ZAGROŻENIA ZE STRONY ORGANIZACJI TERRORYSTYCZNYCH I OBCYCH SŁUŻB SPECJALNYCH W AFGANISTANIE

Sebastian Malinowski

Akademia Obrony Narodowej

Streszczenie: Artykuł podejmuje zagadnienia wybranych zagrożeń dla bezpieczeństwa informacji niejawnych w aspekcie zagrożeń ze strony obcych służb specjalnych i organizacji terrorystycznych oraz przedsięwzięć realizowanych w przedmiotowym zakresie w odniesieniu do funkcji pełnionej przez kierownika jednostki organizacyjnej. Autor koncentruje się na przedstawieniu podstawowych doświadczeń w tym zakresie w ramach PKW w Afganistanie. Opisane doświadczenia poświadczają konieczność ochrony w zakresie ataków terrorystycznych i w tym samym stopniu służb wywiadowczych obcych państw.

Słowa kluczowe: Afganistan, Polski Kontyngent Wojskowy, terroryzm, służby specjalne, bezpieczeństwo państwa.

„Nie wystarczy zdobywać mądrości,
trzeba jeszcze z niej korzystać."
Cyceron

Informacje wywiadowcze wykorzystywane w czasie operacji wojskowych, zwłaszcza o charakterze wojennym, mają najczęściej zasadnicze znaczenie dla powodzenia prowadzonych działań. Najistotniejsze z tych informacji służą następnie generowaniu analiz, raportów oraz wypracowywaniu decyzji, także o znaczeniu strategicznym. Następnie wiele z nich ze względu na ich ważność zostanie oznaczonych odpowiednim gryfem niejawności i będzie podlegało tej szczególnej ochronie.

W rejonie operowania ISAF[1] w Afganistanie działają[2]: Służba Wywiadu Wojskowego (SWW) i Służba Kontrwywiadu Wojskowego (SKW). Wywiad i kontrwywiad wojskowy opiera swoje działania w tym rejonie najczęściej na pozyskanych do

[1] ISAF (ang. International Security Assistance Force) – „Międzynarodowa Siła Wsparcia Bezpieczeństwa – struktura wojsk operacyjnych wystawiona głównie przez siły zbrojne państw członkowskich Organizacji Traktatu Północnoatlantyckiego, zajmująca się utrzymaniem pokoju w Afganistanie. Utworzona na mocy Porozumienia z Bonn zawartego 5 grudnia 2001 r. i usankcjonowana prawnie na mocy rezolucji nr 1386 Rady Bezpieczeństwa ONZ z 20 grudnia 2001. 11 sierpnia 2003 siły ISAF przeszły pod kierownictwo NATO, co zostało usankcjonowane kolejną rezolucją ONZ nr 1510 z 13 października 2003. http://pl.wikipedia.org/wiki/Międzynarodowe_Siły_Wsparcia_Bezpieczeństwa [dostęp w dniu: 1.10.2014 r.].

[2] W rejonie misji afgańskiej WSS zdobywają informacje dotyczące bezpieczeństwa wojsk oraz przeciwdziałania zagrożeniom – identyfikują możliwości przeciwnika w zakresie ISTAR – Intelligence, Surveilance, Target Acquisition and Recconnaissance – wywiad, obserwacja, zdobywanie informacji o celach oraz rozpoznanie.

współpracy utajnionych agentach. Duża część tych informacji pochodzi głównie z wywiadu technicznego. Pobyt funkcjonariuszy WSS[3] w środowisku, które ma dostęp do istotnych informacji oraz z którego może pochodzić główne zagrożenie, ma istotne znaczenie dla jakości systemu zbierania informacji wywiadowczych oraz własnego bezpieczeństwa. WSS wykonują ustawowe zadania rozpoznawania zagrożeń związanych z terroryzmem, zapobiegania im i przeciwdziałania. Jednym z zadań służb specjalnych jest między innymi rozpoznawanie i analizowanie zagrożeń występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych mogących wpłynąć na zdolność bojową Sił Zbrojnych RP, jednocześnie z podejmowaniem działań mających na celu wyeliminowanie tych zagrożeń oraz ochronę zdobytych i posiadanych już istotnych informacji, a także zapewnienie im elementarnego bezpieczeństwa.

Wiele opracowań o bezpieczeństwie podkreśla, że bezpieczeństwo organizacji zależy w głównej mierze od poziomu zabezpieczenia jej zasobów informacyjnych. Należy zwrócić uwagę, że nie bez przyczyny ustawodawca, uaktualniając w 2010 r. jeden z ważniejszych aktów normatywnych dotyczących informacji szczególnie wrażliwych, określił potrzebę ochrony przede wszystkim fizycznej przed[4]:

1) działaniem obcych służb specjalnych;
2) zamachem terrorystycznym (terroryzmem).

