiedzi na pytanie dlaczego i w jaki sposób wywiad może mieć wpływ na politykę zagraniczną państwa? Czym jest wywiad i jaką spełnia rolę w obronności państwa? W jaki sposób informacja wywiadowcza jest przydatna dla sił zbrojnych, szczególnie podczas wykonywania misji pokojowych? Na ile cyberprzestrzeń jest domeną technologii i biznesu, a na ile państwa, które wyznacza i realizuje politykę bezpieczeństwa? Jak wytyczyć granice między wolnością a bezpieczeństwem oraz ile wolności można poświęcić w kontekście współczesnych zagrożeń? Praca ma także za zadanie wskazać najważniejsze wyzwania dla służb wywiadowczych we współczesnej

polityce bezpieczeństwa. Czynnik ten jest kluczowym problemem w kształtowaniu decyzji przez decydentów politycznych. Okazuje się bowiem, że zdefiniowanie roli i znaczenia służb w przestrzeni politycznej definiuje również stosunek władz do dwóch ścierających się wzajemnie wartości, jakimi są wolność i bezpieczeństwo.

Aby odpowiedzieć na powyższe pytania warto odnotować stan badań w polskiej literaturze przedmiotu[1]. Poszczególne prace przynoszą – w większości przypadków – odpowiedź na złożone w swej naturze zjawiska. Wartościowym uzupełnieniem są oczywiście artykuły naukowe[2] oraz publicystyczne, które tworzone są na podstawie trudno dostępnych źródeł, dzięki czemu wypełniają one lukę w dotychczasowej wiedzy w zakresie służb wywiadowczych. Ważnym elementem w pracy jest pojęcie informacji, które definiowane jest w artykule w kontekście zarówno cyberprzestrzeni, zagrożeń terrorystycznych, misji pokojowych, jak i poszczególnych elementów bezpieczeństwa składających się na wewnętrzną politykę państwa.

Służby wywiadowcze jako wyzwanie badawcze – wybrane aspekty

Wywiad jest działalnością państwa, która realizowana jest w ukryciu. Tajność tej instytucji jest zarazem największą barierą jeśli chodzi o analizę tego typu służby. Teoretycy w swoich badaniach zazwyczaj dochodzą do pewnego

1 Z. Siemiątkowski, *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009; W. Wróblewski (red.), *Wywiad i kontrwywiad w świecie*, Szczecin 2009; M. Minkina, *Wywiad Federacji Rosyjskiej*, Siedlce 2012; L. Pawlikowicz, *Aparat centralny 1 Zarządu Głównego KGB jako instrument realizacji globalnej strategii Kremla 1954–1991*, Warszawa 2013; M. Minkina, *Gry wywiadów. Sztuka wywiadu w państwie współczesnym*, Warszawa 2014; A. Gruszczak, *Europejska wspólnota wywiadowcza. Prawo – instytucje – mechanizmy*, Kraków 2014; M. Minkina, B. Gałek, *Gry wywiadów. Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015; M. Górka, *Mossad. Porażki i sukcesy tajnych służb izraelskich*, Warszawa 2015; M. Minkina, *FSB. Gwardia Kremla*, Warszawa 2016; M. Berliński, R. Zulczyk, *Federalna Służba Bezpieczeństwa Federacji Rosyjskiej*, Warszawa 2016; M. Górka (red.), *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, Warszawa 2016; M. Górka (red.), *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa: historia i współczesność*, Toruń 2016; J. Larecki, *Wielki leksykon tajnych służb specjalnych świata*, Warszawa 2017; A. Bielska, P. Smółka (red.), *Wywiad biznesowy*, Piaseczno 2017.

2 Na szczególną uwagę zasługuje czasopismo naukowe „Secretum. Służby specjalne. Bezpieczeństwo. Informacja" oraz „Studia Politologiczne" z 2018 r. z numerem 43, które w całości poświęcony jest Służbom specjalnym w państwach poradzieckich.

momentu, który już dalej nie pozwala na wiarygodny i rzeczywisty opis działalności służb. Z kolei praktycy, nawet będący w stanie spoczynku i posiadający szeroką wiedzę, nie mogą wiele ujawnić z powodu obowiązującej ich w dalszym ciągu tajemnicy państwowej. A zatem pozostaje niezagospodarowana przestrzeń, z wieloma niedopowiedzeniami, które tworzą wyobrażenia i domysły. W ten sposób powstają mity na temat tajemniczego, sensacyjnego i na wpół romantycznego świata służb wywiadowczych. Wymownym tego przykładem jest Mossad. Agencja ta nie posiada rzecznika prasowego, a zatem nie ma ona potrzeby komentować czegokolwiek czy też prostować lub wyjaśniać. Tym samym pozostawia ona szeroką przestrzeń dla domysłów, które w pewien sposób tworzą wizerunek wszechpotężnej służby[3].

Wokół wywiadu narosło wiele legend, nie każda z nich jednak jest prawdziwa, podobnie jak z filmami akcji. Okazuje się, że wywiad znacznie odbiega od potocznych wyobrażeń. Jego zadaniem jest m.in. zdobywanie danych i budowanie na ich podstawie wartościowych informacji dla władz. A zatem kwintesencją tej specjalności jest wiedza, która daje przewagę nad przeciwnikiem. Nie bez powodu w języku angielskim wywiad nosi nazwę „intelligence"[4]. Częstym przymiotnikiem występującym podczas określania służb jest słowo „specjalne" albo też „tajne". Można powiedzieć, że służby to normalne instytucje państwowe, które pracują w obszarze nie do końca stabilnym i bezpiecznym. One jako pierwsze posiadają informacje o zagrożeniu dla państwa i jego obywateli, ale też jako pierwsze nawiązując i/lub podtrzymują kontakty między zwaśnionymi stronami. I tak jak w dyplomacji, tak też w wywiadzie nie ma na stałe sojuszników ani wrogów.

Tak zaistniały model rywalizacji wywiadowczej wynika po pierwsze: z sytuacji, w której dzisiejszy przeciwnik może jutro być partnerem do współpracy i odwrotnie obecny sojusznik może jutro być konkurentem, dlatego tak ważna w tej służbie jest tajemnica. Ponadto świat wywiadu to sieć wzajemnie krzyżujących się interesów. Po drugie: nawet zaprzyjaźnione służby wywiadowcze zbierają informację na temat swoich sojuszników. Bardzo dobrym tego przykładem są relacje wywiadowcze pomiędzy USA a Izraelem. Oba państwa

3 P. Tyler, *Twierdza Izrael. Zakulisowa historia elit wojskowych, które uparcie bronią się przed pokojem*, Poznań 2014, s. 13–14; Y. Melman, *Mossad'ssplitpersonality*, „The Jerusalem Report" z dnia 31 grudnia 2012 r., s. 34; G. Shimron, *The Mossad and the Myth*, Tel Awiw 1996, s. 101.

4 M. Minkina, *Gry wywiadów. Sztuka wywiadu w państwie współczesnym*, Warszawa 2014, s. 28.

współpracują ze sobą i uznają, że nie będą podejmować działań wywiadowczych na terytorium sojusznika. Jednak żadna ze stron nie dotrzymuje tej „niepisanej" umowy[5].

