



Grey Scale #13



Part Code ST1316

DANES-PICTA.COM

A 1 2 3 4 5 6 M 8 9 10 11 12 13 14 15 B 17 18 19



**AKADEMIA
SZTABU GENERALNEGO**
IM. GENERAŁA BRONI
KAROLA ŚWIERCZEWSKIEGO

JAWNE

Egz. Nr 1



Kmdr mgr inż. Wiesław KACZMARCZYK
Pik mgr Andrzej STEFAŃSKI

**UWARUNKOWANIA BUDOWY
I FUNKCJONOWANIA SYSTEMU
KONTRWYWIADOWCZEJ OCHRONY
TAJEMNICY W SIŁACH ZBROJNYCH PRL**

Rozprawa doktorska



49170

WARSZAWA 1989





**AKADEMIA
SZTABU GENERALNEGO**

IM. GENERAŁA BRONI
KAROLA ŚWIERCZEWSKIEGO

JAWNE

~~_____~~
Egz. Nr. 1



Kmdr mgr inż. Wiesław KACZMARCZYK
Płk mgr Andrzej STEFAŃSKI

**UWARUNKOWANIA BUDOWY
I FUNKCJONOWANIA SYSTEMU
KONTRWYWIADOWCZEJ OCHRONY
TAJEMNICY W SIŁACH ZBROJNYCH PRL**

Rozprawa doktorska



~~_____~~ 49170

WARSZAWA 1989

AKADEMIA SZTABU GENERALNEGO WP
im. gen. broni Karola ŚWIERCZEWSKIEGO

INSTYTUT BADAŃ STRATEGICZNO-OBRONNYCH

DEKLASYFIKOWANO

Protokół Nr 54305



JAWNE

Egz. Nr 1

Przekł. Prot. 779/21.08.95

kmdr mgr inż. Wiesław KACZMARCZYK
płk mgr Andrzej STEFAŃSKI



UWARUNKOWANIA BUDOWY I FUNKCJONOWANIA SYSTEMU
KONTRWYWIADOWCZEJ OCHRONY TAJEMNICY
W SIŁACH ZBROJNYCH PRL



PRACA DOKTORSKA

Wykonana pod kierownictwem naukowym
płk prof.dr hab. Władysława FILARA

S P I S T R E Ś C I

	Strona
WSTĘP /oprac. A. STEFANSKI, W. KACZMARCZYK/.....	1
ROZDZIAŁ I /oprac. W. KACZMARCZYK/.....	7
<u>TEORETYCZNE ASPEKTY BUDOWY I FUNKCJONOWANIA</u> <u>MODELOWEGO SYSTEMU KONTRWYWIADOWCZEJ OCHRONY</u> <u>TAJEMNICY</u>	
1. Cybernetyczny model systemu kontrwywiadowczej ochrony tajemnicy.....	7
2. Analiza cybernetycznego modelu systemowego kontrwywiadowczej ochrony tajemnicy jako typowego systemu informacyjnego rozwijającego się /SIR/	20
ROZDZIAŁ II /oprac. W. KACZMARCZYK i A. STEFANSKI/....	50
<u>NIEKTÓRE ASPEKTY WSPÓŁCZESNEJ WALKI INFORMACYJNEJ</u> <u>W UKŁADZIE WYWIAD - KONTRWYWIAD</u>	
1. Istota współczesnej wojny informacyjnej.....	50
2. Analiza niektórych aspektów współczesnej walki o informacje.....	54
3. Energetyczne i informacyjne niszczenie systemu kontrwywiadowczej ochrony tajemnicy metodą walki informacyjnej	58
4. Cechy charakterystyczne współczesnej walki o informacje	69
5. Dezorganizacja struktur państwowych strate- gicznym celem walki o informacje	74
ROZDZIAŁ III /oprac. W. KACZMARCZYK i A. STEFANSKI/..	80
<u>WYWIADOWCZA DZIAŁALNOŚĆ GŁÓWNYCH PAŃSTW NATO</u> <u>W LATACH 1981-1985. KIERUNKI ZAINTERESOWAŃ.</u> <u>FORMY I METODY DZIAŁAŃ UKIERUNKOWANYCH NA</u> <u>OSŁABIANIE MOCY OBRONNEJ SIŁ ZBROJNYCH PRL</u>	

1. Totalny charakter działań wywiadowczych NATO	80
2. Współczesne uwarunkowania ogólnych założeń funkcjonowania wywiadów	83
3. Główne kierunki i formy działalności służb wywiadowczych państw NATO na ZTDW	86
4. Wywiad agenturalny. Pozyskiwanie bazy informacyjnej	96
5. Wywiad pozaagenturalny i jego możliwości w pozyskiwaniu informacji.....	100
6. Środki techniczne wykorzystywane przez wywiad państw NATO	106
7. Niektóre formy profilaktyki kontrwywiadowczej wykorzystywane w ochronie wojskowych struktur organizacyjnych NATO.....	109
8. System naboru personelu do pracy w głównych organach NATO.....	122
9. Ocena zagrożeń dla Sił Zbrojnych PRL wynikających z wywiadowczej działalności głównych państw NATO	126
 ROZDZIAŁ IV /oprac. A. STEFAŃSKI/	 131
<u>PRAKTYCZNE ASPEKTY BUDOWY I FUNKCJONOWANIA</u> <u>SYSTEMU KONTRWYWIADOWCZEJ OCHRONY TAJEMNICY</u>	
1. Ogólny model kontrwywiadowczego zabezpieczenia ważnych nośników informacji i jego podstawowe funkcje	131
2. Analiza i ocena sytuacji operacyjnej punktem wyjściowym do organizowania działań w zakresie ochrony tajemnicy	145
3. Kontrwywiadowcze zabezpieczenie newralgicznych nośników tajemnicy państwowej w Siłach Zbrojnych PRL	155

	Strona
4. Przeciwdziałanie penetracji obiektów wojskowych przez dyplomatów i cudzoziemców z KK oraz inne osoby	185
5. Rozpoznawanie utrzymywanych przez kadrę i pracowników wojska kontaktów z krajami kapitalistycznymi	200
6. Ocena skuteczności aktualnie realizowanych działań na rzecz kontrwywiadowczej ochrony tajemnicy	206
 WNIOSKI KONCOWE /oprac. W. KACZMARCZYK i A. STEFANSKI/	 219

BIBLIOGRAFIA

A. Wykaz aktów normatywnych dot. ochrony
tajemnicy w Siłach Zbrojnych PRL.

B. Literatura

W S T E P

Walka wyspecjalizowanych organów państwowych - wywiadu i kontrwywiadu - ukierunkowana na zdobywanie obcych i ochronę własnych tajemnic trwa od wieków.

Jak dowodzą fakty historyczne, dobre strzeżenie własnych tajemnic, przy jednoczesnym pozyskiwaniu tajnych informacji o przeciwniku, stanowiły nierzadko decydujący czynnik powodzenia bitew i kampanii wojennych, a także skutecznego osiągnięcia w warunkach pokojowych celów politycznych.

W latach osiemdziesiątych XX wieku mimo postępujących trendów odprężeniowych między państwami Układu Warszawskiego a państwami NATO, działalność wywiadowcza ukierunkowana między innymi na rozpoznanie Sił Zbrojnych PRL nie maleje, a wręcz przeciwnie, nabiera charakteru totalnego. Działalność ta wspierana jest wysokimi nakładami finansowymi, a także współczesnymi osiągnięciami nauki, techniki i technologii. Możliwości państw zachodnich w rozpoznawaniu terytorium Polski środkami technicznymi i siłami agenturalnymi są znaczne, a dla przeciętnego obywatela wprost niewyobrażalne.

W tej sytuacji walka kontrwywiadu WSW z wywiadowczą działalnością służb specjalnych państw NATO, ukierunkowana na zdobywanie informacji o szczególnym znaczeniu dla obronności kraju, nabiera istotnego znaczenia. Efektywność tej walki prowadzonej przez kontrwywiad uwarunkowana jest sprawnie funkcjonującym systemem kontrwywiadowczej ochrony tajemnicy.

Kontrwywiad Wojskowej Służby Wewnętrznej w ostatnich latach podjął szereg zabiegów koncepcyjnych i zmierzających

do wypracowania skutecznie funkcjonującego systemu kontrwywiadowczej ochrony ważnych nośników informacji, skupionych w newralgicznych komórkach sztabów i innych ogniwach struktury organizacyjnej sił zbrojnych. Na szczególną uwagę zasługuje koncepcja profilaktyki kreatywnej. Podstawowym założeniem w profilaktyce kreatywnej jest położenie akcentu nie tylko na wykrywanie i eliminowanie pojawiających się zagrożeń lecz przede wszystkim na tworzeniu warunków neutralizujących czynniki, negatywnie wpływające na pozytywny rozwój sytuacji.

W profilaktyce kreatywnej szczególnego znaczenia nabierają antycypacja i myślenie probabilistyczne. Znajduje to swój wyraz w ciągłym przewidywaniu i rozpoznawaniu zagrożeń, uświadamianiu ich stanom osobowym wojska i likwidowaniu ich na głębokim przedpolu. W tej systemowej działalności kreatywnej, partycypować muszą - w ramach swych uprawnień i kompetencji - wszystkie ogniwa struktury organizacyjnej wojska, a przede wszystkim dowództwo, aparat partyjno-polityczny, prokuratura, sądownictwo wojskowe, organizacje młodzieżowe oraz instytucje społeczne funkcjonujące w armii.

Profilaktyka kreatywna to działanie systemowe w ciągłym rozwoju, inaczej mówiąc, to stałe poszukiwanie sensownych przedsięwzięć zmierzających do ograniczania lub eliminowania zagrożeń niebezpiecznych dla gotowości obronnej wojska. W tak rozumianej istocie profilaktyki kreatywnej, kontrwywiad wojskowy widzi swoją rolę w udzielaniu pomocy dowódcom w podejmowaniu przez nich wyprzedzających działań, niedopuszczających do pojawienia się stanów i zjawisk godzących w siłę bojową wojska, w szczególności przez ujawnianie tajemnicy

państwowej.

Autorzy niniejszej pracy podjęli próbę wypracowania modelowego systemu kontrwywiadowczej ochrony tajemnicy wykorzystując zdobycze współczesnej nauki, a w szczególności teoretyczne podstawy ogólnej teorii systemów i cybernetyki, aktualną wiedzę o wywiadowczej działalności głównych państw NATO oraz doświadczenia praktyczne kontrwywiadu wojskowego w dziedzinie ochrony tajemnicy.

Główną myślą przewodnią jaką kierowali się autorzy rozprawy doktorskiej, było poszukiwanie odpowiedzi na następujące pytania: w jaki sposób, jakimi środkami i przy zastosowaniu jakich struktur organizacyjnych można zapewnić skuteczną kontrwywiadowczą ochronę tajemnicy w nowych warunkach wynikających z przyjętej doktryny obronnej funkcjonowania Sił Zbrojnych PRL oraz aktualnych i przewidywanych zagrożeń ze strony służb wywiadowczych głównych państw NATO.

Potrzeba podjęcia problematyki kontrwywiadowczej ochrony tajemnicy wynika z braku kompleksowych i analitycznych opracowań dotyczących roli kontrwywiadu wojskowego w zabezpieczaniu systemu obronnego państwa w aspekcie międzysystemowej walki o informacje jaka toczy się aktualnie we współczesnym świecie.

Jako podstawowy kierunek analizy podjętej problematyki uznano zbadanie - w oparciu o udostępnione przez Szefostwo WSW wyniki badań studyjnych - zagrożeń ze strony służb wywiadowczych państw NATO i stosownie do aktualnego i perspektywicznego stanu tych zagrożeń wypracowanie głównych kierunków kontrwywiadowczej ochrony tajemnicy w Siłach Zbrojnych PRL.

Zdaniem autorów kierunkowy cel niniejszej rozprawy został osiągnięty, a zawarte w niej treści wzbogacają aktualną wiedzę o systemowym ujęciu problematyki kontrwywiadowczej ochrony tajemnicy.

W rozdziale pierwszym przedstawiono teoretyczne podstawy budowy modelowego systemu kontrwywiadowczej ochrony tajemnicy, eksponując cybernetyczny model w postaci typowego systemu informacyjnego rozwijającego się /SIR/.

Rozdział II poświęcono niektórym aspektom współczesnej walki informacyjnej w układzie wywiad - kontrwywiad. Ujawnienie mechanizmów destrukcyjnych uruchamianych w walce informacyjnej, przez służby specjalne państw NATO oraz możliwości wkomponowania ich w system obronny naszego państwa pozwoliło, w innym niż dotąd świetle, spojrzeć na złożoność zagrożeń jakie stwarzać może dla Sił Zbrojnych PRL działalność wywiadowcza prowadzona w nowych warunkach i wyrafinowanymi metodami.

W rozdziale III przedstawiono agenturalne i techniczne możliwości służb wywiadowczych państw NATO oraz najbardziej typowe formy i metody działań ukierunkowanych na rozpoznawanie mocy obronnej Sił Zbrojnych PRL. Ujawnienie zakresu możliwości rozpoznawczych naszego potencjału obronnego przez służby wywiadowcze NATO, wskazuje na konieczność selektywnego podejścia do problematyki kontrwywiadowczej ochrony tajemnicy.

Rozdział IV poświęcono praktycznym aspektom budowy ogólnego modelu kontrwywiadowczego zabezpieczenia ważnych nośników informacji i jego podstawowym funkcjom. Z przedstawionego graficznie modelu wynika, że o sprawności systemu

kontrywiadowczej ochrony tajemnicy, jako układu zorganizowanego, decydują trzy podstawowe jego elementy, a mianowicie: osoby stanowiące funkcjonalny system układu, energia - rozumiana jako zdolność robocza podmiotowych elementów układu oraz struktura systemu.

W rozdziale tym zaprezentowane również zostały główne kierunki kontrywiadowczej ochrony tajemnicy oraz możliwości jakimi dysponuje kontrywiad wojskowy w walce ze służbami wywiadowczymi państw NATO w sferze ochrony tajemnicy.

Dużą pomocą, jednocześnie podstawą formułowania teoretycznych aspektów budowy i funkcjonowania systemu kontrywiadowczej ochrony tajemnicy była literatura z zakresu teorii systemów, cybernetyki społecznej, teorii informacji, prakseologii oraz teorii organizacji i kierowania.

Podjęta przez autorów próba adaptacji zawartych w literaturze myśli, tez oraz proponowanych rozwiązań do problematyki systemu ochrony tajemnicy, pozwoliła na stwierdzenie, że jest to system dynamiczny, otwarty i rozwijający się, co ma istotne znaczenie dla innowacyjnej działalności praktycznej.

Bogaty materiał źródłowy i studyjny dotyczący służb specjalnych państw NATO pozwolił na pogłębioną analizę zagrożeń i na tej podstawie zaproponowanie systemowego podejścia do kontrywiadowczej ochrony tajemnicy w Siłach Zbrojnych PRL.

Zebranie bogatego materiału faktologicznego stanowiącego podstawowe tworzywo konstruowania niniejszej pracy stało się możliwe, dzięki pomocy i życzliwości doświadczonych oficerów kontrywiadu z Szefostwa WSW. Szczególne słowa uznania

wyrażają autorzy Szefowi Wojskowej Służby Wewnętrznej, który był siłą sprawczą niniejszej pracy.

Promotorowi płk prof. dr hab. W. FILAROWI wyrażamy swoją wdzięczność i podziękowanie za okazywaną nam życzliwość oraz wszechstronną merytoryczną i metodologiczną pomoc w opracowaniu podjętego tematu rozprawy doktorskiej.

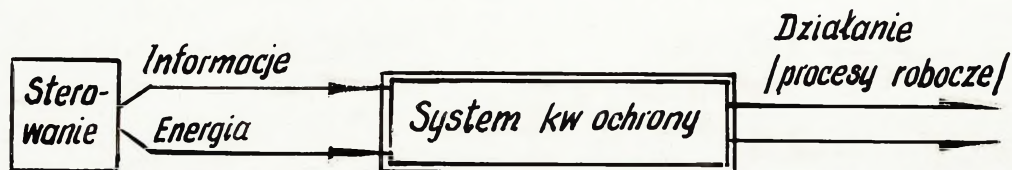
Autorzy dziękują również płk dr DUDZIŃSKIEMU, płk dr BRYLONKOWI, płk mgr WICHRZYŃSKIEMU, płk mgr TOREBCE, płk dr KŁOSOWICZOWI, ppłk dr MAZUROWI, ppłk mgr JANUCHCIE za krytyczne uwagi, dzielenie się fachowym doświadczeniem oraz udostępnienie dokumentów i materiałów źródłowych.

R O Z D Z I A Ł I

TEORETYCZNE ASPEKTY BUDOWY I FUNKCJONOWANIA MODELOWEGO SYSTEMU KONTRWYWIADOWCZEJ OCHRONY TAJEMNICY

1. Cybernetyczny model systemu kontrwywiadowczej ochrony tajemnicy

System kontrwywiadowczej ochrony tajemnicy w ujęciu ogólnej teorii systemów L. BERTALANFFY'EGO^{1/} oraz cybernetycznej teorii układów samodzielnych M. MAZURA^{2/} można przedstawić jako system cybernetyczny autonomiczny otwarty. W najbardziej ogólnej postaci modelowej cybernetyczny obraz takiego systemu daje się zilustrować jako układ składający się z dwóch podsystemów: sterowania i procesów roboczych co przedstawia niżej zamieszczony schemat.



Intensywność funkcjonowania tego systemu zależy od dwóch czynników: informacji i energii. Zwiększenie zaś tej intensywności można uzyskać przez wzrost zużycia energii pobieranej z otoczenia, albo przez usprawnianie procesów

1/ L. BERTALANFFY, Ogólna teoria systemów, Wyd. PWN, Warszawa 1984 r.

2/ M. MAZUR, Cybernetyczna teoria układów samodzielnych, Wyd. PWN, Warszawa 1966 r.

informacyjnych w podsystemie sterowania.

Istotę rozwoju systemu kontrwywiadowczej ochrony tajemnicy, w świetle ogólnej teorii systemów, można przedstawić jako zmiany w strukturze systemu, które umożliwiają utrzymanie dotychczasowej intensywności działania przy zmniejszeniu zużycia energii lub zwiększanie intensywności działania przy tym samym poziomie zużywanej energii. Wynika stąd wniosek, że podstawowym kryterium rozwoju systemu jest minimalizacja energochłonności metod jego funkcjonowania.

Skoro rozwój systemu uwarunkowany jest zmianami w jego strukturze, to powstaje pytanie: jak zmieniać strukturę systemu kontrwywiadowczej ochrony tajemnicy aby zwiększyć sprawność jego działania przez zmniejszenie energochłonności metod jego funkcjonowania. Odpowiedzi na to pytanie należy poszukiwać metodą analizy jaką zastosował BERTALANFFY^{1/} w rozpatrywaniu systemu otwartego.

W ujęciu BERTALANFFY`EGO system to kompleks wzajemnie oddziałujących elementów przedstawiony w formie triady:

$$S = \langle E, R, Q \rangle \quad \text{gdzie:}$$

E - zbiór elementów systemu S,

R - zbiór relacji obejmującej:

R_w - relacje zachodzące między elementami E systemu S,

R_z - relacje zachodzące między elementami E i systemem jako całością a elementami E_o stanowiącymi otoczenie systemu S,

Q - zbiór miar charakteryzujących własności lub zachowanie się systemu lub jego elementów, przy czym $Q \subset R$.

1/ Por. L. BERTALANFFY, op.cit., s.85

Dla zilustrowania matematycznej postaci definicji systemu i pokazania jego podstawowych właściwości, L. BERTALANFFY wykorzystał układ jednoczesnych równań różniczkowych^{1/}, a mianowicie:

$$\frac{dQ_1}{dt} = f_1 / Q_1, Q_2, \dots, Q_n /$$

$$\frac{dQ_2}{dt} = f_2 / Q_1, Q_2, \dots, Q_n /$$

$$\frac{dQ_n}{dt} = f_n / Q_1, Q_2, \dots, Q_n /$$

gdzie: n - ilość elementów E systemu S

f i < R, przy czym i = 1, 2, ..., n

Przedstawiona matematyczna postać definicji systemu wskazuje, że zmiana właściwości jakiegokolwiek elementu systemu powoduje zmiany właściwości wszystkich elementów systemu a także jego otoczenia. Z powyższego można wyprowadzić wniosek, że wprowadzając zmiany w systemie kontrwywiadowczej ochrony tajemnicy należy analizować wszystkie wzajemne oddziaływania elementów systemu, aby usprawniając jeden z elementów nie pogorszyć działalności innego. Stosując powyższe wskazania w praktycznej działalności możemy uniknąć szeregu błędów wynikających z nieuwzględniania, pozornie niewidocznych ale istotnych zależności. Szczególnie w procesie sterowania rozwojem systemu kontrwywiadowczej ochrony tajemnicy należy badać różnorodne zależności na przykład pomiędzy stopniem intensywności wyjazdów osób ze środowiska wojskowego do krajów kapitalistycznych i strukturą tych wyjazdów a możliwością

1/ L. BERTALANFFY, op cit., s. 87

werbunku do pracy wywiadowczej, podatność kadry zawodowej na zjawiska patologii społecznej a sposobem spędzania czasu wolnego od służby itp.

Analiza tych zależności daje możliwość uniknięcia błędów decyzyjnych będących wynikiem niewiedzy o istotnych zależnościach między elementami systemu.

Przedstawiony przez BERTALANFFY`EGO uniwersalny model systemu stanowi równocześnie teoretyczną podstawę dla symulacji komputerowej zachowania się projektowanych szczegółowych systemów i tą drogą budowanie systemu o optymalnych właściwościach funkcjonalnych.

Z analizy warunków stabilności systemu opisanego przedstawionym układem równań - gdy czas "t" dąży do nieskończoności / $t \rightarrow \infty$ / - BERTALANFFY wyprowadza wnioski dotyczące możliwych trzech sposobów zachowania się systemu S w miarę upływu czasu.^{1/} Są nimi:

1. stan równowagi dynamicznej - gdy system trwa w ruchu - działaniu przy okresowych zmianach, w określonych granicach wielkości parametrów jego elementów składowych;
2. stan destabilizacji dynamicznej - przy którym system traci swe właściwości systemowe, a więc upada, na skutek przekroczenia przez poszczególne parametry dopuszczalnych dla systemu wartości granicznych;
3. stan statyczny - równoznaczny z upadkiem systemu na skutek zaniku ruchu jego elementów.

W tych trzech powyżej przytoczonych stanach może znajdować się rozpatrywany system kontrwywiadowczej ochrony

1/ Por. L. von. BERTALANFFY, op.cit., s.88 i dalsze

tajemnicy, lecz aby był on efektywny w walce z agenturą wywiadów NATO, musi dążyć on do stanu równowagi dynamicznej i być zdolny do wykonywania długotrwałej pracy, we wszystkich przypisanych mu funkcjach.

W systemie kontrwywiadowczej ochrony tajemnicy /tak jak w każdym systemie otwartym /dokonuje się równoległe dwa przeciwstawne sobie, komplementarne procesy^{1/}:

1. Proces entropowy - towarzyszący każdemu działaniu systemu, w którym następuje niszczenie elementów składowych systemu, usuwanych przez system do otoczenia. Proces entropowy powoduje wzrost entropii systemu, co jest równoznaczne ze zmniejszeniem sprawności działania systemu i prowadzi do jego upadku. W procesie tym system otwarty przechodzi ze stanu struktury mniej do bardziej prawdopodobnej, lecz mniej sprawnej, oddalając się od stanu równowagi dynamicznej.
2. Proces negentropowy - odbudowy niszczonej w procesie entropowym struktury, zapewniającej systemowi wyższą sprawność działania, a wraz z tym większą jego trwałość. Proces negentropowy jest procesem zbliżającym system do stanu równowagi dynamicznej i powoduje zmniejszenie entropii systemu.

System kontrwywiadowczej ochrony, tak jak każdy system otwarty, powinien posiadać ponadto m.in. następujące właściwości:

1. Zdolność do zmniejszania poziomu entropii systemu, warunkujących jego rozwój.
2. Aktywność "pierwotną", stanowiącą wewnętrzne źródło aktywności systemu. Aktywność ta przejawia się w samoistnym

1/ Por. J. KOSECKI, Cybernetyka społeczna, Warszawa 1981 r.

dążeniu systemu do równowagi dynamicznej. Oddziaływanie otoczenia tworzy warunki dla działania systemu, aktywność tę stymuluje lub tłumi, nie będąc jednak jej główną podstawową przyczyną.

3. Zdolność automatycznej regulacji procesu dążenia do utrzymania przez system stanu równowagi dynamicznej przy różnorodnych i zmieniających się warunkach otoczenia, obejmująca zarówno opór przed negatywnym chwilowym oddziaływaniem otoczenia na system jak i adaptacyjność struktury systemu do trwałych zmian zachodzących w otoczeniu.
4. Hierarchiczną strukturę aktywnych ogniw systemu. System otwarty, zazwyczaj sam będąc podsystemem większej całości /np. system kontrwywiadowczej ochrony tajemnicy jest podsystemem systemu obronnego wojska/ - nadsystemu lub nadsystemów - zbudowany jest z podsystemów, które składają się również z aktywnych ogniw stanowiących elementy systemu otwartego.

Z powyższych rozważań wynika, że warunkiem rozwoju systemu kontrwywiadowczej ochrony jest przewyższanie natężeniem procesu negentropowego, zachodzącego w systemie - procesu entropowego. Aby z kolei system kontrwywiadowczej ochrony zniszczyć, należy intensyfikować w nim natężenie procesów entropowych, a ograniczyć procesy twórcze - negentropowe.

W trakcie rozwoju każdy system otwarty, w tym system kontrwywiadowczej ochrony, tworzy struktury hierarchiczne. Towarzyszy temu występowanie dwu przeciwstawnych komplementarnych procesów: centralizacji, która warunkuje koordynację niezbędną dla bardziej sprawnego działania systemu oraz zróżnicowanie i zwiększenie stopnia samodzielności podrzędnych ogniw systemu.

W przedstawionym modelu niezmiernie istotną rolę

odgrywa właściwość samodzielnego działania systemu otwartego, którą BERTALANFFY nazwał aktywnością "pierwotną". System otwarty samoistnie dąży do zmniejszenia entropii jako warunku trwania, czyli nie jest tylko układem reagującym na zewnętrzne wymuszenia. Uznanie w praktyce kontrwywiadowczej tej właściwości systemu oznacza potrzebę tworzenia takich warunków zewnętrznych, by w ich ramach każdy podmiot ochrony mógł wykorzystać swój potencjał umysłowy w prokontrwywiadowczej działalności obronnej oraz by widoczne efekty pozytywne tej pracy mogły stanowić bodziec dalszej aktywizacji działań.

Dla lepszego wyjaśnienia mechanizmu informacyjnej destrukcji, przydatne wydaje się być podjęcie próby określenia - na podstawie analizy powyższych modeli - sprawnej struktury systemu kontrwywiadowczej ochrony tajemnicy w WP, niezbędnej dla trwania systemu w zmieniających się warunkach otoczenia. Wracając w tym celu do przedstawionego już wzoru BERTALANFFY'EGO trzeba podkreślić, że przedstawiony tam układ równań opisuje nadsystem - składający się z "n" elementów interesującego nas systemu otwartego o właściwościach Q. Elementy o właściwościach $Q_2, Q_3 \dots Q_n$ będą stanowiły otoczenie tego systemu.

Rozpatrując powyższy układ "system - otoczenie", mamy do czynienia z dwoma przypadkami:

- 1 - gdy układ jest w stanie równowagi dynamicznej, a jego otoczenie nie ulega zmianom;
- 2 - gdy otoczenie systemu podlega zmianom.

W przypadku pierwszym, aby zapewnić trwanie systemu, warunkiem koniecznym i wystarczającym jest tu jedynie dokony-

wanie odbudowy niszczonej przez proces entropowy struktury systemu, bez wprowadzania do niej jakichkolwiek zmian.

W tym celu wystarcza dobra pamięć koordynującego działania systemu, niezbędna jedynie do odtwarzania struktury systemu zużywającej się w jego działaniu. W takich warunkach podsystem sterowania działaniem systemu może być wysoce prymitywny. Niepotrzebna jest również głębsza wiedza o samym systemie oraz wiedza o stanie otoczenia systemu. Preferowana jest dla trwania systemu postawa konserwatywna.

W przypadku drugim, gdy w otoczeniu systemu zachodzą istotne zmiany, to w tych warunkach również zasadniczej zmianie ulegają wymagania dotyczące jakości podsystemu sterowania działaniem systemu. Warunkiem trwania systemu jest ciągle, właściwe dostosowywanie struktury systemu do zmian zachodzących w jego otoczeniu. Lecz aby system mógł się zbliżyć do stanu równowagi dynamicznej, wytracony z tego stanu oddziaływaniem zmieniającego się otoczenia, niezbędne jest:

1. poznanie wszystkich istotnych zależności pomiędzy wzajemnie oddziaływującymi elementami układu: system - otoczenie, tzn. funkcji f_1, f_2, \dots, f_n oraz własności elementów powyższego układu Q_1, Q_2, \dots, Q_n ;
2. określenie na podstawie wiedzy /z punktu "1"/ przewidywanego stanu równowagi dynamicznej układu: system - otoczenie;
3. wprowadzanie odpowiednich zmian we wzajemnych konfiguracjach elementów powyższego układu, tzn. zarówno w systemie, jak i jego otoczeniu, mających za cel doprowadzenie układu: system - otoczenie do stanu równowagi dynamicznej;
4. weryfikowanie skutków zmian w oparciu o dokonywane analizy.

Ponadto, jeśli ilość oddziaływujących na system

elementów otoczenia wzrosła, np. stale rosnąca ilość wyjazdów do KK, czyli, gdy $n \rightarrow \infty$, to niezbędnym jest również odpowiedni wzrost sprawności informacyjnej naszego systemu Q_1 jako warunek niezbędny do odwzorowania prawidłowości zachodzących w otoczeniu systemu.

O ile w przypadku pierwszym dla sterowania działaniem systemu wystarczał bardzo prymitywny podsystem sterowania, to w przypadku drugim niezbędne jest wysoce sprawne, oparte na nauce, sterowanie działaniem i rozwojem systemu.

Jeżeli w pierwszym przypadku wystarczało ograniczenie zainteresowań jedynie do własnych działań, to w przypadku drugim warunkiem trwania systemu jest nie tylko doskonalenie własnego systemu, lecz postawa wymagająca aktywnego stosunku do otoczenia i równoczesnego właściwego przekształcania go dla utrzymywania całego układu: system - otoczenie, w stanie równowagi dynamicznej.

Wynika stąd, że warunkiem trwania systemu kontrwywiadowczej ochrony przy zmieniających się warunkach komplikującego się otoczenia jest sukcesywne dokonywanie zmian w relacjach "R" zachodzących pomiędzy elementami układu: system - otoczenie /wzór: $S = \langle E, R, Q \rangle$ / na takie, które umożliwią systemowi bardziej sprawne działanie, a wraz z tym zbliżają system do stanu równowagi dynamicznej. Konieczne jest również sukcesywne zwiększanie ilości elementów systemu, odpowiednio do wzrostu ilości czynników otoczenia oddziałujących na system, m.in. wzrost ilości przeszkolonych środków pracy dla zwiększenia jego pojemności informacyjnej. Proces tworzenia takich nowych relacji "R" w wyniku odpowiedniego tworzenia

nowych konfiguracji elementów układu: system - otoczenie, jest procesem tworzenia informacji.

Informacjami "I" są te spośród relacji "R", które warunkują działanie lub bardziej sprawne działanie systemu, tzn., że $I < R$.

Z powyższych rozważań wynika, że aby system kontrwywiadowczej ochrony tajemnicy mógł trwać w zmieniających się warunkach otoczenia, powinien to być system informacyjny rozwijający się sukcesywnie, odpowiednio do zmian zachodzących w jego otoczeniu.

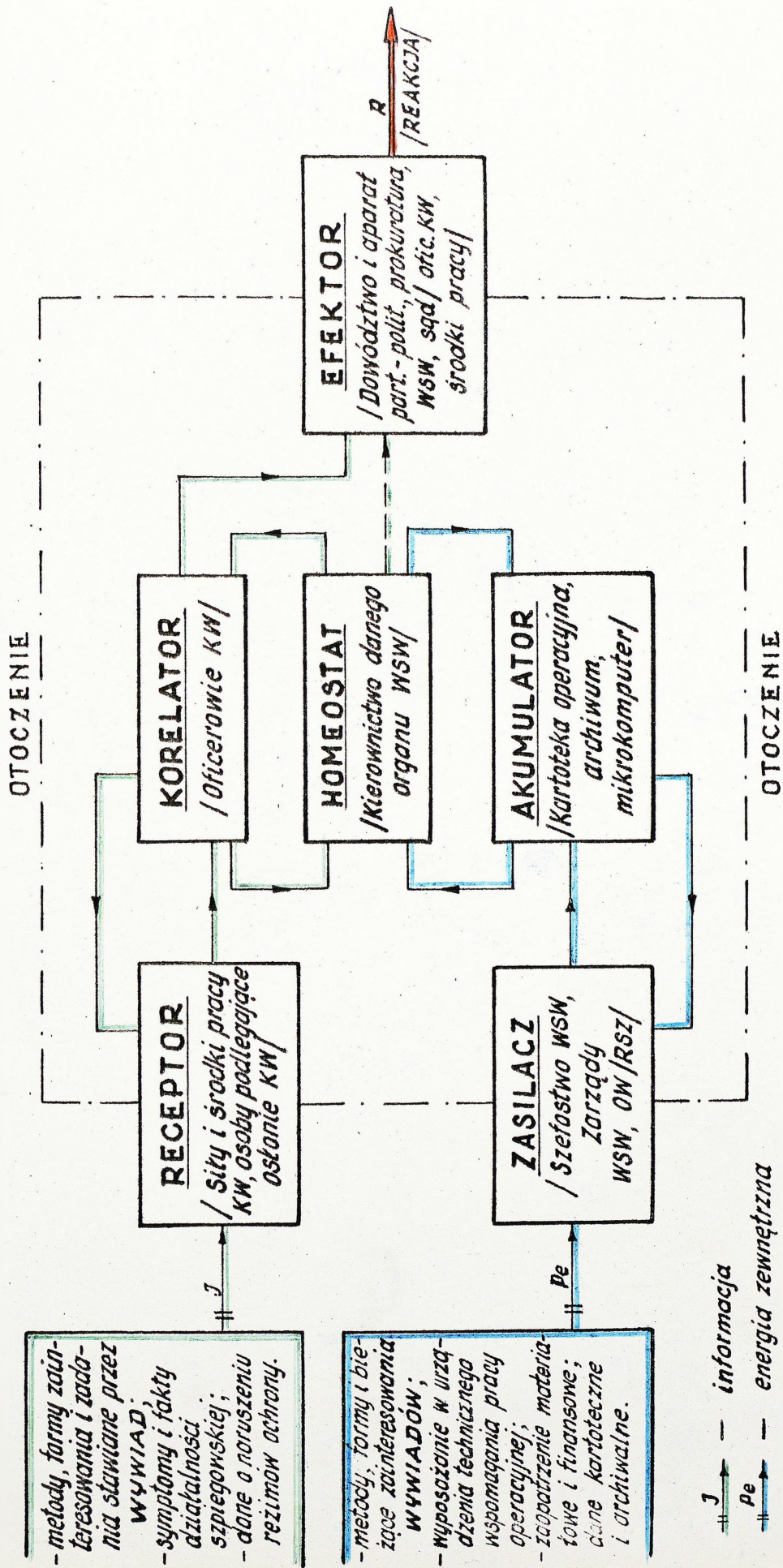
Takim konceptualnym systemem, który spełniałby przedstawione wyżej cybernetyczne uwarunkowania ogólnej teorii budowy systemów może być modelowy system kontrwywiadowczej ochrony tajemnicy w postaci układu samodzielnego.

Graficzną ilustracją układu jest zamieszczony na stronie 17 schemat.

Jak wynika z przedstawionego schematu, modelowy system kontrwywiadowczej ochrony tajemnicy dla spełnienia przewidywanych dla niego funkcji musi on być wyposażony w następujące organy:

- 1/ receptor /REC/ - organ służący do pobierania informacji, czyli wykrywania bodźców /symptomów lub faktów działalności szpiegowskiej oraz naruszania reżimów ochrony tajemnicy/. Są to siły i środki pracy KW oraz osoby podlegające osłonie kontrwywiadowczej.

KONCEPTUALNY MODEL SYSTEMU KW OCHRONY TAJEMNICY W POSTACI UKŁADU SAMODZIELNEGO



- metody, formy zainteresowania i zadania stawiane przez WYWIAD;
- symptomy i fakty działalności szpiegowskiej;
- dane o poruszeniu reżimów ochrony.

- metody, formy i bieżące zainteresowania WYWIADÓW;
- wyposażenie w urządzenia technicznego wspomaganie pracy operacyjnej;
- zapoznaczenie materiałowe i finansowe; dane kartoteczne i archiwalne.

2/ efektor /EF/

- organ, który służy do oddziaływania na otoczenie, czyli wytwarzania reakcji. Są to dowództwa i aparat partyjno-polityczny, organa prokuratury i sądu. Również rolę tą spełniać mogą oficerowie KW i ich środki pracy.

3/ zasilacz /Z/

- organ służący do pobierania energomaterii z otoczenia. Ażeby system KW ochrony mógł funkcjonować musi uzyskiwać z zewnątrz energię, w tym przypadku musi otrzymywać wiedzę /informacje/, przede wszystkim o metodach i formach działania przeciwnika, środki techniki i obserwacji operacyjnej oraz środki finansowe na prowadzenie pracy operacyjnej. Dla oficera KW rolę zasilacza spełnia szef organu WSW, a dla danego organu Zarząd WSW OW/RSZ/.

4/ akumulator /AK/

- organ, którego zadaniem jest przetwarzanie i przechowywanie energomaterii w celu wykorzystania jej w odpowiednim czasie, w zależności od potrzeb. Rolę tego organu, w systemie KW ochrony, spełnia komputer personalny, kartoteka mechaniczna lub klasyczna biblioteka. "Z" i "AK" to dział zabezpieczenia funkcjonowania instytucji w odpowiedni stopień wiedzy /informacji/ o działalności systemów własnych i przeciwnika.

- 5/ korelator /KOR/ - organ służący do przetwarzania i przechowywania informacji w celu wykorzystania ich w dowolnym czasie odpowiednio do potrzeb. Rolę tę spełniają oficerowie KW.
- 6/ homeostat /HOM/ - organ umożliwiający modyfikowanie struktury układu. Wywiera on wpływ na korelator i akumulator. Rolę tę spełnia kierownictwo danego organu WSW

Energia zewnętrzna P_e dopływa do układu torem energetycznym /zaznaczonym linią niebieską/, natomiast informacja /I/ - torem informacyjnym /linia zielona/.

Tor energetyczny nazywamy zasileniowym, tor informacyjny - torem sterowania.

Tak zbudowany układ spełnia warunki cybernetycznego systemu autonomicznego i stanowi teoretyczną podstawę praktycznych działań na rzecz usprawniania systemu kontrwywiadowczej ochrony tajemnicy.

Przeprowadzona analiza teorii systemów, pozwala na sprecyzowanie kilku myśli natury ogólnej stanowiących teoretyczną syntezę cybernetycznego modelowania systemu kontrwywiadowczej ochrony tajemnicy.