Każdy podmiot musi w związku z tym (bez względu na motywy kierujące postepowaniem np. jego kierownictwa) odpowiednio zorganizować system ochrony informacji ważnych ze względu na bezpieczeństwo i ogólnie rozumiany interes podmiotu. Jeżeli przyjrzymy się państwu, to taki system będzie ściśle określony, zwłaszcza w zakresie ochrony informacji niejawnych przez przepisy (ustawy), rozporządzenia, zarządzenia itd. Ochrona interesów, zwłaszcza politycznych i gospodarczych, jest swoistym zobowiązaniem władz państwa[5] do określania, podejmowania oraz realizacji przedsięwzięć chroniących i zabezpieczających przed działaniami obcych służb specjalnych czy też terrorystów. Szczególnie groźna jest penetracja państwa i pozyskiwanie strategicznych informacji przez obce służby specjalne. Działanie polegające na tzw. „gaszeniu pożarów", tj. poprzez reagowanie wyłącznie na stwierdzone lub wykryte przypadki działalności, jest nieskuteczne,

[3] WSS – Wojskowe Służby Specjalne, zdefiniowane [w:] A. Skwarski, *Wojskowe Służby Specjalne…*, rozprawa doktorska, AON, Warszawa 2012.

[4] Art. 45. USTAWY z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych: „1. Jednostki organizacyjne, w których są przetwarzane informacje niejawne, stosują środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, w szczególności chroniące przed:
1) działaniem obcych służb specjalnych;
2) zamachem terrorystycznym lub sabotażem".

[5] Jest to zasada uniwersalna, stosowana bez względu na system polityczny, jaki istnieje w danym państwie.

a na pewno niewystarczające. Podstawą skutecznej ochrony informacji jest tworzenie takich rozwiązań i mechanizmów prawno-organizacyjnych, które umożliwią przeciwdziałanie formom i metodom zdobywania informacji uznawanych przez państwo za nielegalne. Jeżeli przyjmiemy, że bezpieczeństwo informacji zależy od jakości jej ochrony – to należałoby założyć, że im wyższa będzie jakość tej ochrony, tym większe będzie to bezpieczeństwo. Nic bardziej mylnego, niestety zapewnienie nawet najwyższego poziomu bezpieczeństwa nie zlikwiduje zagrożeń, jakie stwarzają obce służby specjalne oraz organizacje o charakterze terrorystycznym. Natomiast pewne jest, że uwzględnienie w przygotowaniu i samej organizacji systemu ochrony informacji rozpoznanych już zagrożeń wywiadowczych i terrorystycznych zapewnia wydatną ich neutralizację i relatywnie niskim kosztem wzrost ich bezpieczeństwa.

Działalność wywiadowcza obcych służb specjalnych

Aktualnie od kilku lat o służbach specjalnych mówi się i pisze relatywnie dużo, zwłaszcza w aspekcie ich działalności po drugiej wojnie światowej. Są to niestety opisy np. wywiadu[6] w zakresie ich funkcjonowania w poszczególnych państwach, ich historii, „ujawnionych" porażek i dokonań – często spektakularnych. Jednocześnie nie zwraca się uwagi tak naprawdę na istotę form ich działalności w postaci sabotażu, dywersji, a nawet niejednokrotnie terroryzmu.

Wśród wielu definicji należy zwrócić uwagę na następującą[7]: wywiad (instytucja wywiadowcza[8]) – „służba specjalna zajmująca się pozyskiwaniem (często niejawnych) informacji oraz ich przetwarzaniem, przechowywaniem, analizą tych informacji i przekazywaniem ich rządowi. Służba wywiadowcza realizuje poza zadaniami o charakterze informacyjnym także zadania o charakterze sprawczym. Taka instytucja poza granicami państwa wykonuje politykę rządu. Politykę zagraniczną rządu może wykonywać w sposób legalny, nielegalny, a także poprzez dyplomację. Czyni to, wpływając (także w sposób brutalny) na osoby mające wpływ na działalność, która jest ważna dla rządu, dla interesu państwa".

Z działaniami wywiadu jako instytucji państwowej wiąże się przede wszystkim jego działalność szpiegowska[9], realizowana przez osoby lub grupy osób (siatki) w sposób świadomy. Działalność tę prowadzi się w sposób skryty, utajniony, ponieważ

---

[6] Ze względu na obszary zainteresowań możemy mówić o wywiadzie: wojskowym, politycznym oraz ekonomicznym, a także w dalszym ciągu o naukowym i elektronicznym (współcześnie komputerowym).

[7] http://pl.wikipedia.org/wiki/Wywiad_(instytucja) [dostęp w dniu: 1.10.2014 r.].

[8] Wywiad to instytucja państwowa działająca głównie na zewnątrz danego kraju.

[9] Szpieg to potoczne określenie osoby zajmującej się szpiegostwem. Zadaniem szpiegów jest odkryć tajemnice innych krajów, ale także innych firm (szpiegostwo przemysłowe) w sposób niepozwalający na zorientowanie się, że tajemnice zostały wykradzione. Pracując w ten sposób, szpiedzy starają się utrzymać w tajemnicy charakter swojej misji – podają się np. za inne osoby, komunikują się z mo-

jej celem jest zdobycie (uzyskanie) informacji, które z założenia stanowią tajemnicę państwową (czasami służbową) ze względu na ważny interes danego kraju. Informacje takie z zasady są niedostępne dla szerokiego grona osób oraz dobrze chronione. Przy tym szpiedzy nie szczędzą starań, by „okradziony" z tajemnic nie zorientował się, że dotarły do nich osoby nieuprawnione. Z dużym powodzeniem działalność wywiadowczą wobec Afganistanu można było uprawiać z terenu własnego kraju, unikając m.in. kłopotliwych zabiegów w celu werbowania agentury szpiegowskiej. Możliwości takie stwarzał przede wszystkim międzynarodowy ruch osobowy o dużej skali i zasięgu oraz transformacje ustrojowe państw.