Zadaniem wywiadu jest więc ocena i diagnoza drugiej strony, na ile ona jest sojusznikiem a na ile przeciwnikiem. Wywiad działa więc na zasadzie ukrytej dyplomacji. Służby pozyskują źródła informacji, które pozwalają im na minimalizowanie niepewności w świecie wysoko niestabilnym. Wywiad to także organizacja odgrywająca pierwszą rolę w rywalizacji między państwami. I to on podobnie jak dyplomacja funkcjonuje poza granicami własnego państwa, często bez zgody władz kraju, na terytorium którego działa[6]. A zatem w pewien sposób jest nielegalny. Wywiad to organizacja, która może działać na poziomie zarówno politycznym, militarnym, jak i gospodarczym. Może to być narzędzie państwa, jak i korporacji. Sektor publiczny współcześnie przejmuje wiele funkcji państwa, odpowiada za funkcjonowanie infrastruktury krytycznej, dlatego też jest istotny z punktu widzenia bezpieczeństwa państwa. Ponadto wchodząc w współpracę z państwem, korporacje nabywają wiele informacji o charakterze tajnym. Obecnie lub w niedalekiej przyszłości wywiad skazany będzie na współpracę z sektorem publicznym. Następuje zatem zacieranie granic nie tylko semantycznych pomiędzy wywiadem i kontrwywiadem, które mają inny obszar działania, ale i również pomiędzy formułą instytucji państwowych i organizacji prywatnych.

Kolejnym wyzwaniem badawczym pojawiającym się przy opisie pracy służb wywiadowczych – zasygnalizowanym już na wstępie artykułu – jest wyznaczenie granicy między wolnością a bezpieczeństwem. Opozycja tych dwóch wartości okazuje się często problemem nie do rozwiązania. W walce z terroryzmem wszystkie te wartości ulegają awarii lub paraliżowi. Nie można mieć 100% bezpieczeństwa i 100% prywatności. Charakterystyczne jest zjawisko, że najwięcej krytyki, co do formy monitorowania oraz inwigilacji obywateli przez służby, mają te osoby, które okazują się największymi ekshibicjonistami na portalach społecznościowych[7].

5 E. Kahana, *Mossad – CIA Cooperation*, „International Journal of Intelligence and CounterIntelligence" 2001, nr 14, s. 410.

6 M. Górka, *Dyplomacja i wywiad. Przyczynek do refleksji nad polityką bezpieczeństwa* [w:] M. Górka (red.), *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, Warszawa 2016, s. 64–82.

7 M. Górka, *Wolność czy bezpieczeństwo? Przyczynek do rozważań na przykładzie ustawy o działaniach antyterrorystycznych z dnia 10 czerwca 2016 r.*, „e-Politikon" 2017, nr 19, s. 49–79.

Działań w cyberprzestrzeni nie można rozpatrywać w oderwaniu od działań wywiadowczych, czy też zagrożeń dotyczących bezpieczeństwa cybernetycznego w danym państwie. W tym celu agencje wywiadowcze przyjęły proaktywne stanowisko wobec środowisk akademickich, biznesowych i obywatelskich oraz ustanowiły ramy współpracy, które pozwoliłyby im wszystkim zapewnić ochronę i bezpieczeństwo swojej pracy.

Analiza wywiadowcza

Wiele analiz wywiadowczych potwierdza i uzupełnia wiedzę środowisk politycznych, co może w potocznym rozumieniu prowadzić do błędnych wniosków, że praca analityków wywiadu jest zbędna. Jak bardzo jest to mylne przekonanie, świadczy szybki postęp technologiczny, który doprowadził do powstania instrumentów, zmieniających proces dostępu do informacji, umożliwiając użytkownikom niemal natychmiastowy wgląd do danych na całym świecie. Dlatego w erze informacyjnej, charakteryzującej się przepełnieniem treści, głównym wyzwaniem nie jest już pozyskiwanie danych, ale identyfikacja istotnych informacji i powiązanie ich z wcześniej określoną wiedzą. A zatem wywiad więcej pozyskuje danych niż może przeanalizować, dlatego też istnieje potrzeba dokonywania selekcji treści, czasem także ich ignorowania, co może być przyczyną późniejszej tragedii, czego przykładem jest niespodziewany atak, który dał początek wojnie YomKippur w 1973 r. czy też symboliczny już zamach z 11 września 2011 r.[8]

Celem analizy wywiadowczej jest zapewnienie wsparcia organom decyzyjnym, a jednym z głównych wymogów skutecznego działania jest zmniejszenie subiektywności przekazywanych informacji, tak aby były one jak najbardziej zbliżone do rzeczywistości. Dlatego tak ważne jest w pracy wywiadu krytyczne myślenie oraz kreatywne rozwiązywanie problemów.

Postęp technologiczny wpłynął również na analizę wywiadu, bowiem w znaczny sposób zróżnicował on środowisko informacyjne. Pojawiło się znacznie więcej źródeł informacji, z których każde ma inny stopień wiarygodności, co może powodować, że informacje będą niekompletne, sprzeczne lub niespójne. Informacje o nieokreślonej wiarygodności są charakterystyczne dla

8 E. Stephens, *Caught on the hop: the Yom Kippur war*, „History Today" 2008, vol. 58/10, s. 44–50.

działań wywiadowczych, a zatem są warunkiem koniecznym do ich skutecznej oceny, nawet w przypadku, gdy obraz określonych wydarzeń nie jest kompletny[9].

Obecnie zasady wywiadu są przyjmowane i stosowane nie tylko na szczeblu politycznym i wojskowym, ale również na szczeblu gospodarczym i społecznym, gdzie potrzebna jest strategia. Wywiad obejmuje gromadzenie, przetwarzanie, analizę i rozpowszechnianie informacji wywiadowczych potrzebnych do opracowania i wdrożenia strategii, a zatem polityki i planów na poziomie krajowym, regionalnym i międzynarodowym.

Pierwszym krokiem do opracowania strategii bezpieczeństwa narodowego jest analiza strategiczna środowiska (krajowego i międzynarodowego), w którym działa państwo, identyfikacja głównych zagrożeń i szans związanych z interesem narodowym. Drugim krokiem jest opracowanie i wybór celów, po którym następuje opcja odpowiednich kierunków działania niezbędnych do osiągnięcia celów. Zasadniczo strategia musi być zgodna z interesem narodowym państwa na podstawie jego instrumentów władzy. W wyniku zaangażowania decydentów w opracowywanie i wdrażanie strategii zakłada się, że przedstawiciele obywateli będą dbać o dobro państwa na wszystkich szczeblach: politycznym, gospodarczym, wojskowym, społecznym, kulturalnym i środowiskowym. Ponadto decydenci strategiczni muszą mieć dokładny obraz międzynarodowego środowiska strategicznego oraz ryzyka, zagrożeń i możliwości, a także kosztów związanych z wyborem określonego sposobu działania. W tym celu elity polityczne potrzebują wiedzy, a wywiad może ją dostarczyć. Służby mogą przekazywać nie tylko fakty, ale również, przy wsparciu działań wywiadowczych, gromadzić dane, które są przetwarzane, a uzyskane w jego wyniku informacje przekazywać odpowiednim organom lub analitykom wywiadu do ponownego wykorzystania[10]. I to oni muszą zweryfikować integralność i prawidłowość zgromadzonych danych, wybierając i wykorzystując nowe wybrane informacje w celu opracowania trwałych danych wywiadowczych przedstawiających środowisko strategiczne i zapewniających oceny na przyszłość[11].

9 T. Mattern, J. Felker, R. Borum, G. Bamford, *Operational Levels of Cyber Intelligence*, „International Journal of Intelligence and CounterIntelligence" 2014, vol. 27/4, s. 702–719.
10 W.J. Lahneman, *The Need for a New Intelligence Paradigm*, „International Journal of Intelligence and Counterintelligence" 2010, vol. 23/2, s. 209.
11 R. Omilianowicz, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej* [w:] W. Wróblewski, *Wywiad i kontrwywiad w świecie*, Szczecin 2009, s. 145–158.