1. Sprawność i intensywność funkcjonowania cybernetycznego systemu kontrwywiadowczej ochrony tajemnicy uwarunkowana jest skutecznością funkcjonowania podsystemów sterowania i procesów roboczych.
2. Z cybernetycznej definicji systemu wynika, że jest on kompleksem wzajemnie oddziałujących na siebie elementów. Oznacza to, że w działaniach zmierzających do usprawniania

systemu należy uwzględniać wszystkie wzajemne oddziaływania jego elementów, tak aby usprawniając jeden z nich nie osłabić innego.

3. Istotną cechą systemu decydującą o jego zdolności do długotrwałej pracy jest stan równowagi dynamicznej. Naruszenie równowagi dynamicznej systemu prowadzi do jego destabilizacji co powoduje utratę sprawności oraz właściwości funkcjonowania.
4. Dla zachowania równowagi dynamicznej systemu należy wspomagać procesy negentropowe powodujące organiczenie negatywnych zjawisk, entropii systemu, oraz dostarczać zasobu energii do działań w warunkach nieprzewidywanych zagrożeń.
5. Trwałość systemu kontrwywiadowczej ochrony tajemnicy w zmieniających się warunkach otoczenia można zapewnić nadając temu systemowi postać systemu informacyjnego rozwijającego się SIR.

2. Analiza cybernetycznego modelu systemowego
kontrwywiadowczej ochrony tajemnicy jako
typowego systemu informacyjnego rozwijającego
się /SIR/

Strukturę systemu KW ochrony tajemnicy mierzyć możemy informacją nagromadzoną w tym systemie, przetwarzaną przezeń oraz informacją, którą system może przetworzyć.^{1/}

1/ Por. J. KOSSECKI, op. cit., s.32

Samo pojęcie informacji nie doczekało się dotąd powszechnie akceptowanej definicji. Jednakże do celów praktycznych za wygodną można przyjąć następującą definicję: "Informacje to zbiór faktów, zdarzeń, cech obiektów itp. zawarty w określonej wiadomości, tak ujęty i podany w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne"^{1/}

Stąd za informacje kontrwywiadowcze należy uznawać te wiadomości, które w sposób bezpośredni lub pośredni dotyczą podmiotów lub przedmiotów kontrwywiadowczej ochrony i zmuszają dany organ WSW /oficera KW/ do rzeczowego ustosunkowania się do zaistniałej sytuacji a także do podjęcia adekwatnych działań umysłowych lub fizycznych.

System kontrwywiadowczej ochrony tajemnicy jest typowym systemem informacyjnym, którego celem jest zbieranie, przetwarzanie, przechowywanie i udostępnianie informacji zgodnie z potrzebami i wymaganiami użytkowników. Jest to taki system działania, który tworzą M^I - zbiór elementów informacyjnych /źródeł informacji Z/ i R^I - zbiór powiązań /korelacji/ pomiędzy elementami informacyjnymi / $R^I \subset M^I$ /, czyli:

$$SI = \langle M^I, R^I \rangle \text{ 2/}$$

Musi on w związku z tym spełniać rygory wynikające z aktualnego poziomu rozwoju teorii informacji.

Z teorii informacji można wnioskować, że dany komunikat /np. meldunek ZI/ zawiera tym więcej informacji, im

1/ Por. P. SIENKIEWICZ, Inżynieria systemów, MON, W-wa 1983, s.61

2/ Tamże, s. 89 i 90

mniejsze jest prawdopodobieństwo jego wystąpienia. Oznacza to, że ilość informacji jest tym większa, im większa była niepewność, że określoną wiadomość możemy znaleźć w komunikacji. Zatem otrzymać informację - znaczy dowiedzieć się czegoś więcej o tym, o czym wiedziało się mniej.

Z założeń tych wynika, że informacja związana jest z nieokreślonością danej sytuacji, a z kolei nieokreśloność zdarzenia jest, w ujęciu probablistycznym, cechą jego rozkładu prawdopodobieństwa. Pamiętać również należy, aby nieokreśloność zdarzenia, a więc i ilość informacji zawartej w kilku statystycznie niezależnych wiadomościach, była równa sumie miar nieokreśloności w nich zawartych, czyli by miała cechę addytywności.^{1/}

Miarą ilości informacji, jaką niesie sygnał, jest różnica pomiędzy niepewnością początkową a niepewnością po otrzymaniu sygnału, czyli niepewnością warunkową ze względu na sygnał

$$I/X, Y/ = H/X/ - H/X/Y/$$

co oznacza: ilość informacji, jaką przeciętnie przynosi sygnał ze zbioru możliwych sygnałów Y o zdarzeniu ze zbioru możliwych zdarzeń X, równa jest różnicy pomiędzy niepewnością bezwarunkową co do zajścia jednego ze zdarzeń ze zbioru X a niepewnością warunkową co do otrzymania sygnałów ze zbioru Y.

Ze ścisłego ujęcia ilości informacji wynikają dodatkowe wnioski:

1/ Por. P. SIENKIEWICZ, op.cit., s. 63

- a/ niepewność jest pewną cechą sytuacji /zbioru możliwych zdarzeń/, a informacja pewną cechą sygnału polegającą na tym, że redukuje niepewność - ale nie jest sygnałem;
- b/ pojęcia niepewności i informacji nie pozostają w żadnym stosunku do sensu /znaczenia/ sygnałów /wiadomości/;
- c/ miara ilości informacji nie uwzględnia jej wartości /jakości/;
- d/ niepewność i informacja nie uwzględniają wariacji możliwych zdarzeń, ani "nieoczekiwalności" zdarzenia.^{1/}

Kolejnym istotnym elementem w systemach informacyjnych, w tym w systemie kontrwywiadowczej ochrony tajemnicy, stanowi zagadnienie przenoszenia sygnałów od nadawcy do odbiorcy /np. środki pracy - oficer KW, oficer KW - szef organu WSW/. Chodzi o to, ażeby informacja, która dotarła do odbiorcy - użytkownika, była informacją przez niego pożądaną, tj. taką, która powstała po oddzieleniu od informacji nadanej szumów, w tym przede wszystkim szumu semantycznego i pragmatycznego. Wynika stąd, że uzyskana informacja musi być przez odbiorcę jednoznacznie zrozumiała /aspekt semantyczny związany jest z pytaniem o ścisłość przekazywania znaczenia treści przez sygnały/ oraz musi być informacją potrzebną ze względu na spełniane przez system funkcje /aspekt pragmatyczny wiąże się z pytaniem o skuteczność wpływania otrzymanych treści na zachowanie się odbiorcy w określony sposób/.

W zbiorze komunikatów wprowadza się trzy podstawowe relacje:^{2/}

1/ Tamże, s.66

2/ Por. J. JARON, Podstawy cybernetyki, Wrocław 1976r.,

- równoważność syntaktyczną;
- równoważność semantyczną;
- równoważność pragmatyczną,

które pozwalają określić kiedy dwa dowolne komunikaty są równoważne w sensie podstawowych aspektów informacji w nich zawartych. Określenie powyższych relacji jest niezbędne do wartościowania uzyskiwanych informacji i wyprowadzania ocen funkcjonujących systemów informacyjnych /np. pracy poszczególnych organów WSW/.

Pomiędzy określonym źródłem informacji a odbiorcą informacji zachodzi sytuacja informacyjna, w związku z wystąpieniem określonego zadania informacyjnego, formułowanego w określonym języku opartym na danym modelu.^{1/}

Sytuację informacyjną można określić następująco:

$$S_{ij}^I = [M^I, I_M^I; z, /n_i, o_j/, u_{ij}]$$

gdzie:

- z - dane zadanie informacyjne, $z \in Z$ - zbiór zadań informacyjnych;
- n_i - nazwa /numer/ i - tego nadawcy źródła informacji, $n_i \in N^I$ - zbiór nadawców - źródeł;
- o_j - nazwa /numer/ j - tego odbiorcy /adresata/ informacji, $o_j \in O^I$ - zbiór odbiorców - adresatów;
- u_{ij} - kanał /tor/ informacyjny łączący i - tego nadawcę z j - tym adresatem;
- M^I - przyjęty model informacyjny /zbiór zmiennych informacyjnych/;
- I_M^I - język formułowania zadań informacyjnych opartych na modelu M^I .

1/ Por. P. SIENKIEWICZ, op.cit., s. 71

Dowolną sytuację informacyjną charakteryzują dwie podstawowe charakterystyki ilościowe: N_I - stopień nieokreśloności i H_I - entropia oraz charakterystyka identyfikacyjna $y_I = /y_1^I, y_2^I, y_3^I/$ taka, że:

- $y_1^I =$ 1 - informacja pełna
0 - informacja niepełna
- $y_2^I =$ 1 - informacja aktualna
0 - informacja nieaktualna
- $y_3^I =$ 1 - informacja wiarygodna
0 - informacja niewiarygodna

W związku z powyższym dowolnej sytuacji informacyjnej można przypisać jeden ze stanów:

<u>Stan</u>	<u>Wartość parametrów</u>
S_1	111
S_2	110
S_3	101
S_4	011
S_5	001
S_6	010
S_7	100
S_8	000

Najbardziej pożądanym jest, oczywiście, stan S_1 ; zaś najmniej pożądanym stan S_8 .

Pomiędzy nadawcą a odbiorcą występuje oddziaływanie informacyjne, oparte na przekazywanych komunikatach, związane z występowaniem określonej sytuacji informacyjnej.^{1/}

Powyższe oddziaływanie informacyjne /informowanie/ będące procesem /trwa w czasie/ i ciągiem realizowanych w czasie

1/ Por. P. SIENKIEWICZ, op.cit., s.72

sytuacji informacyjnych musi zaspokajać potrzeby informacyjne określonych uczestników sytuacji informacyjnej.

W systemach informacyjnych istotne znaczenie posiada podział rodzajów informowania - procesów informacyjnych, z punktu widzenia zniekształceń tych procesów. Z tej przyczyny wyróżnia się:

- 1/ transinformowanie, czyli informowanie wierne, które jest zapewnione, gdy meldunek nadany staje się meldunkiem odebrany, gdy opis sytuacji jest identyczny z jej przebiegiem itd.;
- 2/ pseudoinformowanie, czyli informowanie pozorne, mające miejsce wtedy, gdy przekazywane dane, choć zupełne, są nieoddzielne, tj. mają pewne komunikaty wspólne, przy czym może to być:
 - informowanie rozwlekłe,
 - informowanie ogólnikowe,
 - informowanie niejasne;
- 3/ dezinformowanie, czyli informowanie fałszywe, powstające wówczas, gdy przekazywane dane są niezupełne, choć oddzielne, przy czym może to być:
 - zmyślanie,
 - zatajenie,
 - przekręcanie;
- 4/ parainformowanie, czyli informowanie oparte na parainformacjach, tj. informacjach powstających ze skojarzeń lub domniemywań. Parainformowanie obejmuje:
 - a/ domniemywania trafne, np. zrozumienie aluzji,
 - b/ domniemywania nietrafne, do których zalicza się:
 - domniemywania bezpodstawne /np. dopatrzenie się aluzji, której nie było/;
 - c/ domniemywania niedomyślne, np. niedopatrzenie się aluzji, która była;

- domniemywanie opaczne, np. dopatrywanie się aluzji innej niż była;

5/ metainformowanie, czyli informowanie o informowaniu. Mamy tutaj także do czynienia z metainformacją, czyli informacją o informacjach.^{1/}

Z punktu widzenia funkcjonowania systemu kontrwywiadowczej ochrony tajemnicy dopuszczalne jest jedynie informowanie wierne, co nie wyklucza występowania w określonych sytuacjach operacyjnych dezinformowania /w stanach wyższej konieczności/.

W systemach informacyjnych istotnym jest również dokonywanie oceny informacji w aspekcie pragmatycznym, a więc udzielenie odpowiedzi na pytanie: w jaki sposób oceniać wartość informacji? Uznaje się, że informacja przedstawia wartość wówczas, jeżeli po jej otrzymaniu zwiększone zostaje prawdopodobieństwo osiągnięcia danego celu.^{2/} Przypuśćmy, że przed otrzymaniem informacji prawdopodobieństwo osiągnięcia interesującego nas celu było równe P_0 , zaś po jej otrzymaniu przyjęło ono wartość równą P_1 .

Wówczas wartość informacji dana jest wzorem:

$$U/I/ = \log_2 P_1 - \log_2 P_0 = \log_2 \frac{P_1}{P_0}$$

Jeżeli $U/I/$ przyjmuje wielkości dodatnie oznacza to, że otrzymana informacja zwiększyła prawdopodobieństwo osiągnięcia założonego przez nas celu, a więc jest ona wartościowa.

Ogólnie można powiedzieć, że informacja, która niewiedzę użytkownika częściowo lub całkowicie redukuje bądź zaspokaja

1/ Por. M. MAZUR, Cybernetyka i charakter, PIW, Warszawa 1975r., s. 121 i dalsze

2/ Por. P. SIENKIEWICZ, op.cit., s. 75 i 76

jego uświadomione lub nieuświadomione potrzeby informacyjne, jest - z punktu widzenia użytkownika - pożądana. Można przyjąć, że ważność informacji dla użytkownika zależy od:

- problemu, czyli określonej sytuacji informacyjnej. Im ważniejsze jest zadanie informacyjne, tym informacja uzyskana w wyniku jego zrealizowania jest ważniejsza;
- efektywności systemu informacyjnego realizującego dany proces informacyjny. Jeśli system zapewnia otrzymanie informacji pełnej, dokładnej i aktualnej, to informacja ta przedstawiać będzie dla użytkownika większą wartość, niżli byłaby to informacja niepełna, niedokładna i nieaktualna.

Z powyższych rozważań wynika, że za jakość informacji Q należy przyjąć cechę informacji wyrażającą stopień spełnienia wymagań stawianych przez użytkownika dotyczących:

- 1/ aktualności α , czyli cechy wyrażającej fakt otrzymania przez użytkownika informacji w pożądanym /wymaganym/ czasie;
- 2/ pełności β , czyli cechy wyrażającej zawartość rzeczywistych informacji o obiekcie w danej wiadomości;
- 3/ niezawodności γ , czyli cechy wyrażającej stopień wpływu zniekształceń i zakłóceń na informacje dostarczane użytkownikowi w danej wiadomości.

Jakość informacji jako kompleksową cechę wiadomości przedstawić można w postaci:

$$Q = Q[\alpha, \beta, \gamma]^{1/}$$

Z analizy funkcjonujących systemów kontrwywiadowczej ochrony tajemnicy /SI/ wynika, że aktualność zależy między innymi od następujących charakterystyk systemu:

1/ Por. P. SIENKIEWICZ, op.cit., s. 102 i 103

- metod zdobywania /zbierania/ informacji przez siły i środki pracy operacyjnej;
- struktury środków pracy operacyjnej i ich możliwości w zdobywaniu określonych informacji;
- niezawodności środków pracy operacyjnej i dyspozycyjności oficera KW;
- sposobów łączności pomiędzy środkami pracy operacyjnej a oficerem KW;
- intensywności przepływu informacji /obciążenie systemu/.

Pełność /kompletność/ informacji zależy przede wszystkim od metod obserwacji wartości cech obiektu i dokładności tej obserwacji.

Niezawodność /wiarygodność/ informacji uzależniona jest od stopnia zniekształceń, które mogą być obiektywne lub subiektywne. Zależy więc przede wszystkim od przeszkolenia i stopnia powiązania środków pracy operacyjnej z organami WSW.

Wartość informacji stanowi systemową cechę wyrażającą jakość i użyteczność informacji, czyli:

$$V/I/ = V [Q/I, U/I] = V [Q(\alpha, \beta, \gamma), U(\log_2 \frac{P_1}{P_0})]$$

Ocenę wartości /jakości, użyteczności/ informacji należy wiązać z oceną efektywności systemów informacyjnych.^{1/} Dotychczasowe doświadczenia wskazują, że efektywność systemu kontrwywiadowczej ochrony tajemnicy należy oceniać według trzech wskaźników, a mianowicie:

1/ wartości informacji V_1 /t/ udostępnionych użytkownikom w danym procesie działania, w określonym okresie i warunkach;

1/ Por. P. SIENKIEWICZ, op.cit., s. 104

- 2/ niezawodności systemu R /t/ oraz jego sił i środków pracy KW;
- 3/ wielkości efektu organizacyjnego ΔI , będącego rezultatem wdrożenia tego systemu w danej organizacji, która jest przedmiotem KW ochrony.

Jeżeli weźmiemy pod uwagę sformułowaną przez C.E. SHANONA miarę ilości informacji,^{1/} to należy wyciągnąć wniosek, że miarą wzrostu stopnia organizacji systemu KW ochrony tajemnicy jest przyrost ilości informacji, gdyż:

$$I = H_0 - H_1 = \Delta$$

gdzie:

H_0 - entropia systemu w stanie Y_0 , przed jego zorganizowaniem;

H_1 - entropia systemu w stanie Y_1 , po jego zorganizowaniu.

W przypadku całkowitej niezależności elementów w skrajnie niezorganizowanym systemie entropia ogólna, tj. systemu jako całości, będzie maksymalna i równa sumie entropii poszczególnych elementów:

$$H_0 /X_1, X_2/ = H/X_1/ + H/X_2/$$

gdzie:

$H_0 /X_1, X_2/$ oznacza entropię systemu jako całości;

$H/X_1/$ entropię elementu X_1 ;

$H/X_2/$ entropię elementu X_2 .

Jeżeli w systemie wprowadzimy sprzężenie między elementami, w wyniku czego te elementy będą na siebie oddziaływać i stany jednego /dowolnego/ z nich będą zależeć od stanów

1/ Por. J. KOSSECKI, op. cit., s. 18

drugiego - tzn. jeśli zwiększymy stopień organizacji systemu /czyli będziemy organizować system/ - to ogólna entropia systemu stanie się mniejsza od sumy entropii poszczególnych elementów:

$$H_1 /X_1, X_2/ < H/X_1/ + H/X_2/$$

To zmniejszenie entropii systemu jako całości, stanowi ilościową miarę stopnia zorganizowania systemu, czyli jest ono ilościową miarą wzrostu stopnia organizacji systemu, który nastąpił w wyniku wprowadzenia sprzężeń między jego elementami, stąd:

$$\Delta = H_0 - H_1 = H/X_1/ + H/X_2/ - H_1/X_1, X_2/$$

Jeżeli w stanie y_0 układ X_1, X_2 posiadał entropię H_0 , a potem w stanie y_1 entropię H_1 , przy czym $H_1 < H_0$, przyjęc należy, że po przejściu ze stanu y_1 , do stanu y_2 , stopień organizacji systemu X_1, X_2 wzrósł o:

$$\Delta = H_0 - H_1 > 0$$

Ponieważ wzrost stopnia organizacji systemu jest równoznaczny z ubytkiem entropii, dla określenia jego używana jest nazwa "negentropia". Negentropia będąca miarą wzrostu stopnia organizacji układu oznacza więc przyrost ilości informacji.

W związku z powyższymi rozważaniami można wnioskować, że zmiany stopnia organizacji systemu kontrwywiadowczej ochrony tajemnicy są równoznaczne ze zmianami ilości informacji. Organizacja systemu więc wzrasta lub maleje w takim stopniu, w jakim wzrasta lub maleje informacja.

Należy również dodać, że wzrost organizacji systemu /kontrwywiadowczej ochrony tajemnicy/ stanowi skutek wzmocnienia powiązań między jego elementami, a przede wszystkim po-

między oficerem KW, jego środkami pracy a poznawczymi podmiotami lub przedmiotami. Można interpretować to jako wprowadzenie informacji do systemu.

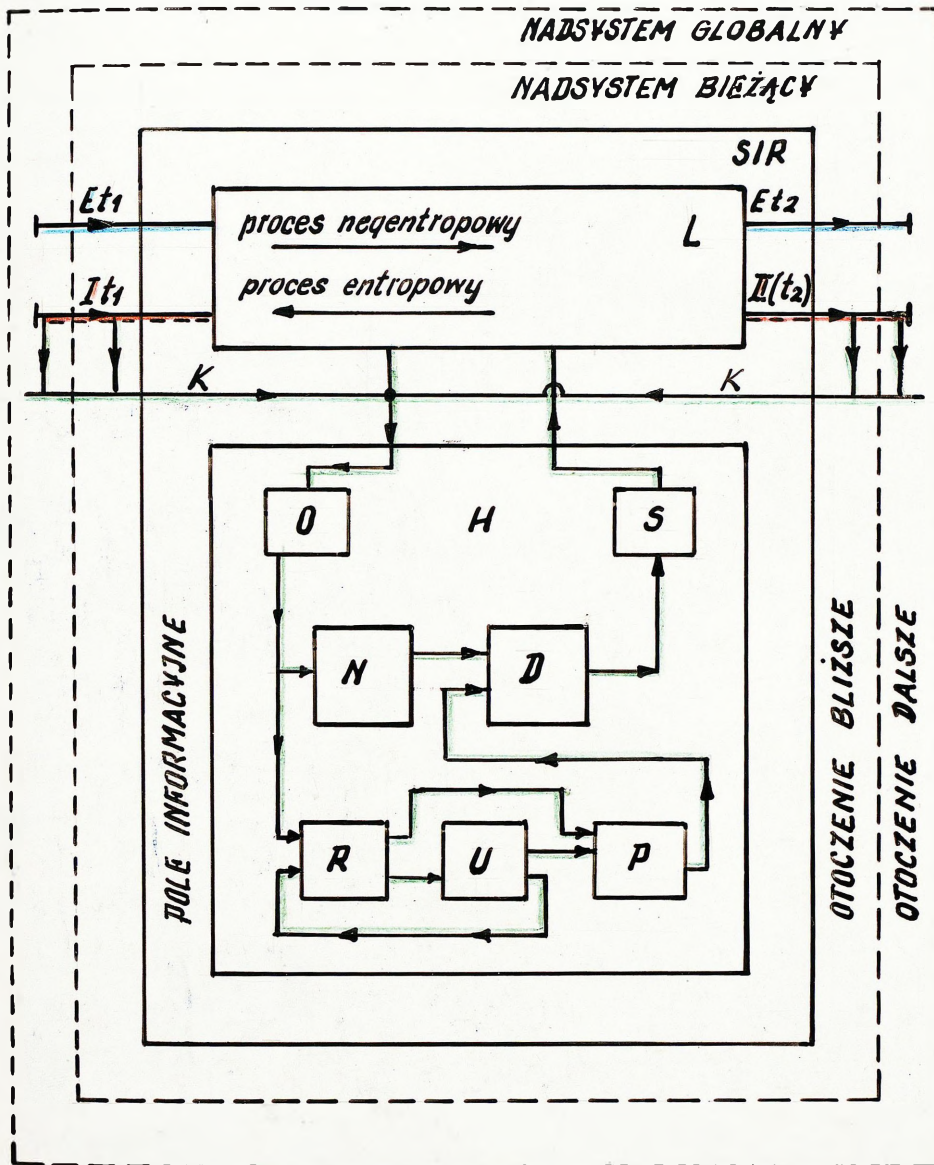
Jeżeli więc chcemy sterować systemem w taki sposób, aby uzyskiwać permanentny wzrost informacji, musimy odpowiednio wpływać na zmiany sprzężeń między jego elementami, czyli zmieniać stopień jego organizacji. Ponieważ sterowanie jest wywieraniem pożądanego wpływu na określone zjawiska, a wobec zasady zachowania masy i energii nie można wywierać wpływu na te czynniki inaczej niż przez zmianę ich rozmieszczenia w przestrzeni i czasie, można stwierdzić, że sterowanie jest to wywoływanie pożądaných zmian struktury. Zatem informacja stanowi miarę struktury, a zmiany struktury opisujemy poprzez zmiany ilości informacji.

Ponieważ system jest to obiekt określony co do struktury, zatem informacje dotyczące jednego systemu dotyczą zarazem wszystkich systemów o takiej samej strukturze bez względu na to, z jakich materiałów są ukonstytuowane i jaki rodzaj energii przetwarzają. Np. na podstawie badania zachowania się grupy nowo wcielonych żołnierzy do jednego z pułków o strukturze takiej samej jak ogół wcielonych do WP żołnierzy w danym poborze, do którego ta grupa należy, możemy zdobywać informacje dotyczące zachowania całego poboru.

Przedstawione rozważania dotyczące istoty procesu tworzenia informacji oraz uwarunkowania maksymalizowania z pomocą informacji organizacji systemu, umożliwiają bardziej precyzyjne - i uzupełniające poprzednie - określenie systemu kontrwywiadowczej ochrony tajemnicy jako systemu informacyj-

nego rozwijającego się - SIR.

Można go przedstawić w następującej postaci:



Oznaczenia :

- E - energia
- I - informacja realna
- K - kanały informacji odwzorowującej
- L - podsystemy pracy /układ realizacji pracy/
- H - homeostat /układ sterowania przebiegiem pracy/
- t - czas w sensie długim

Podstawowe podukłady homeostatu SIR:

- 1/ "O" - obserwowanie;
- 2/ "R" - rejestrowanie;
- 3/ "U" - intelektualne uogólnienie;
- 4/ "P" - wartościowanie i projektowanie;
- 5/ "D" - decydowanie i koordynacja;
- 6/ "N" - ocena intuicyjna;
- 7/ "S" - dziedzinowe sterowanie realizacją zamierzeń;
- 8/ "K" - kanały informacyjne.

Zadaniem podukładu obserwowania jest:

- obserwowanie poszczególnych punktów czasoprzestrzeni układu "SYSTEM - OTOCZENIE" /podmiotów i przedmiotów ochrony/ i zachodzących tu zdarzeń, w tym procesów zmian stanu układu w odniesieniu do punktów obserwowanych;
- obserwowanie skutków zmian zachodzących lub realizowanych w układzie, w tym w poziomie informacji.

Zadaniem podukładu rejestrowania jest:

- gromadzenie wyników obserwacji /dot. informacji użytecznych/;
- prowadzenie rejestru danych dotyczących podlegającego zmianom stanu statystycznego oraz dotychczasowej charakterystyki dynamicznej układu: "SYSTEM - OTOCZENIE" /miary $Q_1 - Q_n$ w tym $f_1 - f_n$ /.

Podukład intelektualnego uogólnienia ma za zadanie:

- formułowanie na podstawie wyników obserwacji, odpowiadających im praw statystycznych /czyli funkcji $f_1 - f_n$ dotyczących procesów i prawidłowości występujących w obserwowanym ruchu elementów układu: "SYSTEM - OTOCZENIE"/ wyznaczających podlegającą zmianom wraz z upływem czasu charakterystykę dynamiczną wymienionego układu.

W podukładzie wartościowania i projektowania zmian wypracowywane są wariantowe prognozy odnośnie przyszłego stanu układu "SYSTEM - OTOCZENIE". Na podstawie tych prognoz wypracowywane są tu - również wariantowe - projekty zmian właściwych w układzie "SYSTEM - OTOCZENIE", jak również oceny i korekty dotyczące zmian już realizowanych.

Zadaniem podukładu decydowania i koordynacji jest:

- dokonywanie wyboru w procesie decyzyjnym, kierowanego do realizacji wariantu projektu zmian właściwych lub rodzaju korekty, odnośnie zmian już zrealizowanych;
- koordynacja przebiegu zmian właściwych, realizowanych przez wyspecjalizowane dziedzinowo podsystemy SIR.

Podukład oceny intuicyjnej spełnia dwie funkcje:

- f_1 - wspomaganie procesu decyzyjnego, co ułatwia dobór wariantu zmian z uwzględnieniem aktualnego stanu układu "SYSTEM - OTOCZENIE";
- f_2 - ocena skutków dokonanych już zmian i sprowadza się głównie do sygnalizacji potrzeby:
 - a/ korekt odnośnie realizowanych zmian lub
 - b/ zmian w istniejącej strukturze układu "SYSTEM - OTOCZENIE".

Podukład dziedzinowego sterowania realizacją zmian właściwych ujmuje układ sterowania dziedzinowo wyspecjalizowanych podsystemów SIR, wspólnie realizujących określone fragmenty projektów zmian właściwych /dla jasności rysunku pominięto na nim sieć kanałów informacyjnych niezbędnych dla realizacji tych zadań sterowniczych/.

Podukład kanałów informacyjnych ma za zadanie zapew-

nić SIR niezbędny dla jego rozwoju transfer informacji odwzorowujących, w tym sterowniczych.

System Informacyjny Rozwijający się /SIR/ można, w zapisie teoriomnogościowym, przedstawić jako:

$$\text{SIR} = \langle S_t, H, P, R_z, i, \zeta_t, Q, t \rangle \text{ gdzie:}$$

S_t - konkretna struktura systemu;

H - homeostat systemu;

P - pole informacyjne systemu;

R_z - oddziaływanie na system jego otoczenia;

i - poziom informacji systemu;

ζ_t - sprawność twórcza systemu;

Q - okres życia systemu;

t - czas w sensie długim, dotyczący układu "SYSTEM - OTOCZENIE" /zmienna niezależna/.

Wszystkie powyższe składniki SIR są tak wzajemnie sprzężone, że zmiana jednego z nich powoduje zmianę wszystkich pozostałych składników / za wyjątkiem "t"/. SIR jest systemem samoorganizującym się oraz systemem dynamicznym o charakterze układu oscylacyjnego i zachowaniu celowym. Jest on równocześnie systemem otwartym w ujęciu L. von BERTALANFFY`EGO.

SIR zbudowany jest z:

- układu realizacji pracy - "L";
- układu sterowania przebiegiem pracy, tzw. homeostatu "H";
- pola informacyjnego.

Celami SIR są:

- 1/ tworzenie informacji w układzie "SIR - OTOCZENIE";
- 2/ maksymalizowanie okresu rozwoju systemu i jego "aktywnych" ogniw;

- 3/ minimalizowanie energochłonności metod działania systemu;
- 4/ maksymalizowanie sprawności informacyjnej systemu.

Istota działania systemu KW ochrony tajemnicy jako SIR polega na ukierunkowanym na realizację powyższych celów - doskonaleniu pracy systemu oraz postaci energii stanowiącej jego nadsystem, czyli układ "SYSTEM - OTOCZENIE". Na wejściu do SIR znajduje się zatem energia nadsystemu $E /t_1/$, której strukturę i jakość /poziom uorganizowania/ w chwili t_1 czasu w sensie długim t , wyznacza informacja $I/t_1/$. Informację tę stanowi odpowiednia konfiguracja elementów układu: "SYSTEM-OTOCZENIE", wyznaczająca konkretną jego strukturę oraz postać energii stanowiącej wymieniony układ, jak również jej jakość. Na wyjściu SIR znajduje się przekształcona oddziaływaniem i pracą SIR energia układu: "SYSTEM - OTOCZENIE" - $E/t_2/$, której nową strukturę i jakość w kolejnej chwili czasu t_2 , wyznacza informacja $I/t_2/$.

Skutkiem właściwej pracy SIR jest postępujący wraz z jego rozwojem wzrost poziomu informacji, a wraz z tym i okresu aktywnego trwania SIR i jego nadsystemu. Wzrostowi poziomu informacji SIR towarzyszy zmniejszenie energochłonności jego metod działania jako skutek doskonalącego przekształcania, czyli awansowania energii układu "SYSTEM-OTOCZENIE". Awansowanie energii, czyli doskonalące przekształcanie konkretnej struktury układu "SYSTEM-OTOCZENIE" dokonywane jest pracą systemu z wykorzystaniem sił pola informacyjnego, ukierunkowanych na nową strukturę SIR o mniejszym poziomie energii i wyższym niż dotychczas poziomie informacji systemu. Siły pola informacyjnego wywołują w układzie "SYSTEM-OTOCZENIE" dwa

stanowiące pozornie jedność, a przeciwstawne, procesy powodowania zmian właściwych w strukturze układu: entropowy i negentropowy.

Skutkiem procesu entropowego jest "rozsadzanie" ze względu na potrzeby rozwojowe SIR już nieaktualnych więzów - relacji wyznaczających dotychczasową, zdezaktualizowaną strukturę układu "SYSTEM - OTOCZENIE".

Skutkiem procesu negentropowego jest kształtowanie, z "uwolnionych" tak elementów układu, nowej postaci konkretnej jego struktury, o wyższym poziomie informacji, pod warunkiem przewyższania jego natężeniom, natężenia procesu entropowego.

Stymulowana oddziaływaniem pola informacyjnego praca tak "aktywnego pierwotnie" SIR, ukierunkowana jest na rozwój systemu i warunkujący ten rozwój jego otoczenie.

Efektywność rozwojowej działalności SIR wyznacza wskaźnik jego sprawności twórczej \mathcal{Z}_T

$$\mathcal{Z}_T = \frac{\Delta i_n}{\Delta e_{on}} \quad \text{gdzie:}$$

Δi_n - przyrost poziomu informacji w układzie "SYSTEM-OTOCZENIE", czyli w nadsystemie SIR jako skutek jego rozwojowej działalności;

Δe_{on} - energia odtwarzania nadsystemu, czyli ilości energii niezbędnej dla wyeliminowania skutków dla układu "SYSTEM - OTOCZENIE" wewnętrznego i zewnętrznego procesu entropowego, warunkującego wymieniony Δi_n .

W przedstawionym równaniu Δi_n wyznacza efekt na jednostkę czasu, odnoszony przez nadsystem SIR z jego rozwojo-

wej działalności. Efekt ten dotyczy zarówno systemu jak i podsystemów oraz jego otoczenia. Natomiast Δe_{on} wyznacza energetyczny koszt pozyskania wymienionego rozwojowego efektu i również odnosi się zarówno do systemu, jego podsystemów i otoczenia SIR. Określa on wielkość degradacji energii układu "SYSTEM - OTOCZENIE", jaka towarzyszy nieuchronnie rozwojowej działalności SIR.

Przebiegiem procesu pracy SIR, w tym procesie entropowego i negentropowego, steruje - wykorzystaniem pola informacyjnego - homeostatem SIR. Składa się on z dwóch podukładów: homeostazy intelektualnej i homeostazy naturanej. Homeostat wiąże w całość wszystkie elementy SIR i czątkowe ich działania, dla realizacji celów systemu.

Podstawę dla działania homeostatu dają:

- informacja odwzorowująca "a posteriori" i "a priori" układ "SYSTEM - OTOCZENIE", w zakresie działania układu homeostazy intelektualnej oraz
- oddziaływanie pola informacyjnego, zwłaszcza w zakresie układu homeostazy naturanej.

Wskaźnik sprawności twórczej ζ_T odniesiony do chwili czasu w sensie długim, wyznacza stan aktualny tej sprawności SIR. Jednakże stan SIR określa również wskaźnik jego sprawności wzrostu

$$\zeta_w = \frac{i_s}{e_{os}} \quad \text{gdzie:}$$

- Δi_s - przyrost poziomu informacji SIR, jako wskutek działalności systemu;
- Δe_{os} - energia odtworzenia systemu, czyli ilość energii niezbędnej dla wyeliminowania skutków dla SIR jego wewnętrznego procesu entropowego, warunkującego wymieniony Δi_s .

Powyższe wskaźniki SIR - \dot{z}_T i \dot{z}_W umożliwiają bardziej ściśle, choć tylko konceptualne, określenie poszczególnych okresów życia SIR. I tak:

- w okresie powstania systemu: $\dot{z}_W \gg 0$,zaś $\dot{z}_T < 0$;
- w okresie wzrostu SIR: $\dot{z}_W > 0$,zaś $\dot{z}_T > 0$;
- w okresie rozwoju SIR: $\dot{z}_W < 0$ i $\dot{z}_T > 0$;
- w okresie wieku dojrzałego SIR: $\dot{z}_W < 0$,zaś $\dot{z}_T > 0$;
- w okresie schyłku lub regresu SIR: $\dot{z}_W < 0$ i $\dot{z}_T < 0$;
- w okresie upadku $\dot{z}_W = 0$,zaś $\dot{z}_T > 0$.

Uwzględniając zależność długotrwałej egzystencji SIR od egzystencji jego nadsystemu, warunkiem maksymalizowania jego funkcjonowania /życia/ jest utrzymanie takiego jego stanu, przy którym zarówno \dot{z}_W jak i \dot{z}_T mają wartość dodatnią. Stąd wniosek, że maksymalizowanie przez SIR jego poziomu informacji wymaga maksymalizowania przez SIR okresu jego rozwoju. Maksymalizowanie natomiast funkcjonowania /życia/ nadsystemu SIR wymaga minimalizowania okresu wzrostu i okresu schyłku systemów współtworzących ten nadsystem.

Maksymalizowanie okresu rozwoju wymaga między innymi minimalizowania okresu wzrostu, co uwarunkowane jest maksymalizowaniem wskaźnika sprawności wzrostu \dot{z}_W . Z zależności zaś struktury SIR od stanu jego otoczenia wynika, że zdolność rozwoju SIR zapewnić może jedynie taka struktura SIR, która będzie się odznaczała dodatnią wartością wskaźnika sprawności twórczej \dot{z}_T .

Aby więc przyspieszyć okres wzrostu rozwoju należy:

- 1/ maksymalizować zasób informacji realnej SIR, w tym odwzorowującej;

2/ minimalizować destrukcyjne oddziaływanie otoczenia na
wzrastający system.

Warunek pierwszy oznacza potrzebę maksymalizowania
potencjału informacyjnego systemu, natomiast drugi oznacza
między innymi zapewnienie zgodności działań systemu z jego
nadsystemem, w tym z otoczeniem. Stąd można wnioskować, że
wartość wskaźnika sprawności wzrostu \hat{Z}_w uzależniony jest od
wielkości potencjału informacyjnego oraz od stopnia zgodności
działań systemu i otoczenia, czyli

$$\hat{Z}_w = \hat{Z}_w / P_i, Z/ \quad \text{gdzie:}$$

P_i - potencjał informacyjny SIR;

Z - współczynnik zgodności działań systemu i otoczenia.

Maksymalizowanie okresu rozwoju SIR wymaga również maksy-
malizowania współczynnika sprawności twórczej \hat{Z}_T .

Wartość współczynnika sprawności twórczej \hat{Z}_T uzależniony
jest od tych samych czynników co \hat{Z}_w :

$$\hat{Z}_T = \hat{Z}_T / P_i, Z/$$

Zatem zarówno przyspieszenie procesu wzrostu jak i maksymali-
zowania okresu rozwoju wymaga maksymalizowania potencjału
informacyjnego systemu i zapewnienia zgodności jego działań z
celami i działaniami nadsystemu.

Potencjał informacyjny systemu zależy natomiast od
zasobów informacji realnej, zgromadzonych w systemie i jest
proporcjonalny do odwrotności prawdopodobieństwa przypadkowego
utworzenia struktury systemu, w której zgromadzone są te
zasoby informacji, a także od pojemności informacyjnej sys-

temu P_i . Stąd:

$$P_i = P_i / Z_i, \frac{1}{P}, p_i/, \quad \text{gdzie:}$$

Z_i - zasoby informacji realnej, w tym odwzorowującej;

P - prawdopodobieństwo przypadkowego utworzenia danej struktury;

P_i - pojemność informacyjna systemu.

Potencjał informacyjny można również przedstawić zależnością następujących elementów:

$$P_i = f / I_0, P_{nt}, P_{it}, S_i, Z_i / = f / \frac{1}{P} / \quad \text{gdzie:}$$

I_0 - zasób dostępnej informacji odwzorowującej /a posteriori i a priori, w tym informacji naukowo-technicznej/;

P_{nt} - potencjał naukowo-techniczny /kadra, środki techniczne/;

S_i - czynnik ludzki - samodzielność intelektualna;

P_{it} - potencjał informacyjny pozostałych elementów systemu;

i - sprawność organizacyjna /dostępność informacji odwzorowującej, elastyczność działania/;

P - prawdopodobieństwo struktury.