Z względu na ukształtowaną w ostatnim półwieczu wysoką specjalizację w służbach specjalnych, a szczególnie w wywiadzie w postaci podziału wywiadu na: wywiad polityczny, wywiad ekonomiczny, wywiad wojskowy, wywiad naukowy i komputerowy – wywiad realizuje swoje cele poprzez zbieranie interesujących informacji, wykorzystując do tego głównie tzw. „biały wywiad"[10] (około 80% danych), agenturę[11] (około 18% danych) i środki techniczne[12] (około 2% danych).

Obszary i skoncentrowanie na nich zainteresowania służb wywiadowczych w Afganistanie prawdopodobnie przebiegały według m.in. następującego schematu[13]:

codawcą w ukryty sposób itd. Zwalczaniem szpiegostwa i rozpoznawaniem go w Polsce zajmuje się kontrwywiad, np. Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego. Współcześnie szpiegów w zależności od przynależności i specjalizacji można podzielić na:

a) funkcjonariuszy i żołnierzy organizacji wywiadowczej – etatowi oficerowie wywiadu cywilnego lub wojskowego wykonujący tajne misje na terenie innych krajów;

b) agentów – są to zwykle obywatele państwa, którego tajemnice wykradają, zwerbowani przez obcy wywiad;

c) szpiegów uśpionych (śpioch, matrioszka, nielegalny, nielegał itp.) – szpieg, który został zwerbowany i przeszkolony (lub funkcjonariusz/żołnierz nielegalny), jednak nie rozpoczyna swojej działalności, czekając na polecenie lub rozkaz instytucji, która go zwerbowała lub w której służy;

d) ze względu na posiadany immunitet dyplomatyczny lub jego brak;

e) szpieg pod przykryciem dyplomaty;

f) szpieg bez immunitetu dyplomatycznego, tzw. nielegalny, nielegał itp.

Źródło: http://pl.wikipedia.org/wiki/Szpieg [dostęp w dniu: 1.10.2014 r.].

[10] „Biały wywiad" to informacje uzyskane z ogólnie dostępnych mediów, tj.: prasy, radia, telewizji i wydawnictw np. książkowych. Wartość tych informacji oceniana jest na około 10-15% ogólnej wartości wszystkich uzyskiwanych przez wywiad informacji.

[11] Informacje uzyskane od agentury – około 18%, o wartości ocenianej na około 75-80%, ponieważ są to zazwyczaj informacje zawierające tajemnice państwowe lub służbowe, które mają bardzo istotne znaczenie.

[12] Dane ze środków technicznych to około 2% o wartości około 5-15%; zazwyczaj są one potwierdzeniem informacji z „białego wywiadu" lub stanowią podstawę do postawienia konkretnego zadania dla agentury (zdobycie informacji).

[13] Kluczową rolę w każdym systemie ochrony informacji odgrywają osoby, które mają do nich dostęp. Są one szczególnie narażone na próby nawiązania kontaktu ze strony obcych służb wywiadowczych. Warunkiem powodzenia werbunku danej osoby jest uprzednie uzyskanie na jej temat jak najpełniejszej wiedzy (otoczenie, praca, życie towarzyskie i rodzinne). Na podstawie: https://www.abw.gov.pl/pl/zadania/

a) ośrodki decyzyjne państwa (następuje tu pozyskanie ważnych informacji i plasowanie tzw. „agentury wpływu");
b) węzły informacyjne (przejęcie informacji i jej deformacja lub dezinformacja);
c) ośrodki (organy) opiniotwórcze;
d) obiekty i służby specjalne;
e) osoby, które mają dostęp do ważnych informacji lub ze względu na możliwości (np. przebieg kariery zawodowej, posiadane wpływy, ranga polityczna itp.), lub w przyszłości mogą być wpływowe (tzw. opracowanie agentury wpływu);
f) siły zbrojne[14].

Znaczna część obywateli Afganistanu dysponuje, dysponowała lub miała dostęp do wiadomości, informacji lub dokumentów stanowiących często tajemnicę państwową lub służbową. Posiadanie takich wiadomości lub dostęp do nich wynikał głównie z tytułu zatrudnienia i stanowisk zajmowanych w administracji państwowej, przedsiębiorstwach o znaczeniu strategicznym (np. przemysł zbrojeniowy, energetyczny, paliwowy, informatyczny), instytucjach kierujących gospodarką państwa, jego systemem bankowym oraz polityką zagraniczną i wypełnianiem zobowiązań wynikających z porozumień i umów zawartych z innymi krajami i organizacjami międzynarodowymi.

