Adam Rogala-Lewicki

Adiunkt Wydziału Studiów Europejskich

Wyższa Szkoła Gospodarki Krajowej w Kutnie

Usytuowanie funkcjonalne służb specjalnych w systemie politycznym państwa na przykładzie Polski

Nowe typy zagrożeń stawiają przed organami odpowiedzialnymi za bezpieczeństwo nowe zadania. Nieprzewidywalność procesów społecznych, wieloaspektowość, dyferencjacja struktur. Katalog wyzwań jest szeroki. Różne modele polityczne i ekonomiczne państw, przy których afiliowane są służby wpływają na ich architekturę (wywiad, kontrwywiad, pion cywilny i wojskowy). Czynnikami determinującymi ich strukturę są m.in.: ustrój polityczny, tradycja administracyjna, czynniki historyczne, kultura polityczna i prawna. Uznaje się, że agencje spełniają co najmniej jedną z następujących funkcji (najczęściej je łącząc): procesową (jako organy ścigania najważniejszych przestępstw, np. amerykańskie FBI, polskie ABW, czy rosyjskie FSB), ochronno-kontrolną (kontrwywiadowcza w szczególności w zakresie ochrony poufnych zasobów informacyjnych), informacyjną (proces pozyskiwania informacji, jej analizy i dostarczenia w postaci gotowego produktu decydentom politycznym). Dane wywiadowcze pochodzą z różnych źródeł: (a) osobowych, określanych mianem HUMINT (*human intelligence*), (b) radioelektronicznych – SIGINT (*signals intelligence*), w tym radiowych – COMINT (*communications intelligence*), oraz radioelektronicznych – ELINT (*electronic intelligence*), które z kolei dzieli się na NUCINT (*nuclear intelligence*), czyli rozpoznanie nuklearne, RADINT (*radar intelligence*), rozpoznanie przy pomocy radarów dalekiego zasięgu, oraz ACOUSTINT, czyli rozpoznanie dźwiękowe pod powierzchnią wody, (c) analizy szpiegowskich zdjęć lotniczych – IMINT. Współczesne zagrożenia nie jest ani łatwo definiować, ani lokalizować. Widoczna jest tendencja do poszerzania metod i narzędzi pozyskiwania informacji. Widoczne jest zjawisko zwiększania kompetencji organów bezpieczeństwa kosztem zmniejszania sfery prywatności obywateli. Koniecznym jest racjonalne połączenie ich samodzielności i skutecznego działania z warunkiem przestrzegania norm konstytucyjnych.

Słowa kluczowe: *Wywiad, struktura, informacja, system, źródła danych, funkcje*

New types of threats confronts the authorities responsible for the safety with new tasks. The unpredictability of social processes, multiversity, differentiation of structures. The catalogue of challenges is wide. Various models of political and economic states where the secret services are affiliated affects their architecture (intelligence, counterintelligence, civil and military division). The factors determining their structure are mainly: political regime, administrative tradition,

historical factors, political and legal culture. It is recognized that the agencies meet at least one of the following functions (usually by combining them): process (as the law enforcement agencies of major crimes for example: American FBI, Polish ABW, or Russian FSB), protective and control (counterintelligence in particular for the protection of confidential information resources), information (the process of gathering information, analyzing it and delivering the finished product to the decison-makers). Intelligence data comes from different sources: (a) personal, referred to as HUMINT (human intelligence), (b) radio-electronic – SIGINT (signals intelligence), including radio – COMINT (communications intelligence), and radio-electronic – ELINT (electronic intelligence), which in turn are divided into NUCINT (nuclear intelligence), RADINT (radar intelligence), and ACOUSTINT (sound under water), (c) the analysis spy aerial photographs, referred to as IMINT. Today's threats are neither easy to define nor to locate. The general trend is to extend the methods and tools of information retrieval. Visible is the phenomenon of increasing the competence of security services and at the same time reducing the sphere of citizens' privacy. It is necessary that a rational combination of independence and the effective operation skills must meet the conditions of observance of the constitutional norms.

Keywords: *Intelligence, structure, information, system, data sources, functions*

Historia wywiadu rozpoczęła się w tym samym momencie dziejowym, w którym pojawiły się konflikty, a więc w momencie w którym człowiek świadom własnej egzystencji i celów musiał zmierzyć się z oporem innych. W najprostszych słowach, pozyskiwanie informacji dotyczących przeciwnika i ochrona wiadomości o własnych zasobach oraz zamierzeniach to podstawowe i nieodłączne elementy zarówno sztuki wojennej, jak i sztuki wywiadowczej. W historii łatwo znaleźć wiele przykładów, w których to informacja a nie ilość dywizji miała decydujące znaczenie dla losów bitew[1]. Tu jeden z przykładów: „przebywający w kwaterze Wellingtona Nathan Meyer Rothschild, zorientowawszy się w wyniku starcia pod Waterloo, pędzi co koń wyskoczy do Brukseli, stamtąd powozem do Ostendy (...). Na angielskim brzegu szpieg pędzi na złamanie karku do Londynu. Wyprzedza oficjalną służbę kurierską, której przebycie tej drogi zajęło trzy dni. Wie więc o zwycięstwie wcześniej niż rząd Jego Królewskiej Mości. Dom Rothschildów skupuje brytyjskie papiery wartościowe, które od czasu ucieczki Napoleona bezustannie taniały.

[1] Dlatego też poszukując początków szpiegostwa warto zajrzeć do najstarszej cywilizacji świata. To w Chinach bowiem działał i tworzył pierwszy teoretyk sztuki wojennej Sun Tzu (nazywany również Sun Tsu, Sun Cy czy Sun Tzy). Swoje doświadczenia i spostrzeżenia zawarł w traktacie *Trzynaście nakazów*. Rady tego wybitnego stratega stanęły u zarania pierwszych taktycznych bitew, dlatego warto je w tym miejscu odświeżyć: (a) dyskredytujcie wszystko co dobre w kraju przeciwnika, (b) wciągajcie przeciwnika w przestępcze przedsięwzięcia, (c) podrywajcie ich dobre imię, (d) korzystajcie ze współpracy istot najpodlejszych i najbardziej odrażających, (e) dezorganizujcie wszelkim sposobami działalność, (f) zasiewajcie waśnie i niezgodę, (g) buntujcie młodych przeciwko starym, (h) ośmieszajcie tradycję, (i) wprowadzajcie zamieszanie na zapleczu, w zaopatrzeniu, (j) osłabiajcie wolę walki nieprzyjacielskich żołnierzy za pomocą zmysłowej muzyki i piosenek, (k) podeślijcie im nierządnice, żeby dokończyły dzieła zniszczenia, (l) nie szczędźcie obietnic i podarunków; nie żałujcie pieniędzy, bo pieniądz w ten sposób wydany zwróci się stukrotnie, (m) infiltrujcie wszędzie swoich szpiegów. M. Karpiński, *Historia szpiegostwa*, Warszawa 2003, s. 22.

Kiedy rozchodzi się wieść o klęsce pod Waterloo, kursy tych papierów gwałtownie zwyżkują. Rothschild zarobił już pierwszego dnia ponad milion funtów"[2].

Andrzej Żebrowski stoi na stanowisku, że „rzeczywistość, w której ludzkość funkcjonuje składa się z trzech podstawowych elementów do których zaliczamy: materię, energię, informacje (...). Ta ostatnia była zawsze integralnym elementem środowiska pracy każdego człowieka. Jej znaczenie wynika z coraz bardziej złożonego otoczenia zewnętrznego jak i wewnętrznego w jakim działają poszczególne organizacje i z coraz większej ilości danych, którą ta złożoność rodzi. Każdy kto otrzymuje informacje bez względu na jej treść i istotę musi podjąć decyzję, co z nią zrobić. Niektóre informacje można przechowywać do ewentualnego dalszego wykorzystania, natomiast inne grupuje się tak by utworzyły nową jakościowo informacje. Niektóre z tych informacji wykorzystuje się na bieżąco, część z nich przekazuje się innym użytkownikom, a niektóre w ogóle się odrzuca"[3].

Informacja jest zatem niezbędnym elementem całości jaką stanowi system polityczny, społecznych czy ekonomiczny. Wieloaspektowość, wielokulturowość, dyferencjacja życia społecznego, globalizacja, to wszystko czynniki wymagające od współczesnych uczestników gry politycznej dużej ilości danych. Rośnie odpowiedzialność decydentów[4]. Państwa nie zwlekają wyposażając swoje organy zajmujących się w sposób jawny i poufny zbieraniem wiedzy w odpowiednie instrumenty – szczególnie w obliczu rosnących zagrożeń i nowych ich form. „Dla sprawowania władzy potrzebna jest wiedza o otoczeniu – tym bliższym i dalszym. Potrzebna jest informacja o zagrożeniach i ich charakterze. Wykonywanie funkcji władczych wymaga także pełnej identyfikacji w relacjach podstawowych, jak choćby swój – obcy, odnoszonej w relacji do obywateli danego państwa, a więc poddanych działaniu norm obowiązujących na jego obszarze"[5].

W zakreślonej sytuacji służby specjalne stają się nieuniknionym elementem struktury każdego państwa. Prawidłowość ta miała swoje potwierdzenie w historii i ma je współcześnie. Należy zaznaczyć, że w klasycznym rozwiązaniu służby specjalne dzielą się na wywiad i kontrwywiad. Te z kolei operują zarówno w sferze cywilnej, jak i wojskowej. Współczesne zagrożenia i złożony charakter zadań wpływają na zjawisko zbliżania się do siebie różnych typów i form organizacyjnych. Wobec coraz trudniejszych misji służby podejmują ze sobą współpracę. Tym samym różnice w zadaniach służb cywilnych i wojskowych, wywiadu i kontrwywiadu, systematycznie się zmniejszają. Najistotniejszą cechą ich pracy jest skuteczność – to element łączący. W praktyce występują jednak takie zjawiska jak faworyzowanie przez decydenta jednej z agencji (bardziej zaufanej) kosztem innych, zabieganie służb o względy tegoż, rywalizacja w kontekście zadaniowania i nadzoru skutkująca dysfunkcjonalnością czy wreszcie faktyczna możliwość poszukiwania i uzyskiwania od służb legitymizacji i usprawiedliwienia dla decyzji

[2] Tamże, s. 82.

[3] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000, s. 36.

[4] Szerzej zob. A. Rogala-Lewicki, *Informacyjny aspekt decyzji w środowisku politycznym* [w:] *Interdyscyplinarne ujęcie prawa*, red. Żuralska, M., Warszawa 2013.

[5] S. Zalewski, *Funkcja informacyjna służb specjalnych w systemie bezpieczeństwa RP*, Warszawa 2005, s. 8.

politycznych wcześniej już podjętych. Immanentna cecha służb – tajność – otwiera szerokie możliwości pisania scenariuszy politycznych. Nie jest to tylko polską specyfika. Raporty amerykańskich i brytyjskich służb nt. broni masowej w Iraku, uzasadniającej atak na to państwo, pisane na zamówienie ówczesnych liderów politycznych były największą i najbardziej spektakularna kompromitacją tych instytucji w ostatnich latach. Eliminacja zatem takich zjawisk, jak: dublowanie, asymetria, rywalizacja, nieproporcjonalność działań czy środków, nadużycia kompetencji, chaos informacyjny jest nie tyle kluczowa, co aspiruję do rangi z poziomu życia a śmierci. Warto przypomnieć, że w Polsce aktualnie mamy następujące służby: AW, ABW, SWW, SKW, CBA, CBŚ a także biura informacyjne Policji, Służby Granicznej, Żandarmerii, Służby Celnej i inne instytucje. Umiejętność stymulowania działań międzyinstytucjonalnych jest potrzebna. Musimy ponadto dokładnie wiedzieć, kto odpowiada za rzeczowe i merytoryczne koordynowanie służb na etapie przed dostarczaniem produktów na ręce decydentów politycznych. Standard *Intelligence Community* może tu być przydatny[6].

Bez względu na ocenę praktyki, organizacje wywiadowcze stanowią jeden z podstawowych elementów funkcjonowania państw, który daje się wyodrębnić spośród innych narzędzi i instrumentów ochrony. Nowoczesne służby specjalne wchodzą w zakres ogólnie pojętego sektora bezpieczeństwa, jako jeden z podmiotów realizujących strategię osiągania zarówno długofalowych jak i doraźnych celów. Bronią one interesów państwa, będąc wykorzystywane w działaniach ofensywnych, jak i defensywnych. Mimo to tematyka służb specjalnych nadal pozostaje słabo zrealizowanym wyzwaniem badawczym. Stwierdzenie to nabiera znaczenia szczególnie, w świetle niedoboru profesjonalnych opracowań naukowych, które podejmują zagadnienie od strony systemowej. Oceny te odnoszą się również do badań politologicznych. Tymczasem, jak pokazują liczne przykłady z historii politycznej oraz czasów współczesnych – tak Polski jak i innych państw – służby specjalne mają istotną pozycję w kreowaniu i modelowaniu licznych procesów politycznych, czy też procesów o znaczeniu politycznym. Na tym tle fundamentalnego znaczenia politologicznego nabierają takie zagadnienia jak: funkcje tych służb, zakres i sposoby ich powiązania z polityką, granice ich działania widziane w powiązaniu z zasadami ustrojów politycznych oraz gwarancjami praw i wolności jednostek, a także metody kontroli i nadzoru.