Pojemność informacyjna " p_i " zależy natomiast od ilości i różnorodności elementów systemu, stąd:

$$P_i = P_i / n, r / \quad \text{gdzie:}$$

n - ilość elementów systemu;

r - różnorodność elementów systemu.

Współczynnik zgodności " Z " jest bezpośrednio uzależniony od potencjału informacyjnego systemu, stąd

$$Z = z / P_i /$$

Nie można bowiem zapewnić zgodności samodzielnych działań systemu i jego otoczenia, gdy między innymi system nie zna swego otoczenia i nie zna uwarunkowań swej egzystencji od stanu otoczenia, jak również, gdy nie posiada wiedzy niezbędnej dla zapewnienia tej zgodności. Brak wiedzy i znajomości tych uwarunkowań może być czynnikiem wykorzystywania dość wysokiego już potencjału informacyjnego w niszczonej przez system otoczeniu, nadmiernym jego wzroście kosztem otoczenia.

Z powyższych rozważań wynika, że problemem węzłowym dla rozwoju systemu /kontrwywiadowczej ochrony tajemnicy również/ jest maksymalizowanie jego potencjału informacyjnego poprzez odpowiednie zwiększanie pojemności informacyjnej systemu w drodze rozwoju ilościowego elementów systemu i odpowiedniego ich zróżnicowania.

Pamiętać jednak należy, że nadmierny ilościowy rozwój systemu, któremu nie będzie towarzyszył odpowiedni wzrost potencjału informacyjnego, w tym zasobów informacji, będzie czynnikiem wstrzymania rozwoju systemu lub jego regresu.

Wstrzymanie rozwoju SIR i jego przejście do okresu "wieku dojrzałego" albo "schyłku", jest skutkiem braku możliwości dalszego zwiększania przez system jego potencjału informacyjnego. Przy określonej ilości elementów systemu i jakością ich zróżnicowania /a także elastyczności SIR/ pojemności informacyjnej, SIR bez dalszej ilościowej rozbudowy swej struktury nie jest w stanie zwiększyć swych zasobów informacji. Nie pozwala na to wyczerpana już i ograniczona pojemność jego dotychczasowej struktury.

Reasumując dotychczasowe rozważania należy przyjąć,

w oparciu o ogólną teorię systemów i cybernetykę, że zorganizowany system kontrwywiadowczej ochrony tajemnicy funkcjonując przy szybko zachodzących zmianach w jego otoczeniu powinien cechować się:

- 1/ wysoka pojemnością informacyjną, która w tym systemie zależna jest przede wszystkim od jakości środków pracy, ich możliwości i rozmieszczenia /struktury/ oraz od pozostałych elementów podmiotowych systemu /oficerów KW i pozostałych pracowników WSW/ i ich rozmieszczenia w strukturze organów WSW;
- 2/ wysoka sprawnością informacyjną polegającą na szybkim pozyskiwaniu i wykorzystywaniu posiadanych przez ten system informacji;
- 3/ duża elastycznością działania polegającą na dostosowaniu się do nowych sytuacji; musi zapewnić przewidywanie i podejmowanie działań z wyprzedzeniem;
- 4/ niska energochłonnością metod jego działania /struktura systemu wyspecjalizowana dziedzinowo, sprawna, nadmiarowa i sprzężona właściwie/.

Ponadto system ten spełniać powinien pięć rygorów metody systemowej,^{1/} a więc:

- 1/ Ścisłość, czyli system powinien być ściśle określony, aby było wiadomo, co do niego należy.
- 2/ Niezmiennność, a więc określenie systemu powinno być niezmiennie w całym toku rozważań. Jest niedopuszczalne, żeby jakieś elementy były czasem traktowane jako należące do systemu, czasem zaś jako nie należące.

1/ Por. M. MAZUR, Szkoła podstaw inżynierii systemów, cz.II, Szefostwo Badań i Rozwoju TW, Orzysz 1976r., s.3 i dalsze.

Rygor ten nie oznacza niezmienności systemu, lecz niezmiennosc jego określenia.

Zmiany zachodzące w systemie muszą mieścić się w ramach jego określenia.

3/ Zupełność,

czyli podział systemu na podsystemy powinien być zupełny. Znaczy to, że system nie może zawierać elementów nie należących do żadnego z jego podsystemów. Rygor ten odgrywa istotną rolę w traktowaniu torów oddziaływań jednego podsystemu na inny. Jeżeli tor tylko przenosi oddziaływanie, to uważa się go za nie istniejący - tak - jak gdyby podsystemy były połączone ze sobą bezpośrednio. Natomiast jeżeli tor przetwarza oddziaływanie, to musi być uwidoczniiony jako osobny podsystem, pośredniczący między dwoma podsystemami, np. jeżeli szef sztabu przekazuje polecenia ogólne dowódcy do podwładnego w formie szczegółowych zadań, to i on powinien być uwidoczniiony jako podsystem.

4/ Rozłączność,

czyli podział systemu na podsystemy powinien być rozłączny. Znaczy to, że system nie może zawierać elementów należących do kilku podsystemów naraz. Przynależność jakichś elementów do jednego podsystemu /np. podsystemu środków pracy/ musi być równoznaczne z tym, że na pewno elementy te nie należą do żadnego innego podsystemu /np. podsystemu oficerów KW/.

5/ Funkcjonalność,

czyli systemy powinny być wyodrębnione ze względu na spełniane funkcje, a nie ze względu na oddzielność przestrzenną. W systemie KW ochrony tajemnicy szczególną rolę

odgrywają przede wszystkim kanały obiegu chronionych wiadomości /tajemnic/. I tak, dla przykładu, Sztab Generalny WP powinien być chroniony łącznie z instytucjami, z którymi bezpośrednio współpracuje, a które podlegają pod Szefa Sztabu Gen. WP. Naruszenie tego rygoru jest częstym błędem, gdyż niektórzy organizatorzy systemów ochronnych kierują się oddzielną przetrzenną.

Struktura zorganizowanego systemu kontrwywiadowczej ochrony tajemnicy powinna spełniać ponadto następujące funkcje:

- 1/ Rozpoznawanie zmian uwarunkowania egzystencji i zagrożeń.
- 2/ Formułowanie celów i zadań.
- 3/ Dzielenie zadań i deficytowych zasobów /np. środków techniki operacyjnej/.
4. Koordynowanie działań /po przydzieleniu zadań/.
- 5/ Harmonizowanie osiągnięć.
- 6/ Antycypacyjnie adaptowanie struktury, czyli umiejętność przewidywania, ażeby nie podejmować działań po czasie.

Pamiętać również należy o tym, że podmioty i przedmioty ochrony kontrwywiadowczej są obiektami dynamicznymi, uwarunkowanymi zmianami zewnętrznymi i wewnętrznymi. Dlatego też w ocenie elementów systemu KW ochrony tajemnicy należy ujmować wpływ czasu na zmienność obiektu ochrony ze względu na wartość chronionej w nim tajemnicy, gdyż może być skuteczny, ale zabezpieczać obiekt bezwartościowy.

System kontrwywiadowczej ochrony tajemnicy Sił Zbrojnych PRL /SIR_{KW}/, ażeby był w pełni skuteczny, musi dominować

nad systemem wywiadowczego rozpoznania NATO /SIR_{NATO}/ skierowanego na nasz kraj. Warunkiem dominacji naszego systemu nad przeciwnikiem będzie przewaga sprawności twórczej naszego systemu ochrony λ_{T1} nad sprawnością twórczą systemu przeciwnika λ_{T2} , czyli

$$\lambda_{T1} > \lambda_{T2}$$

System SIR_{KW} dominuje, czyli szybciej rozwija się lub wzrasta nad SIR_{NATO} jeżeli:

$$\lambda_{T1} \approx \frac{\Delta i_{P_1} + \Delta i_{S_1} + \Delta i_{n_1}}{\Delta e_{oP_1} + \Delta e_{oS_1} + \Delta e_{on_1}} > \lambda_{T2} \approx \frac{\Delta i_{P_2} + \Delta i_{S_2} + \Delta i_{n_2}}{\Delta e_{oP_2} + \Delta e_{oS_2} + \Delta e_{on_2}}$$

gdzie:

- Δi - przyrost informacji
- Δe - przyrost energii
- p - dotyczy jednostek
- s - dotyczy systemu
- n - dotyczy nadsystemu

Z warunku dominacji, a więc posiadanej przewagi wynika możliwość sterowania układem: "SIR_{KW} - OTOCZENIE" nad SIR_{NATO}.

Odpowiednie sterowanie może utrzymywać wymienioną nierówność.

W ramach dominacji $P_{iKW} > P_{iNATO}$ wynika możliwość jej przełamania i uzyskania chwilowej przewagi przez przeciwnika

$$\lambda_{T2} > \lambda_{T1}, \text{ jeżeli } Z_2 \gg Z_1 \quad \text{wówczas}$$

$$(P_{iNATO}, Z_2) > (P_{iKW}, Z_1) \quad \text{gdzie:}$$

P_{iKW} - potencjał informacyjny organów KW;

P_{iNATO} - potencjał informacyjny służb wywiadowczych NATO;

- Z_1 - współczynnik zgodności celów i działań organów KW;
 Z_2 - współczynnik zgodności celów i działań wywiadów NATO.

Współczynnik zgodności celów i działań "Z" można określić jako

$$Z = f / S_w, 2_{Hn}, Z_p, Z_s / \quad \text{gdzie:}$$

- S_w - wymierny, adekwatny system wartości;
 H_n - sprawność układu homeostazy naturalnej;
 Z_p - zdolność przewidywania - prognozowania zmian i skutków działań;
 Z_s - współczynnik synchronizacji działań "P" - jednostek, "S" - systemu, "n" - nadsystemu.

Aby tę przewagę utrwalić przeciwnik dąży do uzyskania stanu, aby $P_{iNATO} > P_{iKW}$ - co jest warunkiem trwałej zmiany dominacji.

Wnioskować więc można, że system kontrwywiadowczej ochrony tajemnicy Sił Zbrojnych PRL będzie dominował nad systemem wywiadowczego rozpoznania naszego wojska ze strony służb wywiadowczych NATO jedynie w przypadku przewagi potencjału informacyjnego naszego systemu nad systemem przeciwnika oraz przestrzegania zasady zgodności celów i działań SIR_{KW} /współczynnika "z"/.

Z przeprowadzonej analizy cybernetycznego modelu systemowego kontrwywiadowczej ochrony tajemnicy jako typowego systemu informacyjnego rozwijającego się można wyprowadzić następujące wnioski:

1. System kontrwywiadowczej ochrony tajemnicy jest w swej istocie typowym systemem informacyjnym, którego podstawowe

funkcje sprowadzają się do zbierania, przetwarzania, przechowywania i udostępniania informacji stosownie do potrzeb i wymagań użytkowników, a zatem w procesie analizy tego systemu ma pełne zastosowanie wiedza z teorii informacji.

2. Przedstawienie systemu kontrwywiadowczej ochrony tajemnicy w postaci systemu informacyjnego rozwijającego się /SIR/ pozwala w oparciu o współczesną teorię informacji - na stwierdzenie, że sprawność funkcjonowania zorganizowanego systemu kontrwywiadowczej ochrony tajemnicy, w warunkach szybko zachodzących zmian w jego otoczeniu uzależnione jest od wysokiej pojemności i sprawności informacyjnej oraz dużej elastyczności działania.
3. Miarą skuteczności systemu kontrwywiadowczej ochrony tajemnicy Sił Zbrojnych PRL jest poziom dominacji nad systemem wywiadowczego rozpoznania NATO w potencjale informacyjnym.

R O Z D Z I A Ł II

NIEKTÓRE ASPEKTY WSPÓCZESNEJ WALKI
INFORMACYJNEJ W UKŁADZIE WYWIAD -
KONTRWYWIAD

1. Istota współczesnej wojny informacyjnej

Jednym z warunków wszelkiej racjonalnej działalności we współczesnym świecie jest możliwość korzystania z informacji. Obok zasobów surowcowych i energetycznych, zasoby informacyjne obejmujące istotne osiągnięcia nauki, kultury i sztuki, stanowią najistotniejszy czynnik potencjału cywilizacyjnego. Bez racjonalnie ukształtowanej sfery informacyjnej nie może obecnie funkcjonować gospodarka narodowa i siły zbrojne poszczególnych państw, w tym również organa kontrwywiadu wojskowego.^{1/}

Aktualny układ stosunków między systemem kapitalistycznym a socjalistycznym i przewidywane perspektywy jego rozwoju na zasadzie współdziałania stwarza szansę odchodzenia od rozwiązywania konfliktów drogą wojny. W tej sytuacji szczególnego znaczenia nabiera wysiłek państw NATO ukierunkowany na zdobywanie informacji o państwach socjalistycznych, niezbędnych do realizacji celu strategicznego w innych warunkach i innymi metodami.

Celem prowadzonej aktualnie przez państwa NATO "wojny informacyjnej" jest inspirowanie i podtrzymywanie działalności

1/ P. SIENKIEWICZ "Inżynieria systemów", MON, Warszawa 1983r., s. 57

destrukcyjnej w państwach socjalistycznych we wszystkich dziedzinach życia oraz dążenie do obniżenia równowagi w sferze konwencjonalnych środków walki, wojna informacyjna będzie przez system kapitalistyczny doskonalona i przekształcana w główny mechanizm realizacji jego celów strategicznych.

Ten typ walki jest jakościowo nowy, a istota informacyjnej destrukcji w zasadzie prosta. Wystarczy bowiem odpowiednio wspomagać zachodzące w systemie przeciwnika naturalne procesy rozkładowe /entropowe/ i jednocześnie osłabiać intensywność występowania procesów twórczych /negentropowych/, do tego zaś potrzebne są pewne i na czas napływające informacje.

Praktyczna realizacja tego typu niszczących działań dla odniesienia sukcesów, w postaci ograniczenia rozwoju zwalczanego systemu socjalistycznego wymaga systematycznego dopływu informacji do central służb specjalnych państw NATO w celu podjęcia odpowiednich studiów i wypracowania wiedzy w szczególności o:

- 1/ mechanizmach działania i rozwoju zwalczanego systemu socjalistycznego, poziomie rozwoju nauk społecznych oraz nauk ogólnych i systemowych, prawidłowościach rozwoju oraz sposobach reakcji państw socjalistycznych na różnorodne nań oddziaływania;
- 2/ zmieniającym się stanie struktury systemu socjalistycznego w tym o nastrojach społecznych, szczególnie wśród kadry MON i MSW, kwalifikacjach przywódców, nastrojach poszczególnych części społeczeństwa, potencjale naukowo-wytwórczym, stosowanych metodach wytwarzania oraz występujących sprzecznościach społecznych;

- 3/ poziomie rozwoju informatyki, w tym metod symulacji komputerowej wielkich systemów, niezbędnych dla naukowego wypracowania takiej postaci struktury systemu socjalistycznego, która będzie odznaczała się największym możliwie natężeniem niszczących go procesów rozkładowych, a także opracowywanie sukcesywnie korygowanych metod przeprowadzania operacji destrukcyjnych;
- 4/ skutecznych metodach walki skierowanej przeciwko systemowi socjalistycznemu powodującej obniżenie progu jego zdolności adaptacyjnej;
- 5/ odpowiednio wysokiej mocy realizacyjnej wypracowywanych działań destrukcyjnych, wspartych odpowiednim potencjałem finansowym.

Zgromadzona przez służby specjalne państw NATO wiedza o aktualnych mechanizmach funkcjonowania systemu socjalistycznego, o jego słabościach i mocnych stronach wykorzystywana jest do prowadzenia - w ramach wojny informacyjnej - działań destrukcyjnych, obniżających skuteczność procesów przebudowy i sprawność działań reformatorskich.

Powstaje zatem pytanie, czy prowadzona przez państwa NATO wojna informacyjna ukierunkowana na rozsadzenie wspólnoty państw socjalistycznych od wewnątrz ma szansę praktycznej realizacji? Aby na to pytanie odpowiedzieć należy poddać bardziej szczegółowej analizie możliwe potencjalne mechanizmy samodestrukcji, które wszczepione w system obronny naszego państwa, mogą przyczynić się do obniżenia jego funkcjonalnej skuteczności. Poznawanie mechanizmów samodestrukcji oraz potencjalnych możliwości wdrażania ich do naszej działalności obronnej stanowi podstawę rozpoznawania faktycznych zagrożeń dla gotowości obronnej państwa oraz wypracowania systemu

przeciwdziałania przepływowi informacji do służb specjalnych państw NATO.

Teoretyczne podstawy skutecznego prowadzenia wojny informacyjnej daje między innymi ogólna teoria systemów i cybernetyka. Z nauk tych wynika, że odpowiednio oddziaływując - nawet z zewnątrz - na system obronny kraju przeciwnika, mając przy tym odpowiednie ku temu możliwości naukowo-techniczne, można dany system tak wytrącać ze stanu równowagi dynamicznej, że nie będzie on w stanie właściwie dostosowywać się do zachodzących destrukcyjnych zmian w jego otoczeniu.

Szczególną rolę w tej międzysystemowej walce o informacje odgrywają wyspecjalizowane instytucje służb specjalnych:

- wywiadu, bo zdobywa on przy wykorzystaniu specyficznych środków pracy /przede wszystkim agentury informacyjnej/ istotne wiadomości o przeciwniku /zwalczanym systemie/ oraz dane o zamiarach przeciwnika w stosunku do własnego systemu /wyprzedzająco rozpoznaje zagrożenia/, a także po odpowiednim przetworzeniu zdobytych informacji bierze czynny udział w destrukcyjnym oddziaływaniu na system przeciwnika /wykorzystując, oprócz sił i środków umieszczonych w kanale informacyjnym, również agenturę energetyczną/;
- kontrwywiadu, bo konstruuje on zabezpieczenie systemu obronnego własnego państwa poprzez organizowanie reżimów ochrony tajemnicy oraz poprzez wykrywanie, rozpracowywanie i likwidację agentury informacyjnej oraz energetycznej przeciwnika. Uodparnia także chroniony przez siebie system na występujące w praktyce lub mogące wystąpić w najbliższej przyszłości zagrożenia.

Ochronę systemu obronnego PRL przed agresją informacyjną państw NATO w odniesieniu do naszych Sił Zbrojnych realizują w sposób statutowo przypisany organa kontrwywiadu

Wojskowej Służby Wewnętrznej we współdziałaniu przede wszystkim z dowództwem i aparatem partyjno-politycznym. Organizują one system kontrwywiadowczej ochrony tajemnicy, którego celem jest ograniczenie do minimum możliwości ich zdobycia przez przeciwnika, a także wykrywanie i likwidację odpowiednich sygnałów przesyłanych przez przeciwnika do ochranianej struktury wojskowej i ich adresatów /agentury i osób podatnych na wrogie treści/ oraz neutralizowanie możliwości odbierania przez przeciwnika komunikatów zawierających dane dotyczące rozpoznawanych elementów podmiotowych i przedmiotowych ochra-
nianych sił zbrojnych.

2. Analiza niektórych aspektów współczesnej walki o informacje

W walce o "informacje" stronami walczącymi państw od zarania dziejów są organa wywiadu i kontrwywiadu. Wywiad "walczy" przede wszystkim z obiektem chronionym przez kontrwywiad, a kontrwywiad "walczy" z wywiadem współdziałając z zabezpieczaną instytucją.

Oddziaływanie wywiadów na zabezpieczane kontrwywiadowczo instytucje /obiekty/ ma zawsze charakter destrukcyjny i zmierza ono do dezorganizacji chronionych struktur państwowych. Pomiędzy wymienionymi służbami specjalnymi występuje relacja tworząca tzw. "łańcuch niszczenia": niszczyciel - środek niszczenia - obiekt niszczenia.

Uczestnicy tej walki muszą spełniać podstawowe jej warunki, a przede wszystkim:

- 1/ cele działania stron są przeciwstawne;
- 2/ zadanie, które realizują obiekty należące do danej grupy podporządkowane są jej celom;
- 3/ każda ze stron dysponuje siłami i środkami należącymi do klasy aktywnych niszczycieli obiektów przeciwnika /agencji wywiadu, receptory kontrwywiadu/;
- 4/ obiekty należące do tej samej strony nie niszczą się wzajemnie.^{1/}

Powyższe warunki oznaczają, że strony w rozpatrywanym przez nas przypadku będą w stanie walki tak długo, dopóki prowadzona będzie działalność szpiegowska. Proces walki ze stroną przeciwną może odbywać się zarówno na drodze energetycznej /zasileniowej/ jak również na drodze informacyjnej.

O ile do niedawna w sposób uproszczony przyjmowano założenie, że w okresie pokojowym walka między dwoma przeciwstawnymi blokami wojskowymi /Układ Warszawski - NATO/ dokonuje się bezpośrednio na drodze informacyjnej, to dzisiaj zaczyna się dostrzegać, iż dotyczy ona również drogi energetycznej, bowiem celem walki "bezorężnej", w której bronią jest "informacja", staje się powstrzymywanie rozwoju państw socjalistycznych, a więc osłabienie w gruncie rzeczy potencjału energetycznego zwalczanego systemu.

Dla organów kontrwywiadu, będącego podsystemem zabezpieczenia walczącej strony, istotę działania w rozpatrywanym problemie stanowi ochrona tajemnicy, a więc informacji sta-

1/ J. KONIECZNY, Cybernetyka walki, PWN, Warszawa 1970r., s.24

nowiących szczególną wartość dla strony uczestniczącej w walce. Dla "wywiadu" istotę działania stanowi zdobycie informacji o przeciwniku, a następnie umiejętne ich wykorzystanie w celach destrukcyjnych, zarówno w okresie pokoju jak i w czasie wojny.

Wojna informacyjna kojarzy się zazwyczaj w naszej świadomości z tradycyjną walką informacyjną realizowaną między innymi za pomocą środków masowego przekazu, mających za zadanie dezinformowanie zwalczanego społeczeństwa oraz takie destrukcyjne, psychologiczne oddziaływanie, by było ono podatne na przekazywane mu wrogie informacje sterownicze. Z cybernetycznej analizy współczesnych aspektów wojny informacyjnej wynika, że jej celem jest nie tylko bezpośrednie, szkodliwe oddziaływanie przekazywanymi odpowiednio dobranymi wiadomościami.

Istotę tej nowoczesnej formy walki stanowi także wbudowanie w strukturę zwalczanego państwa, we wszystkie żywotne jego dziedziny życia, takich mechanizmów destrukcji, które następnie już w sposób samoczynny - wymagający co najwyżej nieznacznych bieżących korekt sposobu ich funkcjonowania - będą wywoływały niszczące przeciwnika skutki.

Odpowiednio wywoływane destrukcyjne zmiany w strukturze systemu jego deformowania, będą inicjowały odpowiednie przyczynowo-skutkowe ciągi następstw, w wyniku których system nie będzie się mógł rozwijać i będzie podlegał intensywnej, pozornie samoczynnej erozji.^{1/}

Przyjmując, że w walce informacyjnej w ramach danej

1/ Por. L. MICHNOWSKI, "Istota nowoczesnej wojny informacyjnej", WSNS przy KC PZPR, 1984 r., s. 9

strony biorą udział instytucje /organizacje/ wywiadu i kontrwywiadu /podsystemy niszczenia i zabezpieczenia/ oraz ich środki niszczenia i ochrony można powiedzieć, że walka informacyjna to celowe oddziaływanie służb specjalnych przeciwnika na organizację danego państwa, zmierzające do uniemożliwienia lub utrudnienia w jego strukturach określonych procesów sterowniczych, a także obrony własnych instytucji od analogicznych działań służb zwalczanego państwa /przeciwnika/.¹

Oddziaływanie takie polega na dezorganizowaniu przeciwnika tak, aby uczynić go niezdolnym do dalszej walki o informację oraz na obronie własnej struktury przed zagrożeniami strony przeciwnej.

Wielkość zniszczenia możemy mierzyć zmniejszeniem stopnia organizacji przeciwnika albo zmniejszeniem wielkości jego działań lub rezultatów tych działań.

Niszczenie może być energetyczne lub informacyjne, ze względu na sposób, jak i na obiekt niszczenia.

Ze względu na sposób, o niszczeniu energetycznym mówić można wtedy, gdy do likwidacji struktury przeciwnika używana jest energia /np. energia zawarta w pocisku/. Ten sposób niszczenia omawia teoria walki zbrojnej i w dalszych rozważaniach nie będzie on poruszany. Niszczenie informacyjne natomiast występuje wówczas, gdy do dezorganizacji struktur

1/ Por. J. KOSSECKI, Cybernetyka społeczna, Warszawa 1981 r., s. 408

przeciwnika używa się "określonych informacji" /bodźców/.

Ze względu na obiekt, niszczenie energetyczne ma miejsce wówczas, gdy likwidacji ulegają elementy wchodzące w skład toru energetycznego struktury przeciwnika /można je niszczyć energią lub odpowiednią informacją/, natomiast informacyjne, gdy niszczone są elementy wchodzące w skład toru informacyjnego.

3. Energetyczne i informacyjne niszczenie
systemu kontrwywiadowczej ochrony tajemnicy
metoda walki informacyjnej

Aby system kontrwywiadowczej ochrony mógł sprawnie funkcjonować musi posiadać odpowiednią strukturę. Jak wynika z rozważań M. MAZURA^{1/}, określona struktura systemu utrzymuje się przy określonej koncentracji energii, która ze względu na występowanie w systemie procesów samowyrównawczych, maleje. W warunkach zmniejszającej się energii system ulega dezorganizacji, a zjawisku temu system może zapobiec tylko poprzez pobieranie energii z zewnątrz.

Odnosząc to do systemu kontrwywiadowczej ochrony tajemnicy obniżenie jakości elementów systemu jest równoznaczne ze zmniejszeniem się jego trwałości, stanowi więc zakłócenie, które system, a szczególnie jego homeostat^{2/}, musi zwalczać.

1/ M. MAZUR, Cybernetyczna teoria układów samodzielnych, Warszawa 1966 r., s. 130 i 131

2/ Homeostat w kontekście omawianej pracy rozumiany jako oficer KW.

Oficer KW - funkcjonujący w tym systemie - musi dostosować swoje działania do szybkości zachodzących zmian. W związku z tym, postępującej dezorganizacji systemu samodzielnego towarzyszyć musi szybkie jego doskonalenie.^{1/}

Traktując system kontrwywiadowczej ochrony tajemnicy jako przetwornika energii można operować pojęciem mocy. Moc całkowita systemu jest tym większa, im wyższa jest jakość tworzywa "a" i im większa jest ilość tworzywa "c". Moc całkowitą systemu można określić wzorem:

$$P = v \cdot a \cdot c^2/$$

Moc jednostkowa "V" jest wielkością określającą zdolność systemu do przetwarzania energii. Stąd moc całkowita systemu P, jest w danym stanie systemu największą dopuszczalną mocą jaką system może przetworzyć. Jej przekroczenie groziłoby takimi zmianami tworzywa, że zaistniałego naruszenia równowagi homeostat nie zdołałby usunąć i system przestałby istnieć. Sprowadzając wywód na grunt praktyki, posiadanie przez oficera kontrwywiadu nadmiernej ilości środków pracy nie usprawni jej, lecz wręcz zdezorganizuje i zagrozi tajności pracy operacyjnej.

W systemie kontrwywiadowczej ochrony tajemnicy, jako układzie samodzielnym, w związku z procesami starzenia się materiału jakość tworzywa, czyli receptorów kontrwywiadu, stale w sposób naturalny maleje. Ażeby nie utracić swoich

1/ M. MAZUR, op.cit., s. 132

2/ M. MAZUR, op.cit., s. 133

właściwości, w systemie następuje stały wzrost ilości tworzywa, dążąc asymptotycznie do pewnej granicy. Zatem moc całkowita systemu KW ochrony w funkcji czasu - bez właściwej interwencji oficera KW - będzie najpierw wzrastać od pewnej wartości początkowej aż do osiągnięcia pewnego maksimum, a następnie maleć.^{1/}

Podstawową część mocy całkowitej - system kontrwywiadowczej ochrony zużywa na pokrycie strat energii oddanej w zamian za uzyskane od receptorów informacje kontrwywiadowcze. W rozpatrywanym przez nas systemie jest to tzw. moc robocza P_r . Moc robocza pokrywa energię jaką oficer KW zużywa na pracę z wykorzystywanymi w systemie siłami i środkami operacyjnymi skierowanymi na uzyskiwanie informacji, ich przetwarzanie i wykorzystanie. Im większa jest ilość tworzywa, tym większą mocą roboczą musi dysponować system. Dlatego też dla efektywności systemu, przyjmując ograniczoność wielkości posiadanej mocy całkowitej istotną rolę odgrywa jakość tworzywa systemu, szczególnie wykorzystywanych receptorów.

Z powyższego można wnioskować, że system KW ochrony z mocy całkowitej P musi wydać część posiadanej energii na moc roboczą P_r , a dopiero z pozostałej reszty może korzystać do innych potrzeb.

Ta reszta mocy stanowi moc dyspozycyjną P_d , przy czym

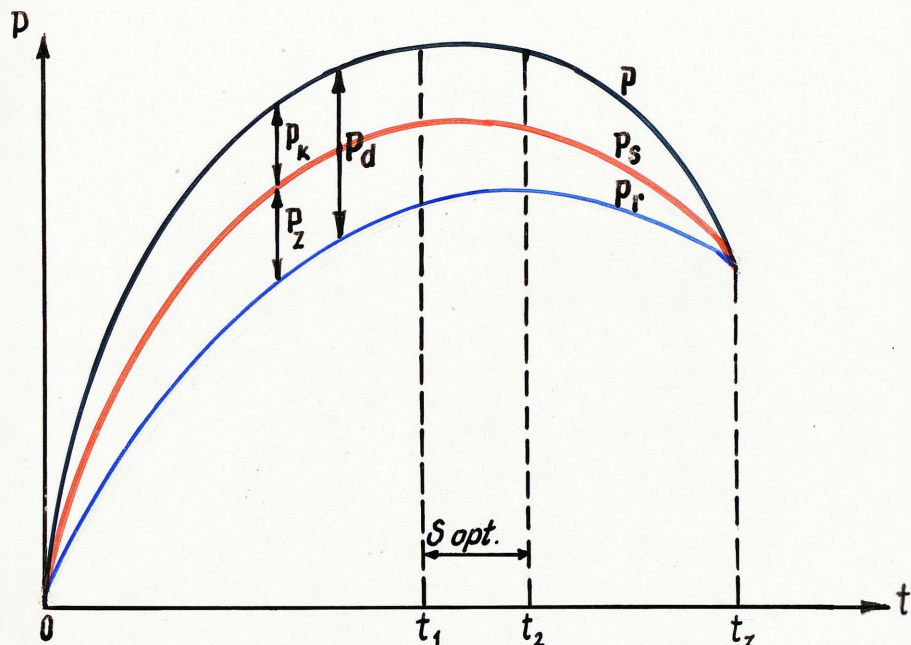
$$P_d = P - P_r$$

wobec czego moc całkowitą systemu można wyrazić wzorem

$$P = P_r + P_d$$

1/ M. MAZUR, op.cit. s. 134

Podział mocy systemu kontrwywiadowczej ochrony obrazuje następujący wykres:



gdzie:

P - moc całkowita

t - czas

P_R - moc robocza

P_d - moc dyspozycyjna

P_s - moc asekuracyjna

P_z - moc zabezpieczenia

P_k - moc koordynacyjna

t₁ - t₂: czas optymalnego funkcjonowania systemu.

Na wykresie krzywa P pokazuje, jak zmienia się w czasie egzystencji systemu jego moc całkowita. Krzywa P_R pokazuje zmienność mocy roboczej w czasie egzystencji systemu. Moc robocza rośnie początkowo szybko, a potem coraz wolniej, dążąc asymptotycznie do pewnej stałej wielkości. Moc dyspo-

zycyjna P_d , której wielkość reprezentuje długość odcinka między krzywą mocy całkowitej a krzywą mocy roboczej, początkowo wzrasta, a następnie po przejściu przez maksimum maleje i staje się równa zero w pewnym momencie t_z , wyznaczonym przez przecięcie krzywej P z krzywą P_r . Czas t_z oznacza koniec egzystencji systemu samodzielnego.^{1/}

Odcinek czasu zawarty między początkiem egzystencji systemu samodzielnego /chwila 0/ a końcem jego egzystencji, czyli momentem t_z określonym warunkiem zrównania się mocy całkowitej z mocą roboczą jest czasem egzystencji systemu samodzielnego. W chwili t_z moc systemu idzie w całości na pokrycie mocy roboczej. Po przekroczeniu czasu t_z moc systemu nie wystarczałaby nawet na pokrycie mocy roboczej, co oznacza, że system KW ochrony nie mogąc zapobiec dezorganizacji musi przestać istnieć jako system samodzielny.^{2/}

Stąd wniosek, że warunkiem nieskończenie długiej egzystencji systemu KW ochrony jest spełnienie warunku aby moc całkowita była zawsze większa od mocy roboczej. Warunek ten może być spełniony jedynie, przy utrzymywaniu wysokiej jakości środków pracy KW tak, ażeby moc całkowita była wystarczająca do pokrywania strat energii wydatkowanej na uzyskiwanie informacji KW.

Oprócz energii zużywanej na pokrycie mocy roboczej, część energii systemu KW ochrony tajemnicy musi zużywać na pracę wykonywaną dla zapewnienia działań związanych z prawid-

1/ Por. M. MAZUR, op.cit., s. 139-160

2/ Tamże, s. 139

łowym funkcjonowaniem warunków uzyskiwania informacji przez oficera KW oraz pokonywanie związanych z tym trudności. Musi więc dysponować dodatkową energią, która umożliwi mu wykonanie tej pracy. Moc, która odpowiada tej dodatkowej energii to moc zabezpieczenia P_Z . Oczywiście, im mniej korzystne warunki dla funkcjonowania systemu KW ochrony panują w jego otoczeniu, tym większą pracę musi wykonać oficer KW, a zatem tym większą ilość posiadanej energii całkowitej musi wykorzystywać w charakterze mocy zabezpieczenia. Do wzrostu mocy P_Z przyczynia się również w sposób negatywny ilość środków pracy KW. Generalnie oficer KW posiadaną moc P_Z wykorzystuje przede wszystkim na poszukiwanie nowych źródeł informacji i ich pozyskiwanie.

Suma mocy roboczej P_R i mocy zabezpieczenia P_Z nazywa się mocą asekuracyjną P_S .^{1/}

$$P_S = P_R + P_Z$$

Moc asekuracyjna zapewnia względnie poprawne jego funkcjonowanie, a jej posiadanie jest żywotną cechą systemu KW ochrony tajemnicy. Gdyby moc całkowita P była mniejsza od mocy asekuracyjnej P_S , system nie mógłby wydawać dostatecznej mocy zabezpieczenia P_Z i w konsekwencji zapewnić sobie potrzebnej mocy roboczej P_R , wskutek czego uległby dezorganizacji.^{2/}

Dla funkcjonowania w optymalnych warunkach, system kontrwywiadowczej ochrony, z posiadanej mocy całkowitej P , po odliczeniu mocy asekuracyjnej P_S na pokrycie mocy roboczej P_R

1/ Por. M. MAZUR, op.cit., s. 153

2/ Tamże, s. 157

i mocy zabezpieczenia P_z , musi pozostawić do dyspozycji pewną nadwyżkę mocy, którą jest moc koordynacyjna P_k .^{1/}

$$P_k = P - P_s$$

Moc całkowita systemu KW ochrony wyrazi się więc wzorem:

$$P = P_s + P_k$$

Moc koordynacyjna jest niezbędna dla uzyskania przez oficera KW możliwości do kreowania pożądanych warunków w otoczeniu, czyli polepszenia warunków egzystencji systemu w otoczeniu.

Dysponowanie mocą koordynacyjną P_k , jej właściwe spożytkowanie i wykreowanie pożądanych warunków w otoczeniu powoduje zmniejszenie potrzeb ilości energii wykorzystywanej do zabezpieczenia działań operacyjnych /następuje spadek P_z / co daje w końcowym efekcie wzrost mocy roboczej P_r systemu. W ten sposób następuje optymalizacja warunków działania systemu KW ochrony, system zwiększa swoje potencjalne możliwości funkcjonowania.

Traktując system kontrwywiadowczej ochrony jako otwarty, a więc funkcjonujący z otoczeniem na zasadzie sprzężeń zwrotnych i wraz z tym otoczeniem rozwijający się, moc całkowitą P możemy uznać w danym momencie jako moc wewnętrzną P_i tego systemu.

Z drugiej strony otoczenie stanowi źródło, z którego system może tę moc pobierać. Moc, której otoczenie może dostarczać do danego systemu samodzielnego, można określić jako moc

1/ Por. M. MAZUR, op.cit., s. 159

zewnętrzną P_e tego systemu.^{1/} W przypadku systemu kontrwywiadowczej ochrony wielkość mocy zewnętrznej zależy między innymi od:

- dostarczania oficerowi KW z centrali danych o metodach i formach działania oraz bieżących zainteresowaniach służb specjalnych przeciwnika;
- kształtowania przez dowództwo i aparat partyjno-polityczny właściwych postaw kadry i pracowników cywilnych oraz przez władze polityczno-administracyjne takich postaw w środowisku cywilnym;
- wyposażenie oficera KW w urządzenia techniczne pozwalające na kontrolę operacyjną określonych osób;
- ilości pieniędzy, dzięki którym można zabezpieczyć koszty działań operacyjnych.

Oficer KW, w ramach posiadanej mocy koordynacyjnej P_k również zobowiązany jest do udziału w zwiększaniu mocy zewnętrznej P_e systemu KW ochrony. Musi w tym względzie przejawiać szczególną aktywność, gdyż wpływanie na wzrost mocy zewnętrznej P_e przyczynia się w konsekwencji do maksymalizowania mocy roboczej P_r systemu. Mamy więc w tym przypadku do czynienia ze sprzężeniem zwrotnym dodatnim, gdyż moc koordynacyjna P_k zwiększa moc zewnętrzną P_e , a ona $/P_e/$ zwiększa z kolei moc koordynacyjną P_k . Prowadzi to do sytuacji, w której system ma największą możliwą moc zewnętrzną P_e czyli największą odporność na działanie przeciwnika a najmniejszą moc asekuracyjną P_s . W praktyce kontrwywiadowczej powyższe rozważania oznaczają konieczność uwzględnienia w organizacji systemu

1/ Por. M. MAZUR, op.cit., s. 152

kontrwywiadowczej ochrony bilansu energetycznego i dostrzeżenie tego problemu w sposób dynamiczny.