Gromadzenie, analizowanie i rozpowszechnianie trwałych danych wywiadowczych do wykorzystania przez politycznych decydentów oznacza w rzeczywistości, że narzędzie do przewidywania różnych kierunków działań jest dostarczane poprzez identyfikację kluczowych punktów innych regionalnych lub międzynarodowych podmiotów. W związku z tym można zidentyfikować główne tendencje i czynniki, które prowadzą do określonej sytuacji strategicznej. W tym cyklu wywiadowczym kluczowym elementem całego procesu jest faza analizy, w związku z czym analityk odgrywa kluczową rolę w powodzeniu tego procesu, ponieważ wnosi wiedzę fachową i ramy analityczne niezbędne do wyjaśnienia perspektywy strategicznej, na podstawie której podejmuje się decyzje. Analitycy wnoszą wkład na każdym etapie procesu decyzyjnego, począwszy od właściwego zdefiniowania interesów państwowych, a skończywszy na celach i kierunkach działań[12]. Analityk wywiadu zapewnia ocenę reakcji otoczenia po wprowadzeniu i realizacji przygotowanych działań, pozwalając w ten sposób decydentom na wybór najlepszego rozwiązania w danym przedziale czasowym. Mając na uwadze rolę analityka w opisywanym powyżej procesie, można stwierdzić, że wywiad nie ogranicza się do pierwszego etapu rozwoju strategii, czyli analizy strategicznej, ale koncentruje się na ciągłym, dogłębnym procesie wspierania sformułowanej strategii państwa.

Cyberprzestrzeń jako wymiar polityki bezpieczeństwa

Debata na temat cyberbezpieczeństwa nie powinna być tylko prowadzona z perspektywy, technologicznej. Do pełnego zrozumienia cyberzagrożeń konieczna jest opinia prawników, socjologów, politologów w celu wyjaśnień wielu krzyżujących się procesów zarówno w skali lokalnej, jak i globalnej. Aby więc zredukować zagrożenia do najniżej możliwego poziomu, potrzebna jest świadomość, że o stopniu poczucia cyberbezpieczeństwa nie stanowi tylko technologia, ale i ludzkie motywacje oraz zachowania.

Cyfrowa rewolucja ma wpływ na funkcjonowanie większości rządów na świecie oraz na bezpieczeństwo przedsiębiorstw i obywateli. Trudność jednak w analizie tych procesów polega na ich bardzo dynamicznej i złożonej naturze. Wczorajsze technologie oraz aplikacje są dziś – jak często się okazuje – już nie

12 M. Degaut, *Spies and Policymakers: Intelligence in the Information Age*, „Intelligence and National Security" 2016, vol. 31/4, s. 509–531.

aktualne i nieadekwatne do potrzeb ich użytkowników. Dużą rolę spełnia tu nauka, której zadaniem jest wyjaśnienie i zrozumienie zachodzących procesów. Ta perspektywa pozwala łączyć analizę ryzyka w cyberprzestrzeni z dyscyplinami humanistycznymi.

Cyberataki mogą pochodzić z dowolnego miejsca na świecie, bez ponoszenia dużych kosztów po stronie atakujących. Jest to z pewnością największe wyzwanie dla bezpieczeństwa i stabilności instytucji wykonywujących zadania w strategicznym obszarze państwa. Jednak przedsiębiorstwa lub osoby będące ofiarą cyberataku zwykle nie udzielają informacji na ten temat, a zatem profilaktyka w zakresie cyberbezpieczeństwa jest utrudniona. Ważną rolę w tej sytuacji spełniają służby wywiadowcze i kontrwywiadowcze, które z jednej strony poprzez swą specjalizację udzielają pomocy, a z drugiej strony w sposób poufny – czyli bez informowania opinii publicznej – są w stanie podjąć określone działania. Obecnie zdecydowana większość organizacji ulega – bądź może ulec – zagrożeniom płynącym ze strony podmiotów funkcjonujących w cyberprzestrzeni[13].

Okazuje się, że nawet demokratyczne reguły wyborcze w wielu państwach mogą być naruszone w wyniku dezinformacji, jaka ma miejsce w cyberprzestrzeni. Kampania prezydencka w USA w 2016 r. jest tego przykładem. Śledztwo prowadzone przez stronę amerykańską ujawniło zastosowanie cybertechnologii w celu podejmowania wysiłków obcych służb wywiadowczych mających wpłynąć na wewnętrzną politykę innego państwa. Kolejne zeznania złożone w 2017 r. przez kilku urzędników amerykańskich, w szczególności przez byłego dyrektora FBI Jamesa Comeya oraz dyrektora NSA Admiral Mike Rogers, potwierdziły wcześniejsze podejrzenia, że Rosja za pomocą swoich służb podejmowała próby ingerencji w wybory w USA w nadziei na ukształtowanie wyników głosowania zgodnie z własnymi celami[14]. Ponadto stwierdzono, że Rosja, korzystała m.in. z programów komputerowych tzw. „botów", które imitują ludzkie zachowania[15]. Dzięki właśnie tym narzędziom, próbowano poprzez m.in. dezinformację rozpowszechniać fałszywe treści, które następnie miały wpływać na zachowania wyborcze. Według badań Uniwersyte-

13 M. Rudner, *Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge*, „International Journal of Intelligence and CounterIntelligence" 2013, vol. 26/3, s. 453–481.
14 A. Wilner, *Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation*, „Comparative Strategy" 2017, vol. 36/4, s. 309–318.
15 L. Barber, *Fake news in the post-factual age*, „Financial Times" z dnia 16 września 2017, https://www.ft.com/content/c8c749e0-996d-11e7-b83c-9588e51488a0.

tu Oxfordzkiego prawie jedna czwarta treści internetowych udostępnianych na Twitterze przez użytkowników w stanie Michigan, podczas ostatnich dni kampanii wyborczej w USA, stanowiła tzw. „fake newsy". W opublikowanym raporcie stwierdza się ponadto, że fałszywe wiadomości stanowiły 23% treści domen internetowych. Rozpowszechnianie fałszywych wiadomości, w szczególności za pośrednictwem mediów społecznościowych, może okazać się kluczowe dla sposobu postrzegania debaty politycznej[16]. A jeśli jeszcze bierze się pod uwagę, iż około 62% dorosłych Amerykanów ma dostęp do wiadomości m.in. poprzez portale społecznościowe, to można sądzić, że każda informacja zamieszczona w cyberprzestrzeni może wywołać ogromny rezonans społeczny[17]. Wzrastająca liczba użytkowników internetu zauważalna jest także w państwach europejskich i może stanowić dowód potwierdzający zjawisko uzależnienia społecznego od technologii.

Tabela. Liczba użytkowników internetu w państwach Unii Europejskiej w 2016 r.[18]

2016 rok			
Państwo UE	Użytkownicy internetu	Stosunek użytkowników internetu do ogółu populacji	Populacja państwa
Austria	6,953,400	81.1%	8,569,633
Belgia	10,060,745	88.5%	11,371,928
Bułgaria	4,155,050	58.5%	7,097,796
Chorwacja	3,133,485	74.2%	4,225,001
Cypr	844,680	71.8%	1,176,598
Czechy	9,323,428	88.4%	10,548,058
Dania	5,479,054	96.3%	5,690,750
Estonia	1,196,521	91.4%	1,309,104
Finlandia	5,107,402	92.5%	5,523,904
Francja	55,860,330	86.4%	64,668,129
Grecja	7,072,534	64.8%	10,919,459
Hiszpania	37,865,104	82.2%	46,064,604
Holandia	15,915,076	93.7%	16,979,729
Irlandia	3,817,392	81%	4,713,993
Litwa	2,199,938	77.2%	2,850,030
Luksemburg	548,807	95.2%	576,243

16 D. Blood, *Fake news is shared as widely as the real thing*, „Financial Times" z dnia 27 marca 2017, https://www.ft.com/content/99ea2fae-107c-11e7-b030-768954394623,
17 L. Barber, *Fake…*, op. cit.
18 Obliczenia własne na podstawie, za: http://www.internetlivestats.com/internet-users-by-country.