Podstawową metodą pracy obcych służb specjalnych jest działalność agenturalna. Do zdobywania informacji w coraz większym stopniu wykorzystywane są metody pozaagenturalne, w postaci:

– wywiadu satelitarnego,
– nasłuchu elektronicznego,
– wywiadu gospodarczego,
– białego wywiadu (głównie analiza oficjalnych publikacji),
– indagacje wywiadowcze – tj. różnego rodzaju rozmowy z przedstawicielami interesujących wywiad środowisk, prowadzone m.in. w trakcie oficjalnych spotkań, przyjęć lub w ramach kontaktów służbowych czy nawet prywatnych.

Skupmy się na działaniach pozaagenturalnych, zwłaszcza istotny jest w tym proces indagacji wywiadowczej oraz próby zdobywania ważnych informacji przy

kontrwywiad/ochrona-kontrwywiadowc/40,Ochrona-kontrwywiadowcza-kraju.html oraz https://www.abw.gov.pl/pl/zadania/kontrwywiad/zainteresowania-sluzb/38,Zainteresowania-sluzb-wywiadowczych.html [dostęp w dniu: 1.10.2014 r.].

[14] Służby wywiadowcze koncentrują często największą uwagę na armii innego państwa, wynika to z tego, że wojsko jako pierwsze wykorzystuje najnowsze zdobycze nauki i techniki, skupia w sobie poziom wiedzy społecznej, frustracje i nastroje ludności oraz jest najczulszym, a jednocześnie najważniejszym instrumentem w systemie obrony i bezpieczeństwa państwa. W wojsku zazwyczaj skupiają się ważne tajemnice, w tym przede wszystkim państwowe.

okazji rozmów dotyczących różnych spraw, są one z reguły podejmowane przez przebywających w danym obszarze: akredytowanych dyplomatów, członków oficjalnych delegacji, przedstawicieli firm handlowych, ośrodków naukowych, dziennikarzy itp. Należy zwrócić uwagę, że część tych osób może być niestety kadrowymi pracownikami wywiadu lub działać na zlecenie obcych służb specjalnych.

Najczęściej stosowane metody uzyskiwania informacji[15] wywiadowczych w trakcie różnego rodzaju rozmów to:

1) inspirowanie interesującego dla osoby podejmującej próbę indagacji tematu rozmowy, w tym w dalszym etapie wywoływanie dyskusji na określony temat lub wyrażanie przeciwstawnych opinii w celu wywołania określonej reakcji rozmówców;
2) dowartościowanie rozmówcy celem pozyskania jego przychylności i nakłonienia do wyrażania sądów;
3) próby przeniesienia kontaktów służbowych lub oficjalnych na płaszczyznę prywatną;
4) oferowanie pomocy w załatwieniu różnego rodzaju spraw lub rozwiązaniu problemów osobistych bądź wręczanie wartościowych prezentów, które mają skłonić rozmówcę do kontynuowania znajomości, również na zasadzie rewanżu;
5) inicjowanie wspólnych spotkań (np. imprez o charakterze rozrywkowym lub nawet turystycznym), podczas których, niejednokrotnie przy alkoholu, podejmowane są rozmowy na określony temat.

Biorąc pod uwagę powyższe, osoby wyjeżdżające i przebywające służbowo za granicą muszą zdawać sobie sprawę, że będą potencjalnym obiektem zainteresowania obcych służb specjalnych. Główne zagrożenia, z jakimi mogą się z ich strony spotkać, to m.in.:

- przegląd rzeczy osobistych, podsłuch i dokumentowanie prowadzonych rozmów;
- tajne przeszukania w zajmowanych pomieszczeniach (z dokonaniem „dokumentacji" znalezionych dokumentów służbowych i osobistych, jak notesy, wizytówki, korespondencja prywatna, notatki z obrad, spotkań itp.);
- mogą być także podejmowane próby wikłania osoby w różnego rodzaju sytuacje kompromitujące w celu późniejszego szantażu, np. przy próbie pozyskania do stałej lub doraźnej współpracy w przyszłości.

Wynika stąd, że podczas pobytu poza terenem własnego państwa należy przestrzegać kilku podstawowych zasad i reguł:

[15] Przy opracowaniu informacji w sposób kompleksowy służby wywiadowcze z reguły muszą i korzystają z wielu źródeł, zarówno tych agenturalnych, jak i pozaagenturalnych oraz w dużej mierze środków technicznych. Zgromadzone w ten sposób informacje wzajemnie się uzupełniają, dzięki temu możliwa jest pełna ocena określonej sytuacji, zdarzenia czy problemu.

- nie pozostawiać bez nadzoru żadnych dokumentów służbowych lub osobistych w pomieszczeniach hotelowych, socjalnych lub innych;
- nie prowadzić w pomieszczeniach zamkniętych i nieprzystosowanych poufnych rozmów na tematy służbowe lub zawierające treści niejawne;
- bardzo rygorystycznie przestrzegać przepisów prawa i zwyczajów obowiązujących w danym kraju;
- nie nawiązywać przypadkowych kontaktów i nie podtrzymywać znajomości z osobami, których zachowanie wskazuje na to, że mogą być one inspirowane przez służby specjalne;
- unikać spożywania alkoholu i bezwzględnie pod żadnym pozorem nie nadużywać alkoholu;
- nie uczestniczyć w przypadkowych rozmowach na tematy dotyczące spraw służbowych (nawet w swojej ocenie mało istotnych);
- bezwzględnie o wszystkich faktach i zdarzeniach mogących wskazywać na działalność służb specjalnych wobec swojej osoby lub innych natychmiast informować bezpośrednich przełożonych lub wskazane tzw. osoby kierunkowe i funkcyjne.