Im większą mocą koordynacyjną dysponuje system, tym większe ma możliwości kształtowania warunków otoczenia i zwiększania mocy zewnętrznej. Stosunek mocy koordynacyjnej do mocy dyspozycyjnej systemu samodzielnego określa się jako współczynnik swobody f ^{1/}

$$f = \frac{P_k}{P_d}$$

Współczynnik swobody f określa, jaką część mocy dyspozycyjnej systemu można przeznaczyć na poprawę warunków otoczenia. W przypadkach skrajnych, co wynika ze wzoru

$$P_d = P_z + P_k,$$

jeżeli system całą moc dyspozycyjną musi zużywać jako moc zabezpieczenia $/P_z = P_d/$, to moc całkowita staje się mocą asekuracyjną $/P_s = P/$, a moc koordynacyjna P_k jest równa zero $/P_k = 0/$, wobec czego i współczynnik swobody $f = 0$. Zachowanie się systemu jest wówczas całkowicie wymuszone przez otoczenie. Na tej zasadzie opera się między innymi energetyczna metoda sterowania społeczeństwem /wymuszenie energetyczne pośrednie/^{2/}

Drugi skrajny przypadek występuje, gdy moc zabezpieczenia jest w całości zastąpiona mocą zewnętrzną $/P_z = 0/$. Wówczas moc asekuracyjna obejmuje tylko moc roboczą $/P_r = P_s/$, moc koordynacyjna staje się równa mocy dyspozycyjnej $/P_d = P_k/$,

1/ Por. M. MAZUR, op.cit., s. 161-162

2/ Tamże, s. 162

a współczynnik swobody systemu $f = 1$.^{1/}

W systemie KW ochrony /tajemnicy/ należy permanentnie dążyć do stanu $f = 1$. Warunek ten spełnia między innymi wprowadzany obecnie w naszym wojsku model profilaktyki kreatywnej.

Z analizy cybernetycznego modelu układów samodzielnych wynika, że niszczenie energetyczne zwalczanego systemu / w tym kontrwywiadowczej ochrony tajemnicy/ polegać będzie na:

- 1/ Zmniejszeniu mocy zewnętrznej P_e stanowiącej źródło mocy pobieranej przez zwalczany system. Środkiem wiodącym do tego celu będzie przede wszystkim niszczenie źródła energii przeciwnika oraz odcinanie go tych źródeł.
- 2/ Zmniejszeniu mocy wewnętrznej P_i systemu przez utrudnianie lub uniemożliwianie pobierania energii zewnętrznej /bez jej zmniejszenia/. Środkiem wiodącym do tego celu będzie dezorganizowanie zasilacza systemu.
- 3/ Zmniejszeniu mocy całkowitej P systemu przez dezorganizowanie akumulatora systemu. Będzie więc to w przypadku rozpatrywanego przez nas systemu dezorganizacja komórek zajmujących się przetwarzaniem i przechowywaniem informacji kontrwywiadowczych /np. dezorganizowanie funkcjonowania OPI, archiwów lub kartotek operacyjnych/.
- 4/ Zmniejszeniu mocy całkowitej systemu poprzez dezorganizację przepływów energii w torze energetycznym. Chodzi tu o dezorganizację połączeń między zasilaczem a akumulatorem, między akumulatorem a organizatorem /homeostatem/ i korelatorem. Może w tym przypadku wchodzić w grę np. odcięcie kierownictwa systemu od niezbędnych informacji.

1/ Por. J. KOSSECKI, op.cit., s. 46

- 5/ Zmniejszeniu mocy koordynacyjnej systemu przez zwiększenie jego mocy asekuracyjnej. Chodzi więc o stworzenie takich warunków działania systemu, że większość posiadanych środków, będzie musiał złużyć jako moc zabezpieczenia działań w rozbudowanej nadmiarowo strukturze /współczynnik swobody $f \approx 0$ /.
- 6/ Na dezorganizowaniu efektorów systemu /ośrodków wykonawczych/.

Analizując cybernetyczny model układów samodzielnych można wnioskować, że niszczenie informacyjne zwalczanego systemu może występować w postaci:

- 1/ Dezorganizowania dopływu z otoczenia komunikatów zawierających wiadomości o odpowiedniej wartości sterowniczej i wykonawczej. Może tu wchodzić w grę dezorganizowanie źródeł informacji przeciwnika przez izolowanie ich od chronionych informacji lub dezinformowanie jego agentów.
- 2/ Bezpośredniego dezorganizowania pracy receptorów. Chodzi tutaj o wykrywanie i likwidację agentury przeciwnika oraz dezorganizowanie instytucji zajmujących się zbieraniem informacji na rzecz wywiadu obcego.
- 3/ Dezorganizowania procesów korelacji i homeostazy u przeciwnika poprzez niszczenie norm społecznych /przede wszystkim poznawczych i konstytutywnych/ oraz dezorganizację instytucji zajmujących się przetwarzaniem i przechowywaniem informacji oraz decydowaniem.
Sposób ten polegał będzie na demoralizowaniu przeciwnika, dezorganizowaniu jego instytucji naukowych, pracy instytucji zajmujących się opracowywaniem informacji dostarczanych przez wywiad oraz demoralizowaniu jego kierownictwa.
- 4/ Dezorganizacji procesów przepływu informacji w torze informacyjnym - między receptorem a korelatorem, między korelatorem i organizatorem /homeostatem/ oraz między

korelatorem a efektorami.^{1/}

Przedstawione metody niszczenia energetycznego i informacyjnego stanowiły ofensywną /zaczepną/ stronę walki informacyjnej. Druga strona walki informacyjnej to strona defensywna /obronna/, która polega na obronie struktury własnej organizacji przed ofensywnymi działaniami przeciwnika. Ale żeby skonstruować adekwatny do występujących współcześnie zagrożeń system kontrwywiadowczej ochrony tajemnicy, należy przeanalizować cechy charakterystyczne współczesnej walki o informacje.

4. Cechy charakterystyczne współczesnej walki o informacje

Aby móc prowadzić walkę, musimy mieć możliwość wpływania nie tylko na strukturę własnego systemu KW ochrony, ale również na strukturę systemu wywiadowczego przeciwnika. Podobnie jak niszczenie przeciwnika przy użyciu środków energetycznych jest możliwe wówczas, gdy można przesłać energię do struktury przeciwnika /przeciwnik musi się znajdować w zasięgu naszej broni/, tak też prowadzenie walki informacyjnej /tzw. niszczenie informacyjne/ jest możliwe wówczas, gdy można przesłać odpowiednie sygnały sterownicze do struktury przeciwnika i

1/ Por. J. KOSSECKI, op.cit., s. 410 i 411

równocześnie odbierać komunikaty zawierające informacje dotyczące sytuacji w strukturze przeciwnika.

Inaczej mówiąc, jeżeli kontrwywiad chce prowadzić walkę informacyjną z wywiadem przeciwnika, musi dysponować odpowiednimi kanałami informacyjnymi między strukturą przeciwnika a strukturą własną, które umożliwiają jej odbiór informacji ze struktury przeciwnika oraz przesyłanie odpowiednich sygnałów do tej struktury.

Istnienie kanałów informacyjnych polega na utrzymywaniu łączności między odpowiednimi receptorami w strukturze przeciwnika /agenci obcego wywiadu, korespondenci środków masowego przekazu, członkowie przedstawicielstw dyplomatycznych, handlowcy, naukowcy, studenci, turyści/, a estymatorami w strukturze własnej /odpowiednie wydziały central wywiadu, rezydentury, organy kierujące działalnością środków masowego przekazu informacji nadających odpowiednie komunikaty/, które wysyłają sygnały sterownicze powodujące reakcje efektorów własnych. Sprawując kontrolę nad tymi kanałami lub mając do nich dostęp kontrwywiad ma możliwość zabezpieczenia się przed działalnością ofensywną przeciwnika.

Ponieważ planowane działania własne muszą być oparte na informacjach dotyczących przeciwnika, pierwszym etapem walki informacyjnej musi być walka o zdobycie wiadomości z jego wnętrza.^{1/}

W celu zdobycia informacji o przeciwniku, warunkiem koniecznym jest umieszczenie własnych receptorów /agentury/

1/ Por. J. KOSSECKI, op.cit., s. 414

w strukturze zwalczanego przeciwnika lub w otoczeniu bliskim jego struktury. Istotne jest więc znalezienie osób, za których pośrednictwem mogą "przenikać" potrzebne informacje, a następnie pozyskanie lub zmuszenie tych osób do ich systematycznego dostarczania. Najczęściej używa się przy tym bodźców o charakterze energetycznym, a więc szantażu, przekupstwa, bądź innych środków uzależnienia.

W trosce o interesy własne, wywiad jest szczególnie zainteresowany by u członków rozpoznawanej instytucji kształtować motywacje energetyczne głównie merkantylne, obliczone na stopniowe zanikanie norm etycznych, moralnych, prawnych. Im w większym stopniu oddziaływanie to obejmuje kadrę - tym większe możliwości powstają dla działania przeciwnika.^{1/}

Walka o zdobycie informacji dotyczących struktury przeciwnika idzie w parze z walką o ochronę analogicznych informacji w strukturze własnej. Po pierwsze, chodzi tu o uodpornienie ogólne własnej organizacji /własnego społeczeństwa, w tym armii/ na działania wywiadu przeciwnika. Polega to na wzmocnieniu norm związanych z motywacjami informacyjnymi, na których opiera się własna organizacja. Wzmocnienie powyższe następuje przez uodpornienie członków własnej struktury na motywacyjną atrakcyjność ofert służb specjalnych oraz przez podnoszenie poziomu etyczno-moralnego i świadomości prawnej ochraniających osób. Wywiad ma wówczas małe szanse pozyskiwania agentury w społeczeństwie, a równocześnie społeczeństwo samo pomaga kontrwywiadowi w wykrywaniu obcej agentury. Istotną

1/ Por., W. KOZACZUK, Bitwa o tajemnicę, Warszawa 1969 r. s. 124-130 i L. GONDEK, Działalność Abwehry na terenie Polski 1933-1939, Warszawa 1971r., s. 162

rolę w uodparnianiu na działalność przeciwnika odgrywa również szerokie zapoznawanie i wyczulanie społeczeństwa na formy i metody pracy wywiadów państw obcych.

Po drugie, chodzi o wykrywanie receptorów /agentury/ przeciwnika w strukturze własnej i ich likwidację.

By to osiągnąć należy:

- 1/ określić zainteresowania przeciwnika elementami ochronianej struktury, a więc wytypować właściwe podmioty i przedmioty KW ochrony;
- 2/ ustalić kanały dotarcia przeciwnika do wyselekcjonowanych podmiotów i przedmiotów ochrony we własnej strukturze;
- 3/ wprowadzić w te kanały własne receptory, które wykryją agenturę przeciwnika i uprzedzą jego działania.

W literaturze jako podstawowe metody walki o informacje między wywiadem a kontrwywiadem wymieniane są:

- 1/ "Uplasowanie" własnych agentów i ludzi zaufanych w służbie przeciwnika.
- 2/ "Odwrócenie" /przewerbowanie/ zdemaskowanych i ujętych agentów, przy pomocy których można przesyłać przeciwnikowi odpowiednią dezinformację.
- 3/ "Inspiracja" /podsunięcie/ przeciwnikowi fałszywych materiałów informacyjnych. Chodzi nie tylko o zmylenie lecz także o rozpoznanie jego metod pracy, powiązań z innymi podobnymi służbami, a także wykrycie agentów przeciwnika w strukturze własnej, którzy będą sprawdzać uzyskane "fałszywe" materiały. Obserwując więc drogi rozchodzenia się fałszywych informacji, możemy niekiedy ustalić tor informacyjny jego struktury.

4/ "Gra radiowa" polegająca na tym, że na własnym obszarze pozwala się działać wykrytym, lecz opanowanym przez siebie radiostacjom przeciwnika, utrzymując go w przekonaniu, że nadal pracują na nich jego ludzie. Nadchodzące depesze mogą wówczas dostarczać danych co do kierunków zainteresowań przeciwnika, niektórych metod pracy i innych spraw. Obecnie "gra radiowa" występuje dość rzadko, ze względu na rozwój innych środków łączności agent - ośrodek wywiadowczy. Niemniej, został on podany ze względu na możliwość wystąpienia tej metody na współczesnym polu walki oraz na pokazanie możliwości wykorzystania przechwyconych kanałów łączności agenta z ośrodkiem.^{1/}

Wymienione metody można uznać jako dążenie do przejęcia sterowania kanałami informacyjnymi przeciwnika. Są one w ten sposób nie tylko obroną informacji własnej, ale również dają możliwości pośredniego sterowania działaniami przeciwnika.

W epoce rewolucji informacyjnej /II połowa XX w./ wydajność procesów produkcji informacji nabiera coraz większego znaczenia we współzawodnictwie międzynarodowym. Podstawowe znaczenie ma tu problem tempa rozwoju rywalizujących państw. Dlatego też państwa wysoko uprzemysłowione optymalnie organizują własne procesy produkcji informacji, ale również hamują rozwój tych procesów u przeciwników lub potencjalnych konkurentów. Stanowi to istotny element walki informacyjnej. W tego rodzaju walce chodzi między innymi o to, aby zmuszać

1/ W. KOZACZUK, op.cit., s. 99

przeciwnika do przebywania dłuższej drogi postępu społeczno-gospodarczego, co wiąże się bezpośrednio z faktycznym osłabieniem jego mocy obronnej. Dlatego też z wojskowego punktu widzenia, przy analizie walki o informację, koniecznym jest uświadomienie metod utrzymywania wysokiego poziomu obronności.

Jedną z najskuteczniejszych metod osiągnięcia tego celu jest ochrona własnych, najbardziej wartościowych i najnowszych informacji i równoczesne serwowanie przeciwnikowi informacji przestarzałych - dotyczących dawniejszych etapów własnego rozwoju /np. sprzedanie przestarzałych licencji/.

Drugą metodą może być zrzeczne sugerowanie przeciwnikowi odpowiedniej, mało istotnej tematyki badawczej w celu "zamulenia" jego środków produkcji informacji. Jeżeli uda się ten cel osiągnąć, przeciwnik będzie zmuszony do ciągłego importu informacji. W tej sytuacji dla utrzymania prymatu wystarczy nawet opóźnienie eksportu informacji.

Zdobycie informacji o przeciwniku nie jest w tej walce celem, lecz ma ono umożliwić skuteczne niszczenie struktur przeciwnika, bądź też, co jest bardziej korzystne, sterowanie nimi.^{1/}

5. Dezorganizacja struktur państwowych strategicznym celem walki o informację

Dotychczasowe rozważania doprowadzają do wniosku ogólnego, że celem walki informacyjnej jest uzyskanie możli-

1/ Por. J. KOSSECKI, op.cit., s. 420

wości oddziaływania bądź sterowania strukturami przeciwnika. Niszcząc go informacyjnie nie tylko wprowadza się chaos organizacyjny ale utrudnia się możliwości prawidłowego sterowania tymi strukturami przez ośrodek kierowniczy. Jedną z form niszczenia informacyjnego jest dezinformacja.

Destrukcyjne efekty dezinformacji uzyskuje się przez:

- bezpośrednie przesyłanie informacji zmienionych czyli fałszywych;
- niszczenie norm poznawczych przeciwnika lub dezorganizując procesy w wyniku których te normy powstały.

Z powyższego wynika, że dezinformowanie należy uznać za rodzaj sterowania strukturą przeciwnika.

Dezinformacja bezpośrednia powodować będzie zmniejszenie skuteczności działania, natomiast dezinformacja pośrednia, niszcząc normy poznawcze, wpływa na spadek aktywności.

Do metod prowadzenia dezinformacji pośredniej można zaliczyć:

- niszczenie motywacji związanych z normami poznawczymi;
- niszczenie norm poznawczych;
- zmniejszenie wydajności procesów produkcji informacji.^{1/}

Niszczenie struktur przeciwnika jest osiągalne również poprzez tzw. dezorganizację właściwą. Jest to też forma sterowania strukturą przeciwnika, którą można realizować poprzez:

- dezorganizację bezpośrednią, polegającą na wysyłaniu bodźców, które wykorzystując normy istniejące w strukturze przeciwnika, wywołują u niego wzrost entropii, czyli zmniejszają stopień jego organizacji;

1/ Por. J. KOSSECKI, op.cit., s. 421

- dezorganizację pośrednią, polegającą na niszczeniu norm społecznych, na których opiera się struktura przeciwnika.

Metody dezorganizacji bezpośredniej polegać będą przede wszystkim na wysyłaniu lub inspirowaniu wysyłania przez kierownictwo przeciwnika sygnałów sterowniczych powodujących dezorganizację systemu oraz utrudnianiu wysyłania sygnałów sterowniczych, które mogłyby spowodować podwyższenie stopnia jego organizacji. Powyższe efekty można uzyskać przez :

- wysyłanie sprzecznych zarządzeń lub zarządzeń niezgodnych;
- wypaczanie słusznych koncepcji zawartych w zarządzeniach wydawanych przez kierownictwo przeciwnika.

Dezorganizację bezpośrednią można również prowadzić poprzez dokonywanie zmian w otoczeniu, na które musi odpowiednio reagować organizacja przeciwnika, co powoduje konieczność wprowadzenia odpowiednich zmian jego struktury, czyli wprowadzenia do własnej struktury odpowiednich informacji sterowniczych. Powyższe informacje wprowadza się przez podejmowanie odpowiednich decyzji w ośrodkach kierowniczych. Nie podjęcie na czas odpowiedniej decyzji powoduje automatycznie dezorganizację systemu zorganizowanego, który w nowej sytuacji nie może podjąć koniecznej działalności, gdyż uniemożliwia mu to utrzymywanie się starej struktury. Oczywiście, podjęcie błędnej decyzji może jeszcze bardziej zwiększyć stopień dezorganizacji. Jeżeli więc władze przeciwnika mają podjąć decyzję zwiększającą stopień jego organizacji, dezorganizację można uzyskać wówczas, gdy uda się nam maksymalnie wydłużyć czas

podejmowania decyzji oraz czas ewentualnego wprowadzenia jej w życie.

Ponieważ moc korelacyjna równa jest ilorazowi energii korelacyjnej i czasu: $K = E_k : t$, zatem zwiększając czas można uzyskać zmniejszenie mocy korelacyjnej nawet przy stałym potencjale energetycznym. Spadek mocy będzie odpowiednio większy, jeżeli niepodjęcie w odpowiednim czasie decyzji spowoduje dezorganizację określonej działalności.

Jeżeli ośrodek kierowniczy przeciwnika chce podjąć błędną decyzję, która wywołać może dezorganizację jego systemu, wówczas dezorganizacja bezpośrednia polegać będzie na maksymalnym skróceniu czasu decyzyjnego /wówczas K rośnie/. W ten sposób działa przede wszystkim "agentura energetyczna" przeciwnika, gdyż jest mało prawdopodobne świadome i celowe dezorganizowanie własnego systemu przez członków jego kierownictwa z innych przyczyn.

W ramach prowadzenia dezorganizacji bezpośredniej można również inspirować odpowiednią politykę personalną u przeciwnika. Chodzi o popieranie ludzi, którzy boją się podejmować odpowiednie decyzje lub podejmują w większości przypadków decyzje błędne. Nie muszą to być agenci wywiadu, ale agentura przeciwnika tych ludzi popiera, a jeśli ma możliwości, inspiruje decydentów do wyznaczania tego typu ludzi na stanowiska.

Dezorganizacja pośrednia polega na niszczeniu norm, na których opiera się struktura przeciwnika. Chodzi oczywiście o niszczenie norm związanych z motywacjami informacyjnymi,

czyli niszczenie u przeciwnika:

- norm poznawczych, wówczas zazębia się ona z dezinformacją pośrednią;
- norm ideologicznych, czyli prowadzenie dywersji ideologicznej;
- norm etycznych, czyli prowadzenie dywersji etycznej, demoralizacji zwalczanych społeczeństw oraz
- norm prawnych, czyli podważanie praworządności działania systemu przeciwnika;
- norm estetycznych, czyli wywieranie dezorganizacyjnego wpływu na całą psychikę ludzi;
- norm ekonomicznych, czyli przyczynianie się do obniżenia wydajności pracy oraz
- norm witalnych, czyli propagowanie szkodliwych dla zdrowia metod leczenia oraz lekarstw, co osłabia stan zdrowia ludzi u przeciwnika.

Najczęściej chodzi jednak o spowodowanie dominacji motywacji energetycznych związanych z krótkofalowo rozumianym interesem społecznym.

Wszelkie działania wchodzące w zakres zarówno dezinformacji jak i dezorganizacji, mogą być prowadzone przez odpowiednie kanały informacyjne - a więc przede wszystkim przez agentury dywersyjne /"agenci energetyczni"/ uplasowane w strukturze przeciwnika, a poza tym, przez środki masowego przekazu oddziałujące na przeciwnika, wreszcie przez "zwyyczajne" kontakty osobiste. Istotne znaczenie w walce informacyjnej ma umiejętność zasugerowania odpowiednich działań czy poglądów członkom organizacji przeciwnika. Duże znaczenie ma przy tym wywieranie wpływu na strukturę personalną przeciwnika.

Chodzi tu mianowicie o typowanie na stanowiska łączące się z możliwościami sterowania strukturą przeciwnika osób, na które można mieć wpływ oraz osób odznaczających się dominacją motywacji energetycznych skierowanych na własny interes a także osób, o których wiadomo, że będą podejmować błędne decyzje. Równocześnie należy wyłączyć z działalności osoby zdolne i ideowe, o wysokim poziomie wiedzy i wysokim poziomie etycznym. Najprostszym środkiem wiodącym do tego celu są intrygi personalne.

Analiza niektórych aspektów współczesnej walki informacyjnej prowadzi do wniosku ogólnego, że w procesie organizacji systemu kontrwywiadowczej ochrony tajemnicy należy uwzględnić te zagrożenia, z których mogą wynikać możliwości niszczenia informacyjnego przez przeciwnika ochranianej przez nas struktury. Należy zatem wypracować stosownie do możliwych zagrożeń metody przeciwdziałania dywersyjnym działaniom informacyjnym jakie może zastosować wobec nas przeciwnik.

R o z d z i a ł III

WYWIADOWCZA DZIAŁALNOŚĆ GŁÓWNYCH PAŃSTW
NATO W LATACH 1981 - 1985. KIERUNKI
ZAINTERESOWAŃ, FORMY I METODY DZIAŁAŃ
UKIERUNKOWANYCH NA OSŁABIEŃIE MOCY
OBRONNEJ SIŁ ZBROJNYCH PRL

1. Totalny charakter działań wywiadowczych

N A T O

Walka między państwami, na odcinku zdobywania obcych i ochrony własnych tajemnic wojskowych trwa od wieków. Szczególnie druga wojna światowa dostarcza wiele dowodów na to, jak poważne znaczenie posiada zabezpieczenie własnych tajemnic i zdobywanie na czas wiadomości o przeciwniku.

W drugiej połowie XX wieku działania wywiadowcze przybrały charakter totalny i mają postać "wojny mózgów".^{1/} Pochłaniają olbrzymie środki, ale równocześnie dostarczają czynnikom powołanym do wytyczania strategii i taktyki państw niewiarygodnej ilości informacji.

Z chwilą powstania państw socjalistycznych obóz kapitalistyczny zaczął dostosowywać struktury swoich tajnych służb do działań przeciwko nim. Prym w tej modernizacji wiodą Stany Zjednoczone Ameryki Północnej, których podstawowy trzon systemu wywiadowczego stanowią następujące służby:

1/ H. PIECUCH, Siedem rozmów z gen. dyw. Wł. Pożogą, Czytelnik, Warszawa 1987 r., s. 223

- Centralna Agencja Wywiadowcza /CIA/;
- Biuro Wywiadu i Badań Departamentu Stanu /BIR/;
- Agencja Wywiadowcza Ministerstwa Obrony /DIA/;
- Służba Wywiadowcza Sił Lotniczych /AIS/;
- Dowództwo Wywiadu Marynarki Wojennej /NIC/;
- Agencja Wywiadowcza Armii Lądowej /INTA/;
- Narodowa Agencja Bezpieczeństwa /NSA/;
- Krajowe Biuro Wczesnego Ostrzegania /NRO/;
- Komórka Wywiadowcza Departamentu Skarbu;
- Komórka Wywiadowcza w Urzędzie d/s Badań i Rozwoju Energii;
- Krajowy Zarząd Lotniczy i Kosmiczny /NASA/;
- Federalne Biuro Śledcze /FBI/.

Koordinacją działań tych służb zajmuje się Rada Bezpieczeństwa Narodowego /NSC/ podległa prezydentowi, a ostatnio w pewnym zakresie sztabowi doradczemu prezydenta.

Organami zajmującymi się działalnością wywiadowczą w Republice Federalnej Niemiec są:

- Federalna Służba Wywiadowcza /BND/;
- Federalny Urząd Ochrony Konstytucji /BFV/;
- Wojskowa Służba Ochronna /MAD/.

We Francji działalność wywiadowczą prowadzą:

- Dyrekcja Generalna Bezpieczeństwa Zewnętrznego /DGSE/;
- Zarząd Wywiadu Sztabu Generalnego oraz podporządkowane mu Drugie Biuro poszczególnych rodzajów wojsk;
- Dyrekcja Nadzoru Terytorialnego /DST/.

Wielka Brytania swoje służby wywiadowcze zorganizowała następująco:

- Tajna Służba Wywiadu /SIS lub MI - 6/;
- Dyrektoriat Generalny Wywiadu Wojskowego /DGI/;
- Rządowy Ośrodek Łączności /GCHO/;
- Kontrwywiad /DI - 5 lub MI - 5/;
- Zarząd Wywiadu Wojskowego;
- Oddział Wyspecjalizowany w Sabotażu i Pracy na Tyłach /SOE/;
- Lotniczy Sztab Informacyjny /AI/;
- Wywiad Marynarki Wojennej /NI/;
- Komórki Wywiadu i Kontrwywiadu przy Armii "REN".^{1/}

Wszystkie wymienione służby kierowały - i nadal to czynią - ostrze swoich zainteresowań na Siły Zbrojne PRL. Totalności i agresywności ich działań, prowadzonych na wysokim poziomie organizacyjnym i technicznym, przeciwdziałają organa kontrwywiadu Wojskowej Służby Wewnętrznej. Realizowane działania kontrwywiadu WSW opiera o zadania wynikające z profilaktyki kontrwywiadowczej w ramach trzech podstawowych, ściśle ze sobą powiązanych funkcji:

- przewidywania zagrożeń;
- uświadamiania w środowiskach wojskowych ich realności;
- ujawniania i eliminowania zjawisk sprzyjających tym zagrożeniom.^{2/}

Dla pełnej realizacji postawionych zadań oraz budowy optymalnych systemów kontrwywiadowczej ochrony tajemnicy niezbędna jest znajomość ogólnych założeń funkcjonowania służb wywiadowczych państw NATO.

1/ H. PIECUCH, op.cit, s.224 - 225

2/ E. BUŁA, Czas - nieodtworzalnym czynnikiem działania, Żołnierz Wolności nr 19 z dn. 25.01.1988 r.

2. Współczesne uwarunkowania ogólnych
założeń funkcjonowania wywiadów
państw NATO

Celem działalności wywiadowczej prowadzonej przez główne państwa NATO w stosunku do państw socjalistycznych jest osłabienie mocy obronnej oraz ekonomiki i życia społeczno-politycznego tych państw. Przeciwnik, poprzez tę działalność dąży przede wszystkim do rozsadzenia od wewnątrz ustroju socjalistycznego. Działalność ta ma charakter globalny i koalicyjny. Uwidacznia się to szczególnie w warunkach zaostrzenia sytuacji międzynarodowej. Mimo różnych wzajemnych tarć, a nawet sprzeczności interesów poszczególnych wywiadów państw kapitalistycznych, zauważa się współdziałanie, szczególnie wówczas, gdy mają podejmować akcje na niekorzyść krajów socjalistycznych.

Organy wywiadowcze państw NATO, a szczególnie USA, podążają kursem rządów swoich państw do zwiększenia naprężenia sytuacji międzynarodowej i uczestniczą w realizacji polityki wojennej konfrontacji. Usiłują przede wszystkim pokonać system środków obronnych, ukierunkowanych na zachowanie w tajemnicy, realizowanych w krajach socjalistycznych przedsięwzięć w zakresie doskonalenia zjednoczonych i narodowych sił zbrojnych oraz rozwijania nowych rodzajów uzbrojenia i techniki wojskowej.

Zaistniałe w ostatnich latach zmiany organizacyjne i strukturalne, a zwłaszcza utworzenie organów koordynujących w służbach specjalnych głównych państw NATO /USA, RFN,

W. Brytanii oraz Francji/, świadczą o dążeniu ich rządów do bezwzględnego podporządkowania działalności wywiadowczej i uczynienia z niej narzędzia dla realizowanej polityki.

Organom wywiadowczym stawiane są zadania zdobywania informacji z różnych dziedzin życia państw socjalistycznych. Dane te wykorzystuje się nie tylko do opracowywania planów strategicznych ale również do ekonomicznego zwalczania naszego systemu, podważania zaufania światowej społeczności do podejmowanych przez UW inicjatyw rozbrojeniowych oraz dyskredytacji naszych państw na arenie międzynarodowej.

Inspiratorem prowadzenia totalnej działalności wywiadowczej wobec państw UW jest administracja amerykańska. Z jej inicjatywy doszło do zacieśnienia więzi pomiędzy służbami specjalnymi NATO, utworzenia systemów wymiany informacji, włączenia do zbierania danych wywiadowczych instytucji państwowych oraz jednostek gospodarczych, utrzymujących kontakty z krajami socjalistycznymi.

Przetwarzaniu i wykorzystywaniu zbieranych w ten sposób danych sprzyja gwałtowny rozwój techniki na Zachodzie, a głównie wprowadzana powszechnie komputeryzacja. Okresowo służbom spec. NATO przedstawiane są priorytety ich działalności, określające główne zadania w zdobywaniu informacji w dziedzinie obronnej, polityczno-społecznej i ekonomicznej państw socjalistycznych. Między tymi płaszczyznami działań zachowane są odpowiednie proporcje na korzyść informacji o sprawach obronnych naszego systemu.

Wobec "pozornie" niskiej efektywności wywiadu agenturalnego w porównaniu do pozaagenturalnego /13% informacji wywiadow-

czych pochodzi od źródeł osobowych/^{1/} zdecydowano, kosztowną i wymagającą wysoko kwalifikowanej kadry, agenturalną działalność wywiadowczą prowadzić przede wszystkim w odniesieniu do instytucji, jednostek wojskowych oraz struktur mających istotne znaczenie dla obronności i polityki państwa. Dużą rangę w tym względzie nadano pozyskiwaniu tzw. źródeł perspektywicznych, mogących mieć w przyszłości dostęp do ważnych tajemnic.

Nie znaczy to, że przeciwnik odstąpił od werbunku osób mniej wartościowych, nie mających bezpośredniego dotarcia do tajemnic źródłowych, szczelnie przechowywanych w sejfach i chronionych przez cały system przedsięwzięć zabezpieczających. Dokonuje on nadal werbunków osób zamieszkałych lub zatrudnionych wokół ważnych obiektów wojskowych, tworząc bazę tzw. agentury sygnalizacyjnej oraz osób zamieszkujących na kierunku działań operacyjnych naszych wojsk, tworząc bazę tzw. agentury strefowej.

Czyni to również w stosunku do osób, nie stwarzających w okresie pokoju potencjalnego zagrożenia dla systemu obronnego naszego państwa. Podstawowym celem tego rodzaju działalności jest przede wszystkim wiązanie naszych sił oraz rozpoznawanie form i metod pracy operacyjnej służb specjalnych państw UW.

W chwili obecnej wywiad spełnia trzy podstawowe funkcje:

- informacyjną, czyli zbieranie i opracowywanie informacji dotyczących spraw militarnych, politycznych, gospodarczych itp. innych państw;

1/ S. RAKOWSKI, Organizacja służb wywiadu i kontrwywiadu Departamentu Obrony USA, Biuletyn Szefostwa WSW nr 1/69, styczeń - marzec 1980 r., s. 79.

- ochrony, czyli kontrwywiadowcze zabezpieczenie własnej działalności oraz rozpoznawanie metod i środków pracy służb specjalnych przeciwnika;
- realizacji zleconych przez rząd państwa, na którego rzecz wywiad działa, misji specjalnych w zakresie dywersji politycznej, sabotażu, dezinformacji itp.^{1/}

3. Główne kierunki i formy działalności służb wywiadowczych państw NATO na ZTDW

Rządzące kręgi państw NATO aktywizują działalność swoich służb specjalnych, stawiając przed nimi wciąż nowe zadania w dziedzinie systemowego rozpoznania państw Układu Warszawskiego. Przedmiotem zainteresowania obcych wywiadów są w zasadzie wszystkie kierunki życia bloku wschodniego. Największą rangę jednak nadaje się nadal zdobywaniu informacji o sytuacji militarnej.

Do pierwszoplanowych zadań w tej dziedzinie przeciwnik zalicza uzyskiwanie informacji o planach strategicznych i operacyjnych, zadaniach i kompetencjach najwyższych organów kierownictwa wojskowego UW, koncepcjach prowadzenia działań bojowych przeciwko siłom NATO przez blok wschodni - na jednym lub kilku teatrach działań wojennych.^{2/}

Na liście wywiadowczych priorytetów coraz ważniejsze

1/ S. HOC, Zagadnienie szpiegostwa i wywiadu w systemie polityczno-prawnym RFN, s. Przegląd Stosunków Międzynarodowych, Opole 1979 r., nr 5/83, s. 75

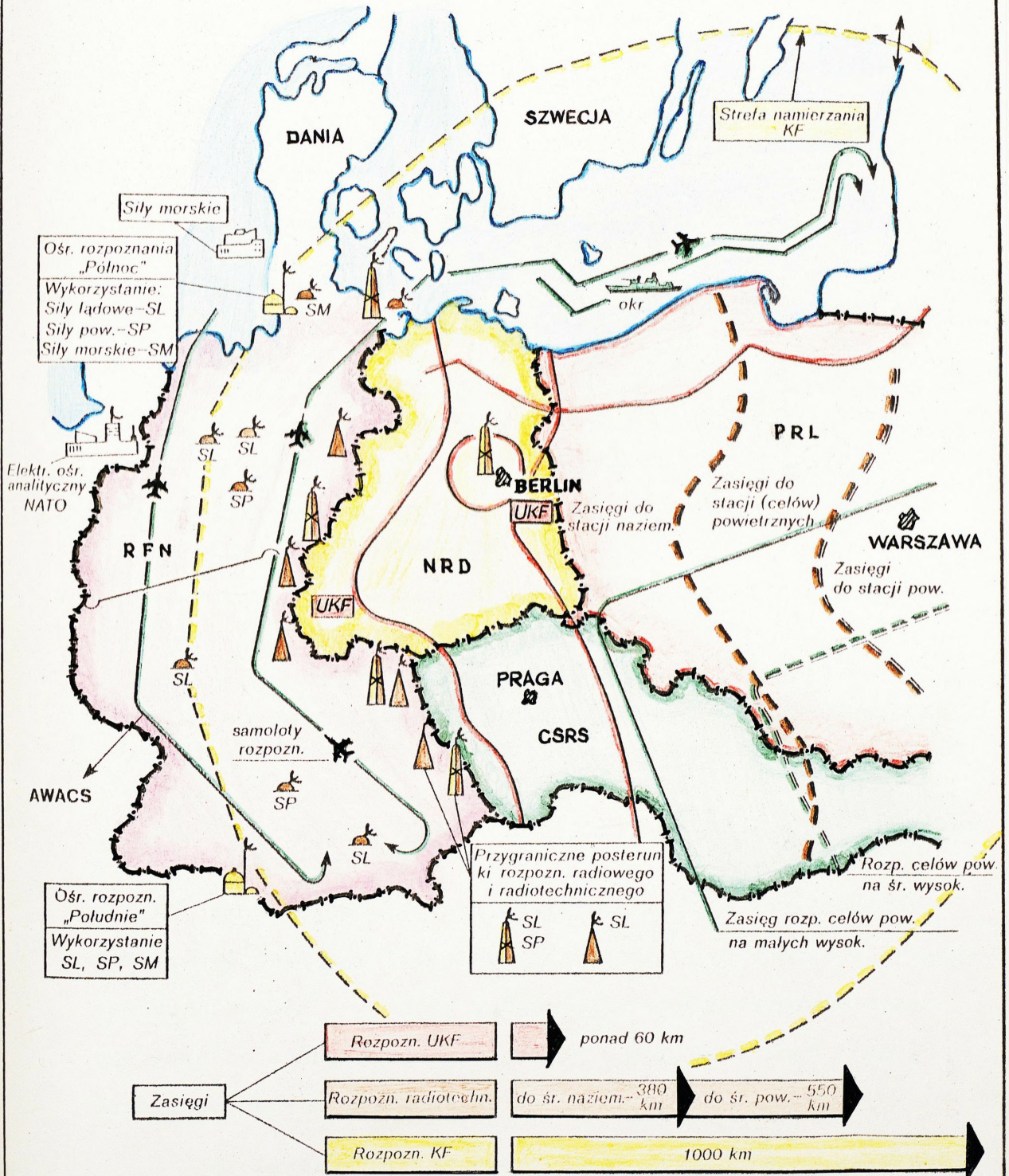
2/ Informacja Szefostwa WSW Nr DB-01414/35 z 27.06.85 r., s. 2 i dalsze.

miejsce zajmuje informacja niezbędna dla organów planistycznych NATO. Szczególne zainteresowania koncentrują na systemach dowodzenia, łączności. Siły Zbrojne UW a w tym Siły Zbrojne PRL poddawane są systematycznemu rozpoznawaniu przez środki radioelektroniczne państw NATO. Możliwości tego rozpoznania przedstawia schemat na stronie 87a.

W zainteresowaniu problematyką militarną Polski dominują:

- a/ informacje odnoszące się do ewentualnych działań wojennych w skali NATO - Układ Warszawski, a w tym:
- możliwości wykonania przez Wojsko Polskie zadań przydzielonych w planach ataku na NATO;
 - stanu gotowości polskich Sił Zbrojnych oraz wpływu różnych czynników na jego poziom /np. braki w zaopatrzeniu/;
 - planów obrony cywilnej, stanu schronów miejskich i w zakładach pracy;
 - lokalizacji alternatywnych stanowisk dowodzenia, miejsc ewakuacji władz, systemu ochrony kierownictwa partii i rządu;
- b/ dane odnoszące się do stanu polskiej produkcji obronnej, zwłaszcza:
- struktura organizacyjna zakładów o tym profilu produkcji;
 - miejsce i rola radzieckich specjalistów wojskowych przebywających w zakładach na terenie Polski;
 - zamówienia sprzętu wojskowego w PRL przez kraje trzecie, ich realizacja, spłaty;
 - zakupy niektórych podzespołów w firmach zachodnich;
 - wyposażenie elektroniczne - poziom urządzeń w porównaniu z Zachodem;

MOŻLIWOŚCI PROWADZENIA ROZPOZNANIA RADIOELEKTRONICZNEGO PRZEZ
SIŁY ZBROJNE NATO



- systemy noktowizyjne i laserowe;
 - wszystkiego typu urządzenia radarowe;
 - ogół danych o broniach chemicznych
- /zagadnieniu temu nadano szczególną rangę w ostatnim okresie, a wzmożoną aktywność w tym kierunku przejawia zachodnioniemiecka BND/.^{1/}

Rozpatrując powyższe w kategoriach strategicznych można uogólnić, że informacje zbierane przez wywiad przeciwnika służą przede wszystkim do:

- planowania strategicznego przez wojska NATO, określenia celów uderzenia, ujawniania nowych rodzajów broni oraz ustalania symptomów gotowości bojowej;
- określenia jednolitej płaszczyzny politycznej w stosunku do państw socjalistycznych;
- prowadzenie określonej polityki ekonomicznej wobec członków RWPG;
- wypracowania doktryn mających na celu "urabianie" polskiego społeczeństwa w stosunku do Zachodu oraz oddziaływanie na określone środowiska, które prowadziłyby działania destrukcyjne.