[6] Po zmianach będących rezultatem dramatu „9/11" Stany Zjednoczone jak i Wlk. Brytania po wieloletnich doświadczeniach wypracowały standard „*Intelligence Community*". Nie wdając się w szczegóły i aspekt historyczny, należy podkreślić, że to co stoi u podstaw stworzenia tej swoistej wspólnoty to wypracowanie reguły, w którym z jednej strony wszystkie Agencje wyciągają do siebie pomocna dłoń i uczą się od siebie, z drugiej strony umiejętnie racjonują dostępne środki do potrzeb wynikających z bezpieczeństwa. Chodzi u uwolnienie wśród wszystkich organów poczucia tzw. sensu wspólnoty (*sense of community*). Oczywiście za tym idą określone rozwiązania instytucjonalne i funkcjonalne. Ma to szczególne znaczenie w krajach, w których lista różnego rodzaju służb jest długa. Dla przykładu, w USA operując skrótami (bardziej zainteresowanych odsyłam do źródeł) obejmuje ona takie organizacje, jak, CIA, DIA, NSA, FBI, AFOSI, NCIS, CGIS, USACIC a także biura zajmujące się wywiadem w Departamencie Obrony, Stanu, Bezpieczeństwa Stanowego i mnóstwo innych biur w różnych instytucjach na poziomie stanowym i federalnym (nie licząc prywatnych instytucji wywiadowczych). Szerzej zob. Rogala-Lewicki, A., *Czy polskie służby specjalne potrzebują formuły Intelligence Community*, Forum Studiów i Analiz Politycznych im. Maurycego Mochnackiego, [ISSN 2082-7997], http://www.fsap.pl/index.php?option=com_content&view=article&id=21%3Aczy-polskie-suby-specjalne-potrzebuj-formuy-intelligence-community&catid=7%3Acomments&Itemid=9&lang=pl, dostęp: 20.07.2016; Por. A. Rogala-Lewicki, *Służby specjalne po zamachach terrorystycznych w USA i Europie – Patriot Act versus dyrektywa retencyjna, czyli legitymizowanie nadużyć sferze prywatności w demokratycznych państwach prawa – studium porównawcze*, Myśl Ekonomiczna i Polityczna 2015, Nr 3(50).

Abram Shulsky wręcz stoi na stanowisku, iż zagadnienia związane z funkcjonowaniem wywiadu i kontrwywiadu stanowią odrębną, uniwersalną naukę społeczną, która wg. niego ma nie tylko za zadanie zrozumieć, ale i prognozować wydarzenia polityczne, gospodarcze, społeczne i militarne[7]. Nie ulega wątpliwości, że sam termin „służby specjalne" wzbudza wiele mieszanych uczuć, implikujących utratę wywarzonego i racjonalnego podejścia do oceny tej sfery aktywności ludzkiej. Wzmagają to zjawisko niedopowiedzenia, brak wiedzy, a nade wszystko ich usytuowanie w niejawnej sferze aktywności ludzkiej. Tajemnica towarzyszy pracownikom służb specjalnych nieodłącznie. Wymusza ona odpowiednie procedury w postępowaniu, mającym na celu zarówno zdobycie informacji, jak i jej ochronę. Organy wywiadowcze muszą chronić nie tylko swoje metody pracy ale również informatorów. Służby wywiadowcze utrzymują w tajemnicy wszelkie ślady własnej działalności. Przykładowo „funkcjonariusze MI – 6 nie maja prawa pisać wspomnień ani udzielać wywiadów i nie dotyczy ich trzydziestoletnia klauzula zachowania tajemnicy"[8]. Tajność stawia przed kandydatami na pracowników specjalne wymagania zarówno kompetencyjne jak również psychofizyczne. Z wielu opracowań popularnonaukowych wiemy jakie umiejętności, wiedza i cechy charakterologiczne są przydatne w służbie. Dla przykładu pracownicy amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA) „musieli poddawać się niesamowicie dokładnym przesłuchaniom na temat własnej przeszłości, ze swoimi seksualnymi upodobaniami włącznie, a ponadto musieli składać takie same oświadczenia o swoich krewnych"[9]. Podobnie rzecz ma się w niemieckim BND. „Konspirowanie życia osobistego i zawodowego, chociaż w stopniu zróżnicowanym, jest zasadą generalną i obowiązuje wszystkich funkcjonariuszy BND. W książkach adresowych miast, gdzie mieszkają pracownicy BND, umieszcza się ich prawdziwe nazwiska z podaniem fikcyjnych zawodów (kupcy, dziennikarze itp.). Pracownikom BND zabroniono informować kogokolwiek o miejscu i charakterze zatrudnienia (...). Pracownicy jednostek hierarchicznie niższych nie znają nazwisk swoich szefów ani siedziby jednostki nadrzędnej"[10].

Całość może tworzyć obraz, w którym trudno wytoczyć sensowna granicę oddzielającą absurd od prawdy. Poufność jest niewątpliwie atrybutem przypisanym służbom specjalnym, ale na jej bazie nie można tworzyć wizji, w której uznaje się organizacje wywiadowcze za zamaskowane, zakamuflowane, wszechpotężne instytucje manipulujące biegiem wydarzeń światowych.

Bez względu na ww. kontekst należy podkreślić, iż służby specjalne wykonują zadania na rzecz ochrony porządku konstytucyjnego. Ich rola, jako źródła informacji o konkurentach, a także partnerach pozostaje niezmienna od wieków. Służby specjalne wraz z innymi wyspecjalizowanymi instytucjami tworzą system mający zapewnić bezpieczeństwo polityczne oraz ekonomiczne obywateli. Skuteczność ich działania w dużej mierze determinuje pozycję państwa, jego możliwość

[7] Szerzej zob. A.N. Shulsky, G.J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, Waszyngton DC 1991.
[8] N. West, *MI – 6, Operacje brytyjskiej Tajnej Służby Wywiadu 1909 – 1945*, Warszawa 2000, s. 8.
[9] E.R. Koch, J. Sperber, *Infomafia*, Gdynia 1999, s. 213.
[10] F. Bielak, *Służby uywiadowcze Republiki Federalnej Niemiec*, Warszawa 1985, s. 75.

decyzyjną, przygotowanie taktyczne, a także skuteczną reakcje w sytuacjach kryzysowych. Do ustawowych zadań wywiadu i kontrwywiadu należy pozyskiwanie informacji, potrzebnych do realizacji polityki państwa, następnie przetworzenie zebranych danych, analiza i odpowiednie przygotowanie, jako materiału gotowego do przekazania organom władzy. „W ten sposób mamy do czynienia ze specjalizacją trzech podstawowych pionów wywiadowczych: operacyjnego (pozyskiwanie informacji), analitycznego (porównywanie i weryfikowanie informacji) i łączności (przekazywanie informacji). Ten trójpodział utrzymał się do dzisiaj"[11].

Na aspekt związany z funkcjonowaniem konkretnej agencji wywiadowczej, czy kontrwywiadowczej nie można patrzeć bez uwzględnienia specyfiki kulturowej, ekonomicznej i politycznej państwa, przy którym agencja jest afiliowana. Często model strukturalny służb specjalnych wypływa bezpośrednio z historii danego państwa. Uwarunkowania polityczne danego społeczeństwa, nawet tradycja czy kultura, determinują ocenę i obraz społeczny organów wywiadowczych. Współczesne służby specjalne w Polsce nadal borykają się z problemem dziedzictwa PRL. Służby często traktowane są jako relikt minionego systemu, w którym nie zaszło wiele zmian (co jest dyskusyjne w obliczu danych, pokazujących, że średnia wieku funkcjonariuszy AW i ABW, wynosi trzydzieści pięć lat). Potęgują ten obraz wiadomości o upolitycznieniu tych organów. Nie lepiej sytuacja rysowała się przed wojną. Andrzej Misiuk konstatuje następująco. „W II Rzeczypospolitej stosunek społeczeństwa do rodzimych służb specjalnych był dość szczególny. Nie darzono ich estymą. Duży wpływ na to miały tradycje narodowe. Poszczególni zaborcy często korzystali z metod policyjnych (konfidentów) przy zwalczaniu polskich ruchów niepodległościowych. Dlatego też, gdy II Rzeczpospolita odrodziła się po wieloletniej niewoli państwowej współpraca ze służbami wywiadowczymi, także własnymi nie stanowiła powodu do dumy, a wielokrotnie była wykorzystywana w walce politycznej w celu spotwarzenia przeciwnika politycznego"[12]. Wpływ tradycji i kultury na funkcjonowanie wywiadu widać również w innych państwach. Hrabia de Marenches, oceniając francuskie służby podkreślał, że „temperament narodowy [francuski] sprawia, iż nie lubimy nazbyt ludzi wykonujących ten rodzaj pracy. W Wielkiej Brytanii liczba osób zatrudnionych w służbach wywiadowczych jest prawie nieznana. Do ostatnich lat nie znano nazwiska szefa Intelligence Service. Oficjalnie słynny MI 6 nie istnieje (...). Oni potrafili zwerbować – często penetrując najlepsze sfery swych wielkich uniwersytetów – intelektualną elitę, której może istotnie my nie umieliśmy przyciągnąć. We Francji nie uchodziło należeć do wywiadu"[13]. Wniosek jest przejrzysty. Ile państw, tyle rodzajów służb. To co pozostaje niezmienne to funkcje, które wykonują. Co do zasady można wyróżnić następujące: (1) procesową, (2) ochronno-kontrolną, (3) oraz informacyjną

[11] M. Karpiński, op. cit., s. 42.

[12] A. Misiuk, *Służby specjalne II Rzeczypospolitej* ,Warszawa 1998, s. 9.

[13] Ch. Ockrent, A. De Marenches, *Sekrety szpiegów i książąt*, Warszawa 1992, s. 112.

Funkcja procesowa

Jedną z ról, jakie pełnią w systemie państwowym, jest rola aparatu ścigania, która polega na uczestniczeniu obok typowych, mundurowych służb bezpieczeństwa i porządku publicznego, w procesie wykrywania i udaremniania przestępstw karnych. Funkcja ta w literaturze przedmiotu nosi miano funkcji procesowej. Jest to zatem ten zakres działalności, który pokrywa się z zakresem działania instytucji ochrony porządku. „Istotą funkcji procesowej w działalności służb specjalnych jest rozpatrywanie ich zadań oraz miejsca w systemie bezpieczeństwa państwa w kategoriach organów ścigania"[14].

Najczęściej jednak ta poszerzona część, całości zadań służb specjalnych obejmuję zwalczanie tylko wyjątkowo ciężkich przestępstw, zagrażających bezpieczeństwu państwa, często o charakterze międzynarodowym. Trzeba zaznaczyć, że wyposażanie służb specjalnych w kompetencje śledcze nie jest powszechnym zabiegiem. Oczywiście rzecz odnosi się wyłącznie do kontrwywiadu, bowiem nowoczesne służby wywiadowcze nie zajmują się niczym ponad zdobywanie, analizowanie i dostarczanie informacji jako gotowego, odpowiednio przygotowanego towaru. Jest to ta działalność, która występuje obok naturalnej funkcji kontrwywiadu, czyli przeciwdziałaniu obcym wywiadom. W tym świetle doskonale widać, iż model cywilnego UOP, funkcjonującego w Polsce do 2002 roku, łączącego w sobie zadania pozyskiwania informacji, analizowania i dostarczania ich organom władzy, wypełniania wszystkich kontrwywiadowczych obowiązków, z dbaniem o ochronę informacji niejawnych oraz ściganie przestępstw był modelem przestarzałym, nie przewidującym instytucjonalnego rozdzielenia kompetencji. Wydaje się, że węższa specjalizacja oznacza w rezultacie większą profesjonalizację, a tym samym efektywność działania.

W ostatnim okresie można jednak dostrzec tendencję włączania do kompetencji instytucji kontrwywiadowczych, zadań o charakterze śledczym, obejmującym ściganie najcięższych przestępstw. Wiąże się to zwłaszcza ze zjawiskiem tworzenia się doskonale zorganizowanych grup przestępczych, często o ponadnarodowym zasięgu, wyposażonych w nowoczesny sprzęt, którym szeregowe oddziały służb porządku publicznego nie są w stanie się przeciwstawić. W tym zakresie „wywiad, a szczególnie jego aparat zdobywający, jest w stanie prowadzić wysoce specjalistyczne działania, koordynować oraz prowadzić dogłębne studia i analizy informacji ze wszelkich dostępnych źródeł. Wywiad bowiem zajmuje się zwykle bardziej samą osobą przestępcy niż natura przestępstw. Może on przygotowywać oceny i prognozy, potrzebne do działań na wszelkich poziomach instytucji ochrony porządku publicznego"[15].

Prawne włączanie instytucji wywiadowczych do państwowego systemu śledczego jest zatem odpowiedzią i próba reagowania na nowe zagrożenia, płynące przede wszystkim ze strony przestępczości zorganizowanej. Nigdy jednak służby specjalne nie będą traktowane jako kolejny organ śledczy, na wzór policji. Funkcja procesowa służb nie jest główną funkcją lecz pochodną nowych wyzwań przed, którymi stoją współczesne społeczeństwa, i tak też należy ją traktować.

[14] S. Zalewski, *Służby specjalne w państwie demokratycznym*, Warszawa 2005, s. 83.

[15] M. Herman, *Potęga wywiadu*, Warszawa 2002, s. 343.

Martin Bożek, zastanawiając się nad procesową funkcją polskich służb specjalnych, zwraca uwagę na zbyt szeroki zakres samego pojęcia. Polskie postępowanie karne bowiem składa się trzech podstawowych etapów, natomiast zadania w których uczestniczą służby specjalne jako organy śledcze, wchodzą w zakres wyłącznie postępowania przygotowawczego. Ponadto ich rola w procesie jest ukierunkowania na ujawnienie i wykrycie określonego przestępstwa w drodze czynności dowodowych"[16].

Najbardziej typowymi przykładami rozwiązań dla obu przypadków są z jednej strony służby specjalne w Wielkiej Brytanii i w Niemczech oraz z drugiej strony służby amerykańskiego i rosyjskiego wywiadu, które oprócz funkcji informacyjnych, pełnią również funkcje organów ścigania. Zatem ani brytyjski Security Service (dawny MI 5), ani niemiecki Federalny Urząd Ochrony Konstytucji nie mają samodzielnych uprawnień do prowadzenia postępowania karnego. „Z racji brytyjskich uwarunkowań ustrojowych informacje pochodzące od służb trafiają w szczególności do premiera oraz do najbliższych współpracowników. (...) Wyjątek stanowi tylko informacja dotycząca działalności przestępczej, która jest przekazywana także organom ścigania w celu prowadzenia przez nie postępowań karnych"[17].