2016 rok			
Państwo UE	Użytkownicy internetu	Stosunek użytkowników internetu do ogółu populacji	Populacja państwa
Łotwa	1,491,951	76.3%	1,955,742
Malta	334,056	79.6%	419,615
Niemcy	71,016,605	88%	80,682,351
Polska	27,922,152	72.4%	38,593,161
Portugalia	6,930,762	67.3%	10,304,434
Rumunia	11,236,186	58%	19,372,734
Słowacja	4,477,641	82.5%	5,429,418
Słowenia	1,490,358	72%	2,069,362
Szwecja	9,169,705	93.1%	9,851,852
Węgry	7,874,733	80.2%	9,821,318
Wielka Brytania	60,273,385	92.6%	65,111,143
Włochy	39,211,518	65.6%	59,801,004

Zgodnie z powyższymi danymi, okazuje się, że wśród państw tzw. „nowej Europy", (lub inaczej państw postkomunistycznych), średnia użytkowników internetu wynosi 77,28%. Natomiast jeśli chodzi o państwa tzw. „starej Europy", czyli te o znacznie dłuższym doświadczeniu w funkcjonowaniu w warunkach gospodarki liberalnej, średnia ta jest wyższa i wynosi 82,71%. Różnica ta wynika – jak już zasygnalizowano – z posiadania znacznie zaawansowanych zasobów technologicznych przez gospodarkę danego państwa, a także wyższy poziom rozwoju naukowego oraz innowacyjności. A czynniki te, jak można sądzić, są m.in. pokłosiem wielu lat funkcjonowania tych państw w rzeczywistości gospodarki wolnorynkowej. Paradoksalnie jednak większy rozwój cybertechnologii nie musi oznaczać wzrostu poziomu cyberbezpieczeństwa, bowiem dotychczasowe, analogowe systemy odpowiedzialne za m.in. pracę infrastruktury krytycznej, są znacznie bardziej odporne na jakiekolwiek cyberincydenty.

Każdego dnia coraz częściej społeczeństwo, w wyniku wielu cyber udogodnień, staje się uzależnione w wielu dziedzinach życia od urządzeń elektronicznych. Jednak budowanie przyszłości w oparciu o cybertechnologię, którą coraz trudniej jest chronić i kontrolować, może skutkować wieloma zagrożeniami. Globalna ekspansja sieci społecznościowych (takich jak Facebook, Twitter) wraz z rosnącą komunikacją sieciową może doprowadzić do tego, że cybertechnologia wymknie się spod kontroli. Już dziś wiele informacji, błędnie zinterpretowanych lub umyślnie fałszowanych, żyje swoim życiem i tworzy fikcyjną rzeczywistość.

Istnieją realne obawy, że cyberprzestępcy będą blokować nie tylko komputery, ale i pozostałe urządzenia podłączone do internetu, z których na co dzień społeczeństwo korzysta. Awarii mogą więc ulec, np. telefony, telewizory, zegarki, urządzenia medyczne, opaski sportowe czy też choćby aparaty służące do pomiaru glukozy. Celem paraliżu tego typu systemów jest m.in. wyłudzenie okupu od właścicieli tychże urządzeń. Ostatnie cyberataki zaistniałe przy pomocy złośliwego oprogramowania typu ransomware jak „WannaCry" i „Petya" stanowią doskonałą ilustrację tego, jakie skutki mogą one przynieść[19].

Ataki na strony internetowe poważnych instytucji politycznych, gospodarczych są dowodem na to, że nikt nie jest odporny na działania hakerów, które są coraz bardziej wyrafinowane. Administracja publiczna, systemy finansowe, centralne sieci energetyczne zawsze były celem hakerów ze względu po pierwsze na wartość informacji, jakie te instytucje posiadają, a po drugie ze względu na rozmiar konsekwencji, które mogą zaistnieć na skutek zastosowania złośliwego oprogramowania. Patrząc w niedaleką przyszłość można sądzić, że zagrożenia bezpieczeństwa komputerowego będą dominować na tle dzisiejszych zagrożeń gospodarczych i społecznych.

Kradzież danych z karty kredytowej lub z innych dokumentów osobistych oraz oszustwa bankowe, masowy spam oraz szantaż, to tylko kilka przykładów, które świadczą o tym, jak szerokie spektrum przestępstw oferuje cyberprzestrzeń. Każde z urządzeń podłączonych do internetu jest okazją do włamania. Cyberatak jest stosunkowo prostą czynnością, bo nie ma doskonałych programów. Jednak dla skutecznego uzyskania danych nie zawsze konieczny jest cyberatak. Zazwyczaj wymaga to połączenia dwóch czynników: podatności technicznych oraz innego człowieka, którego frustracja, brak motywacji lub też nadmierne zaufanie (połączona z naiwnością) prowadzi do współudziału umożliwiającego dostęp do poufnych informacji. Obecnie, gdy coraz więcej instytucji zapewnia większy dostęp online swoim klientom, profesjonalni przestępcy z powodzeniem wykorzystują techniki phishingowe w celu kradzieży danych umożliwiających podszywanie się pod dowolną osobę lub bezpośrednie pozyskiwanie w nielegalny sposób środków finansowych.

Większość metod fałszowania wykorzystuje określoną formę oszustwa technicznego, która ma na celu utworzenie łącza w e-mailu oraz sfałszowanej – ale łudząco podobnej – strony internetowej, która prowadzi ofiarę do

19 W. Fripp, *The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age*, „Intelligence and National Security" 2018, vol. 33/4, s. 623–626.

fałszywej organizacji. Ten rodzaj kradzieży staje się coraz popularniejszy ze względu na łatwość, z jaką nie podejrzewający ludzie często ujawniają osobiste informacje oszustom, w tym numery kart kredytowych, numery ubezpieczenia społecznego, imiona członków rodziny itp. Istnieje również realna możliwość, że złodzieje tożsamości mogą pozyskiwać informacje poprzez dostęp do rejestrów publicznych. Po uzyskaniu tych informacji oszuści mogą używać danych osobowych do tworzenia fałszywych kont w imieniu ofiary, czy też uniemożliwiać ofiarom dostęp do własnych kont.

Popularną metodą jest także wysyłanie e-maili, które ostrzegają użytkownika, z niewielkim lub nieznacznym wyprzedzeniem, że konto zostanie zamknięte, dopóki osoba będąca właścicielem konta nie potwierdzi ponownie danych wymaganych przy operacjach finansowych. Do częstych przypadków można zaliczyć także otrzymywanie wiadomości na pocztę elektroniczną z dołączonymi formularzami zgłoszeniowymi. Tego typu informacje są zazwyczaj opatrzone uzasadnionym i wiarygodnym komunikatem, tylko po to, by przekonać ofiarę do udostępnienia danych do konta[20]. Innymi słowy: każdy przestępca, który spędza trochę czasu przed ekranem monitora może pozyskać bogatą wiedzę o każdej, wybranej osobie. Może on wykorzystać te informacje, aby spreparować wiarygodną wiadomość, która w zamierzeniu oszusta ma pochodzić od nadawcy np. członka rodziny, przyjaciela lub kolegi, którego darzymy zaufaniem, w celu wyłudzenia danych, a za ich pomocą naszych pieniędzy.