Zagrożenie ze strony organizacji terrorystycznych

Działań terrorystycznych nie należy w zasadzie wiązać z działalnością służb specjalnych. Biorąc pod uwagę szereg różnych współczesnych wydarzeń, można przypuszczać, że niektóre państwa zezwalają (lub mogą zezwolić w określonych sytuacjach) własnym służbom specjalnym na inspirowanie także działalności terrorystycznej. Szeroko rozumiana działalność terrorystyczna[16] jest najczęściej organizowana przez różnego rodzaju organizacje polityczne lub przestępcze. Poniższa definicja terroryzmu[17], a dalej aktu sabotażu i dywersji wyjaśnia ich zasadnicze cele.

Terroryzm[18] – „użycie siły[19] lub przemocy psychicznej przeciwko osobom lub własności z pogwałceniem prawa, mające na celu zastraszenie i wymuszenie na

[16] Zgodnie z tą definicją działania ugrupowań sił zbrojnej opozycji (Opposing Militant Forces – OMF) w Afganistanie, skierowane przeciwko legalnej władzy państwowej oraz społeczeństwu, należy określić jako terrorystyczne. R. Jędrychowski, P. Wojtasik, *Znaczenie informacji*…, „Kwartalnik Bellona", Nr 2/2012 (669), s. 135.

[17] Ciekawą analizę pojęciową zagadnienia przedstawił w swoim opracowaniu S. Wojciechowski, *Terroryzm – analiza pojęcia*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 1/09, ABW, Warszawa 2009, s. 54-60.

[18] http://pl.wikipedia.org/wiki/Terroryzm [dostęp w dniu: 1.10.2014 r.].

[19] Zwłaszcza w kontekście zorganizowanej działalności ugrupowań ekstremistycznych (np. uprowadzenia samolotów, mordowanie polityków, zamachy bombowe itp.) prowadzonej dla wywarcia presji na społeczeństwie i władzach, poruszenia opinii publicznej. Jego przejawem jest także uzyskiwanie informacji szczególnie chronionych, np. informacji o nowych rodzajach broni, dotyczy to zwłaszcza broni masowego rażenia (broń jądrowa i chemiczna). Działania terrorystyczne można klasyfikować,

danej grupie ludności lub państwie ustępstw w drodze do realizacji określonych celów. Działania terrorystyczne mogą dotyczyć całej populacji, jednak najczęściej są one uderzeniem w jej niewielką część, aby pozostałych obywateli zmusić do odpowiednich zachowań".

Sabotaż[20] – „umyślne niewypełnienie albo wypełnianie wadliwie swoich obowiązków[21] **w zamiarze wywołania dezorganizacji, strat i szkód. Sabotaż ma na celu uniemożliwienie lub utrudnienie prawidłowego funkcjonowania zakładów albo urządzeń lub instytucji o poważnym znaczeniu dla działania państwa**".

Dywersja[22] – „niszczące działanie wojenne na zapleczu, element z arsenału walki mający na celu odwrócenie uwagi przeciwnika. Działanie z ukrycia w celu osłabienia obronności lub gospodarki nieprzyjaciela w czasie wojny czy też wrogiego państwa w czasie pokoju. Dezorganizacja sił przeciwnika polegająca na niszczeniu lub uszkadzaniu zasobów zbrojnych wroga"[23].

Biorąc pod uwagę ww. materiał do oceny zagrożeń, możemy stwierdzić, że akty terrorystyczne mogą być skierowane zarówno na urządzenia i instytucje mające bardzo duże znaczenie dla gospodarki, obronności i bezpieczeństwa państwa, jak i na elementy codziennego życia całego społeczeństwa. Mając na uwadze ostatnie zamachy terrorystyczne, można stwierdzić, że przedmiotem zamachu może być praktycznie każdy obiekt użyteczności publicznej, a także dowolne inne duże skupiska ludzi (im większe i bardziej przypadkowe, tym lepiej dla osiągnięcia celu terrorystów). Co więcej, zagrożenia tego typu mogą być również ukierunkowane na instytucje i skierowane na te jednostki organizacyjne, które na swoim terenie (w swoich obiektach) wytwarzają, przetwarzają, przekazują i przechowują informacje niejawne stanowiące ich najważniejsze tajemnice. Będą to głównie jednostki wojskowe, jednostki administracji państwowej oraz przedsiębiorcy realizujący umowy z dostępem do informacji niejawnych.

Z tego względu ich kancelarie tajne nie będą prawdopodobnie jakoś specjalnie narażone na sabotaż i dywersję, zwłaszcza w warunkach względnego spokoju i stabilizacji sytuacji operacyjnej. Niemniej jednak brak odpowiednich środków zabezpieczenia obiektów takich jak kancelarie tajne naraża je na realne niebezpieczeństwo. Okoliczności, w których może dojść do sabotażu, są nieprzewidywalne, dlatego pełnomocnicy do spraw ochrony informacji niejawnych muszą

odwołując się do rozmaitych kryteriów, m.in.: działającego podmiotu, celu ataku, taktyki walki, politycznej strategii, założeń doktrynalnych i celów ideologicznych.