Michael Herman zauważył, że współpraca między służbami specjalnymi a organami porządku publicznego była przedmiotem dyskusji publicznej w połowie lat dziewięćdziesiątych w Wielkiej Brytanii. „Rząd ogłosił w listopadzie 1995 roku, że zakres działania Security Service będzie poszerzony o pomoc w wykrywaniu ciężkich przestępstw kryminalnych i walkę z nimi. Komentatorzy potraktowali tę zmianę głównie jako wynik coraz mniejszego zagrożenia irlandzkim terroryzmem. (...) Komunikat z 1995 roku, dotyczący modyfikacji zadań SS, traktował ten problem w kategoriach wspierania działań instytucji porządku publicznego"[18]. Co ciekawe modyfikacja zadań SIS nastąpiła już w 1994 roku, przy okazji reform służb specjalnych przeprowadzonych przez premiera Johna Majora. W Intelligence Service Act czytamy, że jednym z zadań i funkcji SIS, jest także wspieranie działań przy zapobieganiu i wykrywaniu groźnych przestępstw"[19].

Najbardziej znanym przykładem służb, realizujących mieszane funkcje jest amerykańskie Federalne Biuro Śledcze. „FBI funkcjonuje w ramach Departamentu Sprawiedliwości, z czym łączy się jego podległość sekretarzowi sprawiedliwości – prokuratorowi generalnemu USA kierującemu tym departamentem. (...) We wszystkich kierunkach działalność FBI przybiera postać czynności operacyjno-rozpoznawczych, informacyjno-analitycznych oraz dochodzeniowo-śledczych. FBI pełni też funkcję policji federalnej, która prowadzi śledztwa w sprawach

[16] M. Bożek, *Współczesny model polskich służb specjalnych. Służby informacyjne czy policyjne?*, Zeszyty Naukowe Akademii Obrony Narodowej, 2005, nr 1 (58), s. 93.

[17] Tamże, s. 94.

[18] M. Herman, op. cit., s. 343, 345. Międzynarodowy charakter, prowadzonej przez zorganizowane grupy przestępcze, działalności sprawia że organy ścigania poszczególnych krajów muszą zdecydować się na ściślejszą współpracę w ramach prowadzonych śledztw. Wciąż nie do końca właściwie wykorzystywane są takie struktury współpracy jak: Interpol i Europol. Pojawia się również problem współpracy, a właściwie pomocy udzielanej przez organizacje wywiadowcze w zakresie działań analitycznych. M. Herman stoi na stanowisku, że korzystniejszym rozwiązaniem jest sytuacja, w której organy porządku publicznego dysponują własnym aparatem analitycznym. Tamże, s. 342 – 346.

[19] Intelligence Service Act z 26 maja 1994 roku. W oryginale tekst brzmi następująco: "*support of the prevention or detection of serious crime*".

o przestępstwa określone w federalnym kodeksie karnym oraz ustawodawstwie federalnym. W obu przypadkach celem działań podejmowanych przez FBI jest zapobieganie, wykrywanie, i inicjowanie przewodu sądowego w sprawach o złamanie przepisów federalnych"[20]. Podobne kompetencje posiada również Federalna Służba Bezpieczeństwa Federacji Rosyjskiej.

Jak łatwo można się domyśleć polski model cywilnych służb specjalnych opiera się w zdecydowanej większości, bardziej na doświadczeniach amerykańskich niż angielskich czy niemieckich. Współczesne ABW wzorowane jest na amerykańskim FBI, co widać gołym okiem nie tylko po konstrukcji prawnej instytucji, ale chociażby po realizowanych zadaniach, sposobie zachowania funkcjonariuszy, czy nawet w charakterystycznym stylu wykonanych nadrukach na kurtkach służbowych. Jeszcze raz należy podkreślić, że o mieszanym charakterze polskich służb specjalnych można mówić wyłącznie w odniesieniu do Agencji Bezpieczeństwa Wewnętrznego.

Aby dowiedzieć się co należy do obowiązków ABW, w ramach funkcji procesowej należy zajrzeć do ustawy. Z tego źródła dowiadujemy się, że „do zadań ABW należy:

1. rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa,
2. rozpoznawanie, zapobieganie i wykrywanie przestępstw:
   a. szpiegostwa, terroryzmu, naruszenia tajemnicy państwowej i innych przestępstw godzących w bezpieczeństwo państwa,
   b. godzących w podstawy ekonomiczne państwa,
   c. korupcji osób pełniących funkcje publiczne, o których mowa w art. 1 i 2 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne, jeśli może to godzić w bezpieczeństwo państwa,
   d. w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa,
   e. nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym oraz ściganie ich sprawców"[21].

W granicach zadań im powierzonych funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego dokonują czynności operacyjno-rozpoznawcze oraz dochodzeniowo-śledcze. „Funkcjonariusze ABW wykonują czynności tylko w zakresie właściwości tej Agencji i w tym zakresie

[20] M. Bożek, op. cit., s. 95.

[21] Ustawa o Agencji Wywiadu i Agencji Bezpieczeństwa Wewnętrznego z dnia 24 maja 2002 roku (Dz. U. z 2002 r. Nr 7, poz. 676 z późn. zm).

przysługują im uprawnienia procesowe policjantów, wynikające z przepisów Kodeksu postępowania karnego"[22].

Funkcjonariusze Agencji mają pełne prawo wszczynać i prowadzić dochodzenia oraz śledztwa, które są rezultatem ich pracy dochodzeniowej lub wynikają z informacji im dostarczonych[23]. Oczywiście, ta działalność obejmuje wyłącznie sprawy dotyczące przestępstw ściganych przez ABW. Zgodnie z art. 305 § 3 kpk, ABW informuje właściwego miejscowo prokuratora, który przejmuje nad takim postępowaniem nadzór. W ramach prowadzonych czynności Agencja może np. przeprowadzić postępowanie dowodowe[24].

Model polskich służb specjalnych, w których przewiduje się miejsce na realizację funkcji procesowej, można ocenić pozytywnie, kwalifikując to rozwiązanie jako reakcja na wyzwania współczesnych zagrożeń. Konstrukcja ta, tym bardziej wydaje się uzasadniona, w świetle widocznej tendencji do odchodzenia od modelu wyłącznie informacyjnego służb wywiadowczych. Nie ulega wątpliwości, że ściganie przestępstw nadal powinno pozostać wyłączną domeną organów policyjnych. Nie widać jednak przeszkód, w pozytywnych próbach włączenia instytucji posiadających lepszy dostęp do baz informacyjnych i analitycznych, jeżeli ma to przynieść lepszy końcowy efekt w walce z zagrożeniami. Wykorzystywanie służb specjalnych w tym zakresie nie może jednak być nadużywane. Zdecydowanie nie może dojść do redefinicji pozycji i roli służb specjalnych w systemie bezpieczeństwa. Dlatego organy wywiadowcze powinny być włączane do czynności śledczych tylko w ostateczności, w przypadkach, w których ranga zagrożenia przerasta możliwości operacyjne podstawowych instytucji do tego powołanych.

Funkcja ochronno-kontrolna

Na służby specjalne można spojrzeć również pod kątem zadań zmierzających do zapewnienia bezpieczeństwa własnych zasobom informacyjnym. Ochrona informacji niejawnych odbierana jest współcześnie jako poważny problem. „W warunkach coraz szybszego rozwoju naukowo-technicznego i technologicznego możliwości potencjalnego przeciwnika w dziedzinie pozyskiwania informacji poważnie wzrosły. Ten kierunek rozwoju sytuacji, potęguje wzrost zagrożenia bezpieczeństwa dla informacji charakteru niejawnego, mających szczególne znaczenie dla bezpieczeństwa i obronności państwa. Konsekwencją tego stanu rzeczy jest konieczność

[22] Tamże. W ramach policyjnych uprawnień procesowych funkcjonariusze ABW mają prawo m. in.: wydawać polecenia określonego zachowania się, legitymowania, zatrzymania i przeszukania osób oraz pomieszczeń. Mogą również dokonywać kontroli osobistej, przeglądania zawartości bagażu, a także sprawdzania ładunku w środkach transportu. Posiadają także prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń i dźwięku. Instytucje państwowe, organy administracji rządowej i samorządu terytorialnego oraz przedsiębiorcy prowadzący działalność w zakresie użyteczności publicznej a także inni przedsiębiorcy, jednostki organizacyjne i organizacje społeczne nie mogą odmówić funkcjonariuszom, na ich wezwanie, niezbędnej pomocy.

[23] ABW nie ma prawa prowadzić dochodzenia w sprawach rozpoznawanych w trybie procesu uproszczonego. Jest to następstwem rozporządzenia ministra sprawiedliwości z 13 czerwca 2003 roku, w sprawie określenia organów uprawnionych obok Policji do prowadzenia dochodzeń oraz organów uprawnionych do wnoszenia i popierania oskarżenia przed sądem pierwszej instancji w sprawach podlegających rozpoznaniu w postępowaniu uproszczonym, jak również zakresu spraw zleconych tym organom (Dz. U. z 2003 r. Nr 108, poz. 1019).

[24] Czynności dokonywane przez Agencje wymagają wcześniejszej zgody prokuratora bądź jego zatwierdzenia bądź tylko poinformowania. Zob. M. Bożek, op. cit., s. 103.

stałego przeciwdziałania temu zagrożeniu, polegające na doskonaleniu systemu bezpieczeństwa informacji niejawnych"[25].

Bezpieczeństwo systemów informacyjnych zależy obecnie od efektywności zarządzania organizacjami. Andrzej Żebrowski wyróżnił kilka elementów, które należy uwzględnić realizując politykę bezpieczeństwa informacyjnego. Są nimi: planowanie zapotrzebowania na bezpieczeństwo, analiza metod ochrony, analiza ekonomiczna, opracowanie zasad postępowania na wypadek katastrofy i awarii, opracowanie dokumentu – polityka bezpieczeństwa, wprowadzanie w życie polityki bezpieczeństwa, analiza skuteczności i kontrola sytemu oraz ewentualna korekta polityki bezpieczeństwa"[26]. Polityka bezpieczeństwa ma głównie na celu zabezpieczenie informacji niejawnych przed działalnością obcych wywiadów, zniszczeniem czy sabotażem. Tajemnica państwowa lub służbowa nie może się dostać w niepowołane ręce. W innym przypadku grozi to nieprzewidywalnymi konsekwencjami.

Każde państwo natowskie, w tym Polska musi posiadać swój własny, krajowy system ochrony tajemnicy państwowej i służbowej. Fundamenty takiego systemu wśród państw należących do Paktu Północnoatlantyckiego stanowią:

1. krajowa instytucja bezpieczeństwa odpowiedzialna za:
   - pozyskiwanie, gromadzenie i przetwarzanie informacji o zagrożeniach wywiadowczych, w tym terrorystycznych, sabotażowych itp.,
   - przedkładanie władzy wykonawczej zwięzłych analiz na temat zagrożeń i sposobów na ich przeciwdziałanie;
2. systematyczna współpraca wszystkich agend rządowych realizowana w celu uzgadniania:

- kategorii informacji, aktywów oraz zasobów podlegających ochronie,
- wspólnych zasad bezpieczeństwa[27].

Funkcję ochronno-kontrolną służb specjalnych, realizujących politykę bezpieczeństwa informacji, doskonale zaprezentować można na przykładzie polskich rozwiązań normatywnych. Konstytucja z 1997 roku nie przewidziała dla tajemnicy państwowej, roli odrębnej wartości konstytucyjnej. Jednak wraz z uchwaleniem w 1999 roku Ustawy o ochronie informacji niejawnych, której celem było uwzględnienie interesu bezpieczeństwa państwa oraz wypełnienie obowiązku wobec państw Paktu Północnoatlantyckiego, do grona których Polska dołączyła, na służby specjalne został nałożony dodatkowy obowiązek. Prowadzą one „postępowania sprawdzające wobec osób zatrudnionych na stanowiskach związanych z dostępem do informacji

[25] A. Żebrowski, W. Kwiatkowski, op. cit., s. 126.

[26] Tamże, s. 131. Autor podkreśla, że na etapie planowania koniecznym procesem jest określenie podmiotu bądź przedmiotu, który zamierzamy chronić, zdefiniowanie zagrożenia, przed którym zamierzamy się chronić oraz przeprowadzenia analizy ryzyka. Tamże, s. 131-147.

[27] Tamże, s. 181 – 182.

niejawnych bądź aspirujących do uzyskania takiego zatrudnienia, przeprowadzają procedury w zakresie bezpieczeństwa przemysłowego wobec podmiotów gospodarczych oraz wydają certyfikaty w zakresie bezpieczeństwa teleinformatycznego"[28]. Potwierdziła to nowa ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych[29]. Działalność służb w zakresie ochrony informacji niejawnych zatem, dotyczy i obejmuje tylko te trzy sfery.

Realizację zadań wynikających z ustawy przewidziana była dla ściśle określonych organów, które z racji nowych zadań musiały dostosować się organizacyjnie do wypełniania obowiązków o charakterze quasi administracyjnym. Wobec reformy służb specjalnych w Polsce z 2002 roku, rolę instytucji wypełniających funkcję ochronno-kontrolną zajęły: Agencja Bezpieczeństwa Wewnętrznego w sferze cywilnej oraz Służba Kontrwywiadu Wojskowego (wcześniej Wojskowe Służby Informacyjne) w sferze obronności. Oba organy w ustawie zostały określone, jako służby ochrony państwa, które „kontrolują przestrzeganie przepisów, wydanych w zakresie ochrony informacji niejawnych we wszystkich organach władzy publicznej, w siłach zbrojnych Rzeczpospolitej polskiej, bankach państwowych i innych państwowych jednostkach organizacyjnych oraz przedsiębiorstwach i jednostkach naukowcy lub badawczo-rozwojowych"[30].