Wywiad gospodarczy

Zakres narzędzi socjotechnicznych jest ogromny, ponieważ można tworzyć fałszywe tożsamości i budować zaufanie bez dokonywania fizycznych włamań. I nie chodzi tu o atakowanie komputerów, bo stanowią one jedynie narzędzie, ostatecznym celem są zawsze ludzie. Informacje, które są zbierane przez aplikacje ze wszystkich sieci społecznych, zarówno w kontekście indywidualnym, jak i zbiorowym (czyli rodzina, przyjaciele, współpracownicy ofiary), są nieocenionym źródłem w rękach oszustów, ponieważ mogą oni dostosowywać atak do konkretnej osoby.

20 M. Górka, *Technologia informacyjna w obszarze cyberbezpieczeństwa państwa i społeczeństwa*, „Systemy wspomagania inżynierii produkcji" 2017, vol. 6/5, s. 73–89.

Obecnie wiele organizacji w sektorze prywatnym działa w analogiczny sposób jak wywiad. Informacje, bardziej niż kiedykolwiek, dają władzę, która umożliwia kradzież jeszcze cenniejszych danych niż dane osobowe. Daje zatem możliwość pozyskania najlepiej strzeżonych tajemnic instytucji państwowej bądź korporacji. Zrozumienie tego zjawiska ma fundamentalne znaczenie dla wyjaśnienia, dlaczego firma powinna bardziej niż kiedykolwiek zwracać uwagę na poufność danych własnego personelu. Z badań wynika też, że większość instytucji po prostu nie jest tego świadoma lub nie chce wiedzieć, czy też nie chce o tym rozmawiać[21]. W tym miejscu warto także zadać pytanie, czy zawsze komputer oraz internet jest wykorzystywany przez personel w trakcie godzin pracy do celów bezpośrednio związanych z wykonywanymi obowiązkami? Jest to ważna kwestia bezpieczeństwa nie tylko w kontekście państwa, ale społeczeństwa i gospodarki opartej na wiedzy.

W tym kontekście warto zauważyć, że aby przetrwać na konkurencyjnym rynku, większość firm korzysta z jakiejś formy analizy konkurencji, w celu zdefiniowania i zrozumienia mocnych i słabych stron konkurencji. Wiele informacji jest dostępnych publicznie i to stosunkowo prosta sprawa, aby je pozyskać i analizować[22].

Przemysł motoryzacyjny i lotniczy wraz z przemysłem stoczniowym, a przede wszystkim w sektorze inżynierii mechanicznej, są często celem ataków ze strony wywiadów gospodarczych. Część korporacji, która padła ofiarą wywiadu gospodarczego niechętnie przyznaje się do tego. Wynika to z pewnością z powodu, że takie zdarzenia mogą mieć negatywny wpływ na wartość akcji na giełdzie, a także na zaufanie klientów.

Często wywiad gospodarczy – przy pomocy byłych oficerów – korzysta z metod oraz doświadczeń wywiadu państwowego. Stosuje się często te same formy działalności, jak: podsłuch, kradzież i kopiowanie nośników pamięci, przechwytywanie e-maili, włamywanie się do sieci wewnętrznej, zdjęcia satelitarne, ale i także tradycyjne sposoby, jak: spotkania i kontakty na targach, konferencjach i sympozjach naukowych. Często także źródłem przecieków poufnych informacji są sami pracownicy instytucji lub kontrahenci.

Wywiad gospodarczy, obok wywiadu politycznego i militarnego, jest najczęstszą formą działania służb, bez względu na to czy reprezentują one reżimy

21 R. Bitton, *The legitimacy of spying among nations*, „American University International Law Review" 2014, nr 29/5, s. 1009–1070.

22 G. Brown, *Spying and Fighting in Cyberspace: What is Which?*, „Journal of National Security Law & Policy" 2016, nr 8/3, s. 1–22.

demokratyczne czy autorytarne. Jest on szeroko stosowany ze względu na swą opłacalność, zwłaszcza że zapewnia obniżenie kosztów badań i rozwoju poprzez odkrywanie tego, co już zostało osiągnięte przez innych, jednak nie wprowadzone jeszcze do użytku. A zatem pozyskanie nowej technologii jest o wiele tańsze i opłacalne niż jej skonstruowanie.

Polityka wewnętrzna

O znaczeniu wywiadu dla bezpieczeństwa państwa świadczy potrzeba prowadzenia polityki bezpieczeństwa, która jest jednym z kluczowych elementów sprawowania władzy. Czynnik ten we współczesnej historii Europy Środkowo-Wschodniej, a szczególnie w okresie transformacji ustrojowej, nabierał wyjątkowego znaczenia. Warto podkreślić, że Polska jest jednym z głównych celów rosyjskiego wywiadu, ze względu na fakt, że jest to państwo, którego granica wschodnia stanowi zewnętrzną granicę NATO i Unii Europejskiej. Polskie środowiska polityczne zaangażowały się w ostatnich latach w konflikt ukraiński oraz intensywnie promują dywersyfikację energetyczną Europy, co nie jest zgodne z interesami Moskwy. Skuteczny kontrwywiad jest niezbędny dla realizacji polityki państwa. Wyzwania, jakie stoją przed polskim kontrwywiadem wynikają przede wszystkim z trudnej i skomplikowanej historii, która kładzie się cieniem na relacje z sąsiadami, ponadto położenie geopolityczne sprawia, że Polska odgrywa często rolę państwa buforowego[23].

Służby wywiadowcze zainteresowane są szczególnie reorganizacją sił zbrojnych wynikającą z przynależności Polski do NATO, rozwojem infrastruktury przemysłu obronnego, zaawansowaną technologią, uzbrojeniem wojskowym, infrastrukturą transportową, a także efektami badań naukowych oraz zasobem surowców energetycznych. Wyzwaniem dla kontrwywiadu jest więc rywalizacja z obcą służbą, która posiada większe zasoby ludzkie i jest znacznie lepiej wyposażona.

W kontekście omówienia przydatności wywiadu dla organizacji państwowych, warto zastanowić się również, czy dla powstałych wojsk obrony terytorialnej przydatna może okazać się wiedza wywiadowcza. Organizacja ta ze swej natury jest formacją wewnętrzną, czyli działającą w granicach państwa.

23 M. Górka, *Rola i zadania kontrwywiadu w obszarze funkcjonowania państwa z uwzględnieniem wybranych aspektów polityki bezpieczeństwa III RP*, „Środkowoeuropejskie Studia Polityczne" 2017, nr 2, s. 103–123.

Trudno sobie wyobrazić, aby oprócz koniecznego sprzętu, oddziały tego typu nie posiadały wiedzy m.in. na temat współczesnych konfliktów, (w tym hybrydowych), ale i także o możliwościach, rozmieszczeniu i wyposażeniu wojsk państw sąsiednich. Naturalna jest więc potrzeba posiadania takiej wiedzy ze źródeł wywiadowczych[24].

Z definicji wywiad działa poza granicami państwa, a zatem można przypuszczać, że OT będzie korzystać z wiedzy służb wywiadowczych. Jednak dominującą rolę będzie odgrywać w tym przypadku kontrwywiad z racji tego, że zadania obu służb w określonym zakresie uzupełniają się. Przede wszystkim współpraca będzie dotyczyć eliminacji zagrożeń i przeciwdziałania służbom wywiadowczym obcych państw. Inną ważną rolą będzie zwalczanie działań organizacji separatystycznych czy też organizacji paramilitarnych, których celem jest destabilizacja państwa.

Bezpieczeństwo wewnętrzne państwa, choć należy w głównej mierze do obszaru zainteresowania służb kontrwywiadowczych, to jednak w kontekście pozyskiwania informacji ze strony tajnych służb, jest kluczowe dla stabilnego funkcjonowania państwa. Cała infrastruktura krytyczna, w tym sieci energetyczne, bankowość i systemy zaopatrzenia w wodę, komunikację i transport, są całkowicie uzależnione od sieci komputerowych. To powiązanie czy też uzależnienie od nowoczesnych technologii jest „pietą achillesową" każdego z rozwiniętych państw[25].