[20] http://pl.wikipedia.org/wiki/Sabotaż [dostęp w dniu: 1.10.2014 r.].

[21] „Ukryte działanie mające na celu przeszkodzenie komuś w realizacji jakiegoś planu" – Słownik Języka Polskiego PWN, http://sjp.pwn.pl/ [dostęp w dniu: 1.10.2014 r.].

[22] http://pl.wikipedia.org/wiki/Dywersja [dostęp w dniu: 1.10.2014 r.].

[23] Porównaj z: *Działania specjalne*, http://pl.wikipedia.org/wiki/Działania_specjalne [dostęp w dniu: 1.10.2014 r.].

planować ich bezpieczeństwo w ramach ogólnego planu ochrony danej jednostki organizacyjnej. Potencjalne zagrożenie akcjami sabotażowymi i terrorystycznymi, skierowanymi przeciwko obiektom jednostek organizacyjnych, w tym kancelariom tajnym i ich personelowi, może mieć miejsce ze strony organizacji terrorystycznych i ugrupowań ekstremistycznych, zwłaszcza gdy są one ulokowane na terytorium obcego państwa. Zarówno jedne, jak i drugie wrogie działanie może być sponsorowane przez jakiś kraj, który może wybrać określony obiekt/kancelarię i personel jako cel ataków z zamiarem osiągnięcia własnych korzyści (pozyskanie informacji o znaczeniu strategicznym) lub jego zniszczenia w celu osiągnięcia różnych korzyści, np. w czasie kryzysu. Można prognozować, że działania te mogą przybierać różnorodny charakter, w tym m.in.:

1) ataków bombowych, obejmujących również bomby umieszczane w samochodach, przenośne bomby walizkowe, urządzenia zapalające i bomby w przesyłkach;
2) morderstw, porwań, brania zakładników oraz wszelkich prób zastraszenia, wymuszenia i podporządkowania;
3) demonstracji organizowanych np. z zamiarem wywołania rozruchów lub spowodowania możliwości konfrontacji;
4) gwałtownych i bezpośrednich ataków na pomieszczenia lub ich okupowania w taki sposób, jaki ma najczęściej miejsce w przypadku ambasad lub misji dyplomatycznych;
5) testowania zachowań i procedur, np. poprzez fałszywe alarmy – szczególnie o podłożonych bombach.

Należy z całą pewnością stwierdzić, że wszelkie planowe działania służb specjalnych lub organizacji terrorystycznych muszą i są zawsze poprzedzone szerokim i dokładnym rozpoznaniem danego obiektu. Rozpoznanie to ma przede wszystkim ustalić, jakie metody i środki oraz formy pracy muszą być zastosowane, aby osiągnąć z gwarancją 100% sukcesu zamierzony cel (w myśl zasady cel uświęca środki). Wobec tego ta działalność rozpoznawcza musi przede wszystkim skoncentrować się na:

1) funkcjonujących systemach ochrony wytypowanej jednostki organizacyjnej, a zwłaszcza zidentyfikowanych wstępnie słabych punktach tych systemów;
2) zastosowanych środkach ochrony fizycznej, szczególnie w stosunku do informacji niejawnych, oraz istniejących możliwościach ich przezwyciężenia;
3) wykorzystywanych systemach bezpieczeństwa elektronicznego (szczególnie alarmowania oraz zawiadamiania) i jednocześnie możliwościach ich unieszkodliwienia oraz dezaktywacji;
4) możliwościach zdalnego (lub bezpośredniego) włamania do wykorzystywanych systemów lub sieci teleinformatycznych;
5) osobach (głównie personel pomocniczy), które mogą udzielić wywiadowi lub organizacji terrorystycznej pomocy w realizacji celu.

Przedstawiona powyżej działalność rozpoznawcza (pomimo najwyższego profesjonalizmu) zazwyczaj pozostawia jakieś ślady, bo musi je pozostawiać, niestety nie zawsze materialne, lecz możliwe do ustalenia i podjęcia skutecznego przeciwdziałania, zwłaszcza dla profesjonalistów ze służb. Tymi najprostszymi przykładami śladów mogą być np.: obecność obcych osób w rejonie danej jednostki organizacyjnej, dziwni interesanci i petenci, włamania lub podejmowanie prób włamania do niektórych pomieszczeń, w tym także wypytywanie pracowników o sprawy dotyczące jednostki organizacyjnej oraz fałszywe alarmy itp.