Formy i metody działań

Zachodzące w ostatnich latach zmiany spowodowane gwałtownym postępem technicznym Zachodu oraz wzrostem wymiany osobowej Wschód - Zachód, spowodowały wypracowywanie coraz skuteczniejszych, trudniejszych do ujawnienia form i metod działania obcych wywiadów.

Szczególny nacisk położono na doskonalenie szkolenia

1/ Informacje Szefostwa WSW nr DB-00220/3 z 10.02.1986r., s.2-3 i nr DB-001921/35 z 14.11.1983 r., s.1-6

agentów, organizowanie trudnych do ujawnienia sposobów przekazywania informacji oraz kierowanie pracą agenta. Obecnie dominują następujące rozpoznane przez kontrwywiad WSW formy i metody działania obcych służb specjalnych:

a/ Typowanie kandydatów na agentów

Odbywa się najczęściej drogą rozmów indagacyjnych z osobami wyjeżdżającymi na Zachód oraz wykorzystywania utrzymywanych przez cudzoziemców /w tym również dyplomatów z KK/ kontaktów prywatnych i służbowych z naszymi obywatelami.

b/ Opracowanie kandydata do werbunku

W zależności od pozycji kandydata, przewidywanych dla niego zadań oraz sytuacji operacyjnej, opracowanie kandydata do werbunku może trwać nawet do kilku lat. W tej fazie działań wywiad dąży głównie do zebrania o kandydacie danych charakterologicznych, jego sytuacji rodzinnej, przyzwyczajzeń i zainteresowań. Informacje te ocenia między innymi pod kątem wypracowania podstawy i sposobu planowanego werbunku.

c/ Werbunek do współpracy

Może być stopniowy lub jednorazowy - ten ostatni realizowany jest najczęściej wobec oferentów lub osób, w stosunku do których zebrano materiały obciążające lub kompromitujące. Nie zawsze praktykowane jest przyjmowanie jakichkolwiek zobowiązań pisemnych. Notowane są przypadki /szczególnie w stosunku do osób zajmujących eksponowane stanowiska/ werbowania do współpracy bez określania w pierwszej jej fazie konkretnych warunków bądź uzgadniania zadań i sposobu ich realizacji. Często, tuż po zwerbowaniu osoby, nie

zleca się jej poleceń. Dopiero po upływie pewnego czasu po przekonaniu się, że nowo zwerbowany agent nie pozostaje pod kontrolą naszych służb kontrwywiadowczych, uruchamiana jest z nim współpraca. Regułą obcych wywiadów jest dokonywanie werbunków naszych obywateli poza terytorium Polski, najczęściej w krajach Europy Zachodniej. Przypadki werbowania na terenie ambasad państw NATO, akredytowanych w PRL, notowano jedynie wobec oferentów. W trakcie werbunku, szczególnie Amerykanie, stosują kontrolę szczerości kandydata za pomocą badań wariograficznych. W przypadku negatywnych wyników, badania są powtarzane, po czym - jeśli wynik pozostaje bez zmian - z reguły odstępuje się od werbunku.

d/Szkolenie agentów

Zakres szkolenia uzależniony jest od przewidywanych zadań, wyposażenia wywiadowczego oraz uplasowania. Obejmuje ono zagadnienia dotyczące problematyki zbierania, opracowywania oraz przekazywania informacji oraz inne, np. wydatkowanie wynagrodzeń, postępowanie w sytuacjach awaryjnych, zagrożenia bezpieczeństwa itp. Może być prowadzone jednorazowo, np. przed przerzutem agenta do Polski bądź cyklicznie - w trakcie odbywanych z nim spotkań. Odbywa się ono przeważnie na terenach państw zachodnich /w ośrodkach wywiadowczych bądź lokalach konspiracyjnych/.^{1/} W stosunku do oferantów wstępny instruktaż może być udzielony w placówkach dyplomatycznych bądź innych umówionych miejscach.

1/ Informacja MSW nr 00604/84 - dot. działalności agentów CIA, Jurzaka i Adamaschka, s.23.

e/ Kierowanie pracą agentów

Aktualnie wywiady NATO coraz częściej stosują zasadę zlecenia zadań agentom w ramach ich możliwości wpływających z życia służbowego bądź towarzyskiego.^{1/} Celem takiego postępowania jest przede wszystkim zapewnienie im większego bezpieczeństwa. Na początku współpracy stopień trudności zadań jest niewielki, co podyktowane jest potrzebą oswojenia agentów z realizacją zadań, sprawdzenia szczerości i ich operatywności w działaniu:

- Stosuje się dwa rodzaje łączności z agentami:
 - osobową /kontakt pracownika wywiadu bezpośrednio z agentem bądź przez osobę łącznikującą/ oraz
 - bezosobową /jednostronną, agent - centrala lub centrala - agent oraz dwustronną: centrala - agent - centrala/.

W łączności bezosobowej wykorzystuje się:

- łączników - wykorzystywani świadomie bądź nieświadomie;
- kontenery;
- sprzęt radiowy z dostosowanymi do niego przystawkami umożliwiającymi odbiór audycji wywiadowczych;
- znaki umowne;
- tajnopisy;
- sprzęt komputerowy, wideokasety;
- mikropunkty.

Wybór sposobu łączności uzależniony jest od możliwości naturalnych wyjazdów agenta za granicę, zakresu zleconych mu zadań oraz stopnia wykształcenia. Najczęściej uzgadniany

1/ Tamże, s. 17-20

jest zasadniczy rodzaj łączności oraz dodatkowy - uruchamiany w sytuacjach awaryjnych. W miarę upływu czasu współpracy, wywiad wyposaża agenta w bardziej doskonały i kosztowniejszy sprzęt łączności. Zmiany te czynione są przede wszystkim w celu usprawnienia przekazywania informacji oraz zapewnienia agentowi większego bezpieczeństwa. Dąży się, aby wyposażenie służące do łączności wywiadowczej, nie różniło się w wyglądzie zewnętrznym od sprzętu krajowej produkcji.

Podjęmowanie i składanie kontenerów służących do przekazania informacji oraz przejęcie instrukcji i wynagrodzenia wykonują najczęściej pracownicy rezydentur wywiadowczych uplasowanych w placówkach dyplomatycznych państw zachodnich. Każdej takiej operacji towarzyszą działania pozoracyjne, mające na celu odciążenie uwagi naszych służb bezpieczeństwa, np. ściąganie sił kontrwywiadu poza teren akcji, pozorowanie penetracji obiektów wojskowych itp.

Natomiast przy przyjmowaniu informacji wywiadowczych od agenta posługującego się miniaturowym przekaźnikiem, pracownicy rezydentur stosują kontrolę pracy w eterze środków radiowych i kontrobserwację /za agentem lub pracownikiem wywiadu/;

- organizowanie spotkań wywiadowczych

Do bezpośredniego kontaktu z agentem, służby specjalne NATO przywiązują dużą wagę. Stąd też dążą one do tego, aby co pewien okres nastąpiła bezpośrednia styczność pracownika wywiadu z agentem. Spotkania umawiane są najczęściej podczas pobytu wykorzystywanej do współpracy osoby na

Zachodzie, a w przypadku niemożliwości takiego wyjazdu - w krajach demokracji ludowej. Prócz dokonywanego w trakcie jego trwania szkolenia agenta i stawiania zadań, sprawdza się również jego szczerość - do czego wykorzystuje się najczęściej wariograf^{1/} oraz stosuje kontrobserwację^{2/}, na przykład podczas dojścia agenta do miejsca spotkania i odejścia.

W przerwach, między bezpośrednim kontaktem, może być wykorzystywana łączność bezosobowa;

- wiązanie agenta do współpracy

Prócz wynagrodzenia za przekazane informacje, wywiady NATO stosują inne formy mające na celu wytworzenie więzi agenta z prowadzącym go pracownikiem. Działania te oparte są najczęściej o sferę życia prywatnego i mają na celu stwarzanie pozorów przyjaźni, np. prezenty imieninowe, przekazanie potrzebnych lekarstw, zakup sprzętu pomocnego do rozwijania zainteresowań osobistych itp.

Inną formą zdobywania przez wywiady NATO informacji są penetracje interesujących ich terenów bądź obiektów /w tym również wojskowych/. Najczęściej dokonują ich dyplomaci oraz ukierunkowani na zdobycie określonych danych cudzoziemcy z KK. Prowadzona może być ona drogą obserwacji wzrokowej bądź wizualnej, z wykorzystaniem sprzętu technicznego /środki do kontroli rozmów radiowych, urządzenia filmujące i inne środki techniczne ułatwiające obserwację itp./.

1/ Tamże, s.12-14

2/ Informacja Szefostwa WSW nr DB-0720/3 z 10.04.1987r. dot. form i metod działalności CIA, s. 3 i 5

Współdziałanie służb wywiadowczych NATO

Narastającemu zbliżeniu politycznemu, ekonomicznemu oraz społecznemu państw zachodnich towarzyszy również nadawanie coraz większej rangi współdziałaniu służb specjalnych. Proces współdziałania organizowany jest w dwóch płaszczyznach:

- wewnętrznej, dot. ścisłej koordynacji działań i wymiany informacji służb spec. danego państwa;
- zewnętrznej, w ramach paktu wojskowego NATO, a niejednokrotnie wychodzący poza ten układ.

Niemal każdorazowo w trakcie "szczytu" szefów rządów NATO podejmowane są tematy i wypracowywane decyzje odnośnie koordynacji działań służb specjalnych Paktu Północnoatlantyckiego. Wiodącą rolę w tym względzie odgrywają służby specjalne USA, z których inspiracji dochodzi do wzajemnych spotkań roboczych na szczeblu szefów wywiadu i kontrwywiadu w celu omawiania efektów współdziałania i podpisywania wzajemnych umów roboczych.

Na podstawie tych spotkań i porozumień współdziałaniem objęto:

- przeszkalanie kadr;
- pozyskiwanie i wymianę wyposażenia operacyjno-technicznego;
- wykorzystywanie wzajemne zainstalowanych systemów informacyjnych;
- regularną wymianę informacji i doświadczeń;
- organizowanie i realizowanie wspólnych akcji wywiadowczych;
- koordynację propagandy przeciwko państwom socjalistycznym.^{1/}

1/ Informacja Zarządu III Szefostwa WSW nr DB-01342/35
z 14.06.1985 r., s. 1-3

Na najbliższe lata służby spec. NATO uzgodniły między sobą następujące dyrektywy współdziałania:

- stopniowe zamykanie kanałów informacyjnych pracownikom przedstawicielstw dyplomatycznych i handlowych państw socjalistycznych na Zachodzie;
- wspólne działania propagandowe w wypadkach wydalania obywateli państw socjalistycznych podejrzanych o prowadzenie działalności wywiadowczej, ze wskazaniem dla opinii publicznej zagrożenia z tego tytułu dla innych dziedzin życia państwowego;
- stopniowe zmniejszanie liczby personelu przedstawicielstw dyplomatycznych i handlowych państw socjalistycznych;
- organizowanie wspólnych akcji prowokacyjnych przeciwko personelowi placówek państw socjalistycznych;
- wzajemne informowanie o ujawnionych pracownikach służb specjalnych państw socjalistycznych i metodach ich działania;
- wykorzystywanie przedstawicielstw handlowych i wywiadowczych /działających pod przykryciem/ do zbierania danych o państwach socjalistycznych;
- podziału zadań, koordynacji działań i wymiany informacji na szczeblu rezydentur wywiadowczych działających w krajach socjalistycznych;
- wykorzystanie turystyki międzynarodowej do prowadzenia działań wywiadowczych;
- koordynacji działań indagacyjnych, realizowanych w obozach dla uchodźców.^{1/}

W celu koordynacji działań wywiadowczych wszystkich placówek dyplomatycznych państw NATO w Polsce, rolę inspiratora i funkcję organizacyjną przejęła ambasada USA. Odbywają się regularne spotkania i narady dyplomatów. Mają one róż-

1/ Tamże, s. 2

nicowany charakter - od wzajemnych konsultacji kierowników placówek, do spotkań attache wojskowych. W czasie narad - oprócz wymiany informacji i prezentacji poglądów na tematy aktualnych spraw polskich - uzgadniane są również wspólne przedsięwzięcia i stanowiska. Dużą operatywność w tym zakresie wykazuje w ostatnim okresie ambasada Francji.^{1/}

4. Wywiad agenturalny. Pozyskiwanie bazy informacyjnej

W działalności werbunkowej wśród obywateli krajów socjalistycznych służby specjalne NATO nastawiają się głównie na pozyskiwanie tzw. agentury perspektywicznej, która może zająć wysokie stanowiska partyjne i państwowe.

Najaktywniejszą działalność werbunkową obce wywiady prowadzą na terytoriach swoich państw oraz w krajach rozwijających się, które charakteryzuje słabość reżimów politycznych oraz zależność ekonomiczna od państw NATO. Elementy te sprzyjają aktywnej działalności werbunkowej naszych obywateli przebywających służbowo w tych krajach.

Natomiast w odniesieniu do amerykańskiego wywiadu, aktywność werbunkowa kształtuje się według następującej kolejności: terytoria krajów rozwijających się i zaprzyjaźnionych z USA państw kapitalistycznych oraz terytorium własne.

Jako sporadyczne mają miejsce przypadki dokonywania

1/ Informacja Zarządu III Szefostwa WSW nr DB-0321/5 z 24.02.82 r., s. 4-5.

werbunków na obszarze państw socjalistycznych. Dotyczy to głównie tzw. "samorodków" oferujących obcemu wywiadowi swoje usługi w zamian za korzyści materialne.

Służby specjalne NATO zbierają szczegółowe dane ustaleniewe i charakterologiczne odpowiedzialnych pracowników wywiadu, MSZ, MSW, MON, różnego rodzaju organizacji i instytucji handlu zagranicznego, instytutów naukowych i uczelni krajów socjalistycznych. Szczególną uwagę zwraca się na pracowników sztabów generalnych oraz kadre oficerską państw Układu Warszawskiego. Prócz tego, prowadzone są dokładne rozpracowania pracowników przedstawicielstw dyplomatycznych, handlowych oraz innych przedstawicielstw zagranicznych krajów socjalistycznych.^{1/}

Najbardziej podatnymi na współpracę z obcym wywiadem - według ocen służb specjalnych przeciwnika - są osoby:

- niezrównoważone psychicznie;
- o słabo wykształconych więziach etnicznych, narodowych, kulturowych;
- będące pod wpływem strachu, rozpacz, nienawiści lub narzuconych im idei.

Są to osoby stanowiące niejako bazę, z której wywiad przeciwnika typuje, opracowuje i werbuje agentów. Przedstawiając sprawę inaczej można stwierdzić, że aby zaistniał fakt zwerbowania osoby przez obcy wywiad, muszą na ogół zaistnieć następujące warunki:

- wywiad musi mieć dotarcie informacyjne do danej osoby;

1/ Informacja Zarządu III Szefostwa WSW nr DB-0752/35 z 11.05.1984r., s.1-2.

- osoba ta winna być atrakcyjna /ze względu na wykonywany zawód lub kontakty, pozycję społeczną itp./ dla przeciwnika tzw. osoba perspektywna;
- musi ona przebywać w którymś z krajów kapitalistycznych;
- muszą wystąpić dodatkowe okoliczności umożliwiające proces zwerbowania danej osoby /kłopoty finansowe, wykroczenia etyczno-moralne, załamania psychiczne, niepowodzenia w pracy itp./.

W indywidualnych przypadkach mogą wystąpić odstępstwa od tych zasad, lecz ogólnie kryteria te należy uznać za obowiązujące.

Do wykonywania zadań wśród przebywającej na Zachodzie Polonii, związanych z łącznikowaniem bądź wyposażaniem agenta, mających na celu zebranie danych charakterologicznych, potwierdzenia fragmentów uzyskanych wcześniej informacji, wywiady przeciwnika wykorzystują agentów pozyskanych najczęściej z emigracji, w tym tej najnowszej - z lat 80-tych.

Okres opracowania kandydata do werbunku dzieli się na cztery etapy:

I etap - nawiązanie wstępnego kontaktu

W większości przypadków następuje w czasie przyjęć dyplomatycznych lub innych oficjalnych imprez protokolarnych. W tym stadium nie stwierdza się z reguły prowadzenia rozmów politycznych. Obserwuje się natomiast duże zainteresowanie ogólnymi danymi biograficznymi, stopniem zadowolenia z pracy, warunkami życiowymi, sytuacją rodzinną, hobby oraz planami na najbliższą przyszłość. Głównym celem takiej rozmowy - a czasami kilku rozmów, jest sprawdzenie oraz uściślenie posiadanych

już przez wywiad informacji.

II etap - przekwalifikowanie kontaktu na stopę "przyjacielska"

Pracownik prowadzi odtąd samodzielne rozpracowanie werbunkowe kandydata. Dąży on do pogłębienia kontaktów z rozpracowywaną osobą, wykorzystując w tym celu ustalone wcześniej zainteresowania i skłonności obiektu. Przechodzi do konspiracji spotkań, co tłumaczy troską, aby obiekt nie został skompromitowany.

W etapie tym wypracowuje się także podstawę werbunku oraz przyzwyczajają się kandydata do przyjmowania prezentów, udzielane jest wsparcie finansowe itp.

III etap - charakteryzuje się przejściem do spotkań "przyjacielskich" do konkretnej współpracy

Na tym etapie szczególną uwagę zwraca się na sprawdzenie szczerości opracowywanej osoby. Pracownicy wywiadu domagają się pokwitowań za przekazane wynagrodzenia lub innych pisemnych dowodów powiązań z wywiadem. Spotkania odbywają się przy zachowaniu pełnej konspiracji.

IV etap - werbunek kandydata oraz organizowanie jego aktywnej współpracy

Przed werbunkiem wypracowywane są podstawy werbunku oraz taktyka prowadzenia rozmowy werbunkowej.^{1/}

Prócz przedstawionego stopniowego angażowania osoby do współpracy z obcym wywiadem notowane są inne sposoby, jak na przykład:

1/ Tamże, s. 3-5

- werbunek z marszu - stosowany wówczas, kiedy interesująca wywiad osoba znalazła się nagle w trudnej sytuacji lub też wyraziła dobrowolnie chęć przekazania posiadanych przez nią informacji;
- zamaskowana propozycja werbunkowa - osoba werbująca występuje w roli pracownika naukowego, kolegi posiadającego tę samą specjalizację itp. Rozpracowanie następuje w trakcie dyskusji i wymiany poglądów. Osoba rozpracowywana proszona jest o napisanie, za wynagrodzeniem, książki, artykułu, udzielenie konsultacji itp. Stopniowo charakter prośby komplikuje się i podwyższa proponowane wynagrodzenie. Jednocześnie kontakty z osobą stają się coraz bardziej zakonspirowane.

Wszyscy nowo zwerbowani agenci przechodzą intensywne szkolenie. W trakcie którego kładzie się nacisk na przyswajanie nawyków potrzebnych przy konspiracyjnych metodach łączności. W toku pracy z agenturą, tajność działania podlega systematycznej kontroli.

5. Wywiad pozaagenturalny i jego możliwości w pozyskiwaniu informacji

Pewne uwarunkowania wpływające z gwałtownego rozwoju w państwach NATO elektroniki i informatyki spowodowały, iż wywiadowi pozaagenturalnemu przeciwnik nadaje obecnie duże znaczenie.

Elementami wywiadu pozaagenturalnego są:

- satelity szpiegowskie - wywiad satelitarny;
- organizacje zajmujące się indagacją i ankietowaniem uciekinierów i osób emigrujących z państw socjalistycznych;
- stacje przechwyty łączności i rozpoznania radiolokacyjnego;
- ośrodki i instytuty badań Europy Wschodniej.

W ramach ukierunkowania wymienionych elementów wywiadu pozaagenturalnego na kraje Układu Warszawskiego, prowadzone jest również - przy ich wykorzystaniu - rozpoznanie naszego kraju, w którym przede wszystkim wykorzystuje się:

- Wywiad satelitarny

Element ten wykorzystywany jest głównie przez Stany Zjednoczone, które począwszy od 1959 r. wprowadzają na orbitę coraz nowsze typy tych urządzeń. Ostatnio, satelity o nazwie KH-11, krążące po orbitach odległych od Ziemi od 40 do 60 km pozwalają na rozpoznanie obiektów znajdujących się na powierzchni Ziemi - o wymiarach od 15 do 30 cm.

Ponieważ w razie konfliktu zbrojnego zakłada się - jako działanie pierwszoplanowe - niszczenie szpiegowskich obiektów kosmicznych, Stany Zjednoczone wprowadzają aktualnie na orbity satelity o nazwie "DARK", które ze względu na odległość od Ziemi /sięgającą około 1000 km/ są bezpieczne przed atakiem środków radzieckich.

Również do prowadzenia rozpoznania z powietrza wykorzystuje się wywiadowcze samoloty /modele U-2 i SR-71/, których pułap lotu sięga 40-50 km a prędkość rzędu 4 macha.^{1/}

1/ Informacja Zarządu III Szefostwa WSW nr DB-2701/5 z 23.12.1981 r., s.2-7

- Urzędy i organizacje indagacyjne

W ramach porozumień między służbami specjalnymi państw Zachodnich /wykraczających w niektórych przypadkach poza państwa "siódemki"/, w obozach dla uchodźców z krajów socjalistycznych znajdują się wyspecjalizowane agendy zajmujące się indagacją i ankietowaniem kwaterowanych tam osób.

Działaniami tymi zajmuje się obecnie m.innymi:

- 18 batalion wywiadu wojskowego Armii USA; stacjonuje w Monachium - miasteczko wojskowe "Koszary Mc Graw".

Jego ogniwa organizacyjne znajdują się m.innymi w: Giessen, Maine, Zirnsdorf - Rottenburgerstrasse 29, Berlin Zach. - Marionfeldstrasse 56-80, Monachium - "Koszary Mc Graw";

- pododdział wywiadowczy 66 grupy wywiadu wojskowego.^{1/}

W ogniwach tych zatrudnione są osoby znające na ogół język, realia życia oraz sytuację w krajach socjalistycznych. Mają one dostęp do banków informacji, co pozwala im w miarę szybko ustalić szczerść indagowanej lub ankietowanej osoby.

Inną formą ankietowania osób z państw socjalistycznych, spotykaną obecnie coraz częściej, jest przesyłanie na adresy uciekinierów lub emigrantów zaproszeń do przybycia w wyznaczone miejsce celem udzielenia informacji o opuszczonej ojczyźnie. Zapraszonym zapewnia się jednocześnie zwrot kosztów podróży, wyżywienie oraz usprawiedliwienie w pracy. Na formularzach zapraszających podaje się m.in. następujące nazwy ośrodków: "Instytut d/s Ochrony Tajemnicy

1/ Informacja Zarządu III Szefostwa WSW nr DB - PF-1103/3 z 30.06.1987r., s. 1 i 5

Państwowej w RFN" mieszczący się w Dusseldorfie, Immalmanstrasse 11; "Amerykańskie Regionalne Biuro Komitetu Koordynacyjnego Sprzymierzonych Sił Zbrojnych" - Monachium, Sintperstrasse 42.^{1/}

- Stacje przechwyty łączności i rozpoznania radiolokacyjnego

Głównymi instytucjami zajmującymi się całodobowym przechwytem radiotelefonicznych i dalekopisowych linii łączności państw Układu Warszawskiego /a w tym również Polski/ jest Augsburgska Stacja Polowa Armii USA oraz Berlińska Stacja Polowa Armii USA.

Stan osobowy ASP wynosi 4 tysiące oficerów i żołnierzy. Sztaby i służby operacyjne stacjonują w Hoiling i Gasthoren /przedmieście Augsburga/, poszczególne służby sztabu oraz koszary stanu osobowego znajdują się w Augsburgu w miasteczku wojskowym "Koszary Sheridana". Natomiast liczebność BSP wynosi około 1000 osób. Służby dyżurne i operacyjne stacji mieszczą się w dzielnicy Grünwald, na górze Teufelsberg.

Prócz prowadzonego podsłuchu, stacje te zajmują się analizowaniem i gromadzeniem zdobytych danych.^{2/}

Państwa NATO, a głównie Stany Zjednoczone, dysponują także szerokim arsenałem elektronicznym środków rozpoznawczych. Terytoria państw socjalistycznych otoczone są pierścieniem namiarowych stacji radiowych wysokiej częstotliwości i stacji radarowych. Namierniki radiowe pracujące

1/Tamże, s. 2 i 3

2/Tamże, s. 7 i 11

w pełnym zakresie częstotliwości, nagrywają niemal każde słowo, emitowane w ster przez państwa UW. Podlegają one natychmiastowej analizie komputerowej pod kątem określenia stanu gotowości bojowej poszczególnych rodzajów sił zbrojnych Bloku Wschodniego.^{1/}

- Ośrodki i instytuty badań Europy Wschodniej

Okres po II wojnie światowej, to czasy coraz szybszego rozwoju badań slawistycznych. W krajach zachodnich powstało kilka grup instytucji zajmujących się problemami państw socjalistycznych /np. "Instytuty Sowieologii", "Ośrodki Sowieologiczne", "Instytuty Wschodnie", "Ostforschung" - RFN i Austria/, ale decydujące znaczenie w każdym z nich ma niewielka grupa instytutów związanych z czynnikami rządowymi, które prowadzą badania interdyscyplinarne i otrzymują na nie rządowe zamówienia.

Struktura tematyczna badań nad komunizmem świadczy dobitnie o usługowym charakterze tych placówek. Istnieje rodzaj sprzężenia zwrotnego między działalnością placówek a praktyką polityczną. Zapotrzebowanie ośrodków wywiadowczych określa ich kierunki badawcze, dzięki czemu zyskują one z kolei, możliwość współuczestniczenia w kształtowaniu strategii i taktyki wobec państw socjalistycznych, Zaznacza się coraz wyraźniej korelacja pomiędzy ośrodkami władzy politycznej a ośrodkami badań nad komunizmem.

Współdziałanie instytutów wschodnich z organizacjami wywiadowczymi gwarantuje im zależność finansową od resortów

1/ Tamże, s. 5-11

obrony, spraw wewnętrznych i spraw zagranicznych. Współpraca ta polega na wytyczaniu kierunków działania wobec państw socjalistycznych i opracowaniu pomocniczych ekspertyz do weryfikacji materiałów uzyskanych przez wywiad.

Ścisła korelacja działań między kontrwywiadami i wywiadami a instytucjami wschodnimi obejmuje także politykę stypendialną, planowanie kontaktów oraz dobór uczestników na sympozja.

Służby specjalne otrzymują szczegółowe sprawozdania ze spotkań przedstawicieli instytucji z naukowcami z państw socjalistycznych. Z inicjatywy wywiadu naukowcy z instytucji wschodnich ułatwiają m.in. polskim uczonym publikowanie ich prac w czasopismach ośrodków badania Wschodu. Forsują także rozwój współpracy naukowej dyscyplin przydatnych dla wywiadu. W ten sposób rozpoznają zasoby polskich archiwów.

Między ośrodkami sowietologicznymi państw kapitalistycznych istnieje stała współpraca i wymiana doświadczeń. Na konferencji sowietologów, jaka odbyła się w 1974 roku w Kanadzie, powołano "Międzynarodowy Komitet Studiów nad Związkiem Radzieckim i Europą Wschodnią", którego celem jest koordynacja i integracja prowadzonych badań. W organizacji tej działa aktualnie 10 różnego rodzaju organizacji slawistycznych.^{1/}

1/ N. BUKOWSKI "Rola i zadania badań Europy Wschodniej głównych państw NATO", skrypt Szefostwa WSW nr 119/84, s. 3-4.

6. Środki techniczne wykorzystywane przez
wywiad państw NATO

Szybki rozwój techniki, a głównie elektroniki i chemii, powoduje wprowadzanie coraz nowszych urządzeń i materiałów na wyposażenie służb specjalnych. Unowocześnienie realizowane jest w wielu płaszczyznach, począwszy od udoskonalania systemów gromadzenia i przetwarzania informacji przez centrale służb specjalnych, do modernizacji urządzeń wykorzystywanych do działań wywiadowczych i kontrwywiadowczych.

Prace w kierunku doskonalenia urządzeń służących do pracy wywiadowczej polegały głównie na doskonaleniu niezawodności łączności bezosobowej. Obejmowały one między innymi:

- udoskonalenie jednostronnej łączności radiowej w zakresie fal krótkich do przekazywania agenturze instrukcji i poleceń:

Jako wyposażenie agentów wprowadzana jest ostatnio miniaturowa przystawka do odbioru zaszyfrowanych, z wykorzystaniem kodu binarnego, informacji. Jej walory techniczne, to: zautomatyzowany proces odbioru i dekodowania szyfrogramów, skrócenie czasu nadawania /400 pięciocyfrowych grup w ciągu niespełna 5 minut/, łatwość obsługi oraz możliwość programowania czasu uruchomienia przystawki;

- wykorzystywanie minikomputerów do kodowania i dekodowania informacji przesyłanych drogą radiową i przewodową:

Przykładem tego mogą być wyprodukowane przez amerykańską firmę /HAYES MICROCOMPUTER PRODUCTS/ moderny, posiada-

jące możliwość automatycznego wybierania numerów telefonicznych zaprogramowanych w komputerze oraz uruchamiania minikomputera po otrzymaniu sygnału z zewnątrz. Dzięki temu istnieje możliwość zaprogramowania komputera, który o określonej godzinie samoczynnie przekaże informacje pod wskazany numer telefonu. Szybkość transmisji danych pozwala na przekazanie jednej strony maszynopisu w ciągu 5 sekund.

Zakodowana w minikomputerze informacja może być również przekazana przy pomocy nadajnika radiowego. Ostatnio pojawiły się na Zachodzie radiostacje typu automatycznej skrzynki pocztowej, których pracą sterują komputery. Posługują się one amatorskimi sygnałami rozpoznawczymi i pracują w pasmach częstotliwości przydzielonych radioamatorom. Posiadając minikomputer sprzężony z nadajnikiem radiowym, można do takiej skrzynki przekazywać informacje przeznaczone dla różnych adresatów, którzy w dowolnym czasie mogą sprawdzać, czy pod umówionym hasłem znajdują się informacje, odebrać ich tekst i ewentualnie wpisać nowy do nadawcy;

- wykorzystywanie systemów łączności satelitarnych do przekazywania informacji agenturalnych:

Wykorzystywanie do łączności satelitów umieszczonych na wysokich orbitach geostacjonarnych, pozwala na bezpośrednie utrzymywanie łączności między korespondentami prawie całej kuli ziemskiej. Aktualnie NATO wykorzystuje kilkanaście systemów łączności satelitarnej, przy czym do przekazywania informacji wywiadowczych, wykorzystywany jest system "MARISAT" /łączność sił morskich i marynarki handlo-

wej/ oraz system "FLTSATCOM" /łączność sił morskich/.

Na terytorium Polski przesyła się /wykorzystując satelity/ kilkanaście informacji agenturalnych na dobę.

Należy dodać, że również placówki dyplomatyczne, w tym ambasada USA w Warszawie, prowadzą łączność za pośrednictwem łączy satelitarnych. Stosowane w tym systemie techniki kodowania sygnałów umożliwiają bezpieczne /nierozszyfrowalne/ prowadzenie rozmów metodą telefoniczną.^{1/}

Działające na terenie Polski rezydentury obcych służb specjalnych wyposażone są między innymi w:

a/ sprzet w samochodach:

- radiodbiorniki umożliwiające kontrolę pasm radiowych pionu obserwacji i MO;
- magnetofony ze sterowaniem nożnym umożliwiające tajne nagrywanie rozmów w samochodach;
- okablowanie pojazdu umożliwiające /przy podłączeniu z magnetofonem/ nagrywanie rozmów i prowadzenie nasłuchu na pewną odległość od samochodów;
- urządzenia sygnalizujące pracę radarów;

b/ wyposażenie osobiste:

- miniaturowe radiodbiorniki służące do: nasłuchu rozmów obserwacji, łączności z obsługiwanym agentem, kontroli pracy innego operatora rezydentury oraz emitowania ciągłego sygnału - w trakcie realizacji zadania wywiadowczego;
- lornetki z oświetlaczem lub na podczerwień, wysokiej klasy aparaty fotograficzne i kamery filmowe.^{2/}

1/ M. KRÓLIKOWSKI, S. MARKOWSKI, Zastosowanie najnowszych zdobyczy elektroniki w łączności wywiadowczej, Skrypt Szefostwa WSW, nr 173/86, Warszawa 1986r., s. 3-24

2/ Informacja Zarządu III Szefostwa WSW nrDB-0936/2 z 14.05.83r., s. 1-2

Niezależnie od tego do zabezpieczenia operacji i działań wywiadowczych państw NATO, wykorzystywany jest szereg innych środków i urządzeń zawierających w sobie najnowsze zdobycze nauki. Wśród tego sprzętu uwagę zwraca:

- zminiaturyzowany sprzęt video służący do filmowania w nocy oraz wielkości główki igły wizjery do stosowania podglądów;
- urządzenie do podsłuchu techniką laserową;
- zminiaturyzowany sprzęt do jednokierunkowej /agent - punkt odbioru/ szybkiej łączności - odległość nadawania do 150 m, czas 3-4 minuty;
- bogate wyposażenie charakterystyczne oraz środki do dokonywania operacji plastycznych;
- światłoczuły papier do wykonywania tajnopisów;
- bogate wyposażenie w środki psychotropowe.^{1/}

W materiały, urządzenia i wymienione środki wyposażony jest m.innymi stacjonujący we Frankfurcie n. Menem, jeden z obiektów pomocniczych Wydziału Służb Technicznych CIA - zadaniem którego jest zabezpieczenie działań i operacji wywiadowczych w Europie.

7. Niektóre formy profilaktyki kontrwywiadowczej
wykorzystywane w ochronie wojskowych struktur
organizacyjnych NATO

W głównych państwach NATO, w ciągu ostatniego okresu nastąpiło zintensyfikowanie działań profilaktyki kontrwywiadowczej, którą określa się jako podstawową metodę działania

1/ Informacja Zarządu III Szefostwa WSW nr DB-01817/3
z 5.09.1985 r., s. 2-6

służb bezpieczeństwa. Działalność ta przejawia się między innymi w:

- zaostreniu przepisów prawnych i sankcji karnych za współpracę z obcymi wywiadami;
- doskonaleniu sposobów ochrony informacji naukowej, technologii, techniki i wszelkich materiałów, które mogłyby zainteresować służby wywiadowcze krajów socjalistycznych. Szeroko wprowadza się do użytku najnowocześniejszą technikę kontrwywiadowczą i nowe systemy komputerowe umożliwiające coraz pełniejszą kontrolę sfer życia prywatnego obywateli i całej sfery społeczno-politycznej kraju;
- nieustannym nasilaniu przez zachodnie ośrodki masowego przekazu, z inspiracji służb specjalnych, propagandy antykomunistycznej i działalności uświadamiającej społeczeństwu metody działania wywiadów państw socjalistycznych;
- wprowadzeniu obowiązku prowadzenia szkoleń kontrwywiadowczych personelu zatrudnionego w instytutach naukowo-badawczych i zakładach pracujących na potrzeby wojska, lub których produkcja ma znaczenie obronne. Szkolenie dotyczy ochrony tajemnicy państwowej i służbowej, a także zachowania się w przypadku kontaktu z obywatelami krajów socjalistycznych;
- wprowadzaniu, głównie pod naciskiem Stanów Zjednoczonych, w większości państw NATO - embarga na przepływ informacji naukowych i technologii do krajów socjalistycznych oraz na sprzedaż nowoczesnej techniki, nie tylko o znaczeniu obronnym, ale także i gospodarczym.

Szczególne nasilenie stosowania masowych działań profilaktyki kontrwywiadowczej występuje w RFN, USA, Wielkiej Brytanii i Francji. Sytuacja w tym względzie w wymienionych państwach przedstawia się następująco:

Republika Federalna Niemiec

Władze polityczne i administracyjne podjęły intensywne prace w zakresie ustawodawstwa dotyczącego sfery bez-

pieczeństwa państwa. Działalność ta ma charakter wielokierunkowy i ma na celu zarówno stworzenie prawnych instrumentów umożliwiających władzom państwowym głębokie ingerowanie we wszystkie dziedziny życia społecznego, jak i zintegrowanie wysiłków wszystkich właściwych organów państwowych w przeciwdziałaniu zagrożeniom wewnętrznym i zewnętrznym.

Parlament zachodnioniemiecki zatwierdził ustawy o wprowadzeniu nowych dowodów osobistych i paszportów przystosowanych do maszynowego ich odczytu oraz o wysokim stopniu zabezpieczenia przed możliwością ich sfałszowania lub podrobienia. Dokumenty te, przy istnieniu odpowiednio rozbudowanej infrastruktury informatycznej, stwarzają możliwość dla służb specjalnych RFN pełnej i efektywnej kontroli wszystkich obywateli.

Wprowadzono też szereg ustaw nowelizujących dotychczasowe zasady bądź też sankcjonujących prawnie dotychczasowe uprawnienia oraz metody działania służb specjalnych.

Do najważniejszych z nich należą:

- ustawa o informacyjnej współpracy służb specjalnych i policji w zakresie spraw ochrony państwa i porządku konstytucyjnego oraz działalności wywiadowczej. Ustawa nakłada obowiązek "współpracy informacyjnej" na Urząd Ochrony Konstytucji, kontrwywiad wojskowy, Federalny Urząd Kryminalny, służby graniczne, władze krajów związkowych i policję;
- nowelizacja ustawy o Urzędzie Ochrony Konstytucji, rozszerzająca jego uprawnienia w zakresie prowadzenia śledztwa metodami wywiadowczymi, również wobec osób potencjalnie zagrożonych - tzn. nosicieli tajemnicy państwowej. Nakłada na służbę graniczną i celną, prokuraturę generalną oraz

federalny urząd kryminalny obowiązek informowania i przekazywania danych mogących zainteresować Urząd Ochrony Konstytucji;

- ustawa o kontrwywiadzie wojskowym, która określa m.innymi ścisłą współpracę kontrwywiadu z Urzędem Ochrony Konstytucji;
- ustawa o ochronie danych.

Zmodyfikowano także zasady prowadzenia sprawdzeń kontrwywiadowczych osób mających dostęp do materiałów niejawnych. Wprowadzono tzw. trzystopniowe sprawdzenia kontrwywiadowcze. Najwyższym - trzecim stopniem - objęte są osoby mające dostęp do materiałów i prac ściśle tajnych. Polega ono na aktywnym rozpracowaniu danej osoby, włącznie z jej przesłuchaniem i dokonaniem wywiadów środowiskowych. Sprawdzeniem tym objęci są m.innymi: referenci, sekretarki i kierowcy ministrów oraz sekretarzy stanu.

Na szczególną uwagę zasługuje, trwający od dłuższego już czasu w RFN, proces gwałtownego rozwoju i integrowania systemów informacyjnych. Obok dużych, centralnych systemów informacyjnych znajdujących się w dyspozycji służb specjalnych /NADIS/, policji /INPOL/ i organów administracji państwowej /ZEVIS/, funkcjonuje stale zwiększająca się ilość systemów informacyjnych w zakładach pracy, organizacjach handlowych i przemysłowych oraz innych instytucjach usługowych, które stanowią bogatą bazę informacyjną obejmującą coraz więcej osób.^{1/}

1/ Informacja Szefostwa WSW nr DB-0686/3 z 29.03.1985 r. s. 7-12 oraz Informacja Szefostwa WSW nr DB-Pf-1184/35 z 21.05.1985 r., s. 2-6.