Przykładem tego może być paraliż informacyjny (wynikający z awarii informatycznej) jeśli chodzi o transport kolejowy, często więc dochodzi w takich sytuacjach do chaosu, agresji społecznej. Innym choćby przykładem są wyniki wyborów samorządowych w 2014 r., których oficjalne ogłoszenie przedłużyło się o kilka dni. Z tego też powodu dochodziło do licznych awantur, domysłów, a także opinii kwestionujących autentyczność wyników, a tym samym podważających zaufanie do państwa.

Zadaniem służb jest więc troska o bezpieczeństwo tego typu instytucji państwowych zarówno pod względem fizycznym, jak i cybernetycznym. Oznacza to, że infrastruktura krytyczna, ze względu na swoje zadania, jest podatnym celem ataków. W tym przypadku wymagana jest współpraca zarówno służb wywiadowczych, jak i kontrwywiadowczych. Z jednej strony wywiad

24 D.C. Stefanescu, *Military capabilities that Romania needs for preventing and waging a hybrid war*, „Review of the Air Force Academy" 2017, nr 1, s. 155–160.

25 R. Bossong, *The European Programme for the protection of critical infrastructures – metagoverning a new security problem?*, „European Security" 2014, vol. 23/2, s. 210–226.

gromadzi i przetwarza informacje o potencjalnych przeciwnikach w celu lepszego przygotowania się na ewentualny atak z ich strony oraz w celu złagodzenia możliwych szkód, które będą jego wynikiem. Z drugiej strony kontrwywiad podejmuje działania dotyczące ochrony przed szpiegostwem lub wewnętrznymi zagrożeniami, a także przed sabotażem będącym wynikiem działań wewnętrznej lub zewnętrznej siły, międzynarodowych działań terrorystycznych lub innych działań wywiadowczych o charakterze wojny informacyjnej bądź akcji dezinformacyjnych w cyberprzestrzeni[26]. Zagrożenia wymuszają stosowanie na większą skalę szkoleń, które miałyby uświadamiać pracowników instytucji publicznych o zagrożeniach związanych z bezpieczeństwem informacji i ich funkcjonowaniem w cyberprzestrzeni.

Terroryzm jako wyzwanie dla wywiadu

Praca wywiadu ewoluuje z upływem czasu. Pierwsza sprawa to nieprzerwany i dynamiczny postęp technologiczny, który daje narzędzia do pracy służbom, druga rzecz to – szczególnie w epoce zagrożeń terrorystycznych – zdobywanie danych nie tylko o przeciwniku, ale i o własnych obywatelach.

W walce z terroryzmem wywiad musi być pierwszy, a zatem musi wyprzedzać swoich wrogów. To także ogromna umiejętność przewidywania zdarzeń, która pozwala służbom na bycie kilka kroków przed przeciwnikiem, w przeciwnym razie służby mogą ponieść porażkę. Trzeba przewidzieć wiele możliwych scenariuszy i być przygotowanym na każdą ewentualność. To także praca dla osób, które starają się i potrafią zrozumieć logikę przeciwnika, wchodzą w jego rolę, dzięki temu dostrzegają słabości własnej strony.

Wywiad jest jako służba – w stosunku do pozostałych – pierwsza w walce z terroryzmem, pozostałe służby, jak oddziały specjalne, antyterroryści czy służby medyczne, mają charakter wtórny, w sensie etapu działania. To właśnie od pozyskania danych zależeć może udaremnienie zamachu[27]. Bardzo trudnym momentem jest także wybór odpowiedniego momentu aresztowania osoby podejrzanej o działalność terrorystyczną. Zbyt wczesna akcja może doprowa-

26 A. Barnea, *Counterintelligence: stepson of the intelligence discipline*, „Israel Affairs" 2017, vol. 23/4, s. 715–726.

27 A. D.M. Svendsen, *The Federal Bureau of Investigation and Change: Addressing US Domestic Counter-terrorism Intelligence*, „Intelligence and National Security" 2012, vol. 27/3, s. 371–397.

dzić do utraty możliwości wykrycia wszystkich członków organizacji terrorystycznej, natomiast zbyt późno podjęta akcja może skutkować zrealizowaniem zamachu, a tym samym tragedią[28].

Terroryzm jest współcześnie zjawiskiem, które najbardziej determinuje debatę publiczną. Problem zachowania bezpieczeństwa państwa jest szeroko omawiany w mediach, ale i również analizowany na poziomie wywiadu. I to właśnie analiza wywiadowcza daje szansę na udzielenie wiarygodnych odpowiedzi o źródła, jak i konsekwencje współczesnych zagrożeń. Paradoksalnie do opinii publicznej nie przedostają się informacje o udaremnionych zamachach, a takich przypadków jest znacznie więcej. Dlatego też trudno jest ocenić działalność służb bez posiadanej wiedzy. Głosy krytyczne pojawiają się dopiero przy towarzyszącej tragedii. Pewnym absurdalnym zjawiskiem jest fakt, że kiedy społeczeństwo jest zagrożone to opinia publiczna twierdzi, że służby słabo działają, ale jeśli społeczeństwo czuje się bezpieczne to zauważalna jest silniejsza krytyka wobec służb m.in. za stosowanie narzędzi wywiadowczych jak np. podsłuchy.

Wymownym przykładem, który mówi wiele o roli wywiadu jest polityka antyterrorystyczna. Przed zamachem z 13 listopada 2015 r. w Paryżu istniały bardzo duże problemy w wymianie informacji między Francją a Belgią. Warto podkreślić, że zamach ten planowano w Brukseli. Belgia w tym czasie miała bardzo nieskuteczne służby bezpieczeństwa – co zresztą bardzo skrzętnie wykorzystali terroryści. Ponadto w Brukseli poszczególne oddziały policji nie wiedziały co robią pozostałe. W takiej sytuacji trudno jest wyłapywać sygnały o zagrożeniu[29]. Istnieje zatem potrzeba zbudowania systemu zbierania i przepływu danych. Jeśli nawet służby greckie lub bułgarskie zidentyfikują kogoś kto wjeżdża do UE z terytorium Turcji, ale przedtem był w Syrii lub w Iraku, to nie jest jeszcze sukces. Sukcesem dopiero będzie, jeśli ta informacja dotrze do służb pozostałych krajów UE. Bez takiej wiedzy służby pozostałych państw nie będą wiedziały w ogóle o istnieniu takiej osoby, nie mówiąc już o miejscu jej pobytu oraz zamiarach. Kluczowa w polityce antyterrorystycznej jest więc wymiana informacji[30].

28 S. Sloan, *Meeting the Terrorist Threat: The Localization of Counter Terrorism Intelligence*, „Police Practice and Research" 2002, vol. 3/4, s. 337–345.

29 S. Lefebvre, *„The Belgians Just Aren't up to It": Belgian Intelligence and Contemporary Terrorism*, „International Journal of Intelligence and CounterIntelligence" 2017, vol. 30/1, s. 1–29.

30 M. Górka, *Wybrane aspekty polityki bezpieczeństwa w kontekście zagrożeń terrorystycznych w Europie*, „Symbolae Europaeae" 2017, nr 11, s. 64.