Ustawa określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne. Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych. Ochronie podlegają wszelkie informacje niejawne, które dzielą się na te klasyfikowane klauzulą: „ściśle tajne", „tajne", „poufne", lub „zastrzeżone".[31] Przykładowo w myśl ustawy „informacjom niejawnym nadaje się klauzulę ściśle tajne, jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że: (1) zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej; (2) zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej; (3) zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej; (4) osłabi gotowość obronną Rzeczypospolitej Polskiej; (5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie; (6) zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności

[28] M. Bożek. I. Stankowska, S. Zalewski, *Ochrona informacji niejawnych – wybrane zagadnienia*, Warszawa 2003, s. 5.

[29] Dz.U. z 2010r. Nr 182, poz. 1228 z późn, zm.

[30] S. Zalewski, *Ewolucja modelu polskich służb specjalnych, Warszawa 2003*, s. 56.

[31] Standardy obowiązujące w NATO klasyfikują informację niejawną *(classified information)*, jako informację lub materiał, który wymaga ochrony przed nieupoważnionym ujawnieniem, zgodnie z nadaną mu klauzulą tajności. Zob. A. Żebrowski, W. Kwiatkowski, op. cit., s. 181.

operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie; (7) zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych, osób, którym udzielono środków ochrony i pomocy przewidzianych w ustawie z dnia 28 listopada 2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka, albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, lub osób dla nich najbliższych[32].

W całym systemie ochrony informacji niejawnych, który stworzyła ustawa interesujące z punktu widzenia tematu pracy są elementy, w których aktywnie uczestniczą służby specjalne. Należy raz jeszcze podkreślić, że zarówno ABW jak i SKW biorą udział w postępowaniu mającym zapewnić ochronę informacji niejawnych w zakresie bezpieczeństwa osobowego, przemysłowego oraz teleinformatycznego.

Postępowanie w sprawie sprawdzenia lub dopuszczenia osób do stanowisk związanych z dostępem do informacji będących tajemnicą państwową lub służbową ma na celu niedopuszczenie, lub uniemożliwienie wykorzystania informacji niejawnych w sposób mogący wywołać potencjalne, lub bezpośrednie zagrożenia dla państwa lub jego obywateli. Postępowanie sprawdzające jest standardem we wszystkich krajach NATO. Szczególna procedura nałożona jest na podmioty, dopuszczające do natowskich tajemnic, co ma istotne znaczenie zwłaszcza na stanowiskach wojskowych. „Każdy kraj członkowski odpowiedzialny jest za sprawdzanie swoich obywateli (cywili i wojskowych), przed wydaniem im upoważnienia dostępu do informacji NATO. (...) Jednocześnie obowiązkiem każdego kraju członkowskiego jest przekazanie, na prośbę dowództwa lub agencji NATO, która zatrudnia daną osobę, świadectwa o sprawdzeniu i prawie dostępu do informacji niejawnych NATO"[33].

Podobne rozwiązanie ustawodawca zastosował w polskich warunkach. Zadaniem krajowych służb, jest bowiem „ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy"[34]. Na potrzeby tej kontroli w ustawie znalazły się kryteria i wymogi jakie zainteresowana osoba musi spełnić by móc być dopuszczoną do informacji niejawnych. Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy. „W toku postępowania sprawdzającego ustala się, czy istnieją uzasadnione wątpliwości dotyczące: (1) uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko Rzeczypospolitej Polskiej; (2) zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania z nią kontaktu; (3) przestrzegania porządku konstytucyjnego Rzeczypospolitej Polskiej, a przede wszystkim, czy osoba sprawdzana uczestniczyła lub uczestniczy w działalności partii politycznych lub innych organizacji, o których mowa w art. 13 Konstytucji Rzeczypospolitej Polskiej, albo współpracowała lub współpracuje z takimi partiami lub organizacjami;

[32] Art. 5 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U. z 2010r. Nr 182, poz. 1228 z późn, zm.).

[33] A. Żebrowski, W. Kwiatkowski, op. cit., s. 188.

[34] S. Zalewski, *Ewolucja modelu polskich służb...*, s. 51.

(4) ukrywania lub świadomego niezgodnego z prawdą podawania w ankiecie bezpieczeństwa osobowego, zwanej dalej „ankietą", lub postępowaniu sprawdzającym przez osobę sprawdzaną informacji mających znaczenie dla ochrony informacji niejawnych; (5) wystąpienia związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji; (6) niewłaściwego postępowania z informacjami niejawnymi, jeżeli: (a) doprowadziło to bezpośrednio do ujawnienia tych informacji osobom nieuprawnionym, (b) było to wynikiem celowego działania, (c) stwarzało to realne zagrożenie ich nieuprawnionym ujawnieniem i nie miało charakteru incydentalnego, (d) dopuściła się tego osoba szczególnie zobowiązana na podstawie ustawy do ochrony informacji niejawnych: pełnomocnik ochrony, jego zastępca lub kierownik kancelarii tajnej. W toku poszerzonego postępowania sprawdzającego ustala się ponadto, czy istnieją wątpliwości dotyczące: (1) poziomu życia osoby sprawdzanej wyraźnie przewyższającego uzyskiwane przez nią dochody; (2) informacji o chorobie psychicznej lub innych zakłóceniach czynności psychicznych ograniczających sprawność umysłową i mogących negatywnie wpłynąć na zdolność osoby sprawdzanej do wykonywania prac, związanych z dostępem do informacji niejawnych; (3) uzależnienia od alkoholu, środków odurzających lub substancji psychotropowych"[35].

Wszczęcie postępowania sprawdzającego następuje wraz ze złożeniem wniosku przez osobę upoważnioną do obsady stanowiska lub przez kierownika jednostki organizacyjnej. Co ważne, na postępowanie musi wyrazić pisemną zgodę, osoba, której kontrola dotyczy. Kandydat do stanowiska z dostępem do informacji niejawnych musi wypełnić ankietę bezpieczeństwa, która następnie jest weryfikowana przez służby ochrony państwa.

„Ustawa nałożyła na kierowników jednostek organizacyjnych obowiązek współdziałania ze służbami ochrony państwa w toku prowadzonych przez nie postępowań sprawdzających. Funkcjonariusze mogą żądać udostępnienia informacji i dokumentów niezbędnych do ustalenia, czy osoba sprawdzana daję rękojmię zachowania tajemnicy. (...) Służby ochrony państwa ustalają czy dane zawarte w ankiecie bezpieczeństwa są prawdziwe poprzez: (a) sprawdzenie w ewidencjach, rejestrach, w tym niedostępnych powszechnie, (b) sprawdzenie w aktach stanu cywilnego, (c) przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej, (d) rozmowę z przełożonymi, (e) sprawdzenie stanu i obrotów na rachunku bankowym, (f) rozmowę z osobą sprawdzaną oraz trzema osobami wskazanymi przez nią, (g) specjalistyczne badania zdrowia psychicznego"[36].

Procedura kontrolna prowadzona przez służby specjalne kończy się dwojako: pozytywnie, wystawieniem przez odpowiedni organ dokumentu, będącego poświadczeniem bezpieczeństwa, lub negatywnie odmową wydania powyższego zaświadczenia. Ustawa z 1999 roku nie przewidziała drogi odwoławczej dla osób, którym odmówiono zajmowania stanowiska z dostępem do informacji niejawnych, co w świetle ogólnej normy konstytucyjnej, jaką jest dwuinstancyjność

[35] Art. 24 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U. z 2010r. Nr 182, poz. 1228 z późn, zm.).

[36] S. Zalewski, *Ewolucja modelu polskich służb...*, s. 53.

postępowań w Polsce stało się przyczynkiem do rozpatrzenia tego zagadnienia prawnego przez Trybunał Konstytucyjny. Wobec jednoznacznego wyroku TK[37] w tej sprawie ustawodawca został zobligowany do przeprowadzenia nowelizacji ustawy, która przewidziała tryb odwoławczy od negatywnie rozpatrzonych wniosków o wystawienie poświadczenia bezpieczeństwa przez służby ochrony państwa. Nowelizacja z 2001 roku wprowadziła tryb odwoławczy od odmowy wydania poświadczenia bezpieczeństwa do prezesa Rady Ministrów oraz tryb skargowy w przedmiocie odmowy wydania poświadczenia bezpieczeństwa do sądu administracyjnego – co znalazło swój wyraz również w nowej ustawie.

Tabela 1. Tryb odwoławczy od odmowy wydania poświadczenia bezpieczeństwa

Odmowa poświadczenia bezpieczeństwa

Osoba sprawdzana

⇩

Odwołanie do prezesa Rady Ministrów
- za pośrednictwem właściwej służby ochrony państwa – postępowanie poszerzone.

Odwołanie do szefa właściwej służby ochrony państwa
- za pośrednictwem pełnomocnika ochrony – postępowanie zwykłe.

⇩

Prezes Rady Ministrów (Szef właściwej służby ochrony państwa) wydaje:

1. **Postanowienia o:**
   - niedopuszczalności odwołania,
   - uchybieniu terminu do wniesienia odwołania (w razie zaistnienia uzasadniających je okoliczności).
2. **Zlecenie służbie ochrony państwa przeprowadzenia dodatkowych czynności**
   (w celu uzupełnienia dowodów i materiałów w postępowaniu sprawdzającym).
3. **Decyzja:**
   - utrzymaniu w mocy odmowy wydania poświadczenia bezpieczeństwa,
   - nakazie wydania poświadczenia bezpieczeństwa.

   (termin 3 miesiące od otrzymania odwołania)

Źródło: S. Zalewski, *Ewolucja modelu polskich służb*, s. 57.

Osoba, której postępowanie kontrolne dotyczy może wnieść skargę do Wojewódzkiego Sądu Administracyjnego w terminie 30 dni od dnia doręczenia jest negatywnego postanowienia lub decyzji prezesa Rady Ministrów lub szefa właściwej służby ochrony państwa.

[37] Wyrok TK z dnia 10. 05. 1000 roku, Sygn. K. 21/99.

Tabela 2. Tryb skargowy do WSA/NSA w przedmiocie odmowy wydania poświadczenia bezpieczeństwa

Odmowa wydania poświadczenia bezpieczeństwa:
- przez służbę ochrony państwa utrzymana w mocy na podstawie decyzji prezesa Rady Ministrów,
- przez pełnomocnika ochrony utrzymana w mocy w wyniku rozpatrzenia odwołania przez szefa właściwej służby ochrony państwa.

Postanowienie prezesa Rady Ministrów (szefa właściwej służby ochrony państwa):
- niedopuszczalności odwołania,
- uchybieniu terminu do wniesienia odwołania.

Osoba sprawdzana, której odmówiono wydania poświadczenia bezpieczeństwa może złożyć skargę do WSA w terminie 30 dni od dnia doręczenia postanowienia lub decyzji.

⇩

Wojewódzki Sąd Administracyjny wydaje wyrok:
- uwzględniający skargę,
- oddalający skargę w razie jej nieuwzględnienia,
- oddalający skargę w razie upływu terminu do jej wniesienia, stwierdzenia niedopuszczalności lub gdy nie uwzględniono w wyznaczonym terminie braków skargi.

⇩

Od wyroku Wojewódzkiego Sądu Administracyjnego przysługuje skarga kasacyjna do Naczelnego Sądu Administracyjnego

Skarga kasacyjna musi być także sporządzona przez osobę do tego uprawnioną (tzw. przymus adwokacko-radcowski). Wniesienie skargi kasacyjnej musi się odbyć w ustawowym terminie, który, w myśl art. 177 § 1, wynosi trzydzieści dni od dnia doręczenia stronie odpisu orzeczenia WSA wraz z uzasadnieniem. Naczelny Sąd Administracyjny może:
- oddalić skargę kasacyjną;
- uchylić orzeczenie wojewódzkiego sądu administracyjnego i:
  - odrzucić skargę skierowaną do tegoż sądu,
  - umorzyć postępowanie przed tym sądem,
  - przekazać temu sądowi sprawę do ponownego rozpoznania,
  - rozpoznać skierowaną do tego sądu skargę,
- umorzyć postępowanie przed Naczelnym Sądem Administracyjnym.

Orzeczenia NSA są prawomocne

Źródło: S. Zalewski, *Ewolucja modelu polskich służb*, s. 58.

Możliwość odwołania się od niekorzystnych dla osoby kontrolowanej decyzji czy postanowień jest swoistą kontrolą cywilno prawną nad jakością, przeprowadzanego przez służby ochrony państwa, postępowania. Ten fakt nabiera jeszcze większego znaczenia w obliczu obowiązku jaki ustawa nakłada na te służby. Jest to bezpośrednio sformułowany przymus kierowania się zasadami bezstronności i obiektywizmu oraz wykazania najwyższej staranności. W zakresie bezpieczeństwa przemysłowego, przedsiębiorca, starający się o zawarcie umowy lub wykonujący umowę, dotyczącą realizacji zadań opłacanych w całości lub w części ze środków publicznych, z wykonaniem której łączy się dostęp do informacji stanowiących tajemnicę, ma obowiązek poddania się postępowaniu sprawdzającemu. Kontrola bezpośrednio dotyka osoby zajmujące stanowiska kierownicze w zainteresowanych przedsiębiorstwach, uczestniczące przy zawieraniu umowy oraz również zawiązane z wykonywaniem umowy. „Sprawdzeniu podlegają również osoby zatrudnione w pionie ochrony osób i mienia, jeżeli działają na rzecz i zlecenie przedsiębiorcy,

mającego dostęp do informacji niejawnych, stanowiących tajemnice państwową. Podobnie jak przy aspekcie osobowym służby specjalne sprawdzają czy, w tym przypadku przedsiębiorca daję odpowiednią wiarygodność i rękojmię zachowania tajemnic. Ustawa przewiduje dodatkowe obowiązki nałożone zarówno na wykonawcę jak i na jednostkę zamawiającą. Ten pierwszy ma obowiązek ustanowienia w swoim przedsiębiorstwie pełnomocnika ds. ochrony informacji niejawnych oraz utworzenia kancelarii tajnej i systemu fizycznej ochrony informacji niejawnych, w sytuacji gdy tajne informacje będą przechowywane w siedzibie przedsiębiorcy. W drugim przypadku zamiast pełnomocnika, urzęduje kierownik kancelarii tajnej.