Podsumowując, można z pełną stanowczością stwierdzić, że istnieją dwie możliwe do zidentyfikowania drogi wypływu informacji stanowiących informację niejawną. Pierwsza droga to człowiek, który jest i pozostanie głównym sprawcą wypływu informacji niejawnych z jednostki organizacyjnej i zarazem najsłabszym ogniwem w każdym systemie bezpieczeństwa. Druga to maszyna (tak naprawdę dowolne urządzenie – często też materiał, z jakiego jest wykonane) – posługujemy się nimi swobodnie i naturalnie. Nie zawsze zdajemy sobie sprawę lub brakuje nam wyobraźni, jak łatwo wykorzystać podsłuchy telefoniczne, radiowe lub w teleinformatycznych sieciach łączności. Ogólnie przyjmuje się, że ok. 80-90% tajemnic jednostki organizacyjnej wypływa z winy zatrudnionego lub „wynajmowanego" personelu i to bez względu na ich status w organizacji. Należy podkreślić, że około 10-20% informacji wrażliwych wydostaje się z organizacji przez urządzenia techniczne często w sposób przypadkowy i niezamierzony – np. z powodu błędnej konfiguracji zwłaszcza systemów i sieci teleinformatycznych. Oczywiście możliwe jest zabezpieczenie używanych urządzeń, zwłaszcza przed wypływem informacji stanowiących informacje niejawne, poprzez wykorzystywanie ekranujących je kabin lub obudów oraz dzięki rozwiązaniom z wykorzystaniem kryptografii. Powyższe działania zwiększają bezpieczeństwo przetwarzanych, gromadzonych i przesyłanych informacji. Ale przegrywają w sytuacji, gdy w działalności rozpoznawczej, wywiadowczej bądź terrorystycznej uczestniczy osoba zatrudniona wewnątrz, w jednostce organizacyjnej. Jest to sytuacja na tyle skomplikowana, że trudno wykryć takie działania, gdzie nawet zaangażowanie dużych sił i środków w przypadku podejrzenia o nielojalność może nie przynieść szybkich i spodziewanych rezultatów. Zazwyczaj na tę sytuację nakładają się jeszcze niedostatki działań kontrolnych personelu kierowniczego jednostki organizacyjnej, ułatwiające uzyskiwanie informacji niejawnych. Do najważniejszych z nich można zaliczyć:

1) niewłaściwą politykę doboru i zatrudnienia pracowników w danym typie jednostki organizacyjnej. W efekcie zwykle może doprowadzić to do zatrudniania osób, które są podatne na pewne działania, np. niezgodne z obowiązującym prawem;
2) brak spójnych zasad i organizacji ochrony wszystkich informacji, w tym niejawnych w organizacji i na jej styku. To w efekcie powoduje, że pracownicy nie mają jasnych kryteriów, co im wolno, a czego nie;

3) brak elementarnej kontroli (a niekiedy również brak zainteresowania taką działalnością) ze strony kierownictwa jednostki organizacyjnej oraz zainteresowania stanem ochrony, sytuacją w zakresie bezpieczeństwa i ochrony fizycznej. To powoduje niewytworzenie się u zatrudnionych nawyku przestrzegania zasad ochrony informacji.

Do istotnych sposobów przeciwdziałania sytuacjom, w których do zdobywania informacji (zwłaszcza niejawnych) jest wykorzystywany czynnik ludzki w organizacji, należą odpowiednio poniżej przedstawione aspekty postepowania.

Po pierwsze odpowiedni dobór personelu do pracy (służby) w danej jednostce organizacyjnej gwarantuje sukces nie tylko w ochronie zasobów informacyjnych. Dobór ten, zwłaszcza osób z dostępem do informacji niejawnych, ma znaczenie pierwszoplanowe w ich bezpośredniej ochronie. To kierownik jednostki organizacyjnej powinien zadbać o to, żeby nie zatrudniać przede wszystkim osób, które:

1) nie mają obywatelstwa polskiego,
2) zostały skazane prawomocnym wyrokiem za przestępstwo umyślne, ścigane z oskarżenia publicznego, także popełnione za granicą,
3) odmówiły poddania się procedurze sprawdzeniowej,
4) odmówiły odpowiedzi na pytania stawiane przez odpowiednich pracowników wykonujących obowiązki w zakresie doboru, sprawdzania i kontroli,
5) przedłożyły fałszywe dane osobowe lub sfałszowane dokumenty urzędowe,
6) nie mają poświadczenia bezpieczeństwa,
7) nie zostały przeszkolone w zakresie ochrony informacji niejawnych;

Po drugie prowadzenie regularnych kontroli postępowania oraz przestrzegania ustalonych przepisów w zakresie ochrony informacji (z głównym naciskiem na informacje niejawne) obowiązujących w danego typu organizacji. Właściwe wypełnianie i realizowanie funkcji kontrolnej w organizacji oddziałuje w olbrzymim stopniu oraz pozytywnie na cały zatrudniony personel. Nie należy zapominać w tym obszarze, że każda kontrola powinna bezwzględnie kończyć się oceną pracownika, a w zależności od wyników karą lub nagrodą.

Po trzecie budowanie oraz prezentowanie właściwych postaw wobec ochrony informacji przede wszystkim (przykład idący z „góry" udziela się personelowi, ponadto trudno egzekwować zasady, których się samemu nie przestrzega) osób na stanowiskach kierowniczych oraz dowódczych, a także bezpośrednio odpowiedzialnych za realizację podstawowych zadań ochronnych.

Po czwarte cykliczne szkolenia na każdym poziomie organizacji z zasad ochrony informacji niejawnych, a zwłaszcza przed udzieleniem pierwszego dostępu do tego typu informacji, a następnie cykliczne szkolenia mające na celu przypominanie o tych zasadach.