Stany Zjednoczone

W 1987 roku prezydent Reagan podpisał ustawę w sprawie przywrócenia kary śmierci za szpiegostwo w czasie pokoju, której podlegają osoby przekazujące obcym wywiadom informacje dot. m.innymi broni jądrowej, satelitów, szyfrów i systemów strategicznych. Celem podjęcia tej decyzji było między innymi wprowadzenie w społeczeństwie elementu zastraszenia przed podejmowaniem się tego typu działalności.

Władze wojskowe wprowadziły obowiązek meldowania przez osoby zatrudnione w siłach zbrojnych faktów otrzymywania prezentów o wartości przekraczającej 165 dolarów USA. Obowiązek ten ma zapobiec ewentualnemu wiązaniu się pracowników wojska z obcymi wywiadami drogą otrzymywania wartościowych upominków i innych korzyści materialnych.

Wzmożono zabezpieczenie kontrwywiadowcze w instytucjach, jednostkach i agencjach podległych Departamentowi Obrony oraz wszędzie tam, gdzie znajdują się dokumenty i informacje dotyczące obronności Stanów Zjednoczonych. W ramach tych działań rozszerzono możliwość użycia poligrafów do badań pracowników w Departamencie Obrony, zaostrzono kontrolę i ochronę wojskowych środków łączności i szyfrów, wprowadzono stałe przeglądy kadrowe pod względem zabezpieczenia kontrwywiadowczego, ograniczono możliwość dostępu do banków informacji komputerowej instytucji działających na rzecz obronności oraz wprowadzono na wyposażenie agencji rządowych nowy model telefonu do rozmów utajnionych - STV-III.

Podobnie, jak ma to miejsce w RFN, w środkach masowej



informacji - zwłaszcza w prasie i telewizji - prowadzone aktywnie, w ramach akcji profilaktycznych, propagandowe kampanie kontrwywiadowcze. Szeroko wykorzystywano w nich wykryte sprawy szpiegowskie oraz ujawnione przecieki informacji niejawnych z kół wojskowych, rządowych i przemysłowych. Jako materiał propagandowy wykorzystano również szeroko sprawy wydaleń pracowników placówek dyplomatycznych z innych państw NATO.

Celem tych akcji było pokazanie społeczeństwu amerykańskiemu z jednej strony sprawności i wszechwiedzy służb specjalnych, z drugiej strony natomiast wyczulano na obecność obcych wywiadów, ich aktywność i zagrożenie dla bezpieczeństwa państwa.

Dla uniemożliwienia przepływu do krajów socjalistycznych technologii objętych embargiem, służby celene pod kierownictwem FBI podjęły akcję "Operation Exodus". Polegała ona na zaostrzeniu kontroli firm handlowych, kierowanych za granicę przesyłek, wymiany naukowej oraz działalności ośrodków informacyjnych, np. bibliotek uniwersyteckich, seminariów naukowych, kursów specjalistycznych itp.^{1/}

Wielka Brytania

Typową formą oddziaływania w zakresie kontrwywiadowczym na społeczeństwo, była szeroka akcja informacyjna w środkach masowego przekazu o wszystkich tzw. aferach szpiegowskich na terenie Wielkiej Brytanii i w innych krajach. Zamierzeniem

1/ Informacja Szefostwa WSW nr DB-0686/3, wyd. cyt., s.2-7

tego działania było destruktywne oddziaływanie na psychikę osób podejmujących współpracę z wywiadami krajów socjalistycznych, przy jednoczesnym podkreśleniu szybkości i skuteczności działania brytyjskich i natowskich służb specjalnych. Z drugiej strony, aktywna i intensywna propaganda antysocjalistyczna wykorzystująca fakty zdrady lub ucieczki obywateli krajów socjalistycznych na Zachód, miała na celu wywołanie niechęci do jakichkolwiek kontaktów z naszymi przedstawicielstwami.

Poprawiono zabezpieczenie danych szczególnie ważnych obiektów wojskowych, a głównie magazynów broni jądrowej i bazy morskiej "FASLANE". Na obiektach tych zainstalowano systemy telewizyjne połączone z komputerem policji, a ponadto wyraźnie zwiększono obsadę etatową pododdziałów ochrony, wyposażając je w nowoczesny sprzęt.

W celu ograniczenia możliwości przeniku ważnych informacji zaostrzono zabezpieczenie rządowego systemu łączności /GCHQ/ oraz zarządzono - decyzją ministra obrony - kontrolę rozmów telefonicznych podległego mu personelu. O prowadzonej kontroli rozmów w telefonicznej sieci wewnętrznej ministerstwa informuje się pracowników.

Równolegle z rozszerzeniem badania na poligrafie pracowników państwowych zatrudnionych w instytucjach szczególnie zagrożonych penetracją wywiadowczą, wprowadzono badania przy pomocy specjalistycznych testów psychologicznych. Testy te mają pomóc w wykrywaniu osób podatnych na podjęcie współpracy z obcymi wywiadami lub narażonych na skuteczny szantaż z powodu zaburzeń osobowych, nałogów itp. Badaniami

obejmowani są wszyscy kandydaci do pracy oraz cyklicznie, co 5 lat, wszyscy pracownicy w ramach tzw. potwierdzenia ich przydatności do służby.

Następuje również sukcesywne wprowadzanie nowych paszportów, przystosowanych do automatycznego odczytu przez odpowiednie urządzenia, w które wyposażone zostaną w najbliższym czasie wszystkie lotniska i porty morskie Wielkiej Brytanii.

Na uwagę zasługuje fakt, że znaczna część przedsięwzięć profilaktyki kontrwywiadowczej, podjęta została przez rząd brytyjski pod presją Stanów Zjednoczonych.^{1/}

Francja

Sytuacja polityczno-społeczna we Francji sprzyjała podejmowaniu decyzji w dziedzinie umacniania reżimu policyjnego i rozbudowy aparatu bezpieczeństwa. Dokonano szeregu zmian organizacyjnych i personalnych w policji, DST i DGSE.

W akcji propagandowej, mającej na celu wyrobienie w społeczeństwie nastrojów zagrożenia ze strony krajów socjalistycznych, publikowano przypadki ujawnionego szpiegostwa oraz cele i obiekty zainteresowań wywiadów państw wschodnich.

Spowodowano wzmożenie ochrony wszystkich osobistości rządowych, co ma realizować powołana w tym celu specjalna służba, podległa ministrowi spraw wewnętrznych.

Nastąpiła gwałtowna rozbudowa różnorodnych systemów informatycznych dla potrzeb policji i służb specjalnych.

1/ Informacja Szefostwa WSW nr DB-0686/3, wyd.cyt., s.12-17

Umożliwia to między innymi szybkie zdobywanie przez te służby interesujących informacji i indentyfikację osób poszukiwanych.

W Paryżu zainstalowano tzw. komputerowy system graficzny oraz system odbioru emisji miniaturowych nadajników, umożliwiających prowadzenie kontroli wizualnej oraz rozmów osób będących w ruchu.

W ramach tzw. akcji zapobiegawczych wzmożono wyrywkowe legitymowanie obywateli, zniesiono możliwość darmowego uzyskiwania materiałów związanych z techniką oraz zaostrzono przepisy w sprawie licencji wywozowych na niektóre rodzaje sprzętu elektronicznego.

Probleмами zabezpieczenia bezpieczeństwa w NATO zajmują się specjalne pododdziały paktu przy ścisłej współpracy z organami KW państw członkowskich.

Organem koordynującym sprawę bezpieczeństwa paktu i bezpośrednio podległym Radzie NATO jest Komitet d/s Bezpieczeństwa. W skład Komitetu z każdego państwa członkowskiego wchodzi jeden przedstawiciel kompetentny w zagadnieniach bezpieczeństwa swego kraju. Komitet zajmuje się badaniem problemów, które pozostają w związku z ogólną polityką paktu w zakresie bezpieczeństwa, koordynuje politykę państw członkowskich w tym przedmiocie, ustala jej zasadnicze kierunki oraz przygotowuje rekomendacje dla Rady NATO.

Organem wykonawczym Komitetu jest Biuro d/s Bezpieczeństwa, które zapewnia bezpieczeństwo Międzynarodowego Sekretariatu, koordynuje i kontroluje problemy służące zapewnieniu bezpieczeństwa paktu, przygotowuje zalecenia dla naro-

dowych służb specjalnych, rozpracowuje i ustala przedsięwzięcia w zakresie zabezpieczenia tajności dla wszystkich pododdziałów. Biuro to organizuje też szkolenie mające na celu wyrabianie wśród personelu czujności, wykłady i przeglądy filmów, utrzymuje kontakty z oficerami bezpieczeństwa w pododdziałach NATO. W skład Biura d/s Bezpieczeństwa wchodzi specjaliści zarówno wojskowi jak i cywilni. Na czele biura stoi przedstawiciel Stanów Zjednoczonych AP.

W ramach oddziału administracji, kierowania i kadr Międzynarodowego Sekretariatu funkcjonuje Służba Bezpieczeństwa, która zabezpiecza ochronę pomieszczeń sztabowych NATO na podległym jej obszarze. Cięży na niej również obowiązek zapewnienia wymaganego reżimu tajności i ochrony tajnych materiałów, znajdujących się w pomieszczeniach roboczych.

Oprócz pododdziałów specjalnych, zagadnieniami bezpieczeństwa w zarządach Międzynarodowego Sekretariatu NATO i narodowych przedstawicielstwach przy Radzie NATO zajmują się oficerowie i pełnomocnicy d/s bezpieczeństwa, będący według stanowisk służbowych zastępcami szefów oddziałów. Spełniają oni rolę konsultantów w zakresie bezpieczeństwa przy szefie, utrzymują łączność z pododdziałami bezpieczeństwa, zabezpieczają kopie akt dot. przypadków naruszenia wymogów tajności przez pracowników, nadzorują przebieg szkolenia z zakresu bezpieczeństwa.

Obszar gmachów sztabowych NATO posiada wewnętrzną i zewnętrzną strefę bezpieczeństwa. Strefa zewnętrzna obejmuje wejścia do obiektów /na obszar/, parkingi samochodowe, salę dla interesantów. Wejście do tej strefy jest dozwolone tylko

za przepustką lub na sygnał telefoniczny do biura przepustek od pracownika oczekującego interesanta.

Wejście do strefy wewnętrznej, gdzie znajdują się pomieszczenia służbowe, możliwe jest tylko na podstawie przepustki i w towarzystwie strażnika lub współpracownika, który zapotrzebował przepustkę dla interesanta. Wszystkie wejścia do strefy wewnętrznej są ściśle chronione.

Pomieszczenia obiektów sztabowych NATO zajmujące szczególnie miejsca w systemie tajności, zabezpieczone są zamkami z kodem cyfrowym, sygnalizacją i siatkami w oknach. Zabezpieczenie szaf i sejfów zapewniają wmontowane tajne zamki z kodem cyfrowym. Kody podlegają wymianie co pół roku oraz każdorazowo po zwolnieniu pracowników, którzy mieli z nimi kontakt.

Załatwianiem przepustek dla osób pracujących w pomieszczeniach sztabowych NATO, zajmuje się służba bezpieczeństwa oddziału administracji, kierowania i kadr Międzynarodowego Sekretariatu NATO. Prowadzi ona kartotekę całego personelu, według której można określić stopień dostępu pracownika do tajnych materiałów. Wymiana przepustek następuje raz na jeden - dwa lata.

W stosunku do pracowników zatrudnionych w obiektach sztabowych NATO przeprowadza się coroczne, ukryte sprawdzenia dla wyjaśnienia okoliczności życia prywatnego i utrzymywanych kontaktów, do czego wykorzystuje się siły belgijskiego KW.

Raz do roku w NATO dokonuje się sprawdzenia liczby tajnych dokumentów. Na każdy brakujący dokument sporządzana

jest notatka wyjaśniająca. W ostatnich latach przedsięwzięte zostały kroki uzupełniające /dodatkowe/ w zakresie wzmocnienia ochrony reżimu tajności w siedzibie NATO, w szczególności wyposażono specjalne pomieszczenia do rewizji osobistych, zaostrzono reżim sprawdzania dokumentów w wewnętrznej strefie bezpieczeństwa, ograniczono liczbę uczestników ważniejszych konferencji, coraz częściej stosuje się praktykę zwoływania konferencji bez protokołowania oraz aktywizuje się działalność służb specjalnych.

Z kadrami w zakresie kreowania bezpieczeństwa i czujności prowadzona jest szeroka praca wychowawcza. Zapoznaje się ją z instrukcjami, regulaminami i broszurami, okresowo udziela instruktaży oraz prezentuje filmy specjalne. Ekspozuje się w nich metody pracy wywiadów państw socjalistycznych, niebezpieczeństwo i następstwa kontaktów z przedstawicielami państw wspólnoty socjalistycznej a także wskazuje się na konieczność meldowania o naruszeniu zasad bezpieczeństwa przez innych pracowników.

Szczególnie starannie prowadzi się pracę w zakresie zapobiegania przeciekowi informacji. Dla przykładu instrukcje Komitetu d/s Bezpieczeństwa zabraniają wysyłania informacji z gryfem "Tajne" do przedstawicielstw dyplomatycznych państw członkowskich paktu w państwach socjalistycznych. Natomiast do ambasad znajdujących się w państwach członkowskich NATO dokumenty wysyła się dopiero po określeniu konieczności i możliwości ryzyka.

W instrukcjach traktujących o pracy z tajnymi dokumentami NATO przewiduje się między innymi:

- wydawanie tajnych dokumentów jedynie osobom które mają odpowiednie upoważnienie;
- przechowywanie ich tylko w pewnych sejfach, nie mających zewnętrznych oznak wskazujących na charakter przechowywanych w nich materiałów;
- dokonywanie regularnej kontroli przestrzegania zasad zabezpieczenia dokumentów;
- przesyłanie w kopertach, które z wyglądu zewnętrznego nie sugerują faktycznej ich zawartości;
- niezawodną ochronę pomieszczeń, w których znajdują się dokumenty tajne;
- przestrzeganie wszystkich zasad obchodzenia się z dokumentami tajnymi oraz ochronę pomieszczeń w czasie konferencji i odpraw NATO.

Zabezpieczenie ochrony tajnych wiadomości NATO, kierowanych do państw członkowskich paktu lub przez nie posiadanych, spoczywa na narodowych służbach bezpieczeństwa.

Zasadnicze zadania tych służb to:

- zapewnienie ochrony tajnych wiadomości paktu w narodowych, wojskowych i cywilnych organizacjach, znajdujących się na terenie państwa lub poza jego granicami;
- przeprowadzanie regularnych kontroli w zakresie ochrony tajnych wiadomości NATO;
- zapewnienie kontroli sprawdzeń wszystkich obywateli danego państwa, którzy mają dostęp do tajnych wiadomości paktu;
- zabezpieczenie kontroli przy opracowywaniu planów w zakresie zapobiegania przeciekowi tajnych wiadomości NATO.

Komitet Wojskowy ponosi odpowiedzialność przed Radą NATO za bezpieczeństwo sztabów wojskowych, pododdziałów i instytucji paktu. Przedstawiciele Komitetu Wojskowego i ND PSZ NATO w Europie biorący udział w konferencjach Komitetu

d/s Bezpieczeństwa, wnoszą propozycje w przedmiocie ulepszeń systemu tajności w NATO.

Oddziały bezpieczeństwa i KW występują w zarządach rozpoznawczych /wywiadowczych/ ND i innych sztabach PSZ NATO. Zabezpieczają one wykonawstwo potrzeb i norm bezpieczeństwa w dziedzinie wojskowej. Oddziały te i ich pododdziały operacyjne /posterunki KW/ w jednostkach wojskowych i instytucjach wojskowych paktu wykonują zadania kontrwywiadowcze w granicach przydzielonych im obiektów.

8. System naboru personelu do pracy w głównych organach NATO

Naborem i zgłaszaniem kandydatur do pracy w organach i instytucjach paktu zajmują się odpowiednie komórki bezpieczeństwa państw członkowskich, a także biuro do spraw administracyjnych i kadrowych Międzynarodowego Sekretariatu NATO.

Nabór kadr na stanowiska techniczne prowadzą także określone urzędy zatrudnienia, zlokalizowane w rejonie dyslokacji instytucji paktu. Przy przyjmowaniu do pracy w organach NATO pierwszeństwo mają byli wojskowi z sił zbrojnych państw członkowskich.

Obecnie pracownicy organów i instytucji paktu NATO są podzieleni na trzy kategorie: "A", "B/C" i "L".

Do kategorii "A" należą: szefowie zarządów i oddziałów

oraz ich zastępcy, a także administratorzy. Pracownicy zaszeregowani do stopni A.4, A.5, A.6 i A.7 mają status członków korpusu dyplomatycznego. Natomiast pracownicy z zaszeregowaniem A.1, A.2 i A.3 statusu dyplomatycznego nie posiadają.

Z reguły pracownicy tej kategorii są kierowani do pracy w NATO przez urzędy państwowe krajów należących do paktu.

Do kategorii "B/C" należy głównie personel techniczny i obsługujący. Kategoria ta dzieli się na dwie grupy: "B" i "C".

Do grupy "B" należą kierownicy kancelarii, kanceliści, archiwiści, maszynistki i stenografistki. Pracownicy tej grupy powinni posiadać znajomość jednego lub dwóch języków obcych. Do grupy "C" należy personel obsługujący /kurierzy, ochrona, telefonistki, specjaliści od obsługi urządzeń radiowych i telewizyjnych/.

Nabór pracowników kategorii "B/C" przeprowadza się poprzez typowanie kandydatur przez urzędy państwowe oraz poprzez ogłoszenia konkursowe.

Do kategorii "L" /nielicznej/ należą pracownicy ze specjalnym przygotowaniem językowym, głównie tłumacze, a ich status jest analogiczny ze statusem drugiej grupy kategorii "A". W jej skład wchodzi osoby, które zdały egzaminy konkursowe na obsadzenie wolnych stanowisk oraz osoby delegowane do NATO przez instytucje państwowe.

Liczba stanowisk obsadzanych przez poszczególne państwa w instytucjach NATO zależy zasadniczo od wkładu danego

państwa do ogólnego budżetu paktu. Pracownicy najwyższych i średnich ogniw kierowniczych oraz eksperci zatrudnieni w oddziałach Międzynarodowego Sekretariatu NATO z reguły są kierowani do pracy przez urzędy państwowe. Osoby wojskowe do pracy w dowództwach i sztabach NATO mogą być delegowane również przez narodowe resorty wojskowe.

Do pracy w organach i instytucjach NATO przyjmowani są wyłącznie obywatele państw członkowskich. Wszyscy kandydaci do pracy są dokładnie sprawdzani przez narodowe służby bezpieczeństwa. W trakcie sprawdzania zasięga się informacji z różnych archiwów /cywilnych, wojskowych/ danego państwa, a w razie konieczności również z innych państw. Stopień i czas trwania sprawdzeń zależą głównie od stanowiska, na które wyznacza się daną osobę, a także od zakresu dopuszczenia do pracy z dokumentami tajnymi.

Zawsze i obowiązkowo sprawdzane są następujące dane: data i miejsce urodzenia; miejsca zamieszkania /mogą być przy tym wypytywani gospodarze domów /; obywatelstwo, wykształcenie; miejsca pracy w ciągu ostatnich 10 lat /osoby ze stażem pracy poniżej 3 lat z zasady nie są zatrudniane w NATO/; przebieg służby wojskowej; wyjazdy zagraniczne /szczególnie zamieszkiwanie za granicą/; stan majątkowy; przynależność do organizacji politycznych i społecznych.

Kandydat wypełnia ankietę oraz przedstawia uzyskane od trzech obywateli swego państwa poświadczenie o prawomyślności politycznej i charakterystykę cech osobistych i zawodowych. Jeżeli sprawdzenie wypadnie pomyślnie, kandydat jest proszony na rozmowę wstępną. Ci, którzy przebrną ten etap,

wypełniają kolejną ankietę, której zasadnicze pytania sprawdzają się do ujawnienia kontaktów kandydata z organizacjami lewicowymi i przedstawicielami państw socjalistycznych. Po oddaniu ankiety rozpoczyna się sprawdzanie na prawdziwość i prawdopodobność. Trwa ono od dwóch do sześciu miesięcy, niekiedy dłużej.

Kolejne sprawdzania pracowników przeprowadzane są co każde 5 lat, przy czym za każdym razem w narodowych organach bezpieczeństwa zapotrzebowuje się potwierdzenia prawdziwości danej osoby.

W NATO przeprowadzana jest regularnie wymiana /rotacja/ kadr w cyklach od dwóch do czterech lat, co z punktu widzenia wywiadu ma zarówno dodatnie, jak i ujemne strony. Na przykład, agent jest obiektywnie pozbawiony możliwości pracy w NATO przez długi okres, ponieważ jeżeli nie udaje mu się przedłużyć kontraktu w ciągu dwóch-czterech lat jest on zmuszony do opuszczenia zajmowanego stanowiska.

Rotacja kadrowa wpływa także w dużym stopniu na działalność rezydentur własnych ponieważ stosunkowo krótki okres pobytu pracownika na stanowisku, najczęściej nie daje możliwości dokładnego i wszechstronnego sprawdzenia, rozpracowania i przeprowadzenia werbunku określonych osób. Jednocześnie rotacja pracowników NATO stwarza przesłanki do uplasowania pewnej i sprawdzonej agentury na obiektach wywiadowczego zainteresowania.

Inną ważną okoliczność stanowi rozmieszczenie głównych organów kierowniczych NATO na terenie jednego państwa /Belgię/, co umożliwia zorganizowanie na wysokim poziomie

wszechstronnego zabezpieczenia kontrwywiadowczego. Reasumując, należy stwierdzić, że na możliwości zdobywania informacji i warunki prowadzenia działalności werbunkowej wśród personelu NATO w poważnym stopniu wpływają:

- silny reżim ochronny;
- zaostrzone instrukcje i zarządzenia regulujące sposób przyjmowania do pracy w instytucjach paktu;
- sprawdzenia;
- system dopuszczeń do tajnych dokumentów i ich ewidencja;
- sposób przechowywania /wzorowany na systemie bezpieczeństwa w instytucjach państwowych Stanów Zjednoczonych/.

Z drugiej strony, wielonarodowy skład personelu zatrudnionego w NATO i znaczna liczba obiektów paktu w państwach członkowskich, stwarzają sprzyjające warunki do szerokiego udziału własnych rezydentur przy realizacji zadań dotyczących wywiadowczego przenikania.

9. Ocena zagrożeń dla Sił Zbrojnych PRL
wynikających z wywiadowczej działalności
głównych państw NATO

Wydarzenia ostatnich lat, wyraźnie wskazują, że proces odprężeniowy w relacjach Wschód - Zachód pogłębia się i realne stają się szanse na utrwalenie pokoju światowego. Pochodną zmian w sferze polityczno-militarnej jest rozszerzenie się związków osobowych, kulturowych, naukowych i gospodarczych

państw socjalistycznych z Zachodem. Odblokowane zostały możliwości i uruchomione są różnorodne mechanizmy wymiany myśli i idei, wzajemnych kontaktów państw o różnych systemach polityczno-ustrojowych. Bez względu na bardziej lub mniej optymistyczną ocenę warunków do trwałej stabilizacji, trzeba mieć pełną świadomość, że:

- pozytywne procesy odprężenia politycznego i militarnego nie wyeliminują podstawowych różnic między dwoma systemami ustrojowymi;
- toczyć się będzie nadal walka systemów: socjalistycznego i kapitalistycznego na wielu - często nowych - płaszczyznach;
- nie znikną spory polityczne - prowadzone przez państwa kapitalistyczne z pozycji siły;
- elementy sytuacji wewnętrznej kraju są bacznie śledzone przez państwa zachodnie i nadal w szeregu przypadkach wydarzenia destrukcyjne inspiruje i wspiera materialnie przeciwnik.

Stąd wniosek, że w działaniach służb specjalnych nie należy spodziewać się osłabienia aktywności, wręcz przeciwnie sytuacja obecna stanowi okazję do zdynamizowania wywiadowczej penetracji. W naszej ocenie przeciwnik będzie starał się zdyskontować na swą korzyść między innymi:

- zachowania w świadomości społecznej oraz powstanie realnej opozycji politycznej podatnej na sterowanie z zewnątrz, a nawet na współpracę z obcym wywiadem;
- nasilenie się emigracji, a w tym z pobudek politycznych, podejmującej działalność w ośrodkach opozycyjnych na Zachodzie współdziałających ze służbami specjalnymi przeciwnika;

- wzrost wyjazdów służbowych, turystycznych i zarobkowych naszych obywateli na Zachód oraz przyjazdów turystycznych i służbowych cudzoziemców do Polski;
- przyrost ilości powiązań i kontaktów z KK utrzymywanych przez środowiska wojskowe;
- stagnacja w rozwoju techniki, a w tym będącej na wyposażeniu naszych służb specjalnych, mogącej skutecznie wykrywać przejawy działań wywiadowczych;
- nadanie przez państwa NATO dużej rangi profilaktyce kontrwywiadowczej, ukierunkowanej między innymi na ujawnianie naszych źródeł informacji, a stąd wpływające ograniczenie możliwości rozpoznawania metod pracy i agentury przeciwnika;
- masowe wykorzystywanie przez służby specjalne NATO najnowszych zdobyczy techniki, ułatwiającej zbieranie, przetwarzanie i wykorzystywanie uzyskanych informacji.

Prognozy nasze uzasadnia coraz szersze zapotrzebowanie zachodnich ośrodków politycznych na informacje oraz rozbudowa struktur central wywiadu państw NATO, wzmocnienia kadrowe i wzbogacenia techniczne.

Realne zagrożenie stanowi między innymi:

- tworzenie szeregu komórek - agend wywiadów amerykańskiego i zachodniemieckiego na terytorium RFN, przeznaczonych do organizowania operacji wobec Polski i innych krajów socjalistycznych;
- powstanie nowych biur indagacyjnych i ośrodków ankietowania zbierających informacje od osób czasowo wyjeżdżających na Zachód;
- organizowanie w obozach przejściowych - siłami wywiadu - dodatkowych komórek do przesłuchań przesiedleńców z krajów socjalistycznych;

- zwiększenie liczebności tzw. naganiaczy spośród emigrantów i uciekinierów, do wyszukiwania osób dysponujących informacjami atrakcyjnymi dla wywiadu, przede wszystkim z zakresu obronności. Szereg osób na Zachodzie rolę naganiacza odbiera jako swoisty zawód;
- wzmocnienie rezydentur wywiadowczych działających z pozycji przedstawicielstw dyplomatycznych i konsularnych w Polsce.

W ślad za posunięciami organizacyjnymi poszły praktyczne działania. Uzyskujemy informacje, że pracownicy rezydentur prowadzą już na terenie placówek wstępne rozpoznanie osób ubiegających się o wizy, wyszukując powiązanych z administracją państwową, władzami partyjnymi, resortem spraw wewnętrznych i wojskiem, a więc mogących dysponować źródłowymi wiadomościami istotnymi dla central wywiadowczych. Niejednokrotnie wydanie wizy uzależnione jest od ocen wystawionych ubiegającym się o wyjazd pod kątem ich podatności do rozmów indagacyjnych. Ustalamy, że nawet prozaiczne motywy wyjazdów - jak znalezienie pracy, chęć szybkiego dorobienia się, uzyskanie profitów z nielegalnego handlu, połączenie z rodziną wykorzystywane są przez służby specjalne państw NATO do uzależnienia osób wcześniej wyselekcjonowanych do indagacji lub wytypowanych do werbunku.

Powracający do kraju niejednokrotnie sygnalizują, iż wywierano na nich różnorodne naciski. Szantaż, oddziaływanie psychiczne, groźby, próby przekupstwa to tylko wybrane metody z arsenału działań werbunkowych służb specjalnych NATO. Jest oczywistym, że jednym z podstawowych celów jest przeniknięcie do wnętrza armii. Próby tego rodzaju przeciwnik przeprowadza zarówno w kraju jak i za granicą. W tym celu bezwzględnie

wykorzystuje każdą sprzyjającą sposobność dotarcia do żołnierzy zawodowych - dla przykładu: pełniących służbę w misjach pokojowych ONZ, wyjeżdżających służbowo i prywatnie na Zachód, oddelegowanych do polskich placówek dyplomatycznych w krajach kapitalistycznych.

Przedstawione w ocenie uwarunkowania i trendy oddziaływań służb specjalnych NATO, stworzyły niejako szereg - do tej pory nie występujących powszechnie - zagrożeń, które umożliwiają przeciwnikowi infiltrację wywiadowczą różnych dziedzin naszego życia.

Rozpoznaniem bieżących i perspektywicznych zagrożeń wywiadowczych skierowanych na nasze wojska zajmuje się przede wszystkim służba kontrwywiadu WSW.

We wdrażanym aktualnie modelu profilaktyki o cechach powszechności i kreatywności, kontrwywiad spełnia - z racji posiadanych możliwości - rolę inspiratorską. Odpowiedzialność za organizację szczelnej ochrony tajemnicy rozkłada się jednak na wszystkie organa władzy wojskowej - zobowiązane do przedsięwzięć ochronnych, każdy w granicach swych uprawnień i kompetencji.

R o z d z i a ł IV

FAKTYCZNE ASPEKTY BUDOWY I FUNKCJONOWANIA
SYSTEMU KONTRWYWIADOWCZEJ OCHRONY TAJEMNICY

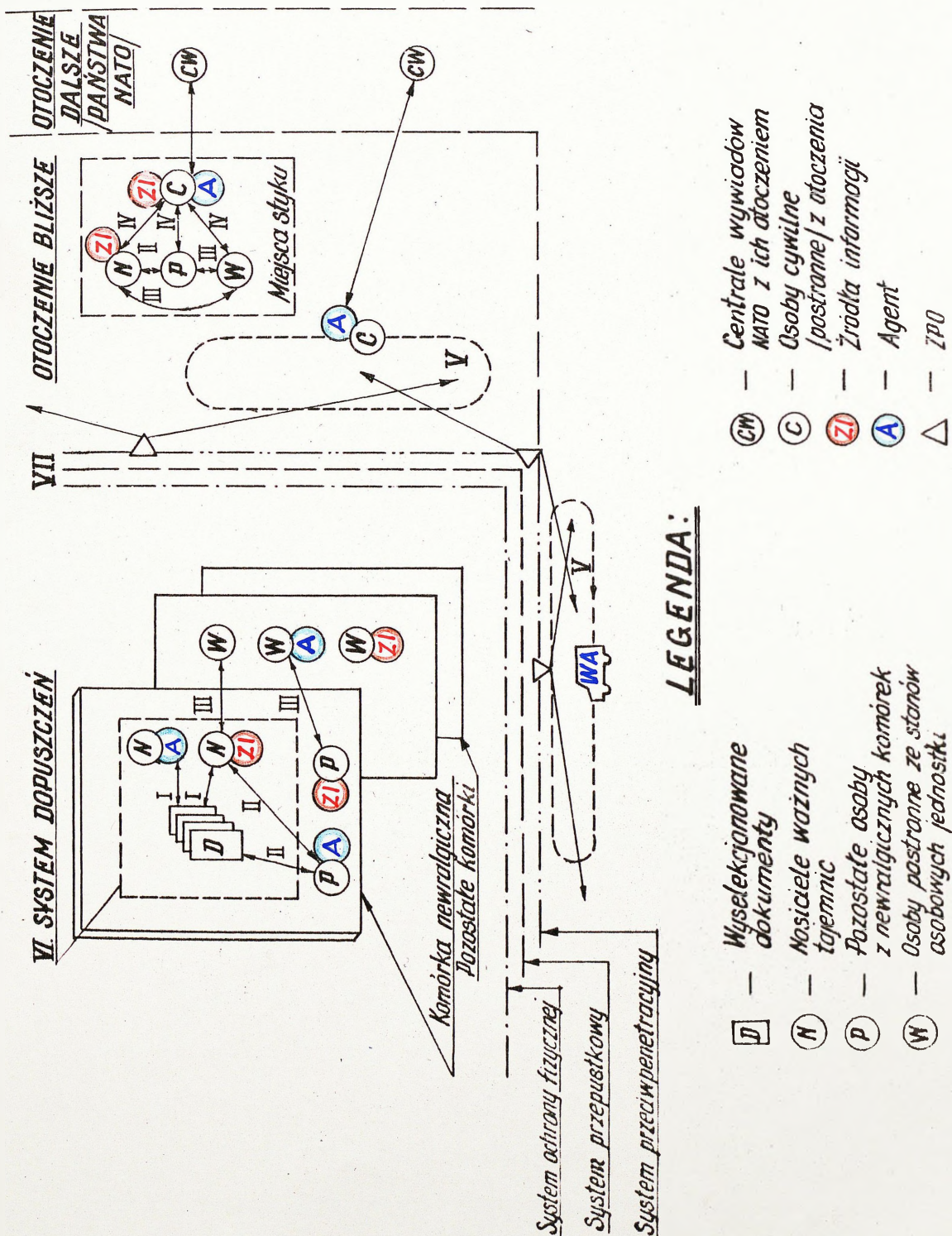
1. Ogólny model kontrwywiadowczego zabezpieczenia
ważnych nośników informacji i jego podstawowe
funkcje

Podstawowe znaczenie w walce ze szpiegostwem odgrywa właściwa organizacja systemu ochrony tajemnicy, w tym głównie wiadomości o szczególnym znaczeniu dla obronności kraju. Od szeregu lat organa WSW czynią zabiegi organizacyjne zmierzające do zwiększenia dopływu informacji o sytuacji operacyjnej w wyselekcjonowanych newralgicznych komórkach sztabów i ogniwach tych jednostek, gdzie skupione są tajemnice państwowe oraz o osobach tam zatrudnionych, objętych "osłoną kontrwywiadowczą". Zbudowanie skutecznego systemu kontrwywiadowczej ochrony tajemnicy wymaga opracowania modelu opartego o zdobycze współczesnej nauki, w tym o teoretyczne podstawy ogólnej teorii systemów i cybernetyki. Koncepcję takiego systemu przedstawiono graficznie na stronie 132. Model zabezpieczenia nośników ważnych informacji i ochrony kontrwywiadowczej obiektów"/.

Z przedstawionej graficznie koncepcji wynika, że najistotniejszymi elementami systemu kontrwywiadowczej ochrony tajemnicy są:

- nosiciele ważnych tajemnic - "N";
- wyselekcjonowane dokumenty - "D"
- pozostałe osoby z newralgicznych komórek - "P"

MODEL ZABEZPIECZENIA NOŚNIKÓW WAŻNYCH INFORMACJI I OCHRONY KONTRWYWIADOWCZEJ OBIEKTU



- osoby postronne ze stanów osobowych jednostki - "W" ;
- oficerowie KW i ich środki pracy - "ZI";
- osoby cywilne /postronne/ z otoczenia systemu - "C";
- agenci wywiadów NATO - "A";
- centrale wywiadów NATO i ich otoczenie - "CW".

Między tymi elementami zachodzą jedno i dwustronne relacje /sprzężenia/. Wśród tych podmiotów poszukiwać należy agentury źródłowej i sygnalizacyjnej przeciwnika.

W określonych warunkach, wymienione elementy połączone są w różne podsystemy, do których należą:

- podsystem dopuszczeń warunkujący relacje między wyselekcjonowanymi dokumentami "D" a osobami upoważnionymi do pracy na nich, nosicielami ważnych tajemnic "N";
- nweralgiczna komórka, w skład której wchodzi elementy wyznaczone przez podsystem dopuszczeń wraz z pozostałymi osobami "P";
- sztab /jednostka wojskowa, instytucja, obiekt/, który połączony jest w określony system przez etat.

Dla potrzeb właściwie zorganizowanej kontrwywiadowczej ochrony, nie można granic tego systemu wyznaczyć jedynie poprzez:

- podsystem ochrony fizycznej wraz z systemem przepustkowym oraz
- podsystem przeciwpeneracyjny.

Obiekt do ochrony kontrwywiadowczej znajduje się na tle otoczenia bliższego oraz dalszego i z tym otoczeniem rozwija się. W otoczeniu bliższym należy jeszcze dodatkowo wyróżnić podsystem oznaczony jako "miejsca styku", czyli miejsca najbardziej wrażliwe na działanie przeciwnika.

Efektywność ochrony kontrwywiadowczej obiektu przedstawionego w ujęciu systemowym będzie więc funkcją dopływu informacji o rodzaju i charakterze wzajemnych relacji. Wynika stąd oczywista potrzeba, by elementem każdego wskazanego podsystemu, był receptor organów KW jakim są środki pracy operacyjnej.

I tak, wiarygodne informacje o charakterze relacji dokument "D" - nosiciel "N" mogą pochodzić tylko od receptorów wywodzących się z kręgu nosicieli "N". Z kolei dane o rodzaju i charakterze relacji między nosicielami "N" a pozostałymi elementami podsystemu oznaczonego jako "miejsca styku" będą stosunkowo pełne i wiarygodne tylko w przypadku, gdy receptor będzie uplasowany w bliskim kręgu towarzyskim tego nosiciela.

Niewiadomą prezentowanego systemu jest jego "pozorny" element oznaczony jako "A" - tj. agent służb wywiadowczych przeciwnika. Jego wykrycie będzie uzależnione od efektywności ochrony kontrwywiadowczej obiektu, czyli głównie od stopnia dopływu informacji o rodzaju i charakterze wzajemnych relacji pomiędzy poszczególnymi elementami podmiotowymi systemu.

W zainteresowaniu oficera KW /homeostat systemu/ winny znaleźć się przede wszystkim te informacje, które mówią o naruszeniu reżimów ochrony i mogą wskazywać na możliwość wywiadowczej infiltracji obiektu.

Przed wszystkim będą to w poszczególnych relacjach następujące informacje:

1/ relacja I

- pozostawianie osób pracujących na wyselekcjonowanych dokumentach po godzinach służbowych bez uzasadnienia;

- przechowywanie lub wnoszenie poza obiekt brudnopisów;
- posiadanie magnetofonów osobistych lub miniaturowych aparatów fotograficznych podczas pracy na tych dokumentach;
- próby wglądu do dokumentów przez osoby nie mające stosownych upoważnień.

2/ relacja II

- próby ewentualnego docierania kadry nieupoważnionej do pracy na wyselekcjonowanych dokumentach do nosicieli i dokumentów;
- indagowanie nosicieli "N" przez kadrę "P";
- gadulstwo "N" w gronie "P".

3/ relacja III

- próby indagowania przez "W" osób z newralgicznych komórek "N" i "P";
- próby docierania "W" do dokumentów "D";
- gadulstwo "N" w gronie "W".

4/ relacja IV

- próby docierania osób z otoczenia "C" do nosicieli i pozostałej kadry;
- gadulstwo nosicieli "N" po godzinach służbowych w miejscu zamieszkania i pozostałych miejscach styku z ludnością cywilną;
- także wcześniej omówione relacje II i III - w warunkach pozasłużbowych.

5/ relacja V

- symptomy nieuzasadnionego zainteresowania sprzętem jednostki oraz samym obiektem ze strony osób z otoczenia, a także ze strony dyplomatów państw NATO.

6/ relacja VI

- wnikliwość opiniowania, w tym ustalanie osób, które w przeszłości miały styk z przeciwnikiem;
- szczelność systemu dopuszczeń, w tym eliminowanie osób zagrożeniogennych.

7/ relacja VII

- funkcjonowanie fizycznego zabezpieczenia obiektu wraz z podsystemem przepustkowym i podsystemem przeciwpent-racyjnym - ustalanie zagrożeń tkwiących na zewnątrz chronionego obiektu /w jego otoczeniu bliższym/.