Warto w tym miejscu wspomnieć o natowskich standardach w dziedzinie bezpieczeństwa przemysłowego. Państwa członkowskie zobligowane są do kompleksowego sprawdzania podmiotu gospodarczego, przed powierzeniem mu informacji niejawnych. „Wnikliwej analizie i ocenie poddawana jest stabilność statusu własnościowego, kondycja finansowo-ekonomiczna, możliwość występowania lokalnych zagrożeń”[38]. Jako gwarant spełnienia kryteriów, wprowadzono instytucję certyfikatu bezpieczeństwa obiektowego, jako swoiste potwierdzenie solidności podmiotu.

Polska ustawa wprowadza również regulacje w zakresie bezpieczeństwa teleinformatycznego, ustanawiając ochronę systemów i sieci teleinformatycznych odpowiadających za wytwarzanie, przechowywanie oraz przekazywanie informacji niejawnych. Informacje te, w szczególności stanowiące tajemnicę państwową, zgodnie z prawem mogą być przekazywane tylko za pośrednictwem takich systemów i sieci teleinformatycznych, które zapewniają gwarancję ich ochrony[39]. Wykorzystywane mogą być jedynie te urządzenia, które otrzymały specjalny certyfikat wydany przez służby ochrony państwa.

Przepisy związane z odpowiedzialnością karną za bezprawne ujawnianie bądź wykorzystywanie informacji niejawnych znajdują się w XXXIII rozdziale kodeksu karnego, zatytułowanym „Przestępstwa przeciwko ochronie informacji”. Kodeks wprowadził rozróżnienie przestępstw, segregując je w trzech różnych grupach tematycznych przepisów: „chroniących informację jako tajemnicę, zabezpieczających informację przed zniszczeniem lub uszkodzeniem wreszcie chroniących urządzenia służące do utrwalania i przekazywania informacji”[40].

Funkcja informacyjna

Pozyskiwanie i dostarczanie informacji było najstarszym i podstawowym zajęciem jakim trudniły się służby specjalne. W tym zakresie poza nielicznymi wyjątkami nie zaszły do dziś żadne zmiany. Wywiad żyje i karmi się informacją. „Posiadanie wiedzy o zagrożeniach dla państwa

[38] A. Żebrowski, W. Kwiatkowski, op. cit., s. 193.

[39] Tamże.

[40] M. Bożek. I. Stankowska, S. Zalewski, op. cit, s. 102.

wymaga z jednej strony stałego dopływu informacji z różnych źródeł, ich analizy oraz przetwarzania, wnioskowania oraz wykorzystywania w procesach decyzyjnych polityki bezpieczeństwa"[41].

Na potrzeby zobrazowania funkcji informacyjnej wywiadu swobodnie można posłużyć się metaforą. Mianowicie, wywiad w swojej naturze przypomina ludzki mózg. Sam nie jest w stanie egzystować, potrzebuje fizycznego wsparcia, którym jest ciało ludzkie. W tym rozumieniu człowiek jest władzą, która wydaje polecenia, określa cele, wyznacza potrzeby. Mózg i ciało nie mogą funkcjonować w rozłące, są od siebie uzależnione. Ich relację tworzą zamknięty obwód. Ciało jest receptorem wszystkich bodźców zewnętrznych, mózg dokonuję analizy i umożliwia właściwe dostosowanie ciała do warunków. Metafora ta posiada jednak słabe punkty. Pierwszy z nich to fakt, że to ciało zbiera informację z zewnątrz poprzez narządy wzroku, węchu itd. W tym przypadku jednak, mózg należy interpretować jako narząd uczestniczący bezpośrednio w pozyskiwaniu informacji. To on bowiem kieruję naszym zainteresowaniem, wybiera cele, które obieramy. Tutaj natrafiamy na drugi słaby punkt porównania. Władza nie może być ciałem, bowiem to ona programuje zadania, a same ciało pomimo tego że jest organizmem żywym to jednak bezwiednym. Rozwiązanie tego dylematu jest proste. Mózg jest elementem całości istoty ludzkiej. Wywiad, zatem jako cząstka struktury organów państwowych jest elementem władzy. Władza jest człowiekiem a mózg, jako jego element jest częścią władzy. Przyjmując, że zmysły są fundamentalnym składnikiem mózgu, już bez żadnych wątpliwości metafora wytrzymuję krytykę. Mózg poprzez swoje zmysły zbiera informacje, następnie je analizuje i dostarcza, jako spreparowany materiał człowiekowi. Człowiek, czyli władza, mając swój mózg programuję go na zadania jakie chce zrealizować, czyli wyznacza cele. Jednocześnie wywiad, czyli mózg, będąc wyposażony we wszystkie potrzebne mechanizmy odbierająco-analityczne ma możliwość wpływania na bieżące potrzeby człowieka, czyli władzy oraz co najważniejsze natychmiastowo informuje go o zagrożeniach, które on w swoim majestacie może najzwyczajniej nie dostrzegać. Wywiad i władza zatem podobnie jak ciało i mózg tworzą jedną całość, jeden doskonały mechanizm powiązany ze sobą milionami komórek i kanalików nerwowych.

Michael Herman wyróżnił trzy etapy działalności wywiadowczej. „Wywiad to proces sekwencyjny i międzyinstytucjonalny. Pierwszym etapem pracy wywiadowczej jest zbieranie informacji i danych z pojedynczego źródła, zwykle w formie pisemnych meldunków czy raportów. Drugi etap to analiza danych wywiadowczych ze wszystkich źródeł (*all-source analysis*), który daje analityczny produkt końcowy (*finished intelligence*). Po tych dwóch etapach następuje dystrybucja raportów wywiadowczych poza instytucje wywiadowcze, do decydentów i polityków. Pracujący w wywiadowczym fachu profesjonaliści nazywają ich odbiorcami lub konsumentami"[42]. Warto zauważyć, że między etapem analitycznym a dystrybucją może występować etap pośredni, w którym różne resorty i organizacje rządowe mogą przygotowywać swoje oceny, odnośnie uzyskanych materiałów wywiadowczych.

[41] S. Zalewski, *Funkcja informacyjna służb...* s. 35.

[42] M. Herman, op. cit., s. 46.

Istnieją różnice między wywiadem a kontrwywiadem w spełnianiu funkcji informacyjnej. Służby wywiadowcze koncentrują swoje wysiłki na kolekcjonowaniu wszelkich informacji, potencjalnie mogących mieć znaczenie dla interesu państwowego. Kontrwywiad skupia uwagę na informacjach będących podstawa do udaremniania prób penetracji przez obce służby, organizmu państwowego.

Współczesne służby informacyjne mierzą się z problemem gromadzenia zbyt dużej ilości informacji, które są całkowicie obojętne, a tym samym dysfunkcjonalne dla ich odbiorcy. Dla porównania w niemieckich służbach wywiadowczych, „maniakalne gromadzenie informacji jest ciągle jeszcze największym problemem. Na przykład do Höfen zwożono całe tony zapisanego papieru. Materiał trzeba było posortować i część spalić w podziemnych piecach, których dwa kominy do dzisiaj jeszcze wystają z ziemi. Zgodnie z cytowaną instrukcją służbową każdy zwiadowca w Höfen zajmujący się teleksami jest zobowiązany wszystkie nie przeznaczone do ujęcia w raporcie lub już opracowane teleksy regularnie przekazywać do zniszczenia. Dla tej oraz każdej innej wykonywanej czynności precyzyjnie, z pruską dokładnością, określano przewidywany nakład pracy: sortowanie przechwyconych tekstów (10%), kontrola treści istotnej ze względów wywiadowczych (25%), formułowanie poszczególnych raportów (55%), porównywanie ze zgłoszonymi zapotrzebowaniami (5%), zgłębianie wiedzy podstawowej (4%) i niszczenie (1%)"[43].

Problem mętliku informacyjnego wynika przede wszystkim ze zmian społeczno-cywilizacyjnych. W ostatnich kilkudziesięciu latach powstało wiele nowych państw, które siłą rzeczy dołączyły jako dodatkowi uczestnicy gry wywiadowczej. Liczba ludności na świecie systematycznie rośnie.

Najważniejszą jednak przyczyną są szeroko rozumiane konsekwencje płynące z rewolucji informacyjnej. Rozmnożyły się miejsca mogące stanowić potencjalne zagrożenie. Terroryści z całego globu dysponują nieograniczonymi możliwościami. Dzięki Internetowi mogą na bieżąco mieć ze sobą kontakt, zasięgać informacji od specjalistów, aktualizować swoje dane o przeciwniku. Dla służb specjalnych oznacza to nic innego jak dodatkowe obowiązki. To zjawisko multikulturowości etnicznej, poglądowej, politycznej, połączone z nieograniczonymi możliwościami transportu, przemieszczania się, zdobywania informacji, jaki współczesny świat proponuje, implikuje większą ilością zagrożeń i przeciwników trudnych do zlokalizowania i zidentyfikowania. Może to prowadzić do paraliżu informacyjnego i ograniczyć skuteczność służb specjalnych. „Skutki globalizacji widoczne są z jednej strony, poprzez zakres swobód i obiektywnie zwiększających się możliwości działania, z drugiej zaś, poprzez negatywne skutki społeczne, będące konsekwencją tych swobód a ściślej, możliwości ich nadużywania"[44].

Natłok informacji powoduję, że wywiad, pomimo że nimi dysponuje, nie jest w stanie trzeźwo ocenić, które z nich mogą okazać się przydatne a które są najzwyklejszymi codziennymi śmieciami. Przysłuchajmy się wypowiedzi oficera niemieckiego BND: „Nasi pracownicy

[43] E.R. Koch, J. Sperber, op. cit., s. 256.

[44] S. Zalewski, *Funkcja informacyjna służb...* s. 31.

w punktach kontrolnych nie są prawnikami i często nie mogą ocenić, co powinni zachować, a co zniszczyć"[45]. Najboleśniejszym przykładem, na potwierdzenie tego efektu, była klęska kontrwywiadowcza amerykańskich służb w 2001 roku.

Trzeba jednak podkreślić, że służby specjalne mają zdolność do natychmiastowego dostosowania swoich struktur i metod pracy do nowych zagrożeń i zawsze korzystają, obok wojska z najnowocześniejszych, dostępnych środków technicznych. Jako że od lat osiemdziesiątych duża cześć informacji pozyskiwanych przez służby wywiadowcze pochodziła ze źródeł informatycznych, instytucje te potrzebowały programów komputerowych, które umożliwiłyby sprawniejsze selekcjonowanie i analizowanie napływających materiałów. Problemem rozwiązała amerykańska National Security Agency do pomocy z izraelskim Mossadem, którzy z asystą najwyższych organów rządowych wykradli pewnej niewielkiej firmie software'owej, program komputerowy o nazwie PROMIS. W niedługim odstępie czasu stał się on przebojem wśród większości liczących się służb specjalnych. Z jego pomocą można było odcedzać informacje z całego świata i bezpośrednio docierać do punktów zainteresowania. „Program Billa Hamiltona poszedł sobie w świat (...). Z początkiem lat osiemdziesiątych stworzył on uniwersalny program, który przede wszystkim miał ułatwiać organizację pracy prokuraturze. Program ten doskonale nadawał się do wyszukiwania powiązań pomiędzy bardzo różnymi sprawami. Dzięki niemu udawało się na przykład ustalić, czy przestępcy nie byli również zamieszani w inne sprawy"[46].

Program PROMIS, wbrew jemu początkowemu przeznaczeniu stał się w latach osiemdziesiątych podstawowym produktem wykorzystania szpiegowskiego na świecie. Warto również wspomnieć, że na jego bazie napisano najbardziej powszechny do dziś wirus komputerowy. Nie każdy wie, że kariera konia trojańskiego rozpoczęła się od umożliwiania amerykańskiemu wywiadowi i Mossadowi śledzenie każdej instytucji, która posiadała program PROMIS. Amerykańskie i izraelskie służby, „rozprowadziły program PROMIS po całym świecie, a każdy kto go używał, ryzykował, że inny wywiad zaglądał mu w karty"[47].

Źródła elektroniczne są obecnie jednym z podstawowych rynków penetracji. Służby specjalne dysponują programami, które reagują na słowa klucze, aktywizujące natychmiast mechanizm rejestracji i namierzenia. Wobec potrzeby antycypowania zagrożeń opracowano i wdrożono nowe rozwiązania technologiczne pozwalające agencjom państwowym na zachowanie i poszerzanie swoich aktywów informacyjnych. Przykładowo amerykański system *Echelon* skonstruowany przy udziale Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii, to *de facto*, milcząco zaakceptowane przez społeczność międzynarodową, globalne narzędzie podsłuchu. System powstał w ramach tzw. porozumienia *AUSCANNZUKUS*. Elementy systemu są zainstalowane w różnych częściach świata i wyposażone

[45] E. R. Koch, J. Sperber, op. cit., s. 257.

[46] Tamże, s. 42.