W ramach podsumowania należy pamiętać, że szczególnym obowiązkiem[24] kierowników jednostek organizacyjnych w przedstawionym obszarze jest:

- dokonywanie cyklicznej oceny zagrożeń ze strony obcych służb specjalnych oraz organizacji o charakterze terrorystycznym. Podstawą analizy powinien być charakter zgromadzonych informacji niejawnych oraz funkcjonujący w tym zakresie system zabezpieczeń i ograniczeń dostępu do tych informacji w kontekście możliwych i realnych zagrożeń;
- stosowanie adekwatnych do istniejących zagrożeń środków bezpieczeństwa dla ochrony informacji niejawnych. Jeśli w wyniku przeprowadzonej analizy ryzyka stosowane podstawowe zabezpieczenia nie są wystarczające, to zastosowanie innych uzupełniających i eliminujących wykryte podatności;
- szczególne uwzględnienie bezpieczeństwa informacji niejawnych znajdujących się w wykorzystywanych w organizacji systemach i sieciach teleinformatycznych, zwłaszcza w zakresie emisji promieniowania elektromagnetycznego;
- uświadomienie podległemu personelowi, że podobne zasady bezpieczeństwa powinny funkcjonować nie tylko w dziedzinach objętych ochroną informacji niejawnych. Materiały jawne (niesklasyfikowane) także mogą mieć znaczenie dla całego obszaru bezpieczeństwa, również prywatnego kadry;
- utrzymanie stałego kontaktu ze służbą ABW i SKW[25], a także służbami porządkowymi, tj. policją i żandarmerią wojskową, w celu bieżącego dopływu informacji o istniejących zagrożeniach, a także ich stopniu nasilania się w otoczeniu na zewnątrz lub wewnątrz danej jednostki organizacyjnej.

LITERATURA

1. A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2006.
2. K. Danielewicz, *Rozpoznanie osobowe HUMINT i kontrwywiad w operacjach typu COIN*, „Kwartalnik Bellona", Nr 1/2013 (672), s. 178-194.
3. D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, WNT, Warszawa 2002.
4. J. Depo, *Teoretyczne i prawne aspekty przeciwdziałania i zwalczania destrukcyjnej działalności obcych służb specjalnych*, [w:] *Kultura bezpieczeństwa. Nauka – Praktyka*

[24] Zgodnie z art. 14 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228), zwanej dalej ustawą, na kierowniku jednostki organizacyjnej, w której przetwarzane są informacje niejawne, spoczywa obowiązek zorganizowania i zapewnienia funkcjonowania ochrony.

[25] W rejonie operowania ISAF (International Security Assistance Force) w Afganistanie służby specjalne NATO wykonują zadania polegające na pozyskiwaniu informacji o zagrożeniach TESSOC – Terrorism, Espionage, Subversion, Sabotage, Organised Crime (terroryzm, szpiegostwo, dywersja, sabotaż, przestępczość zorganizowana), op. cit., R. Jędrychowski, P. Wojtasik, *Znaczenie informacji*…, s. 136.

– *Refleksje*, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Nr 12 lipiec – grudzień 2013, s. 76-96.

5. S. Hoc, *Ustawa o ochronie informacji niejawnych. Komentarz*, LexisNexis, Warszawa 2010.
6. R. Jędrychowski, P. Wojtasik, *Znaczenie informacji wywiadowczych w zwalczaniu terroryzmu*, „Kwartalnik Bellona", Nr 2/2012 (669), s. 134-138.
7. K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011.
8. S. Malinowski, *Wybrane problemy badań zarządzania bezpieczeństwem informacji jednostki organizacyjnej o specjalnym przeznaczeniu (JWSP)*, „Studia Bezpieczeństwa Narodowego (National Security Studies)" Nr 4, Wojskowa Akademia Techniczna, Instytut Organizacji i Zarządzania WCY, Warszawa 2013.
9. S. Malinowski, *Zarządzanie bezpieczeństwem informacji jednostki wojskowej specjalnego przeznaczenia*, rozprawa doktorska, promotor prof. dr hab. inż. A.A. Barczak, AON, Warszawa 2012.
10. J. McNamara, *Arkana szpiegostwa komputerowego*, Helion, Gliwice 2004.
11. D.L. Pipkin, *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, WNT, Warszawa 2002.
12. F. Russel, *Wojna wywiadów*, Wydawnictwo Amber, Warszawa 1997.
13. A. Skwarski, *Wojskowe Służby Specjalne w operacjach międzynarodowych polskich Sił Zbrojnych*: rozprawa doktorska, promotor J. Gryz, AON, Warszawa 2012.
14. *Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych*, Dz.U. Nr 182, poz. 1228.
15. http://pl.wikipedia.org/wiki/.

THE THREATS FROM TERRORIST ORGANIZATIONS AND FOREIGN SPECIAL SERVICES IN AFGHANISTAN

Abstract: The article is a description of particular security aspects of dealing with the dangers undermining the protection of classified information. The threats usually arise from the actions of terrorist organizations and foreign secret services. The field of experience within this spectrum lies within a range of functions of the chief of organizational units. Author focuses on an overview of experiences found around the works of Polish Military Contingent in Afghanistan. The experiences give prove that the most dangers arise from the unforeseen actions of the terrorist organizations and foreign secret services.
Keywords: Afghanistan, Polish Military Contingent, terrorism, secret service, state security.