Z opracowanego modelu wynika, że system kontrwywiadow-
czej ochrony tajemnicy, jako układ zorganizowany może być
całkowicie określony za pomocą trzech najogólniejszych
czynników:

- 1/ materiału, z którego jest ukonstytuowany, a więc osób
stanowiących poszczególne elementy układu, w tym ofi-
cerów KW, środków pracy, elementów "N", "P", "W" i "C".
Miarą ilości tego materiału jest ich liczebność /socio-
masa/;
- 2/ energii, którą układ przetwarza /względnie może przet-
warzać/ albo też która jest w nim nagromadzona. Za
energię nagromadzoną w układzie należy uważać pracę,
którą jego elementy podmiotowe mogą wykonać. Będzie
więc to zdolność robocza lub zdolność wykonawcza pod-
miotowych elementów układu. Wielkość tej energii możemy
mierzyć ilością i jakością zadań ochronnych wykonywanych
przez te elementy /socioenergia/. Zależy ona głównie od
wykształcenia oraz wiedzy fachowej i ogólnej oficerów
KW, stopnia przeszkolenia i zaangażowania środków pracy
oraz stopnia znajomości metod i form działania przeciw-
nika przez wszystkie elementy podmiotowe systemu /wysoka
świadomość zagrożeniogenna/;

3/ struktury, czyli rozmieszczenia materiałów i energii w przestrzeni oraz w czasie, czyli w czasoprzestrzeni.^{1/} Strukturę stanowić będzie sposób zorganizowania sił i środków pracy kontrwywiadowczej do realizacji postawionych zadań oraz ich rozmieszczenie w taki sposób, ażeby były one źródłem informacji dynamicznej o wszystkich wymienionych relacjach zachodzących w systemie.

Funkcje systemu KW ochrony tajemnicy

Prawidłowo zorganizowany system KW ochrony tajemnicy, w tym przede wszystkim ochrony wiadomości o istotnym znaczeniu dla obronności kraju musi spełniać trzy podstawowe funkcje: OGRANICZENIA, WYKRYWANIA i ROZPOZNAWCZĄ.

1/ Funkcja ograniczania możliwości wywiadowczej infiltracji obiektu

Funkcja ograniczania spełnia podstawową rolę w systemie ochrony, gdyż w jej ramach należy wypracować takie reżimy pracy systemu, aby wykluczały one możliwość swobodnego wprowadzenia przez przeciwnika jego agentury do systemu. Dla jej wypełnienia niezbędne jest:

- wnikliwe kwalifikowanie osób na stanowiska;
- wnioskowanie wycofywania upoważnień osobom nie dającym gwarancji przestrzegania tajemnicy;
- instruowanie osób objętych ochroną kontrwywiadowczą o zagrożeniach wynikających z nieprzestrzegania przepisów o ochronie tajemnicy oraz z tytułu infiltracji wywiadowczej;
- kontrola operacyjna systemu zabezpieczenia szczególnie ważnych dokumentów /w fazie opracowywania, ich prze-

1/ Por. M. MAZUR, Cybernetyczna teoria układów samodzielnych, Warszawa 1966, s. 47.

chowywania i obiegu/ lub techniki awangardowej;

- kontrola operacyjna fizycznego zabezpieczenia sztabów /newralgicznych komórek/ i jednostek oraz skuteczność funkcjonowania systemu przepustkowego /organizowanych w oparciu o zasady tzw. "ochrony w głąb"/.

2/ Funkcja wykrywania symptomów wywiadowczego zagrożenia

Rola tej funkcji w systemie ochrony sprowadza się, przy funkcjonujących reżimach ochrony, do ustalania symptomów lub faktów działalności agenturalnej w systemie oraz jego otoczeniu, a także do ustalania naruszeń reżimów ochrony przez elementy podmiotowe systemu. Realizowana jest ona poprzez:

- uplasowanie i ukierunkowanie receptorów na wykrywanie sytuacji zagrożeniogennych;
- uzyskiwanie informacji od osób objętych osłoną KW o zabezpieczeniu wyselekcjonowanych dokumentów, sytuacji w newralgicznych komórkach i różnych aspektach życia tych osób;
- rozpoznanie nosicieli ważnych tajemnic w godzinach służbowych i po pracy;
- ustalanie symptomów zainteresowania wiadomościami objętymi szczególną ochroną ze strony osób nieuprawnionych z wyselekcjonowanych komórek "P", jednostki "W" i osób postronnych z otoczenia "C";
- ustalenie symptomów docierania osób postronnych do nosicieli ważnych tajemnic w otoczeniu obiektu;
- prowadzenie rozmów operacyjnych z osobami przebywającymi w krajach kapitalistycznych i wykorzystanie uzyskanych tą drogą informacji do ukierunkowania pracy ochronno-wykrywczej na obiekcie;
- poprawność oceny informacji kontrwywiadowczych i efektywność ich sprawdzania.

3/ Funkcja rozpoznawcza

System, ażeby mógł skutecznie się chronić, musi posiadać niezbędną, możliwie aktualną wiedzę o przeciwniku, w tym między innymi o jego zainteresowaniach oraz metodach i formach zdobywania informacji. Musi też mieć możliwość osłabiania energii systemu przeciwnika - poprzez wiązanie jego sił i dezinformowanie. Prowadzenie rozpoznania przeciwnika z pozycji zagranicy stanowi więc żywotną potrzebę funkcjonowania systemu i polega na wypracowaniu sytuacji oraz warunków związanych z obiektem do nawiązania styku ze służbami wywiadowczymi przeciwnika. Polega to na:

- wykorzystaniu ustalonych kanałów docierania przeciwnika do wprowadzenia w nie naszych receptorów i wyłaniania sytuacji rokujących nadzieję na ofensywne wykorzystanie;
- podejmowanie inicjatyw zmierzających do wiązania sił przeciwnika i prowadzeniu dezinformacji;
- poprawności dokonywanych analiz z zakresu działalności przeciwnika oraz wykorzystywaniu wypracowanych wniosków z pracy ofensywnej do doskonalenia pracy operacyjnej na chronionych obiektach.

Systemowej ochronie tajemnicy nadaje się wysoką rangę we wszystkich armiach świata. Dla przykładu można podać, że ministerstwo obrony USA w ostatnim pięcioleciu podejmowało szereg przedsięwzięć dla ochrony tajemnicy materiałów i informacji dotyczących obronności kraju. Sporządzony wykaz ważniejszych dla przemysłu wojennego technologii liczy około 800 stron.

Ograniczenia w dostępie do tajemnic wojskowych podejmują wszystkie liczące się armie we współczesnym świecie.

Również w Siłach Zbrojnych PRL w ostatnim pięcioleciu można

odnotować szereg podjętych przedsięwzięć blokujących dostęp do wiadomości i obiektów wymagających szczególnej ochrony. W coraz szerszym wymiarze stosuje się rozwiązania systemowe, nowelizuje przepisy, określa priorytety ochrony.

W aktualnie funkcjonujących działaniach systemowych ochrony tajemnicy na uwagę zasługuje stosowanie zespołu środków zabezpieczających tajemnicę "w głąb". Istotę tego działania ilustruje przedstawiony na stronie 141 schemat. Koncentryczne pierścienie - to poszczególne linie obrony tworzące ochronę przed różnymi typami zagrożeń. Do grupy zewnętrznej zaliczamy wszelkie formy prób rozpoznania potencjału militarnego naszego państwa przez obce służby specjalne. Jako zagrożenia wewnętrzne - działające od i do wewnątrz - traktujemy uwarunkowania subiektywne osłabiające spójność i skuteczność systemu ochrony. Mowa tu więc zarówno o naruszeniu systemów przepustkowych, lekceważeniu zasad pracy przy dokumentach niejawnym, właściwym nadzorze przełożonych jak i gadulstwa i nieprawidłowym korzystaniu z technicznych środków łączności.

Dwie zewnętrzne linie to organizacyjne /administracyjne/ środki ochrony. Główne zadania to koncentracja uwagi na problemach otoczenia chronionego systemu, a więc uniemożliwienie dotarcia do zabezpieczonych wiadomości osobom postronnym, uwrażliwienie na próby przeniknięcia do wewnątrz, techniczne zabezpieczenie obiektu. Granice między pierścieniami w praktyce są płynne, poszczególne przedsięwzięcia z reguły zają- białają się, stanowią swoiste uzupełnienie. Przedsięwzięcia stanowiące treść tych elementów zabezpieczenia realizują w zasadzie dowódcy jednostek /samodzielnie, bądź wypełniając



zlecane zadania szczebla nadrzędnego - np. maskowanie - legendowanie obiektu/.

Każdy obiekt wojskowy posiada stosowne zabezpieczenie wnętrza. Zakres, reżimy i środki zabezpieczenia zależne są od jego charakteru. Im wyższa ranga obiektu w rozumieniu zgromadzonego sprzętu bądź koncentracji wiadomości szczególnie chronionych - tym więcej przedsięwzięć zabezpieczających. Z reguły niezależnie od posterunków stałych w rejonie obiektów specjalnych, wyposażonych w technikę awangardową wystawia się patrole ruchome kontrolujące miejsca z których istnieje dogodny bądź skryty wgląd na teren jednostki. Uzupełnienie stanowią środki techniczne. Skuteczność zabezpieczenia w dużej mierze zależy od jakości przedsięwzięć i środków. Dlatego też tak duży nacisk kładzie się na szkolenie zespołów wyznaczonych do ochrony oraz na wypracowanie prawidłowego systemu kontroli. Ważnym elementem zabezpieczenia jest odpowiednie rozstawienie znaków administracyjnych /głównie zakazu/. Działania te obliczane są przede wszystkim na neutralizację /likwidację/ zagrożeń zewnętrznych, Idzie więc o penetrację dyplomatów, próby zewnętrznego rozpoznania obiektu przez cudzoziemców z kk, bądź inne osoby, jak również uniemożliwienie podrzucenia przez pracowników wywiadów w pobliżu obiektów rozpoznawczych, urządzeń elektrotechnicznych. Są to generalnie rzecz biorąc działania stosunkowo proste i przy dobrze przeszkolonych i właściwie spełniających zadania załogach ochronnych dające odpowiednie efekty..

Główne zadania w zakresie wykrywania i zneutralizowania /zlikwidowania/ wrogiej agentury spoczywają na oficerach

KW. Działają oni w ramach przedstawionego wyżej systemu. Wykorzystując oddane do ich dyspozycji siły i środki, ustalają tą drogą, występujące jeszcze w systemie słabe punkty, we współdziałaniu z dowództwem likwidują istniejące zagrożenia wewnętrzne a więc wszelkie nieprawidłowości w działaniu stanów osobowych, przypadki ujawniania na zewnątrz informacji niejawnych itp. W tym etapie działania, przez stworzenie określonych trudności w dotarciu do interesujących agenta informacji, istnieje większe prawdopodobieństwo ujawnienia jego wrogiej działalności. Chcąc bowiem wykonać określone zadanie musi podejmować działania, które powinny zostać ujawnione. Dlatego tak dużą uwagę przywiązuje się do szkolenia kontrwywiadowczego kadry zwłaszcza tej która zatrudniona jest przy pracach tajnych szczególnie chronionych. Tą drogą można przecież uzyskać tą niesłychanie ważną informację wstępną o nietypowych zainteresowaniach określonej osoby, próbach wejścia w posiadanie informacji wykraczające poza jej kompetencje. Wszelkie tego charakteru sygnały podlegają oczywiście dokładnemu operacyjnemu sprawdzeniu, część określonych postaw czy zachowań może wynikać z cech charakterologicznych, nawyków, a więc może nie mieć nic wspólnego z wrogą działalnością. Systematyczna analiza i selekcja wpływających materiałów daje jednak możliwość oficerom KW koncentracji na sytuacjach czy osobach, gdzie nie ma pewności co do celu działania. Równie aktywne działania oficerowie kontrwywiadu prowadzą dla ujawnienia wrogiej agentury w otoczeniu obiektu. W prawie wszystkich tego charakteru przypadkach, przedsięwzięcia operacyjne prowadzone są we współdziałaniu ze Służbą Bezpie-

czeństwa. Analizuje się przyjazdy cudzoziemców w te rejony, częstotliwość, cel przyjazdu, związki pokrewieństwa. Ustala się wszelkie przypadki prób docierania do jednostki /obiekta, strzeżonej komórki/, nawiązywania kontaktów z kadrą i żołnierzami. Poza rutynowymi sprawdzeniami, bada się powody zabiegania o pracę w jednostce mimo np. niższych stawek. Ciekawsze operacyjnie sygnały są przedmiotem szczegółowych wyjaśnień.

W ramach systemu ochronnego działania operacyjne zastosowane w ochronie tajemnicy "w głąb" uplasowano w centrum. Niezależnie bowiem od zadań zasadniczych - wykrywanie i likwidacja wrogiej struktury - ważnym zadaniem pozostaje operacyjne sprawdzenie skuteczności funkcjonowania pozostałych barier ochronnych. Idzie tu zarówno o prawidłową ochronę fizyczną obiektu, właściwą organizację systemu przepustkowego, odpowiedni nadzór funkcjonalny, jak i należyte - zgodne z przepisami - obchodzenie się z dokumentami niejawnymi oraz zabezpieczenie pomieszczeń. Wszelkie ujawnione nieprawidłowości powinny być niezwłocznie likwidowane. Sposoby eliminacji są różne zależne od skali i przyczyn. Część z nich mogą usunąć sami wykonawcy - nie ma tu potrzeby - w imię harmonijnej współpracy - informowania dowództwa. Poważniejsze naruszenia powinny być jednakże sygnalizowane przełożonym z uwagi na potencjalne skutki i związane z tym zagrożenia.

Kolejne bariery ochronne w dotarciu do tzw. tajemnicy sejfowej tworzą użytkownicy działający w oparciu o funkcjonujące przepisy. Również i w tym przypadku problematyka

ochronna jest zróżnicowana. Przestrzeganie zasad nie dopuszczania osób postronnych do chronionych wiadomości, czuwanie nad prawidłowym obiegiem dokumentów, nie zatrudnianie w określonych pomieszczeniach osób nie posiadających upoważnienia oraz samokontrola zarówno w miejscu pracy i w otoczeniu to podstawowe czynniki gwarantujące skuteczność zabezpieczenia.

2. Analiza i ocena sytuacji operacyjnej
punktem wyjściowym do organizowania
działań w zakresie ochrony tajemnicy

Skutki zakonspirowanej działalności wywiadowczej w codziennym życiu są praktycznie niezauważalne i to tym bardziej im lepiej do tej działalności przygotowany został agent obcego wywiadu. Dlatego też przeciwdziałanie kontrwywiadowcze zmierzające do rozpoznania i wykrycia tej działalności musi być ciągłe, planowe i systematyczne. Punktem wyjściowym organizacji przeciwdziałania kontrwywiadowczego jest analiza sytuacji operacyjnej w ochranianym obiekcie.

Dotychczas brak jest precyzyjnego, naukowego określenia pojęcia sytuacji operacyjnej. Próbę jego zdefiniowania podjął W. Kaczmarczyk, który "sytuację operacyjną" określił jako "zespół elementów występujących w określonym czasie, wewnątrz i na zewnątrz ochranianego obiektu wojskowego, mających bezpośredni wpływ na organizację działań kontrwywiadowczych zmierzających do skutecznej ochrony obiektu wojskowego".^{1/}

1/ por. W.KACZMARCZYK, H.MATUSIK: Zadania i organizacja pracy oficera kontrwywiadu ochranającego jednostki /instytucje/, CS WSW, Mińsk Maz. 1986 r., s. 19 i 20

Takimi podstawowymi elementami składowymi sytuacji operacyjnej są:

- 1/ charakter jednostki, jej zadania i skład osobowy;
- 2/ wrażliwość obiektu na działalność przeciwnika;
- 3/ środki i możliwości oficera kontrwywiadu;
- 4/ sytuacja operacyjna w otoczeniu bliższym;
- 5/ sytuacja polityczna w kraju i międzynarodowa.

Podstawową metodą kontrwywiadowczego rozpoznawania sytuacji operacyjnej jest analiza. Sytuację operacyjną rozumianą jako układ elementów pozostających w określonych relacjach można analizować:

- na określonym terenie /np. strefa nadgraniczna, charakterystyczne skupiska ludności z przewagą mniejszości narodowych/;
- na obiekcie /sztab wyższego szczebla, obiekt podlegający szczególnej ochronie, jednostka wyposażona w technikę awangardową/;
- w konkretnym problemie /kontakty środowisk wojskowych z osobami zamieszkałymi w państwach kapitalistycznych/;
- w określonej sprawie operacyjnej /inne będą elementy analizy sprawy o zabarwieniu szpiegowskim i np. poszukiwawczej za dezertorem zamierzającym zbiec za granicę/;
- w operacji w ramach sprawy /dokonanie eksperymentu, przeprowadzenie kombinacji operacyjnej/;
- w konkretnym przedsięwzięciu.

Bardzo istotnym przedsięwzięciem w procesie kontrwywiadowczej analizy sytuacji operacyjnej jest prawidłowe określenie celu i przedmiotu analizy. W przedmiocie analizy należy określić w jakim zakresie sytuacje operacyjne podajemy badaniom. Badanie może obejmować całość sytuacji

operacyjnej, wówczas mówimy o analizie kompleksowej, bądź jeden z jej elementów, wówczas mówimy o analizie zagadnieniowej.

Cel analizy formułowany jest zwykle przez ściśle sprecyzowane pytania na jakie, badając sytuację operacyjną, poszukujemy odpowiedzi.

Jeśli przedmiotem analizy sytuacji operacyjnej jest np. badanie stanu zabezpieczenia tajemnicy to w procesie analizy uwzględnia się takie zagadnienia jak: prawidłowość zabezpieczenia pomieszczeń /dokumentów, sprzętu/, sposób ochrony fizycznej, głównie pod kątem czy istniejący system gwarantuje skuteczne zabezpieczenie tajemnicy. W tym samym kontekście analizuje się osoby tam zatrudnione, bada się ich osobowość, zdyscyplinowanie w pracy, ewentualne nałogi, zachowanie po godzinach pracy, utrzymywane kontakty mogące negatywnie wpływać na postawy, najczęściej występujące w codziennej pracy nieprawidłowości w zabezpieczeniu tajemnicy i związane z tym zagrożenia. Takimi zagrożeniami może być lekceważenie przepisów dla ułatwienia sobie pracy, gadulstwo, niefrasobliwe działania wykonawców, niska jakość nadzoru przełożonych i osób funkcyjnych. Do tej kategorii zagrożeń zaliczamy również stopień podatności na przestępczą wrogą działalność, uleganie wpływom elementów antysocjalistycznych, fascynację zachodnim trybem życia.

W analizie sytuacji operacyjnej należy również uwzględnić ujawnione przypadki działań wrogiej agentury uplasowanej w danym rejonie oraz fakty penetracji obiektów ze strony dyplomatów i innych osób. Jest to niezbędne dla ustalenia głów-

nych zainteresowań przeciwnika, stosowanych przez niego form i metod działań wywiadowczych, oraz co i w jakim zakresie udało się mu rozpoznać, gdzie tkwią przyczyny niedoskonałości naszego systemu ochronnego.

W dalszej kolejności należy ocenić racjonalność i skuteczność wykorzystania posiadanych sił i środków, zarówno własnych, jak i stosowanych we współdziałaniu z dowództwem, aparatem partyjno-politycznym i innymi działami pracy WSW oraz organami MSW. Efektem tego powinno być wyłonienie komórek i osób, które szczególnie mogą interesować przeciwnika, określenie przypuszczalnych kanałów docierania oraz takie ustawienie sił własnych by skutecznie paraliżować próby rozpoznania chronionych tajemnic.

Analiza sytuacji operacyjnej w zależności od szczebla kierowania zmienia swój zakres, niemniej każdy oficer kontrwywiadu zobowiązany jest do poszukiwania wyczerpującej odpowiedzi na pytania, które stanowią główną treść analizy sytuacji operacyjnej w kontekście ochrony tajemnicy, a mianowicie:

- jakie aktualnie istnieją i z czego wynikają zagrożenia na ochranianym obiekcie;
- na jakich odcinkach /newralgiczne komórki, problemy, sprzęt/ należy koncentrować pracę operacyjną;
- stan środków pracy operacyjnej jakimi aktualnie dysponujemy i jakie są w tym zakresie potrzeby;
- jakie są bieżące i planowane zasadnicze przedsięwzięcia realizowane przez jednostkę i rola oraz zakres zabezpieczenia ich przez kontrwywiad;
- zakres pomocy - niezbędnej do właściwej ochrony - ze strony nadrzędnego organu WSW oraz dowództwa i MSW.

Uogólniając należy podkreślić, że pierwszoplanową rolę w analizie sytuacji operacyjnej - po sprecyzowaniu co i dlaczego chronić na konkretnym obiekcie - odgrywa informacja o przeciwniku, a w szczególności:

- informacje o prowadzonej przez przeciwnika wrogiej i destrukcyjnej działalności w przywiązaniu do określonego terenu, obiektu, problemu lub konkretnej sprawy;
- siły i środki oraz metody jakie przeciwnik może wykorzystać w konkretnych, interesujących nas działaniach;
- agenturalne kadry przeciwnika oraz sposób /jakość/ przygotowania tych kadr;
- prawdopodobne /przewidywane/ kanały przenikania przeciwnika w ochraniane środowiska i na konkretne obiekty;
- techniczne wyposażenie agentury wroga, sposoby łączności;
- charakterystyka zadań realizowanych przez agenturę wywiadowczą;
- wiadomości znajdujące się w posiadaniu przeciwnika o państwie /warunki ekonomiczne, polityczne, potencjał obronny, a także znane mu informacje o metodach działania, siłach i środkach kontrwywiadu/;
- wrogie ugrupowania i środowiska w kraju, które przeciwnik może wykorzystać w destrukcyjnej działalności.

Końcowym etapem analizy sytuacji operacyjnej to badanie własnych sił i środków pracy kontrwywiadowczej.

W tym zagadnieniu uwzględnia się przede wszystkim:

- kwalifikacje aparatu kadrowego organów kontrwywiadu;
- ilość, jakość i rozmieszczenie środków pracy operacyjnej;
- możliwość użycia środków techniki operacyjnej;
- czujność kontrwywiadowczą ochranianych stanów osobowych;
- współdziałanie - jego skuteczność z organami SB, dowództwem i aparatem partyjno-politycznym.

Niezależnie od wymienionych zagadnień w analizie sytuacji operacyjnej muszą być uwzględnione elementy terenu, zarówno w sensie podmiotowym /charakterystyka demograficzna, powiązania z Zachodem, wrogie ugrupowania, mniejszości narodowe/ jak i przedmiotowym /obiekty podlegające szczególnej ochronie, narażone na wrogie oddziaływanie, stan ich fizycznej ochrony/.

Kontrwywiad wojskowy przystępując do dokonania analizy sytuacji operacyjnej wykorzystuje wszelkie dostępne źródła informacji umożliwiające w miarę precyzyjnie odtworzyć stan faktyczny i wypracować racjonalne wnioski do przyszłych działań. Mówiąc o źródłach informacji, z reguły wymienia się:

- publikacje prasowe, radiowe i telewizyjne zarówno własne jak i z państw kapitalistycznych;
- materiały opracowań historycznych i geograficznych określonego regionu;
- informacje od obywateli, kierowników przedsiębiorstw i instytucji oraz organizacji społecznych utrzymujących kontakty z KK;
- materiały z badań stanu ochrony tajemnicy państwowej i służbowej zwłaszcza z ważnych obiektów;
- materiały o faktach przenikania tajemnicy do przeciwnika;
- materiały ewidencji operacyjnej, dane statystyczne opracowane w sposób umożliwiający ich wszechstronne wykorzystanie;
- zeznania ujawnionych szpiegów oraz emisariuszy wrogich ośrodków dywersji ideologicznej;
- informacje tajnych współpracowników uplasowanych za granicą;
- materiały przechwycone w kanale łączności wywiadowczej;
- materiały ze stosowania środków techniki operacyjnej;

- materiały o stanie pracy profilaktycznej oraz własnych siłach i środkach stosowanych w ochronie tajemnicy;
- informacje od kontrwywiadów państw zaprzyjaźnionych.

Informacje składające się na sytuację operacyjną uzyskuje się w czasie prowadzenia pracy kontrwywiadowczej i wykorzystuje dla odpowiedniego zabezpieczenia państwa /wojska, określonego terenu, obiektu, sprzętu/. Informacje tego typu powinny posiadać określone cechy i spełniać niezbędne warunki, a mianowicie:

- trzeba je uzyskać w odpowiednim czasie /by mieć czas niezbędny do podjęcia decyzji/;
- muszą być prawdziwe, obiektywne i wyczerpujące oraz istotne dla organów kontrwywiadu;

Ocenie podlegają zarówno poszczególne dane, jak i całość informacji dotyczących badanej działalności przeciwnika. Każda informacja o wrogiej działalności, jak i ich zbiór, charakteryzują się określonym stopniem ważności, pełności, wiarygodności i aktualności.

Ważność - polega na ustaleniu, na jakie niebezpieczeństwo naraziłaby państwo /wojsko, jednostkę/, ujawniona działalność przeciwnika. Idzie więc o określenie stopnia zagrożenia płynącego z wrogich poczynań przeciwnika, nie zawsze z pozoru oczywistego. Ocena ważności informacji musi zawierać elementy przewidywania /np. jak najskuteczniej wykorzystać zdobyte informacje/.

Pełność - polega na określeniu na ile posiadane przez nas informacje odzwierciedlają faktyczny stan problemu /zagadnienia/ na ile w oparciu o nie możemy formułować obiektywną ocenę badanego problemu.

Aktualność - to przede wszystkim czas uzyskania informacji pozwalający na podejmowanie skutecznych działań zapobiegawczych, to opisywanie rzeczywistości aktualnej a nie czasu minionego.

Pogłębione efekty poznawcze złożonej sytuacji operacyjnej uzyskuje się przez wykorzystanie w działalności badawczej metody analizy systemowej. Analiza systemowa jest szczególnie przydatna dla ustalenia wzajemnego powiązania zależności i uwarunkowań występujących w badanej sytuacji operacyjnej wymagającej kontrwywiadowczych działań wyprzedzających.

Poznawanie sytuacji operacyjnej metodą analizy systemowej obejmuje:

1. określenie celu analizy;
2. określenie przedmiotu analizy;
3. określenie alternatywnych sposobów osiągnięcia założonego celu;
4. zbudowanie modelu rzeczywistej sytuacji operacyjnej na podstawie zdobytych informacji;
5. ustalenie dynamiki zmian zachodzących w sytuacji operacyjnej w przyjętym przedziale czasu;
6. ujawnienie zagrożeń wymagających zabiegów wyprzedzających.

Jeżeli całość możliwych zagrożeń wywiadowczych przyjmą jako system /Zw/ to zmierzając do matematycznego zobrazowania tego systemu należy wyodrębnić następujące podsystemy:

Podsystem I Percepcja zagrożeń ze strony służb specjalnych państw NATO przez kadre i stan zmienny wojska. /P_Z/

Podstawowymi elementami tego podsystemu będą:

1. Stan świadomości zagrożeń wśród kadry i stanu zmiennego $/S_s/$.
2. Znajomość przepisów o ochronie tajemnicy i stopień ich przestrzegania $/Z_p/$.
3. Poziom wiedzy o metodach pracy wywiadów wśród kadry i stanu zmiennego $/P_w/$.

Pomiar podsystemu I jako jednej z części składowych analizy systemowej należy prowadzić według wzoru:

$$P_z = f / S_s + Z_p + P_w /$$

Uzyskany wynik uwarunkowany jest wiarygodnością i ilością informacji dotyczących składników sumy $S_s + Z_p + P_w$.

Podsystem II Możliwe zagrożenia wynikające z kontaktów kadry, stanu zmiennego i pracowników cywilnych z kk. $/M_z/$

Jako podstawowe elementy tego podsystemu należy przyjąć:

1. Dynamika kontaktów z kk $/D_k/$.
2. Złagodzenie przepisów paszportowych $/Z_{pp}/$.
3. Kontakty z kk osób dopuszczonych do prac tajnych $/K_t/$.

Pomiar podsystemu II według wzoru:

$$M_z = f / D_k + Z_{pp} + K_t /$$

Wynik pomiaru podsystemu II stanowią podstawę wnioskowania w sprawie zakresu podejmowanych przedsięwzięć profilaktycznych stosownie do rzeczywistego stanu zagrożeń.

Podsystem III Zagrożenie ze strony kadrowych pracowników wywiadu usytuowanych w oficjalnych placówkach państw zachodnich na terenie Polski. /Z_{kp}/

Jako podstawowe elementy tego podsystemu należy przyjąć:

1. Dynamika ilościowego wzrostu kadrowych pracowników służb specjalnych w Polsce /D_w/.
2. Możliwości realizacji zadań przez kadrowych pracowników służb specjalnych w Polsce /M_{pk}/.
3. Poziom wyposażenia technicznego pracowników kadrowych służb specjalnych w penetracji obiektów wojskowych /P_{wt}/.

Pomiar podsystemu III według wzoru:

$$Z_{kp} = f /D_w + M_{pk} + P_{wt}/$$

Pomiar aproksymacji rzeczywistych zagrożeń jako systemu według wzoru:

$$A_z = f \left[f/S_s + Z_p + P_w/ + f/D_k + Z_{pp} + K_t/ + f/D_w + M_{pk} + P_{wt}/ \right]$$

Analiza systemowa aproksymacji przyjętych orientacyjnie rzeczywistych zagrożeń ze strony służb specjalnych dla Sił Zbrojnych PRL obejmuje 9 elementów składowych systemu.

Cechą charakterystyczną tych elementów składowych jest to, że funkcjonują one jako całość oraz, że istnieją między nimi związki i współzależność - stąd też poddają się one analizie systemowej.

Kontrwywiadowcze działania uprzedzające nigdy nie są celem samym w sobie, a ich istotą jest ochrona Sił Zbrojnych przed zagrożeniami ze strony służb specjalnych państw NATO.

Badanie relacji między rzeczywistym zagrożeniem a skutecznością przeciwdziałania kontrwywiadowczego stanowi podstawę doskonalenia pracy operacyjnej, a przede wszystkim nadawania jej cech racjonalnych.

3. Kontrwywiadowcze zabezpieczenie newralgicznych nośników tajemnicy państwowej w Siłach Zbrojnych

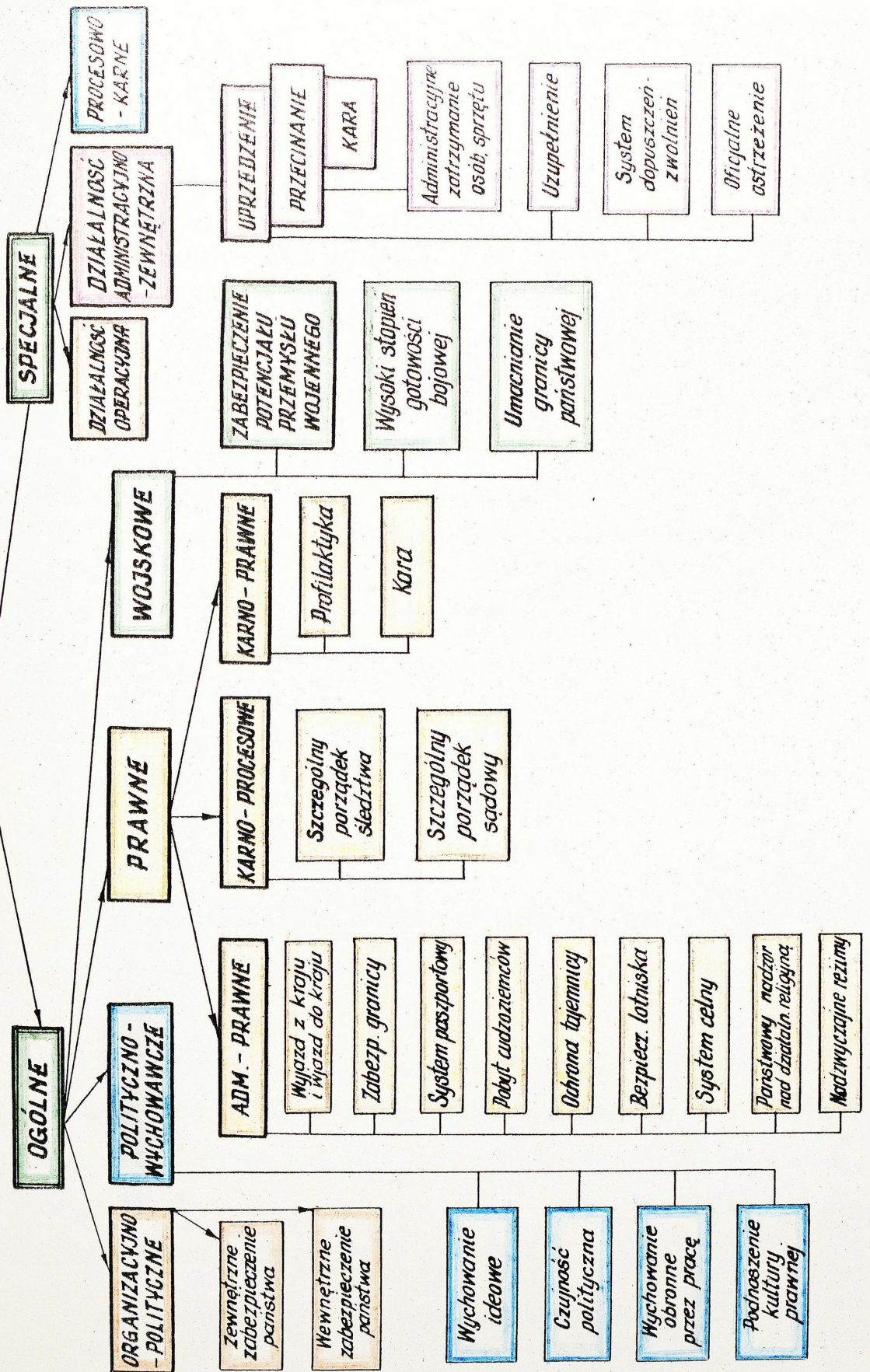
P R L

Każde państwo podejmuje szereg środków gwarantujących jego bezpieczeństwo. Jedną z zasadniczych kwestii w tej dziedzinie jest skuteczne zabezpieczenie tajemnicy państwowej. Pod pojęciem tajemnica państwowa w znaczeniu ogólnym rozumiemy zróżnicowane informacje dotyczące zagadnień politycznych, ekonomicznych, militarnych, naukowo-technicznych mających żywotne znaczenie dla państwa. W celu należytej ochrony wiadomości stanowiących tajemnicę państwową stworzony został w skali państwa system środków pośrednio i bezpośrednio zabezpieczających tajemnicę państwową. System ten ilustruje schemat przedstawiony na stronie 156.

Kontrwywiad wojskowy zajmuje się w zasadzie jednym z elementów tego systemu - ochroną wojsk własnych. Do realizacji tego celu tworzy własny system zabezpieczenia tajemnicy państwowej ukierunkowany na:

- 1/ poszukiwanie, wykrywanie i likwidowanie prób przenikania na obiekty i w ich otoczeniu wrogiej agentury, jak również wykrywanie i rozpracowywanie agentów, którzy zdołali

SYSTEM ŚRODKÓW ZMIERZAJĄCYCH DO ZABEZPIECZENIA TAJEMNICY



przeniknąć w środowiska wojskowe;

- 2/ poszukiwanie, demaskowanie i przecinanie działalności osób, które z własnej inicjatywy zbierają informacje celem przekazania - z różnych powodów - przeciwnikowi;
- 3/ zabezpieczenie obiektów, utrudnianie i niedopuszczenie do infiltracji wojska przez rezydentury wywiadowcze, działające w naszym kraju z pozycji legalnych;
- 4/ udział w pracach dowództwa w zakresie przeciwdziałania wywiadowi technicznemu przeciwnika oraz kontrola skuteczności stosowanych środków zabezpieczających;
- 5/ pomoc dowództwu w wypracowywaniu systemu ochrony tajemnicy;
- 6/ zabezpieczenie osób /posiadających upoważnienie do prac tajnych specjalnego znaczenia wymagających szczególnej ochrony, naukowców, wybitnych specjalistów/ przed wrogimi akcjami przeciwnika;
- 7/ określenie możliwych kanałów przenikania tajemnicy na zewnątrz, wykrywanie źródeł uzyskiwania informacji przez przeciwnika, ujawnianie przesłanek sprzyjających niekontrolowanemu przepływowi informacji niejawnych oraz powodowanie podejmowania przez kompetentnych dowódców przedsięwzięć likwidujących występujące niedomagania.

Jedną z istotnych zasad kontrwywiadowczej działalności na odcinku ochrony tajemnicy jest selektywność, co w praktyce oznacza koncentrowanie sił i środków na wybranych kierunkach zagrożeń. Podejmowanie kontrwywiadowczej ochrony wszystkiego co z wojskiem jest związane w konsekwencji niczego należycie nie chroni, dlatego inaczej trzeba formułować cele i inne stosować środki przy ochronie obiektu specjalnego, a inne w przypadku pułku OT.

W pierwszym przypadku celem ochrony będzie ukrycie

jego rzeczywistego przeznaczenia, parametrów technicznych i wyposażenia. W drugim, rozpoznanie koncentrowane będzie głównie na zabezpieczenie broni, ustaleniu ewentualnych negatywnych postaw lub zdarzeń. W pierwszym przypadku zachodzi konieczność stosowania kompleksowych przedsięwzięć, obliczonych na długoterminową realizację, w drugim wystarczającym jest praca profilaktyczna oficera KW.

Selektywność - jako jedna z naczelných zasad w kontrwywiadowczej ochronie tajemnicy - nabiera szczególnego znaczenia w warunkach funkcjonowania doktryny o wyłącznie obronnym charakterze Sił Zbrojnych PRL. Przyjęta "otwartość" w zakresie restrukturyzacji Sił Zbrojnych oraz ujawnienie danych charakteryzujących moc obronną w poszczególnych rodzajach wojsk i służb, wymaga innego niż dotąd podejścia do problematyki kontrwywiadowczej ochrony tajemnicy.

Nie ulega wątpliwości, że w tej sytuacji, zakres nośników informacji wymagających szczególnej ochrony musi ulec zasadniczemu przewartościowaniu. Uważamy, że Sztab Generalny WP powinien jednoznacznie sprecyzować - dając aneks do części II Instrukcji o ochronie tajemnicy w Siłach Zbrojnych PRL - zakres tematyczny wiadomości, do których dostęp mogą mieć tylko wybrane osoby.

Jesteśmy zdania, że szczególnie chronione winny być tylko te nośniki informacji, które mają charakter strategiczny, OPI, elementy techniki awangardowej, nowe rozwiązania techniczne nie znane stronie przeciwnej oraz te prace naukowo-badawcze, które mogą zrewolucjonizować wykorzystanie określonych rodzajów broni.

Osoby upoważnione do tych prac powinny być z dużym wyprzedzeniem wszechstronnie sprawdzone, odpowiednio przeszkolone, świadome zagrożeń, a w codziennej pracy rygorystycznie przestrzegające ustalonych zasad ochrony tajemnicy.