[47] Tamże, s. 43 Obecnie program PROMIS jest już przeżytkiem. Na początku lat dziewięćdziesiątych firmy informatyczne wprowadziły na rynek tzw. programy typu *workflow*, które miały na celu usprawnienie systemów zarządzania w przedsiębiorstwach i urzędach. W projekcie wzięło udział ponad 50 firm elektronicznych, (m. in. Jujitsu, IBM, Hewlett – Packard, Siemens, czy SAP) oraz uniwersytety i banki. Tamże, s. 34-37.

w urządzenia techniczne do podsłuchiwania i przechwytywania informacji przesyłanych kanałami telekomunikacyjnymi. Przejęta może być jakakolwiek elektromagnetyczna wiązka informacji transferowanych gdziekolwiek na świecie (w postaci faksu, e-maila, czy rozmowy telefonicznej). Wszystkie przechwycone dane trafiają do centrali w Fort Meade w USA, gdzie są następnie kategoryzowane i kompresowane. Szacuje się, że system już na początku XX wieku był w stanie przechwytywać ok. 3 miliardów elektronicznych transferów informacji na dobę[48]. W 2013 roku do przestrzeni publicznej przedostały się rewelacje jednego ze zbuntowanych *insiderów Central Intelligence Agency* – Edwarda Snowdena (współpracującego z przedsiębiorstwem *Booz Allen Hamilton* – podwykonawcą NSA), Snowden zdekonspirował szpiegowski program o nazwie *PRISM*, który jest telekomunikacyjną platformą pozyskiwania danych opracowaną i uruchomioną w 2007 roku przez amerykańskie NSA oraz brytyjskie *Government Communications Headquarters*[49]. Program opracowuje informacje dostarczane przez komercyjne podmioty współpracujące z agencją, w tym m.in.: takie tuzy branży internetowej jak: Microsoft, Yahoo! Inc, Google, Facebook, AVM Software (administrator Paltalk), YouTube, Skype, AOL, czy Apple Inc. Przedsiębiorstwa te zobowiązały się do udostępniania danych przechowywanych na serwerach, dyskach, z transferów plików, tych przekazywanych za pośrednictwem tzw. telefonii internetowej (VoIP), wideokonferencji, czatów, wszelkich informacji gromadzonych na serwisach społecznościowych, a także loginów.

Powyższe przykłady uzmysławiają pewną prawidłowość. Zdecydowana większość nakładów i środków czynionych przez służby specjalne jest przeznaczana na pierwszy etap działalności wywiadowczej, czyli pozyskiwanie informacji. „W latach siedemdziesiątych w amerykańskim kompleksie wywiadowczym cel ten pochłonął ponad dziewięćdziesiąt procent środków. (...) Dane amerykańskie z lat siedemdziesiątych pokazują, że osiemdziesiąt siedem procent kosztów związanych ze zdobywaniem danych i informacji wywiadowczych, to koszty technicznych systemów rozpoznawczych, a jedynie trzynaście procent przeznacza się na zdobywanie informacji z wykorzystaniem źródeł osobowych"[50]

Nowoczesne instytucje wywiadowcze zajmują się nie tylko zdobywaniem informacji, ale również ich analizą i interpretacją. „Rozpoznanie radioelektroniczne wspierają wyniki analiz wstępnych, wskazujące źródła, których emisję należy śledzić i przechwytywać oraz które dane należy zbierać do dalszej obróbki. W rozpoznaniu obrazowym dużą rolę odgrywa proces fotointerpretacji, dzięki któremu można bezpośrednio kierować dalszym przebiegiem działań rozpoznawczych. Instytucje zajmujące się prowadzeniem działalności z wykorzystaniem źródeł osobowych badają z kolei swoich informatorów tak, aby wychwycić wszelkie oznaki wskazujące na nielojalność czy próby wprowadzenia w błąd"[51].

[48] *European Parliament – Temporary Committee on the ECHELON Interception System: Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), [2001/2098 (INI)], 11 lipca 2001, (09.09.2014).*

[49] W przypadku służb specjalnych USA i Wielkiej Brytanii można mówić nie tylko o wieloletniej, historycznie ugruntowanej bliskiej współpracy lecz nawet o wspólnocie wywiadowczej. Zob. A. Podolski, *Europejska współpraca wywiadowcza – brakujące ogniwo europejskiej polityki zagranicznej i bezpieczeństwa?*, Centrum Stosunków Międzynarodowych, Raporty i Analizy nr 10, Warszawa 2004, s. 1.

[50] M. Herman, op. cit., s. 46-47.

[51] Tamże, s. 48.

W początkowym etapie całego procesu zdobywania i obróbki informacji instytucje wywiadowcze dokonują przetworzenia świeżych materiałów z już istniejącymi. Procedura ta ma na celu wprowadzenie pierwszego ładu i segregację. Łączy się informację tworząc z nich wątki problemowe, tematyczne, geograficzne czy czasowe. Określa się zbiór zdarzeń, wykorzystując wyselekcjonowane fakty, które w pierwszym odczuciu mogą nie mieć ze sobą żadnego związku. Jednocześnie dokonuje się konfrontacji z wcześnie zgromadzonym stanem wiedzy. Ten etap pozwala na spreparowanie materiału, które następnie tworzy zorganizowaną całość, przedstawiając już jakąś wartość wywiadowczą. Sprawna realizacja zadań analitycznych możliwa jest tylko dzięki wykorzystaniu najnowocześniejszych systemów informatycznych. „Tylko dzięki nim można szybko odnaleźć i wyselekcjonować z dużego zbioru informacji dane potrzebne do przygotowania ocen. Pozwala to służbom wywiadowczym na szerokie wykorzystanie tzw. mozaikowego systemu zbierania informacji, dzięki czemu ogromnie wzrosła rola drobnych, pozornie mało ważnych i fragmentarycznych wiadomości"[52]. Na etapie pozyskiwania informacji wyraźnie zaobserwować można dwie podstawowe sfery dostępu do informacji:

1. przestrzeń rozpoznania bezpośredniego – w której to najwłaściwsze dla działań służb specjalnych jest rozpoznanie agenturalne, ukierunkowane na zdobywanie informacji od osób fizycznych (agentów) działających w strukturach organizacyjnych przeciwnika;
2. przestrzeń rozpoznania pośredniego – zorientowana na zdobywanie informacji drogą wykorzystania środków elektronicznych, radioelektronicznych, radiolokacyjnych, czujnikowych"[53].

Proces interpretacji zdobytych informacji trwa nieustannie od pierwszego do ostatniego etapu procesu wywiadowczego. W procesie tym jednak można wyróżnić czas, który jest przeznaczony wyłącznie na dokonywanie analizy. Działania wykorzystujące ogólnodostępne informacje w literaturze przedmiotu nazywane są wywiadem białym. „Większość danych spoza instytucji wywiadowczych, jak depesze dyplomatyczne, informacje agencji prasowych czy innych środków masowego przekazu i meldunki wojenne dotyczące kontaktu z przeciwnikiem, może trafiać bezpośrednio do struktur prowadzących działalność analityczną. Opracowanie niektórych z nich, na przykład pochodzących z procesu śledzenia zagranicznej prasy, audycji radiowych i telewizyjnych, wymaga może czasem tworzenia osobnych komórek czy podejmowania nowych ustaleń w ramach, lub pod egidą struktur wywiadowczych"[54]. Aktualnie można zaobserwować zjawisko zwiększania się liczby danych docierających do struktur analitycznych ze źródeł otwartych. Proces ten będzie przybierał na sile wraz z rozpowszechnianiem się środków masowego przekazu i tworzeniem się społeczeństw informacyjnych. W porządku społecznym, w którym najcenniejsza jest informacja, zadaniem bardzo trudnym jest utrzymanie tajemnic.

[52] F. Bielak, op. cit., s. 22.

[53] L. Ciborowski, *Przestrzenie informacyjne działań zbrojnych,* AON, Warszawa 1997, s. 65.

[54] M. Herman, op. cit., s. 108.

Bez względu jednak na powyższe efektywność i jakość dostarczonego do organów władzy raportów, nadal zależeć będzie przede wszystkim od informacji zdobytych drogą niejawną. To one bowiem ostatecznie weryfikują powszechne zamierzenia polityczne obcych państw, czy cele terrorystów. W systemach służb specjalnych występują różne modele analizy: od odrębnych, specjalnie dedykowanych komórek, do których kierowane są informacje, po własne departamenty analityczne. „W Wielkiej Brytanii tego rodzaju oceny (*national assessment*) przygotowywane są przez *Joint Intelligence Committee*, a w Stanach Zjednoczonych w formie narodowych ocen wywiadowczych *National Intelligence Estimates*. Odbywa się to podczas międzyinstytucjonalnych spotkań czy konferencji. Jest to dosyć drogi instrument działania i wykorzystuje się go tylko wtedy, gdy ocen i analiz potrzebuje urzędnik państwowy najwyższego szczebla i dotyczą one szczególnie ważnych spraw"[55].

Celem procesu analitycznego jest uzyskanie produktu informacyjnego, który będzie mógł być przekazany użytkownikowi. Praca komórek analitycznych przypomina zdecydowanie bardziej działalność dziennikarską lub nawet handlową niż tradycyjnie wywiadowczą. Pracownicy tych departamentów to specjaliści w swoich dziedzinach. „Ludzie pozyskiwani do pracy w wywiadzie nie są, jak to się przyjęło potocznie sądzić, żadnymi sensacyjnymi awanturnikami, lecz najczęściej specjalistami w jakiejś interesującej te służby dziedzinie, szkolonymi dodatkowo w zakresie wiedzy wywiadowczej"[56]. Ich zadaniem jest odpowiednie wykorzystanie posiadanej bazy informacyjnej i zrobienie z niej użytku. „Interpretacja polega na zrekonstruowaniu całej fotografii na podstawie kilku jej fragmentów. Zadanie to jest tym łatwiejsze, im a priori mamy większą jasność, czego możemy się spodziewać w wyniku naszych poszukiwań. Wymaga to albo wielkiej wyobraźni, albo ogromnego zbioru modeli"[57].

Struktury analityczne muszą być odpowiednio skonstruowane, by móc efektywnie wykorzystać potencjał organów zdobywających informacje. „Analityk zajmujący się przygotowaniem całościowych ocen i opinii musi pozostawać w bliskim kontakcie z aparatem zdobywającym, zarówno po to, by pokierować procesem zdobywania informacji, jak i móc dokonać szczegółowej, wstępnej analizy specjalistycznej"[58].

Jedna zdobyta informacja, nieodpowiednio skonfrontowana z innymi, może nie mieć żadnego znaczenia. Ta sama informacja we właściwy sposób dobrana i ulokowana, może okazać się kluczową. Analiza to układanie rozsypanych kawałków puzzli w jedną, sensowną całość. Ta żmudna, codzienna praca nie przypomina widowiskowych akcji wywiadowczych, znanych z filmów szpiegowskich. „Doktryna wywiadowcza NATO dzieli ten proces na następujące etapy:

[55] Tamże, s. 50.

[56] F. Bielak, op. cit., s. 24. Do pracy w wywiadzie pozyskuje się absolwentów wyższych uczelni, często obserwowanych i dobieranych do tego zawodu przez personel placówek naukowych, pozostający w kontakcie ze służbami specjalnymi. Do niedawna główną postacią w wywiadzie był pracownik werbujący agentów i kierujący ich pracą. Dzisiaj obok funkcjonariusza pracującego z agentami coraz większego znaczenia wśród kadr wywiadowczych nabiera specjalista: matematyk, fizyk, chemik, elektronik, ekonomista, geograf, socjolog, psycholog itp. Tamże, s. 24 – 25.

[57] B. Martinet, Y. M. Marti, *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*, Warszawa 1999, s. 87.

[58] M. Herman, op. cit., s. 109.

- ewidencja – rutynowa praca biurowa, mająca na celu rejestrowanie napływających danych i informacji;
- ocena – ocena wiarygodności źródła i pewności informacji;
- analiza – zidentyfikowanie znaczących faktów i zdarzeń, porównanie ich z informacjami już posiadanymi, wyciągnięcie wniosków;
- integracja – wykorzystanie przeanalizowanej informacji do tworzenia określonego wzoru działania, opisu sytuacji;
- interpretacja – decydowanie, jaki wpływ przeanalizowane fakty mają na perspektywę wystąpienia określonego rodzaju zdarzenia"[59].

Ocena wiarygodności źródła ma kluczowe znaczenie w procesie przygotowywania produktu wywiadowczego. Wiadomości nieprawdziwe mogą całkowicie sparaliżować pracę analityczną. Z błędnych przesłanek wyciąga się fałszywe tezy. Wnioskowanie oparte na nieprawdziwych danych musi prowadzić do błędów logicznych. Opieranie pracy wywiadowczej na sprawdzonych, wiarygodnych źródłach to podstawa sukcesu. Fakt ten nabiera szczególnego znaczenia, wobec tradycyjnych działań mylących i dezinformacyjnych obcych wywiadów. Nieprawdziwa informacja wprowadzona do obiegu, jest niczym groźny wirus w układzie krwionośnym człowieka. Dlatego tez służby specjalne starają się stosować zabiegi mające na celu potwierdzenie wiarygodności źródła. Najbardziej powszechną bo najprostszą jest metoda potwierdzenia. Tę samą informację dostarczoną przez dwa źródła niewspółpracujące ze sobą można obdarzyć większym kredytem zaufania. Oczywiście nigdy służby nie mają stuprocentowej pewności co do prawdziwości otrzymanych informacji. „W terminologii wojskowej rzetelność źródeł określana jest wielostopniowo:

- źródło w pełni wiarygodne; pochodzące z niego informacje są praktycznie zawsze prawdziwe (np. informacje techniczne pochodzące z pomiarów prowadzonych przez własne laboratorium),
- źródło wiarygodne, ale obarczone ryzykiem wystąpienia błędu lub subiektywizmu (np. doniesienia prasowe),
- źródło mało wiarygodne (większość źródeł nieformalnych),
- źródło podejrzane i subiektywne; pochodzące z niego informacje należy traktować z dużą rezerwą (np. plotki i pogłoski kuluarowe)[60].