Znaczenie wywiadu dla misji pokojowych

Współcześnie granica między pokojem a wojną stała się niewyraźna. Potrzeba wywiadu podczas operacji pokojowych jest oczywista zarówno w celu zapewnienia bezpieczeństwa wojsk, jak i zwiększenia szans na powodzenie misji. Jedną z głównych zalet operacji pokojowych jest bezpośredni dostęp do obszaru i jego mieszkańców oraz interakcji ze zwaśnionymi stronami. Ważne informacje mogą być nabywane poprzez rozmowę z tubylcami i ich obserwację. Informacje te są trudne do uzyskania przez tradycyjne środki wywiadowcze. Jak pokazuje przykład misji w Somali, kobiety i dzieci na ogół dostarczały więcej informacji niż robili to płatni i profesjonalni informatorzy. Jak zawsze w przypadku korzystania z osobowych źródeł informacji (HUMINT), ochrona tożsamości źródła jest niezbędna. Ponadto w przypadku konfliktu, gdzie niektóre strony nie wahają się zabijać cywilów, jak to miało miejsce w latach 90. XX wieku w byłej Jugosławii czy w Rwandzie, konieczne jest unikanie zdarzeń dających powody lokalnym reżimom do zabijania ludności cywilnej.

Siły pokojowe muszą przekonać skonfliktowane strony, że głównym ich celem jest ułatwienie negocjacji pokojowych. Często muszą one brać pod uwagę niezwykle delikatną sytuację, w której np. pojedynczy strzał może wywołać szereg kontrowersji na szczeblu dyplomatycznym. W niektórych przypadkach głównym zadaniem jest niesienie pomocy w nieprzyjaznym środowisku jak np. w Bangladeszu czy w Somalii. W innych przypadkach celem misji jest oddzielenie dwóch walczących armii jak to miało miejsce na półwyspie Synaj. Czasami linia konfrontacji jest niewyraźna, wyznaczana bywa według walczących grup etnicznych na dużej powierzchni jak to było w przypadku Bośni[31].

Wywiad w operacji pokojowej różni się w istotny sposób od wywiadu podczas działań wojennych. Metody zbierania danych są niesłychanie bardziej wrażliwą sferą niż podczas konfliktu. Wykrycie prowadzonych działań wywiadowczych może podważyć zaufanie do sił pokojowych, a tym samym może to w negatywny sposób wpływać na współpracę. Zawsze też pojawią się osoby, które będą oskarżać siły pokojowe o szpiegostwo i stronniczość. Zdarzają się jednak sytuacje, w których skonfliktowane strony uważają, że mają powody, aby sądzić, że poprzez organizacje pokojowe przedostają się informacje do przeciwników. Przyczyny takiego stanu wynikają z tego powodu, że misje ONZ

31 J.A. Edwards, J.M. Valenzano, K. Stevenson, *The Peacekeeping Mission: Bringing Stability to a Chaotic Scene*, „Communication Quarterly" 2011, vol. 59/3, s. 339–358.

składają się głównie z krajowych kontyngentów, które są w rzeczywistości kontrolowane przez rządy tych państw[32].

Warto zauważyć, że potrzeby wywiadowcze określone przez ONZ nie zawsze są akceptowane przez poszczególne państwa. Czasami warunkowo dowódcy mogą zdecydować, że dotychczasowe rozpoznanie na podstawie informacji z ONZ jest niewystarczające dla zapewnienia bezpieczeństwa swojej jednostce i dlatego zmuszeni są do zainicjowania niezależnych operacji wywiadowczych. Siły pokojowe mogą mieć także interesy i powiązania, które są sprzeczne z wyraźnymi celami mandatu, a czasem nawet wbrew oficjalnej retoryce danego państwa. Przykładem tego jest konflikt w byłej Jugosławii. ONZ wykazało, że podczas operacji niektóre rządy nie wahały się dołączyć do operacji jednostek wywiadu, będących poza kontrolą ONZ. Informacje wywiadowcze zbierane pod pretekstem misji pokojowych mogą być więc przeznaczane w celu zaspokajania potrzeb określonego państwa[33].

Niemniej jednak informacje, które są prawidłowo używane i wykorzystane, mogą zapewnić znacznie lepszy obraz funkcjonowania sił pokojowych, szczególnie na poziomie operacyjnym i taktycznym. Wywiad jest niestety bardzo fragmentaryczny, ponieważ jednostki pokojowe często nie mają ani pełnej kontroli nad ich obszarem działalności, ani też wielkiego wyboru co do metod zbierania danych.

Typowa wiedza wywiadowcza podczas misji pokojowych sprowadza się do pozyskiwania danych na temat sytuacji etnicznej, społeczno-ekonomicznej oraz postawy liderów lokalnych. Pomaga to uniknąć błędów kulturowych, jak choćby przy okazji powitań i prowadzenia rozmów żołnierzy z kobietami, czy też częstowania jedzeniem muzułmańskich przywódców w czasie Ramadanu[34].

Wywiad musi także posiadać informację, która pozwoli odpowiedzieć na pytania: dlaczego pewne obszary objęte konfliktem reagują niekorzystnie niż inne na obecność sił pokojowych? Jakie są historyczne oraz obecne powiązania pomiędzy daną społecznością a innymi grupami społecznymi? Czy na wskazanym terytorium obecne są nacjonalistyczne bądź fundamentalistyczne organizacje? Z której ze stron można spodziewać się czystek etnicznych? Czy

32 R.D. Steele, *Peacekeeping Intelligence and Information Peacekeeping*, „International Journal of Intelligence and CounterIntelligence" 2006, vol. 19/3, s. 519–537.

33 P. Shetler-Jones, *Intelligence in Integrated UN Peacekeeping Missions: The Joint Mission Analysis Centre* „International Peacekeeping" 2008, vol. 15/4, s. 517–527.

34 T. Woodhouse, *Peacekeeping, Peace Culture and Conflict Resolution*, „International Peacekeeping" 2010, vol. 17/4, s. 486–498.

siły międzynarodowe postrzegane są jako przyjaciel czy wróg? Są to oczywiście wybrane pytania, których jest o wiele więcej, jednak pokazują one rozmiar i zasięg problemów, z którymi musi zmierzyć się wywiad i który wyposaża w wiedzę siły pokojowe.

Zakończenie

Pojawienie się cybertechnologii wywarło głęboki wpływ na cykl wywiadowczy w zakresie sposobu działania wywiadu oraz na jego interakcje z decydentami politycznymi. Rewolucja informacyjna wpłynęła również na sposób, w jaki decydenci polityczni mają dostęp do wiarygodnych informacji i źródeł, w oparciu o które podejmowane są decyzje. Ewolucja systemów wywiadowczych umożliwiła natychmiastowy wgląd do dotychczas trudno dostępnych miejsc, w których znajdują się nieprzetworzone informacje.

Wywiad polega na systematycznym i ciągłym procesie gromadzenia, przetwarzania, analizowania i rozpowszechniania potrzebnych informacji wywiadowczych o znaczeniu strategicznym, w celu ułatwienia opracowania i wdrożenia strategii i planów na poziomie państwowym, regionalnym i międzynarodowym. Jest zatem użytecznym narzędziem w tworzeniu strategii bezpieczeństwa narodowego w celu zapobiegania lub ograniczania zróżnicowanych zagrożeń dla państwa i jego obywateli lub w celu wykorzystania możliwości wynikających ze stosunków geopolitycznych, regionalnych i międzynarodowych ram bezpieczeństwa.

Wywiad stanowi ważne narzędzie w działaniach informacyjnych i wspierających decydentów politycznych. Aby sprostać zwiększonemu oczekiwaniu władz oraz presji szybkiego gromadzenia nieprzetworzonych danych, wywiad musi stale opracowywać nowe rozwiązania w zakresie zdolności gromadzenia danych, zarządzania informacjami, wykorzystywania alternatywnych metod analizy, zwiększania i udoskonalania analiz długoterminowych, czy też dostosowywania procesów i środków przekazu swoich produktów do potrzeb i oczekiwań decydentów politycznych.