Trzeba podkreślić, że część uzyskanych informacji trafia do organów władzy bezpośrednio, omijając analityków. Dzieje się tak zwłaszcza w szczególnie określonych sytuacjach, np. w trakcie trwania konfliktów. Wtedy właśnie przepływ informacji musi być natychmiastowy, nie ma bowiem czasu na długotrwałe, wnikliwe analizy. Decyzję podejmuję się często w oparciu o dane uzyskane „przed chwilą". W czasie wojny również wzrasta zdecydowanie znaczenie informacji pozyskanych drogą niejawną.

[59] Tamże, s. 107.

[60] B. Martinet, Y. M. Marti, op. cit., s. 75.

Niezwykle istotnym aspektem działalności wywiadowczej jest czas uzyskania i dostarczenia oczekiwanej wiadomości. „Działalność wywiadowcza jest prowadzona pod ścisłym rygorem terminowości. Chodzi bowiem nie tylko o to, aby dotrzymać kroku toczącym się wydarzeniom, ale także by dopasować się do procedur i rozkładu zajęć struktur biurokratycznych państwa"[61]. Informacja, nawet najcenniejsza, ale dostarczona zbyt późno jest dysfunkcjonalna. „Zachodni specjaliści wyliczyli, że na przykład informacje wywiadowcze o charakterze operacyjno-taktycznym w ciągu 5 dni od chwili dostarczenia tracą na aktualności około 50 %, to jest średnio 10 % w ciągu jednego dnia"[62].

Informacje gromadzone przez wywiad posiadają różną wartość. Należy zaznaczyć, że cenność wiadomości zależy od okoliczności politycznych i kontekstu sytuacji międzynarodowej. Bardzo ważny jest również czas. W różnym okresie ta sama informacja posiada inne znaczenie. Wartość informacji zależy od wielu czynników. „Są to przede wszystkim: (a) dobra analiza potrzeb, (b) odpowiedniość i jakość źródeł, (c) jakość analizy, (d) udostępnienie i sprzężenie zwrotne, (e) zabezpieczenie informacji"[63].

Organy władzy i służby wywiadowcze zawierają niepisaną umowę na świadczenie usług. Strony tego stosunku umownego można nazwać z jednej strony zleceniobiorcą, z drugiej zleceniodawcą. Pomiędzy nimi musi istnieć kod porozumiewania się oparty na jednoznacznych symbolach. Jakiekolwiek nieporozumienie prowadzi do rozbieżności we wzajemnych oczekiwaniach. „Odpowiedzi na stawiane pytania muszą być formułowane w tych samych kategoriach, w jakich formułuje się pytania. Musi poza tym istnieć komunikacja (w obie strony) pomiędzy decydentem a środowiskiem informacyjnym (analitykami) czego roboczym skutkiem jest informacja zwrotna pozwalająca na doskonalenie metodyki pracy informacyjnej"[64]

Ostatnim etapem procesu wywiadowczego jest dystrybucja gotowego produktu. „Zwykle materiały dostarcza się użytkownikowi w formie pisemnej, chociaż również można go zaznajomić z opracowaną informacją, wygłaszając oświadczenie na specjalnie zwołanej konferencji czy w bezpośredniej rozmowie. W Wielkiej Brytanii preferuje się informacje pisemne, w Stanach Zjednoczonych natomiast polityka opiera się w większym stopniu na przekazie ustnym, głównie ze względu na tempo zmian politycznych"[65].

Poza możliwością ukierunkowywania trybu w jakim informacja powinna, a raczej może być wykorzystana, służby specjalne nie maja wpływu na sposób jej wykorzystania. Dostarczają przygotowane materiały w uprzednio skonsultowanej formie. Opisując produkt można posłużyć się klasyfikacją Shermana Kenta, który wyróżnił trzy główne kategorie efektów końcowych pracy wywiadu: (1) informowanie bieżące (*current-reportial*), (2) informacja podstawowa/ogólna (*basic-descriptive*), (3) ocena/prognoza (*speculative-evaluative*)[66].

[61] M. Herman, op. cit., s. 52.
[62] F. Bielak, op. cit., s. 31.
[63] B. Martinet, Y. M. Marti, op. cit., 18.
[64] S. Zalewski, *Funkcja informacyjna służb...* s. 40.
[65] M. Herman, op. cit., s. 112.
[66] Tamże, s. 112.

Tabela 3. Etapy procesu wywiadowczego

Zdobywanie danych i informacji wywiadowczych, analiza wstępna, dystrybucja	
⇩	⇩
Całościowa analiza i dystrybucja informacji wywiadowczych	Przygotowanie ocen narodowych i dystrybucja danych wywiadowczych
⇩	
UŻYTKOWNIK	

Źródło: M. Herman, op. cit., s. 45.

Źródła informacji wywiadowczej

Znamienną cechą, przypisaną działalności wywiadowczej jest fakt, że zdobywanie informacji odbywa się, w większości przypadków bez wiedzy, a tym samym zgody obiektów infiltrowanych. Ze względu na powyższe zjawisko, służby specjalne musiały przez lata poszukiwać i wypracować coraz to nowe sposoby realizowania swoich zadań. Z tej perspektywy już u samego zarania można podzielić źródła informacji na ogólnodostępne, o dostępności ograniczonej oraz relatywnie niedostępne[67].

Na przestrzeni lat używano najróżniejszych metod pozyskiwania potrzebnych informacji. Od tradycyjnego kontrolowania przesyłanej korespondencji, praktykowanej już od XVI wieku przez zakładanie podsłuchów i śledzenie, po najnowocześniejsze systemy rozpoznania satelitarnego. Współcześnie wykorzystuje się wszelkie znane metody pozyskiwania wiadomości, ale najstarszą z nich była ta, oparta na wykorzystaniu człowieka, jako źródła informacji, bądź jako podmiotu mogącego wykorzystać swój potencjał do uzyskania wiedzy. Dane wywiadowcze pochodzące z tego źródła określa się obecnie mianem, HUMINT (*human intelligence*). Poza wymienionym istnieją jeszcze dwa główne źródła informacji wywiadowczej. Jedno z nich to rozpoznanie radioelektroniczne – SIGINT (*signals intelligence*), łączone obecnie wraz z upowszechnieniem się nowych technologii. Drugie to rozpoznanie na podstawie analizy zdjęć lotniczych, wykonanych przez wojskowe samoloty szpiegowskie – IMINT.

Źródła osobowe dostarczają zazwyczaj informacji, które występują w środowisku ich pracy i codziennego funkcjonowania. Zdobywają materiały pozostające w zasięgu ich możliwości zdobycia. To co odróżnia to źródło wiedzy od pozostałych, to niedostrzegalne przez urządzenia techniczne, ludzkie odczucia i nastawienie. Informator, poza suchymi danymi, może również wskazać na atmosferę panującą w instytucji, morale w armii, cechy charakterologiczne przywódcy. To co jest mocną stroną rozpoznania typu HUMINT, jest też jej słabą stroną. Informatorzy, jak każdy mają swoje słabe strony, przyzwyczajenia, fobie, urazy. Są podatni na kuszące propozycje innych wywiadów, czy po prostu mają czasami chwile zwątpienia. Każdy taki moment niepewności, dla wywiadu nadzorującego pracę agenta, oznacza nie tylko brak

[67] S. Zalewski, *Służby specjalne w państwie...*, s. 74.

plonów informacyjnych ale czasami również niebezpieczeństwo. „Obecnie wskutek coraz większej otwartości społeczeństw rola zdobywania informacji ze źródeł osobowych znacznie się zmniejszyła, ale nie do końca. Nie wszystko bowiem da się zobaczyć przez obiektywy kamer satelitów rozpoznawczych, a dotyczy to szczególnie tego, co dzieje się za zamkniętymi drzwiami"[68].

Michael Herman, opisując formę pozyskiwania informacji typu HUMINT, rozrysował interesującą piramidę, która ukazuje przedział społeczny przez najczęściej występujące przypadki podmiotów dostarczających wywiadom wiadomości. W piramidzie znalazły się następujące osobowe źródła informacji: (a) agenci/informatorzy, (b) uciekinierzy, (c) opozycja polityczna, emigranci, podziemne struktury opozycyjne, (d) informatorzy okazjonalni, (e) ludność zamieszkała na terytoriach okupowanych, (f) kontakty handlowe, (g) uchodźcy, (h) informacje ekspertów, informacje uzyskane od osób podróżujących do innych krajów. Autor umieścił w powyższym wykazie zarówno źródła osobowe wykorzystywane w czasie pokoju (np. kontakty handlowe), jak i w czasie wojny (jeńcy wojenni). Źródła z którymi można utrzymywać stałe kontakty informacyjne (np. agenci), lub okazjonalne. Wreszcie, znalazło się miejsce zarówno dla informatorów świadomych (np. eksperci), oraz takich, którzy dostarczają materiałów w dobrej wierze nie zdając sobie sprawy, że ich doniesienia zostaną wykorzystane w celach polityczno-wojskowych (np. turyści po powrocie do krajów przekazujący informacje w celach dziennikarskich).

Najpłodniejszym okresem funkcjonowania źródeł osobowych był czas tzw. zimnej wojny. „Wywiad sowiecki wygrywał w tej walce. Przegrywał natomiast kontrwywiad. Na Zachód uciekły setki agentów, wywożąc wiele tajemnic wywiadowczych. (...) Agentów werbowano w najróżniejszy sposób. Podstawę do werbunku stanowią zasadniczo trzy rzeczy: pycha, pieniądze i seks. Szczególnie KGB z premedytacją stosowało przynęty erotyczne. W latach pięćdziesiątych dwunastu pracowników ambasady USA w Moskwie (w tym szef placówki CIA – Edward Elis Smith) przyznało się do utrzymywania kontaktów erotycznych z tzw. jaskółeczkami"[69]. Obecnie w sytuacji rozproszenia niebezpieczeństw i pluralizmu rywalizujących ze sobą obiektów, służby specjalne starają się zdecydowanie częściej korzystać z bardziej uniwersalnych źródeł informacji, które mogą zapewnić dopływ wiadomości na temat różnych podmiotów i obiektów, będących w kręgu ich zainteresowania.

Należy dodać, że najskuteczniejszym typem informatorów są agenci ideolodzy, poświęcający własne życie i narażający się na infamię oraz niebezpieczeństwo w imię własnych przekonań światopoglądowych. Ten rodzaj agentów pojawił po 1917 roku, wraz z urzeczywistnieniem się, dotąd teoretycznych wizji komunizmu. Występują również agenci –cynicy, dla których liczy się głównie aspekt finansowy ich pracy. To dzięki ich zasługom, służby specjalne zawdzięczają również opinię środowiska osób, które nikomu nie ufają i boją się własnych cieni. „W roku 1962

[68] M. Herman, op. cit., s. 67.

[69] M. Karpiński, op. cit., s. 189-190, 197.

Stanisław Lem pisze *Pamiętnik znaleziony w wannie*. Jest to obraz dziwnego świata wywiadu, w którym nie wiadomo, kto dla kogo pracuje. Agenci są bezustannie przewerbowywani, i to nie raz, nie dwa, ale i po osiem razy. W tym surrealistycznym świecie traci się rozeznanie, dla kogo się pracuje, nie mówiąc już po co"[70]. Nadal, bez względu na „nieograniczone możliwości" techniki, dobrze umiejscowiony agent – informator, mający dostęp do najtajniejszych materiałów i dokumentów, stale dostarczający informacji, jest najcenniejszym skarbem dla organów wywiadowczych. „Biorąc pod uwagę wszystkie korzyści płynące z wykorzystania źródeł osobowych, za całkowicie uzasadniony należy więc uznać stały wzrost nakładów finansowych, jakie przeznacza się na działalność organów prowadzących HUMINT w wieku dwudziestym"[71].

Współcześnie jednak nominalnie najwięcej informacji dostarczają programy rozpoznania radioelektronicznego, teleinformatycznego i magnetycznego. Każde elektroniczne urządzenie emituje promieniowanie elektromagnetyczne. Nowoczesne systemy rozpoznania radioelektronicznego umożliwiają wykorzystywanie ich do przechwytywania rozmów, kontaktów prywatnych osób, instytucji prywatnych, państwowych, czy przedsiębiorstw. „Rozpoznanie radioelektroniczne dzieli się zwykle na rozpoznanie radiowe – COMINT (*communications intelligence*), czyli wykrywanie, śledzenie i przechwytywanie emisji radiowych, oraz na rozpoznanie systemów radioelektronicznych – ELINT (*electronic intelligence*), które odnosi się do środków emitujących energię elektromagnetyczną"[72].

Bezpośrednio powiązany ze zdobywaniem informacji drogą radioelektroniczną jest proces łamania szyfrów. Historia dekryptażu rozpoczęła się w tym samym czasie, co historia SIGINT. Już w starożytności stosowano systemy szyfrów, które miały uniemożliwić wrogom odczytanie informacji, pomimo jej przechwycenia. „Juliusz Cezar był twórcą jednego z pierwszych szyfrów w historii. Do odczytywania takiej korespondencji konieczny był klucz, czyli zasada, wedle której litery są zastępowane. Cezar swoje notatki szyfrował, zastępując litery innymi, przesuniętymi o trzy miejsca w kolejności alfabetu. Jest to klasyczny szyfr monoalfabetyczny"[73]. Nowożytna historia szyfrowania i dekryptażu zaczęła się od znakomitego, włoskiego matematyka Gerolama Cardana (*Hieronymus Cardanus*). „Ów znakomity mechanik, matematyk i lekarz podał nie tylko metodę rozwiązywania równań algebraicznych trzeciego stopnia, nie tylko stworzył podwaliny teorii liczb urojonych i rachunku prawdopodobieństwa oraz tak zwanych kół Cardana, ale także na długo przed Braille'em, dotykowy alfabet dla niewidomych. Popełnił on książkę o dekryptażu, o teoretycznych i praktycznych sposobach odczytywania utajnionej korespondencji. Książka ta wpadła w ręce Francisa Walsinghama"[74].

Batalia prowadzona między kryptologami a specjalistami od łamania szyfrów trwa nieustannie. Obie strony są niezmiennie na tym samym etapie udoskonalania swoich systemów.

[70] Tamże, s. 238.
[71] M. Herman, op. cit., s. 72.
[72] Tamże, s. 75.
[73] M. Karpiński, op. cit., s. 31.
[74] Tamże, s. 46

W środowisku osób zajmujących się dekryptażem panuje przekonanie, że nie wymyślono jeszcze na świecie szyfru, którego nie możnaby było złamać. To niewątpliwie prawdziwe twierdzenie musiało być jednak poddane weryfikacji z uwagi na kilka przypadków. Najbardziej znanym przykładem doskonałej „maszyny szyfrującej", jest historia wykorzystania Indian z plemienia Nawaho, w trakcie II wojny światowej. Było to jedyne plemię, żyjące w Ameryce północnej, które nie zostało dokładnie zbadane przez niemieckich antropologów. Dla potwierdzenia pewności szyfru, poddano go kontroli, grupie wybitnych kryptoanalityków, których największym sukcesem było złamanie najtrudniejszego japońskiego szyfru – kodu purpurowego. Ponieśli porażkę na całej linii. Nie tylko, że nie byli w stanie złamać kodu, ale nawet nie potrafili dokonać transkrypcji nagrania[75].

Istnieją także dwa inne sposoby rozpoznania radioelektronicznego. Jednym z nich jest tzw. analiza używalności pasma, „która pozwalała na określenie struktury sieci radiowych i identyfikację poszczególnych abonentów"[76]. Drugim jest tzw. namierzanie, które za pomocą urządzeń zbierających energię elektromagnetyczną, umożliwia z precyzyjna dokładnością, wskazanie współrzędnych obiektu, którym jest się zainteresowanym. „Techniki prowadzenia rozpoznania radioelektronicznego umożliwiają wyznaczenie współrzędnych punktów położenia obiektów i na tej podstawie zidentyfikowania ugrupowania przeciwnika oraz określenie kierunków i sposobów przegrupowania jego sił i środków"[77].

W literaturze przedmiotu zwraca się uwagę także na inne źródła rozpoznania technicznego, mianowicie: (a) NUCINT (*nuclear intelligence*), czyli rozpoznanie nuklearne, (b) RADINT (*radar intelligence*), czyli rozpoznanie przy pomocy radarów dalekiego zasięgu, oraz (c) ACOUSTINT, czyli rozpoznanie dźwiękowe pod powierzchnią wody. Dwa pierwsze rozpoznania prowadzi się na powierzchni przy pomocy radarów i satelit. Pierwsze z nich ma za zadanie wykrywać wszelkie eksplozje jądrowe zarówno na powierzchni, jak i pod ziemią. Wykorzystuje się do tego aparaty sejsmograficzne oraz urządzenia wykrywające promieniowania *gamma.*

[75] Tamże, s. 185. Najsłynniejszą maszyną szyfrującą była, wykorzystywana w trakcie II wojny światowej, niemiecka maszyna szyfrująca, wynaleziona przez inżyniera Arhura Scherbiusa. Maszyna składała się z trzech elementów: klawiatury na 26 liter, części szyfrującej i 26 lampek wyświetlających, jaką literą została zastąpiona inna litera. Maszynę obsługiwały dwie osoby. Jedna zapisywała tekst jawny, druga notowała, które lampki się zapalały tworząc tym samym zaszyfrowany tekst. Istnienie maszyny nie było żadną tajemnicą, co więcej była ogólnodostępna w sprzedaży. Ten fakt wynikał z liczby możliwych kombinacji. Część szyfrująca bowiem składała się z trzech obracających się bębenków, a każdy z nich dawał 26 połączeń. Bębenki można było umieszczać względem siebie na sześć różnych sposobów. Z tyłu maszyna miała łącznicę telefoniczną z sześcioma przewodami i 26 gniazdami wtykowymi. Razem dawało to 10 000 000 000 000 000 kombinacji. Osoby wysyłające i odbierające musiały wiedzieć w jakich pozycjach ustawione są bębenki i przewody, by móc swobodnie prowadzić kontakt za pomocą szyfru. Niemcy nadawali na początku każdej depeszy kluczem dziennym ustalanym dla wszystkich maszyn, sposób ustawienia bębnów szyfrujących dla danego połączenia. Kod złamali słynni polscy matematycy, uczniowie profesora Stefana Banacha: M. Rejewski, H. Zygalski, J. Różycki. Polacy przeprowadzili następujące rozumowanie: łącznica dawała bardzo dużą liczbę kombinacji ale była szyfrem monoalfabetycznym, gdzie jedna litera zastępowana jest inną. Taki rodzaj szyfrowania nie jest odporny na analizę frekwencyjną, o czym wiedziano już w IX wieku. Wystarczyła znać tylko ułożenie bębnów. Rejewski stworzył maszynę, która połączyła sześć zestawów trójbębnowych z Enigmy i mogła swobodnie odczytywać niemieckie komunikaty. Maszynę nazwano „bomba", na cześć porcji lodów, na które wybierali się Polacy w przerwach do Hotelu Europejskiego w Warszawie. Niemcy systematycznie jeszcze udoskonalali maszynę dodając kolejne bębny. Dokumentacja polskiej maszyny została tuż przed wojną przekazana wywiadom, brytyjskiemu i francuskiemu. Brytyjczycy jeszcze wielokrotnie przebudowywali maszynę. Ostatnia najdoskonalsza wersja nazywała się Agnes. Zob. W. Kozaczuk, *W kręgu Enigmy*, Warszawa 1986.

[76] M. Herman, op. cit., s. 76.

[77] Tamże, s. 77.

RADINT śledzi wszelkie „obiekty kosmiczne i pozahoryzontalne (*OTHR – Over the Horizon Radar*)"[78]. ACOUSTINT wreszcie to rozpoznanie akustyczne, proporcjonalne do radioelektronicznego tyle że pod powierzchnią wody.

Na przykładzie różnorodności źródeł, których liczba i dywersyfikacja stale rośnie można pokusić się o następujące spostrzeżenie. Wraz z postępem cywilizacyjnym odchodzi się od tradycyjnych metod pozyskiwania informacji, zastępując je nowoczesnymi technologiami. Zmienił się paradygmat wykorzystania źródeł. Społeczeństwo informacyjne stopniowa samo dostarcza wiadomości o samym sobie. Agenci, którzy musieli wsiąkać do środowiska, które inwigilowali powoli odchodzą do lamusa. Zdjęcia satelitarne oddają obraz rzeczywistości z dokładnością do kilku milimetrów. Obecny wywiad jest na pewno inny niż ten, który zmagał się z zimnowojennym wrogiem. W tym samym czasie jednak zmieniły się obiekty, na które nacelowane są radary. Cały system wywiadowczy, który obecnie funkcjonuje, powstawał jeszcze z myślą o prześwietlaniu wyraźnie zlokalizowanego wroga i jego zasobów militarnych a także zamierzeń politycznych. Jak jednak przy pomocy nawet najdokładniejszych satelit zajrzeć do wnętrza umysłu terrorysty i wysondować jego najbliższe plany. „Powstaje w tym miejscu pytanie, na ile nowoczesna technologia będzie skuteczna w walce z niezrozumiałymi dla otoczenia intencjami zdegenerowanych jednostek ludzkich, czy też psychicznymi lękami, poczuciem krzywdy, zagrożenia, agresją czy apatią, które towarzyszą powstawaniu zjawisk przemocy i terroru"[79].

Wyzwania

Szybko zmieniający się świat wymusza, również na służbach specjalnych, dostosowywanie się do nowych wyzwań. Jeszcze do niedawna większość agencji wywiadowczych funkcjonowała w oparciu o modele ukształtowane w okresie zimnej wojny. Trwająca rewolucja geopolityczna, technologiczna, informacyjna, wreszcie społeczna zmusza służby do ciągłych reform i przekształceń w zakresie metod pracy. Współczesne zagrożenia nie jest ani łatwo definiować, ani lokalizować. Widoczna jest tendencja do bezrefleksyjnego zwiększania metod i narzędzi pozyskiwania informacji. Multiplikowana ilość informacji, wręcz masowe gromadzenie danych za pomocą nowoczesnych technologii, może prowadzić do paraliżu instytucjonalnego. Natłok danych powoduje, że służby muszą znaleźć sposób na umiejętną ich filtrację i analizę. Ważnym zadaniem, przed którym stoją państwa, staje się skuteczna egzekucja kontroli nad działalnością służb. Koniecznym jest racjonalne połączenie ich samodzielności i skutecznego działania z warunkiem przestrzegania norm konstytucyjnych. Stale obserwowane jest zjawisko zwiększania kompetencji organów bezpieczeństwa kosztem zmniejszania sfery prywatności obywateli. We współczesnym turbulentnym świecie niewątpliwie znaczenie służb specjalnych rośnie.

[78] Tamże, s. 85.

[79] S. Zalewski, *Funkcja informacyjna służb*... s. 38.

Bibliografia:

1. Bielak F., *Służby wywiadowcze Republiki Federalnej Niemiec*, Warszawa 1985.
2. Bożek M., Stankowska I., Zalewski S., *Ochrona informacji niejawnych. Wybrane zagadnienia*, Warszawa 2003.
3. Bożek M., *Współczesny model polskich służb specjalnych. Służby informacyjne czy policyjne?*, Zeszyty Naukowe Akademii Obrony Narodowej, 2005, nr 1 (58).
4. Ciborowski L., *Przestrzenie informacyjne działań zbrojnych*, Warszawa 1997.
5. Dominiczak D., *Organa bezpieczeństwa PRL 1944 – 1989. Rozwój i działalność w świetle dokumentów MSW*, Warszawa 1997.
6. *Encyklopedia szpiegostwa*, SPAR, Warszawa 1995,
7. Faligot R., Kauffer R., *Służby specjalne*, Warszawa 1998.
8. Herman M., *Potęga wywiadu*, Warszawa 2002.
9. Karpiński M., *Historia szpiegostwa*, Warszawa 2003.
10. Kessler W., *CIA od środka*, Warszawa 1994.
11. Koch E. R., Sperber J., *Infomafia*, Gdynia 1999.
12. Kozaczuk W., *W kręgu Enigmy*, Warszawa 1986.
13. Martin H.P., Schumann H., *Pułapka globalizacji*, Wrocław 2000.
14. Martinet B., Marti Y. M., *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*, Warszawa 1999.
15. Misiuk A., *Służby specjalne II Rzeczypospolitej*, Warszawa 1998.
16. Ockrent Ch., De Marenches A., *Sekrety szpiegów i książąt*, Warszawa 1992.
17. *Parlamentarny nadzór nad sektorem bezpieczeństwa. Zasady, mechanizmy i praktyki*, Unia Międzyparlamentarna i Genewskie Centrum Demokratycznej Kontroli nad Siłami Zbrojnymi, Warszawa 2004.
18. Pepłoński A., *Kontrwywiad II Rzeczypospolitej*, Warszawa 2002.
19. Piekałkiewicz J., *Dzieje szpiegostwa*, Warszawa 1999.
20. Podolski A., *Europejska współpraca wywiadowcza – brakujące ogniwo europejskiej polityki zagranicznej i bezpieczeństwa?*, Centrum Stosunków Międzynarodowych, Raporty i Analizy nr 10, Warszawa 2004.
21. Rogala-Lewicki, A., *Informacyjny aspekt decyzji w środowisku politycznym* [w:] *Interdyscyplinarne ujęcie prawa*, red. Żuralska, M., Warszawa 2013.
22. Rogala-Lewicki A., *Służby specjalne po zamachach terrorystycznych w USA i Europie – Patriot Act versus dyrektywa retencyjna, czyli legitymizowanie nadużyć sferze prywatności w demokratycznych państwach prawa – studium porównawcze*, Myśl Ekonomiczna i Polityczna 2015, Nr 3(50).
23. Rydlewski G., *Rządowy system decyzyjny w Polsce*, Warszawa 2002.
24. Shulsky, A.N., Schmitt G.J. *Silent Warfare: Understanding the World of Intelligence*, Waszyngton DC 1991.
25. Suworow W., *Akwarium*, Warszawa 1990.
26. Suworow W., *Specnaz*, Gdańsk 1991.

27. Suworow W., *Lodołamacz*, Warszawa 1992.
28. De Villemarest P., *GRU – sowiecki super wywiad*, Warszawa 1998.
29. Volkoff V., *Dezinformacja oręż wojny*, Warszawa 1991.
30. West N., *MI – 5*, Warszawa 1999.
31. West N., *MI – 6, Operacje brytyjskiej Tajnej Służby Wywiadu 1909 – 1945*, Warszawa 2000.
32. Westerby G., *Na terytorium wroga. Tajemnice Mosadu*, Warszawa 2001.
33. Zalewski S., *Ewolucja modelu polskich służb specjalnych*, Warszawa 2003.
34. Zalewski S., *Służby specjalne – programowanie, nadzór, koordynacja*, Warszawa 2003.
35. Zalewski S., *Funkcja informacyjna służb specjalnych w systemie bezpieczeństwa RP*, Warszawa 2005.
36. Zalewski S., *Służby specjalne w państwie demokratycznym*, Warszawa 2005.
37. Żebrowski A., Żmigrodzki M., Babula J., *Rola służb specjalnych w siłach zbrojnych*, Kraków 1999.
38. Żebrowski A., Kwiatkowski W., *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000.