Pierwsze miejsce w wywiadzie zawsze będzie odgrywać informacja. To ona decyduje o przewadze czy też o zwycięstwie w rywalizacji między podmiotami. Wiedza pozwala władzom lepiej funkcjonować i mieć znacznie większe poczucie bezpieczeństwa. Nowe postrzeganie i rozumienie świata polega na przekraczaniu lub też odrzuceniu sztywnych granicy państwowych i dostosowywaniu się do nowych trendów światowych. Agencje bezpieczeństwa, które

do tej pory działały na polu międzynarodowym, szukają zewnętrznego wroga wewnątrz granic własnego państwa, natomiast instytucje działające w sferze bezpieczeństwa wewnętrznego coraz częściej realizują swoje zadania poza granicami państwa.

Wykorzystanie treści pochodzących z otwartych źródeł informacji oraz opracowanie protokołów zbierania danych dotyczących internetowych portali społecznościowych stanowi jedno z głównych wyzwań wywiadu. Ich realizacja stała się obecnie jednym z kluczowych czynników zapewniających dostarczanie informacji decydentom politycznym. Gwarantuje również skuteczne prowadzenie działań przeciwko podmiotom zagrażającym interesom narodowym.

Bibliografia

Barnea A., *Counterintelligence: stepson of the intelligence discipline*, „Israel Affairs" 2017, vol. 23/4.

Berliński M., Zulczyk R., *Federalna Służba Bezpieczeństwa Federacji Rosyjskiej*, Warszawa 2016.

Bielska A., Smółka P. (red.), *Wywiad biznesowy*, Piaseczno 2017.

Bitton R., *The legitimacy of spying among nations*, „American University International Law Review" 2014, nr 29/5.

Bossong R., *The European Programme for the protection of critical infrastructures – meta-governing a new security problem?*, „European Security" 2014, vol. 23/2.

Brown G., *Spying and Fighting in Cyberspace: What is Which?*, „Journal of National Security Law & Policy" 2016, nr 8/3.

Degaut M., *Spies and Policymakers: Intelligence in the Information Age*, „Intelligence and National Security" 2016, vol. 31/4.

Edwards J.A., Valenzano J.M., Stevenson K., *The Peacekeeping Mission: Bringing Stability to a Chaotic Scene*, „Communication Quarterly" 2011, vol. 59/3.

Fripp W., *The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age*, „Intelligence and National Security" 2018, vol. 33/4.

Górka M. (red.), *Służby wywiadowcze jako element polskiej polityki bezpieczeństwa: historia i współczesność*, Toruń 2016.

Górka M. (red.), *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, Warszawa 2016.

Górka M., *Dyplomacja i wywiad. Przyczynek do refleksji nad polityką bezpieczeństwa* [w:] M. Górka (red.), *Wywiad i kontrwywiad w polityce międzynarodowej na przełomie XX i XXI wieku*, Warszawa 2016.

Górka M., *Mossad. Porażki i sukcesy tajnych służb izraelskich*, Warszawa 2015.

Górka M., *Rola i zadania kontrwywiadu w obszarze funkcjonowania państwa z uwzględnieniem wybranych aspektów polityki bezpieczeństwa III RP*, „Środkowoeuropejskie Studia Polityczne" 2017, nr 2.

Górka M., *Technologia informacyjna w obszarze cyberbezpieczeństwa państwa i społeczeństwa*, „Systemy wspomagania inżynierii produkcji" 2017, vol. 6/5.

Górka M., *Wolność czy bezpieczeństwo? Przyczynek do rozważań na przykładzie ustawy o działaniach antyterrorystycznych z dnia 10 czerwca 2016 roku*, „e-Politikon" 2017, nr 19.

Górka M., *Wybrane aspekty polityki bezpieczeństwa w kontekście zagrożeń terrorystycznych w Europie*, „Symbolae Europaeae" 2017, nr 11.

Gruszczak A., *Europejska wspólnota wywiadowcza. Prawo – instytucje – mechanizmy*, Kraków 2014.

Kahana E., *Mossad – CIA Cooperation*, „International Journal of Intelligence and CounterIntelligence" 2010, vol. 23/2.

Lahneman W.J., *The Need for a New Intelligence Paradigm*, „International Journal of Intelligence and Counterintelligence" 2010, vol. 23/2.
Larecki J., *Wielki leksykon tajnych służb specjalnych świata*, Warszawa 2017.
Lefebvre S.,*„The Belgians Just Aren't up to It": Belgian Intelligence and Contemporary Terrorism*, „International Journal of Intelligence and CounterIntelligence" 2017, vol. 30/1.
Mattern T., Felker J., Borum R., Bamford G., *Operational Levels of Cyber Intelligence*, „International Journal of Intelligence and CounterIntelligence" 2014, vol. 27/4.
Minkina M., *FSB. Gwardia Kremla*, Warszawa 2016.
Minkina M., Gałek B., *Gry wywiadów. Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015.
Minkina M., *Gry wywiadów. Sztuka wywiadu w państwie współczesnym*, Warszawa 2014.
Minkina M., *Wywiad Federacji Rosyjskiej*, Siedlce 2012.
Omilianowicz R., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej* [w:] W. Wróblewski, *Wywiad i kontrwywiad w świecie*, Szczecin 2009.
Pawlikowicz L., *Aparat centralny 1 Zarządu Głównego KGB jako instrument realizacji globalnej strategii Kremla 1954–1991*, Warszawa 2013.
Rudner M., *Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge*, „International Journal of Intelligence and CounterIntelligence" 2013, vol. 26/3.
Shetler-Jones P., *Intelligence in Integrated UN Peacekeeping Missions: The Joint Mission Analysis Centre* „International Peacekeeping" 2008, vol. 15/4.
Shimron G., *The Mossad and the Myth*, Tel Awiw 1996.
Siemiątkowski Z., *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009.
Sloan S., *Meeting the Terrorist Threat: The Localization of Counter Terrorism Intelligence*, „Police Practice and Research" 2002, vol. 3/4.
Steele R.D., *Peacekeeping Intelligence and Information Peacekeeping*, „International Journal of Intelligence and CounterIntelligence" 2006, vol. 19/3.
Stefanescu D.C., *Military capabilities that Romania needs for preventing and waging a hybrid war*, „Review of the Air Force Academy" 2017, nr 1.
Stephens E., *Caught on the hop: the Yom Kippur war*, „History Today" 2008, vol. 58/10.
Svendsen D.M., *The Federal Bureau of Investigation and Change: Addressing US Domestic Counter-terrorism Intelligence*, „Intelligence and National Security" 2012, vol. 27/3.
Tyler P., *Twierdza Izrael. Zakulisowa historia elit wojskowych, które uparcie bronią się przed pokojem*, Poznań 2014.
Wilner A., *Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation*, „Comparative Strategy" 2017, vol. 36/4.
Woodhouse T., *Peacekeeping, Peace Culture and Conflict Resolution*, „International Peacekeeping" 2010, vol. 17/4.
Wróblewski W. (red.), *Wywiad i kontrwywiad w świecie*, Szczecin 2009.

Informational actions of the intelligence within the scope of the safety policy, including cyberspace

Abstract

The enormous changes and constant developments in the applications of technology and communication have changed the way the world is perceived. The information revolution has impacted on intelligence gathering, processing, analysis and dissemination, as well as on how decision-makers can access reliable information in a timely manner, and on the sources they are likely to rely on when concrete information is needed to make decisions. This article attempts to describe, analyse and explain the nature of the ongoing information revolution, its main impact on intelligence and security policy, and the importance of intelligence analysis in the context of peacekeeping operations.

Key words: security policy, intelligence, counter-intelligence, cyber-security, peacekeeping missions, informationprocessing, communication, technological development, foreign policy