W naszej ocenie, by sprostać wymogom współczesności konieczna jest pewna nowelizacja obowiązujących przepisów o ochronie tajemnicy. Aktualnie z uwagi na znaczny zakres chronionych tajemnic, stosunkowo często stwierdza się ich naruszanie, bagatelizowanie. W wielu przypadkach występuje swoista "znieczulica", której przyczyn upatrywać można nie tylko w lekceważącym stosunku użytkowników, ale i w tym, że zakwalifikowanie - często niezasadne - znacznej liczby wiadomości jako niejawnych, obniża próg czujności, powoduje bezkrytyczne, jednakowe traktowanie wiadomości zarówno tych istotnych jak i o mniejszym znaczeniu. Podobnie przedstawia się problem ochrony sprzętu, obiektów. Dlatego uważamy, że w systemie ochrony tajemnicy powinna występować gradacja użycia sił i środków zabezpieczających. Ochronę ważnych ze względu na obronność państwa problemów winna cechować kompleksowość. Rozumiemy pod tym pojęciem stosowanie wszelkich dostępnych form i metod ochronnych. W działaniach kontrwywiadowczych szczególny nacisk powinien być położony na przedsięwzięcia profilaktyczne nakierowane na eliminację przesłanek do negatywnych zdarzeń, kontrwywiadowczą osłonę osób oraz wykrywanie obcej agentury. Jako cechę wspólną charakteryzującą ochronę newralgicznych miejsc wojska należy wymienić ścisłe i aktywne współdziałanie z dowództwem w zakresie usprawnienia zabezpieczeń oraz urzędami spraw wewnętrznych głównie pod kątem dokład-

nego rozpoznania bezpośredniego /tzw. bliższego/ otoczenia chronionego obiektu. Idzie tu zarówno o ujawnienie, rozpracowanie i likwidację wrogiej agentury, która może być uplasona na obrzeżach, jak i zabezpieczenie przed penetracją techniczną i wizualną dyplomatów oraz innych osób.

W konkretnych warunkach, priorytet w ochronie musi dotyczyć sztabów, OPI, obiektów specjalnych, techniki awangardowej, prac naukowo-badawczych oraz węzłowych zagadnień ekonomiczno-obronnych. Generalnie nie jest to nowe rozwiązanie, bowiem w latach poprzednich również koncentrowano ochronę na wybranych elementach. Nowum - naszym zdaniem - w tym by w wymienionych komórkach różnicować zabezpieczenie, podnieść rygory tam gdzie wymaga tego interes Państwa i wojska. Rygory te muszą dotyczyć wszystkich elementów systemu. Tak więc poczynając od ochrony fizycznej ściśle należy egzekwować okazywanie dokumentów upoważniających do wejścia, dokładnie identyfikować okazicieli, sukcesywnie sprawdzać stan wewnętrznych urządzeń ochronnych. Mając na uwadze trudności ekonomiczne z jakimi boryka się kraj - postawić na jakość urządzeń alarmowych i instalować je tylko w wybranych nielicznych miejscach mających priorytet w ochronie. Powinien zostać zróżnicowany system przepustkowy /np. nie każda osoba posiadająca prawo wstępu do sztabu mogłaby wejść do pomieszczeń OPI, bądź w których przechowuje się wybrane dokumenty niejawne. Kolejny postulat dotyczy praktycznie sfery świadomości, mianowicie relacji pracowników ściśle chronionych komórek na pojawienie się osoby nieuprawnionej do wejścia.^{1/}

1/ Badania prowadzone w terenowych Zarządach WSW wykazują, że praktycznie żaden z omówionych problemów nie jest w życiu codziennym ściśle przestrzegany.

Celem radykalnego przecięcia przepływu informacji niejawnych na zewnątrz uważamy za wskazane zaprowadzenie ścisłej ewidencji dotyczącej dostępu do wybranych dokumentów niejawnych, precyzyjnego określenia jakie osoby zapoznały się z treścią chronionych wiadomości /dokumentów/. Każdy przypadek udostępnienia tego charakteru dokumentów przez użytkownika innym osobom /przełożeni, współpracownicy - o ile nie wynika to z racji codziennej pracy czy nadzoru/ powinien zostać zaewidencjonowany /kto, kiedy, gdzie, z czyjego polecenia i jak długo materiał wykorzystywał/. Powinna być wprowadzona zasada, że każdy przypadek nawet krótkiej utraty przez użytkownika kontroli nad wybranymi do ochrony dokumentami /wiadomościami, elementami sprzętu/ należy szczegółowo wyjaśnić oraz udokumentować.

Zdecydowanej poprawie musi ulec nadzór służbowy - funkcjonalny. Idzie głównie o wzrost wymagalności w zakresie rozliczania podwładnych, pryncypialnego reagowania na wszelkie naruszenia przepisów, samodzielnego powodowania likwidowania przesłanek sprzyjających ujawnieniu tajemnicy.

Kadra zatrudniona przy pracach niejawnych powinna być systematycznie szkolona w zakresie ochrony, informowania o aktualnych zagrożeniach oraz możliwościach podejmowania przez służby specjalne przeciwnika prób przeniknięcia do wnętrza chronionych przez nas obiektów /komórek/. Należałoby zobowiązać tą część kadry do niezwłocznego meldowania przełożonym o wszelkich stwierdzonych nieprawidłowościach związanych z ochroną obiektu /komórki, pomieszczeń, dokumentów, sprzętu/ jak i wykorzystaniem powierzonych materiałów niejawnych.

Pracę kontrwywiadowczą w newralgicznych miejscach wojska musi cechować bardzo ścisłe współdziałanie z dowództwem. Idzie przede wszystkim o sukcesywną analizę stanu zabezpieczenia, wypracowywanie /modyfikowanie/ przedsięwzięć ochronnych, wymiana informacji na temat ujawnionych nieprawidłowości, omawianie skutecznych środków zapobiegawczych /neutralizujących/. W miejscach tych musi być prowadzona aktywna praca rozpoznawcza w poszukiwaniu wrogiej agentury, zwłaszcza na obrzeżach /otoczeniu/ jak i komórkach administracyjnych spełniających funkcje pomocnicze. Zakres zainteresowań kontrwywiadowczych jest tu szeroki. Poza wyspecjalizowanymi przedsięwzięciami ukierunkowanymi na ujawnianie działalności wywiadowczej, podejmowane muszą być działania dla ustalenia wszelkich przesłanek sprzyjających przenikaniu tajemnicy na zewnątrz. W obszarze kompetencyjnym kontrwywiadu powinny między innymi pozostawać do wyjaśnienia - przypadki nieuzasadnionej wydłużonej pracy przy problematyce szczególnie chronionej, właściwego przechowywania lub wynoszenia poza miejsca pracy materiałów niejawnych, posiadanie osobistych środków technicznego zapisu /utrwalania/ podczas realizacji prac niejawnych. Wyjaśnieniu musi podlegać zestaw zagadnień związanych z próbami wglądu /zapoznania się/ do chronionych wiadomości przez osoby postronne, usiłowania indagacji nosicieli informacji, nieuzasadnione próby nawiązywania z nimi kontaktu przez inne osoby /zarówno w miejscu pracy jak i poza nią/. W sposób zdecydowany oficerowie kontrwywiadu muszą reagować na wszelkie fakty gadulstwa nosicieli ważnych informacji. Oczywiście formy przeciwdziałania mogą tu być zróżnicowane w zależności

od osoby sprawcy, ujawnionych treści, środowiska i okoliczności, niemniej w każdym wypadku należy podjąć działania zmierzające do przecięcia kanału przepływu wiadomości. W uzasadnionych przypadkach powinno się podejmować głębsze wyjaśnienia tych zdarzeń, dla ustalenia powodów, bądź ewentualnych inspiratorów gadulstwa. Jest to jednakże działanie wtórne, głównym bowiem zadaniem w ochronie newralgicznych miejsc wojska, jest jak najszybsza likwidacja kanałów przenikania niejawnych wiadomości na zewnątrz.

Ochrona tajemnicy - jak zaznaczyliśmy wcześniej to realizacja określonych przedsięwzięć w ramach funkcjonującego systemu. Skuteczność działań operacyjnych między innymi będzie zależeć od organizacji systemu wykrywania agentury przeciwnika /konieczność koncentracji na osobach szczególnie zagrożonych wywiadowczo/, podejmowania właściwych metod rozpoznawania wyselekcjonowanych osób /podejrzanych o działalność wywiadowczą/, oraz należytego współdziałania z dowództwem. Duży nacisk należy położyć na systematykę współpracy z Oddziałem V Sztabu Generalnego /właściwymi odpowiednikami na szczeblach niższych/ głównie w zakresie bieżącej wymiany informacji oraz wspólnych analiz stanu wytwarzania, zabezpieczenia i obiegu chronionych szczególnie dokumentów.

I wreszcie skuteczność ochrony zależy od systematycznego doskonalenia metod fizycznego zabezpieczenia newralgicznych miejsc oraz sukcesywnego wprowadzania do ochrony wspomaganie elektronicznego. Jak istotne znaczenie ma ten ostatni element może świadczyć przykład z terenu ZSRR. W rezultacie

ukierunkowanych przedsięwzięć kontrwywiadowczych, podejmowanych przeciwko rezydenturze CIA działającej pod przykryciem ambasady USA w Moskwie, ujawniono a następnie skonfiskowano automatyczne urządzenie wywiadu technicznego przeciwnika, zamontowane na jednym z kabli telefonicznych znajdujących się pod ziemią. Urządzenie składające się z bloku elektronicznego, czujnika indukcyjnego służącego do zbierania informacji oraz anteny KKF było przeznaczone do przechwytywania i zapisywania na magnetofonie rozmów telefonicznych, prowadzonych na tej linii, która łączyła ważny obiekt przemysłu obronnego z instytucjami i organizacjami centralnymi. Z ekspertyzy elementów skonfiskowanego urządzenia wynika, że zostało ono skonstruowane w USA nie wcześniej niż w 1983 r. i jest zunifikowanym seryjnym wyrobem specjalnego przeznaczenia.^{1/}

Zagrożenia podsłuchu niosły z sobą - w naszych warunkach - umieszczone w gabinetach służbowych telewizory lampowe. Oddział Radioelektroniczny WSW stwierdził - i niejednokrotnie demonstrował - że istnieje możliwość dobrego odbioru rozmów prowadzonych w tych pomieszczeniach nawet z odległości około 200 m. Istnieje zatem potrzeba wyprowadzenia z pomieszczeń, w których omawia się problematykę niejawną, tego typu odbiorników. Sukcesywnie powinny być sprawdzane przez fachowców okna pomieszczeń wychodzących na obiekt użytku publicznego w celu sprawdzenia czy nie wykorzystywany jest podsłuch laserowy.

Reasumując - naszym zdaniem - zanim zacznie się tworzyć system ochronny, należy precyzyjnie określić co podlega

1/ Informacja uzyskana z Dep. II MSW za pismem nr ODF-70164/88 z dnia 17.10.1988 r.

szczególnemu zabezpieczeniu. W obecnych warunkach istnieje - przy trwającej restrukturyzacji armii - potrzeba ponownego spojrzenia na problem i konkretnego wypunktowania wiadomości /sprzętu, obiektów/ wymagających ochrony oraz dostosowania do realnych warunków sił i środków zabezpieczających. Niebagatelną rolę będzie tu odgrywać również właściwy dobór kadr przy tych pracach a zatem potrzeba wcześniejszego ich zaopiniowania. Dla przykładu szczególnej ochronie powinny podlegać wybrane komórki sztabowe, pojedyncze obiekty, wyselekcjonowane prace naukowo-badawcze.

Generalnie jako elementy systemu ochronnego dla wyselekcjonowania komórek wojska kumulujących tajemnicę podlegającą szczególnej ochronie przyjęliśmy:

1/ ochrona fizyczna oraz środki zabezpieczające wejście;

zaliczamy tu ogrodzenia, urządzenia alarmowe, posterunki - innymi słowy zewnętrzne środki uniemożliwiające /utrudniające/ nie kontrolowane wejście na teren obiektu;

2/ podsystem przepustkowy;

musi być określony precyzyjnie dokument identyfikacyjny zezwalający na wejście, wyszczególnienie kto ma prawo wydania zezwolenia na wejście osobie spoza kręgu pracowników, oraz funkcjonować właściwie sposób ewidencjonowania osób wchodzących /kto, do kogo, jak długo przebywał, z kim, co wniósł - wynosił, oraz kto udzielił zezwolenia na wejście/;

3/ zabezpieczenie pomieszczeń;

w zależności od możliwości może tu być wykorzystana telewizja przemysłowa /przeгляд korytarzy/, urządzenia alarmowe. Drzwi pomieszczeń chronionych powinny być ponadto plombowane, zaopatrzone w niestandardowe zamki;

4/ nadzór użytkowników i ich przełożonych;

idzie tu - przed przystąpieniem do pracy - o sprawdzenie plomb, zamknięć, a w doraźnych - uzasadnionych - przypadkach sprawdzenie przez przełożonych sposobu złożenia po godzinach pracy chronionych dokumentów /sprzętu/;

5/ nadzór przełożonych w toku pracy;

jako główne elementy należy tu wymienić okresowe sprawdzanie kto pracuje nad problematyką chronioną, w jakich warunkach, jak wygląda bieżący obieg dokumentów, sposób druku i rozliczania oraz ewidencjonowania wiadomości niejawnych, jakość i zakres samokontroli, jej częstotliwość, kontrola przestrzegania przepisów na co dzień, bieżące korygowanie uchybień;

6/ działania operacyjne;

widzimy je w dwóch aspektach: profilaktycznym - bardzo szerokim - ujawniania niedoskonałości w systemie ochronnym, powodowania ich usunięcia oraz utrzymywania szerokiego - systematycznego kontaktu z kadrą dla jej osłony; rozpoznawczo-wykrywczym tj. poszukiwania agentury przeciwnika, jej rozpoznania /w tym kierunki zainteresowań, formy i metody działania, sposoby łączności z ośrodkiem/ i likwidowania. Dotyczyć to będzie zarówno wnętrza obiektu jak i jego otoczenia.

W pracy operacyjnej muszą być przy tym przestrzegane rygorystycznie zasady:

- tajności - czyli metody i formy jakimi kontrwywiad dochodzi do celu nie mogą być znane otoczeniu;
- praworządności - nie wolno więc przekraczać poza ustawowe uprawnienia, formułować bezpodstawnych oskarżeń, powodować dolegliwości o ile nie ma ku temu niepodważalnych dowodów;
- obiektywności^{1/} - czyli uzyskana informacja powinna być przed wykorzystaniem sprawdzona, czy polega na prawdzie, czy we właściwy sposób oddaje stan faktyczny. W działa-

1/ Instrukcja o działalności KW

niach operacyjnych niejednokrotnie spotykamy się jednak z dylematem, że z różnych powodów istnieje konieczność szybkiego poinformowania właściwego dowódcy o zdarzeniu, czy dokonanych ustaleniach, mimo iż nie posiada się pewności co do prawdziwości informacji. Należy w takich wypadkach wyraźnie to zaznaczyć - podając powody dla których nie sprawdzono danych w sposób wyczerpujący;

7/ szkolenie;

widzimy celowość sukcesywnego oddziaływania na świadomość zabezpieczanych stanów osobowych. Chodzi tu o bieżące wskazywanie realnie istniejących zagrożeń zarówno tych obiektywnych jak i subiektywnych, podpowiadanie sposobów ich eliminacji bądź neutralizacji, a także stałe przypominanie obowiązujących norm, ukazywanie skutków ich naruszenia. W działalności szkoleniowej powinni obok przełożonych być wykorzystywani oficerowie KW, a także część - przygotowanej odpowiednio - kadry aparatu partyjno-politycznego;

8/ analiza stanu zabezpieczenia;

skuteczność ochrony musi być poddawana sukcesywnej ocenie na szczeblu dowódcy organizującego zabezpieczenie. Koncentrować należy się na ujawnianiu zagrożeń i słabych punktów ochrony. Mogą to być niedostatki w działaniu sieci telefonicznych i radiowych, może wystąpić emisja promieniowania, niewłaściwe postępowanie z makulaturą, braki w zabezpieczeniu zewnętrznym, wreszcie ułomności ludzkie jak gadulstwo czy lekceważenie obowiązujących przepisów. Stanowi to podstawę do określenia sposobów przeciwdziałania, podjęcia środków do eliminacji przesłanek sprzyjających ujawnianiu tajemnicy oraz do neutralizacji zagrożeń.

Tworzony system dotyczy więc zarówno sfery podmiotowej /chodzi tu przede wszystkim o należyty dobór ludzi - tych tworzących pierścień ochronny, użytkowników, oficerów KW -

legitymujących się określonymi walorami osobowymi, wiedzą specjalistyczną i doświadczeniem oraz personel pomocniczy zatrudniony na obrzeżach/ jak i podmiotowej - gdyż dobór środków ochronnych musi być adekwatny do warunków, miejsca i środowiska w jakich przychodzi nam działać.

Zdaniem autorów - w odniesieniu do wybranych obiektów i zatrudnionych tam stanów osobowych muszą zostać podniesione rygory. Obiekty winny otrzymać dodatkowe zabezpieczenie, w miarę możliwości techniczne, natomiast od ludzi - zwłaszcza kadry - trzeba konsekwentnie i stanowczo żądać pełnego przestrzegania zasad ochrony. Doświadczenia strony przeciwnej wskazują, że podnoszone są systematycznie wymogi wobec osób zatrudnionych przy pracach niejawnych, czynności sprawdzające i zabezpieczające są podejmowane sukcesywnie, nie powoduje to żadnych skojarzeń niedowierzania czy niewiarogodności. Powinna zostać jednocześnie wprowadzona zasada odczuwalnego dodatku finansowego za prace w tego charakteru komórkach.

Kontrwywiadowcza ochrona obiektów specjalnych - a takimi według koncepcji Sztabu Generalnego będzie 1% jednostek WP - wymaga skupienia zarówno wysiłku operacyjnego jak również niezbędnych sił i środków.

Kontrwywiadowczą ochronę obiektu specjalnego należy rozpocząć od momentu podjęcia decyzji o budowie, poprzez prace projektowe, budowę a następnie cały czas eksploatacji. Z uwagi na różnorodność instytucji realizujących poszczególne fragmenty zadania, całość ochrony powinien koordynować szczebel centralny, przeważnie Zarząd.III Szefostwa WSW.

Ochronie przede wszystkim mają podlegać - we wstępnej fazie - dokumenty orientujące o przeznaczeniu obiektu i jego parametrach technicznych, no i oczywiście osoby upoważnione do tych prac. Od momentu rozpoczęcia budowy dochodzą do tego działania zabezpieczające rejon, w którym obiekt powstaje. Część przedsięwzięć operacyjnych musi być realizowana nawet z wyprzedzeniem, a dotyczy ona gruntownego rozpoznania, wspólnie z miejscową Służbą Bezpieczeństwa otoczenia. Niezależnie od organizacji kontroli operacyjnej wyselekcjonowanych osób, sprawdza się jak komentowana jest budowa, na ile "przyjęła" się w miejscowym środowisku legenda, maskująca rzeczywiste przeznaczenia obiektu. W miarę dokonywanych ustaleń należy wprowadzać pewne korekty. Wyłania się osoby przejawiające nadmierne zainteresowanie obiektem, ustala się kontakty, wyjaśnia cel zainteresowań. W rejonach obiektów specjalnych wiele uwagi trzeba poświęcić na ustalenie wszelkich przyjazdów cudzoziemców, analizować ich zachowanie, kontakty, częstotliwość przyjazdów. W podobny sposób traktować należy przyjazdy dyplomatów w pobliżu tych obiektów. Tworzy się więc szczelny system przeciwpeneracyjny. Ma on chronić zarówno przed penetracją osobową jak i elektroniczną. W sumie wyróżnikiem pracy operacyjnej na obiektach specjalnych jest aktywne rozpoznawanie otoczenia, łączenie po analizie sytuacji wydarzeń wewnętrznych z pobytem na obrzeżach osób postronnych.

Równolegle prowadzona powinna być aktywna kontrola stanów osobowych zatrudnionych przy pracach budowlanych. Mimo, iż są to osoby już sprawdzone /a więc uzyskujące w macierzystych jednostkach upoważnienia do określonych prac - jeszcze przed skierowaniem na plac budowy/, ponownie kontroluje się,

czy nie posiadają kontaktów z KK, a w nowych warunkach ustala cel i charakter kontaktów ze środowiskiem cywilnym, ewentualnie zainteresowania wykraczające poza zakres wykonywanych prac, oraz komentarze na temat przeznaczenia budowanego obiektu. Zapewnia się także dopływ informacji o jakości wykonywanych prac oraz funkcjonowaniu systemu ochronnego. Przy obiektach o znaczeniu strategicznym - wyznacza się kolejne strefy ochronne - odpowiednio zabezpieczone ogrodzeniami, sygnalizacją techniczną oraz posterunkami stałymi i ruchomymi. Jądro ochrony w takich przypadkach stanowi strefa zerowa, a więc wewnątrz budowanego obiektu. Wśród stanów osobowych różnicuje się upoważnienia na wstęp do poszczególnych stref. Wewnątrz strefy zerowej podejmuje się również określone rygory ograniczające swobodę poruszania po całym obiekcie poprzez ścisłe wyznaczenie rejonów przebywania.^{1/} Ułatwia to kontrolę, utrudnia orientację o przeznaczeniu obiektów, umożliwia ujawnienie nadmiernych, nieuzasadnionych zainteresowań. Operacyjną kontrolą należy objąć stany osobowe również podczas przebywania poza rejonami zakwaterowania, na przepustkach - idzie o sprawdzenie czy przy tej okazji nie ujawniają oni danych dotyczących obiektów. Praca rozpoznawcza wśród tej kategorii osób musi być kontynuowana również już po zakończeniu budowy - po powrocie do macierzystej jednostki. Sprawdza się ich zachowanie, kontakty, ustala ewentualne komentarze na temat budowy.

Działania rozpoznawcze trzeba prowadzić też wśród osób, które stanowią etatową załogę obiektu. Po zakończeniu służby wojskowej, wykazy tych osób przesyła się do właściwych

^{1/} Mowa tu o zatrudnionych na obiekcie żołnierzach służby zasadniczej, ekipach specjalistycznych instytucji cywilnych.

urzędów spraw wewnętrznych, które zobowiązane są do dalszej kontroli operacyjnej.^{1/} Cykl kontroli operacyjnej kończy się po dwóch latach, o ile nie zaistniały zdarzenia dyktujące konieczność kontynuowania przedsięwzięć operacyjnych.

Okres eksploatacji obiektu wyróżnia się aktywnym rozpoznaniem otoczenia /środowiska cywilnego/, systematycznym sprawdzaniem jakości legendy, zabezpieczenia fizycznego, przestrzegania reżimów pracy na technicznych środkach łączności. O ile w odniesieniu do osób z otoczenia istnieje uzasadnienie prowadzenia długofalowych działań rozpoznawczych, to w stosunku do stanów osobowych, w przypadku istnienia określonych zastrzeżeń /ustalenia uchybień/, należy stosować szeroko rozumiane przedsięwzięcia profilaktyczne. Celem jest niezwłoczna likwidacja stwierdzonych zagrożeń oraz uprzedzenie osób popełniających wykroczenia o konsekwencjach. Od działań profilaktycznych odstępuje się jedynie w przypadkach stwierdzenia znacznego nasilenia złej woli sprawcy.

Podobne zasady doboru osób muszą obowiązywać przy pracach na sprzęcie uznanym za technikę awangardową.^{2/} Obiekty na których sprzęt ten jest rozmieszczony szczególnie zabezpiecza się przed penetracją zewnętrzną, a w otoczeniu prowadzi się rozpoznanie mające na celu ustalenie osób wykazujących zainteresowanie charakterem bądź przeznaczeniem jednostki i posiadany przez nią sprzętem. W tym kontekście też głównie ukierunkowana jest praca wśród pracowników cywilnych zatrud-

1/ Pismo normatywne Szefostwa WSW nr DA-002586 z 4.12.1981 r.

2/ Jaki sprzęt jest zaliczany do tej kategorii, ustala sztab Służb Technicznych. Wykaz na lata 1986-1990 zatwierdził minister Obrony Narodowej w dn. 26.07.1985 r.

nionych na tzw. stanowiskach usługowych /WAK, komórki gospodarcze/. Dużą wagę przywiązuje się do prawidłowej organizacji systemów ochrony, zwłaszcza jakości pełnionych wart. W pracy profilaktycznej kładzie się szczególny nacisk na ujawnienie a jednocześnie przeciwdziałanie wszelkim przypadkom niefrasobliwego ujawniania przed osobami postronnymi walorów sprzętu, jego parametrów technicznych. Należy tu wyjaśnić, iż wysiłek operacyjny przy ochronie techniki awangardowej powinien być zróżnicowany. Chodzi bowiem o pełne utajnienie nie całego sprzętu ale tylko elementów które wpływają na jego tajność /urządzenia elektroniczne, naprowadzające, celownicze/. Należy więc tak organizować działania kontrwywiadowcze by zapewnić dopływ informacji zarówno o stanie i sposobie zabezpieczenia, jak i zachowaniach /postawach/ personelu.

Z zagadnieniem ochrony techniki awangardowej wiąże się problematyka prac naukowo-badawczych. W planie badań i rozwoju techniki wojskowej na lata 1986-1990 ujęto łącznie 22 tematy i prace związane z modernizacją sprzętu, podwyższeniem gotowości technicznej bądź z wprowadzeniem zupełnie nowych urządzeń na wyposażenie wojska.^{1/} Podobnie jak przy obiektach specjalnych kontrwywiadowcza ochrona musi trwać od momentu rozpoczęcia prac projektowych do czasu wdrożenia, czyli wprowadzenia do użytku w jednostkach. W szeregu przypadkach - o ile podwykonawcami są instytucje cywilne - ochrona prac prowadzona powinna być we współdziałaniu ze Służbą Bezpieczeństwa.

Działania ochronne - tak jak w każdym przypadku zabez-

1/ Problematyka powyższa była przedmiotem rozważań Kierownictwa MON na posiedzeniu Zespołu MON w dn. 29.11.1984r.

pieczenia newralgicznych punktów wojska powinna charakteryzować systemowość. Ochrona pomieszczeń, miejsc składowania materiałów naukowych /badawczych/, prowadzona jest na ogólnych zasadach. Wyróżnikiem w tym problemie będzie organizacja i realizacja zadań operacyjnych mających na celu zabezpieczenie naukowców i specjalistów opracowujących określone problemy oraz niedopuszczenie do ich środowiska agentury przeciwnika. Dla zapewnienia bezpieczeństwa podejmuje się przedsięwzięcia:

- utajnienie miejsca pracy i zakresu badań prowadzonych przez te osoby przed otoczeniem;
- instruktaże indywidualne dla naukowców i specjalistów na temat ochrony tajemnicy, szczególnie podczas ich wyjazdów za granicę i w czasie spotkań z przybywającymi do kraju cudzoziemcami z KK;
- zabezpieczenie tych osób na forum międzynarodowym przed wrogimi akcjami przeciwnika /prowokacja, szantaż/.

Szczególne znaczenie ma w zabezpieczeniu tajemnicy prac naukowo-badawczych, precyzyjna analiza sytuacji operacyjnej. W jej ramach należy:

- określać miejsca, gdzie przeciwnik może drogą legalną otrzymywać poszukiwane informacje i wypracowuje środki do zlikwidowania tych kanałów;
- poddawać analizie zachowanie cudzoziemców przybywających na ochroniane obiekty oraz zadawane przez nich pytania, dla ustalenia co przeciwnik wie, z jakiego źródła mógł otrzymać informacje, a także jak zapobiec dalszemu przepływowi wiadomości;
- podejmować konkretne przedsięwzięcia zabezpieczające tajemnicę na czas pobytu zachodnich naukowców bądź specjalistów;
- dążyć do przecięcia niepożądanych kontaktów osób zatrudnionych na tego charakteru obiektach z cudzoziemcami z państw

kapitalistycznych;

- podejmować czynności zabezpieczające przed uzyskaniem niejawnych wiadomości w środkach masowego przekazu.

Uważamy też za wskazane przedstawić postulat, by tym samym naukowcom nie powierzać równolegle kilku szczególnie chronionych prac. Utrudnia to co prawda ochronę oraz rozszerza jej zakres, niemniej prowadzi też - w przypadkach ekstremalnych - że w ręce przeciwnika dostaje się tylko nieznaczny procent naszej myśli technicznej.

Omawiając tą problematykę - naszym zdaniem - należy wskazać na znaczny obszar ochrony kontrwywiadowczej.

Ze względu na hierarchię ważności rozwoju techniki wojskowej wyodrębnia się prace badawczo-rozwojowe "B + R" i wdrożeniowe "W" wchodzące do planu centralnego i resortowego MON.

Istnieje kilka źródeł, z których czerpana jest tematyka prac naukowo-badawczych i rozwojowych, ujmowanych w planach prac B + R + W. Zasadnicze i mające podstawowe znaczenie dla technicznego rozwoju Sił Zbrojnych kierunki rozwoju techniki wojskowej są ustalane w oparciu o wydawane /na okres pięciu lat i rok/ dyrektywy ministra Obrony Narodowej oraz wytyczne szefa Sztabu Generalnego WP. Na ustalenie tych kierunków mają również wpływ wyniki współpracy operacyjno-taktycznej i technicznej, kontynuowanej w ramach wielostronnej i bilateralnej współpracy, koordynowanej przez Dowództwo Zjednoczonych Sił Zbrojnych /Komitet Techniczny/ i Stałą Komisję Przemysłu Obronnego RWPG. Ustalane w tych dokumentach kierunki rozwoju

technicznego są wskazówki do doboru tematyki prac B + R + W.

Ustalana i proponowana do planów przez poszczególne COZ - tematyka prac B + R + W jest rozpatrywana przez Komisje Problemowe Rady MON d/s Naukowo-Technicznych, działające przy tych organizmach. Przy rozpatrywaniu propozycji brane są pod uwagę wyniki przeprowadzonych analiz taktyczno-techniczno-ekonomicznych. W analizach uwzględnia się zasadnicze czynniki i potrzeby docelowe, możliwości krajowej bazy rozwojowej i produkcyjnej, możliwości eksportu, celowość podejmowania prac B + R + W w odniesieniu do możliwości wykorzystania innych źródeł zaopatrzenia, tj. importu gotowego sprzętu, zakupu licencji, możliwości zapewnienia stałej gotowości bojowej i sprawności technicznej nowo wprowadzonego do wyposażenia wojsk uzbrojenia i sprzętu, przez posiadaną w wojskach i kraju bazę obsługową, remontową i szkoleniową.

W przypadkach pozytywnego zaopiniowania przez Komisje Problemowe wysuwanych przez COZ propozycji, przekazuje się je wraz z wstępnymi wymaganiami taktyczno-technicznymi do Szefostwa Badań i Rozwoju Techniki Wojskowej. W propozycjach COZ wysuwają również sugestie co do przyszłych wykonawców.

Na podstawie zgłaszanych propozycji Szefostwo Badań i Rozwoju Techniki Wojskowej sporządza projekt planu badań i rozwoju techniki wojskowej. Opracowany projekt planu jest następnie przedstawiany do zaopiniowania przez Radę MON d/s Naukowo-Technicznych oraz Sztab Generalny. Jednocześnie wysuwane są propozycje odnośnie zakwalifikowania poszczególnych prac do planu centralnego lub resortowego MON.

Po uzyskaniu opinii wymienionych instytucji i wprowadzeniu ewentualnych korekt, projekt planu B + R + W przekazywany jest do uzgodnienia resortom gospodarczym, Komitetowi Przemysłu Obronnego Rady Ministrów, Komisji Planowania przy Radzie Ministrów i Urzędu Postępu Naukowo-Technicznego i Wdrożeń. Po ostatecznych uzgodnieniach do projektu wnoszone są korekty, po czym /o ile istnieje taka potrzeba/ opiniowany jest ponownie przez Radę MON d/s Naukowo-Technicznych, a następnie zatwierdzany przez głównego inspektora techniki WP.

W okresie uzgodnień na szczeblach resortów, opracowywane są przez Szefostwo Badań i Rozwoju Techniki Wojskowej szczegółowe podstawy merytoryczne /wymagania taktyczno-techniczne, zadania naukowe/ oraz prowadzone negocjacje z pośrednikami - wykonawcami, odnośnie szczegółów realizacji i zawarcia przedwstępnych umów lub porozumień.

W pracy kontrwywiadowczej musi się - jak wynika z powyższego - uwzględnić wszystkie etapy zabezpieczenia.^{1/} Szczególną rolę odgrywa w tym względzie ścisłe współdziałanie ze Służbą Bezpieczeństwa, uwzględnianie na określonych etapach i szczeblach wzajemnych przedsięwzięć ochronnych. Z uwagi na liczbę instytucji i osób partycypujących w tych działaniach, są to zadania niezwykle skomplikowane, pracochłonne i wymagające konsekwencji.^{2/}

1/ Zadania dotyczące kontrwywiadowczej ochrony prac naukowo-badawczych i produkcji specjalnej ujęto w Zarządzeniu Szefa WSW nr 06 z dn. 10.07.1985 r. oraz piśmie Szefa WSW nr 0181/16 z dn. 7.02.1984 r.

2/ Dla przykładu można wymienić, że w produkcji zbrojeniowej w Stalowej Woli uczestniczy 88 kooperantów tzw. I stopnia zlokalizowanych w 41 miejscowościach oraz 91 kooperantów II stopnia - dane Wydz. VI Dep. II MSW.

Z reguły przy zasadniczych dla obronności kraju tematach, pracach w których partycypują państwa sojusznicze powinno się je wyodrębnić do oddzielnego prowadzenia i nadzoru. Umożliwia to śledzenie postępu prac, udział w nich konkretnych osób, ujawnianie nieprawidłowości w ochronie, co w rezultacie pozwala na szybką korektę przedsięwzięć własnych i usuwanie niedociągnięć.

W porozumieniu zawartym między Departamentem II, V i VI Ministerstwa Spraw Wewnętrznych a Szefostwem Wojskowej Służby Wewnętrznej określono tryb i zasady współdziałania w zakresie kontrwywiadowczej ochrony prac naukowo-badawczych, projektowo-konstrukcyjnych i produkcji - zleconych przez resort Obrony Narodowej do wykonania w cywilnych instytucjach naukowo-badawczych i zakładach produkcyjnych.

W ramach uzgodnień postanowiono, że organy MSW realizują kontrwywiadowczą ochronę prac od momentu przekazania ich do wykonania cywilnym instytucjom /zakładom/ do czasu skierowania ich rezultatów do ekspertyzy naukowej lub użytkowej eksploatacji w wojsku.

Organy WSW natomiast zabezpieczają pracę od powstania ich koncepcji w wojsku do chwili powierzenia ich dalszemu prowadzeniu instytucjom cywilnym a następnie po przyjęciu efektów tych prac do eksperymentalnej lub użytkowej eksploatacji w Siłach Zbrojnych.

Kontrwywiadowcza ochrona omawianych prac w ramach przysługujących kompetencji podmiotowych obejmuje:

- kwalifikowanie, opiniowanie, kontrwywiadowczą osłonę i rozpoznawanie osób realizujących prace;
- zapobieganie we współdziałaniu z kierownictwem cywilnym instytucji /zakładów/ oraz dowództwem jednostek /instytucji/ wojskowych naruszeniom zasad ochrony tajemnicy państwowej w procesach planowania, organizacji i realizacji prac;
- zapobieganie, wykrywanie, rozpoznawanie i likwidowanie działań obcych wywiadów skierowanych na zdobywanie danych o planowaniu, organizacji i przebiegu zleconych prac oraz ich wyników.

W ramach współdziałania z MSW przewidziano:

- 1/ współpracę w zakresie planowania, organizowania i realizacji wspólnych przedsięwzięć w toku prowadzenia rozpoznania konkretnych osób;
- 2/ uzgadnianie przedsięwzięć wynikających z prowadzonych rozpracowań operacyjnych w tym wszczęcie postępowań przygotowawczych, informowania dowództwa bądź kierownictwa instytucji /jednostek, zakładów/ o ujawnionych nieprawidłowościach, powodowanie odsunięcia określonych osób od wykonywania prac;
- 3/ wzajemne informowanie się o uzyskanych danych dotyczących:
 - zainteresowań wywiadów zachodnich poszczególnymi pracami oraz przejawów tych zainteresowań;
 - symptomów świadczących o zdobyciu przez zachodnie służby wywiadowcze wiadomości związanych z ochranianym problemem /tematem/;
 - przenikania na zewnątrz instytucji /zakładów/ informacji o prowadzonych pracach;
 - faktów lub symptomów przestępczej działalności lub innych ujemnych zjawiskach rzutujących na sprawną realizację prac.

Wojskowa Służba Wewnętrzna zobowiązała się ponadto na etapie powstawania koncepcji /myśli nowatorskiej/ przekazy-

wać właściwym organom MSW informacje o zamiarze, terminie i sposobie zlecenia konkretnym instytucjom prac naukowo-badawczych bądź techniczno-konstrukcyjnych, określić stopień tajności prac i związanej z tym dokumentacji, podać sposób jego obiegu. Podobne informacje przekazuje się na krótko przed przekazaniem określonych prac /tematów/ instytucjom cywilnym, określa się również kooperantów tego zakładu oraz informuje jakie osoby i w jakim zakresie upoważniono do wykonywania prac.

W czasie eksperymentalnego sprawdzania rezultatów prac w jednostkach /poligonach/ wojskowych oraz w stadium wdrażania prototypu do produkcji wymienia się informacje dotyczące:

- terminu, miejsca i sposobu planowanego przekazania rezultatów prac /prototypów/ do eksperymentalnego sprawdzania;
- działań podejmowanych w celu zapewnienia tajności danego przedsięwzięcia;
- sposobu zabezpieczenia prób i osób biorących w tym udział;
- ewentualnych nieprawidłowości wykrytych podczas prób, w toku produkcji i odbioru wojskowego;
- naruszeń zasad ochrony tajemnicy;
- zastrzeżeń co do jakości produktu finalnego i usterek ustalonych podczas eksploatacji w wojsku.

Dla realizacji powyższego oraz oceny skuteczności ochrony organizowane są okresowe narady we właściwych terytorialnie organach.^{1/}

1/ Tematykę prac naukowo-badawczych omówiono stosunkowo szeroko z uwagi na ważność zagadnienia oraz występowanie szeregu niedopracowań w zakresie zabezpieczenia, wynikających głównie z braku przestrzegania pryncypiów systemowych.

Kolejnym istotnym elementem podlegającym szczególnej ochronie są Ośrodki Przetwarzania Informacji.

OPI z uwagi na nagromadzenie w jednym miejscu dużej ilości wiadomości, są obiektami szczególnie narażonymi na oddziaływanie /infiltrację/ ze strony obcych służb specjalnych. Sprzyja temu rosnąca masowość zastosowań środków informatyki w Siłach Zbrojnych oraz nowe metody ich wykorzystywania /praca wielodostępna, przetwarzanie rozproszone, tworzenie sieci komputerowych/. Zwiększa się też możliwość niekontrolowanego dostępu do informacji.

Stąd też podejmowane muszą być odpowiednie środki mające na celu ochronę tajemnicy zgromadzonej w poszczególnych zbiorach informatycznych. Generalnie rozróżnia się trzy zasadnicze grupy ochrony: organizacyjne, techniczne i programowe.^{1/} Z reguły żadna z nich nie występuje samodzielnie, poszczególne elementy są łączone, mówi się wówczas o kompleksowym systemie ochrony zbiorów.^{2/}

Stosowane obecnie w Siłach Zbrojnych przedsięwzięcia ochrony tajemnicy w informatyce w większości bazuje na zabezpieczeniach organizacyjno-administracyjnych oraz częściowo programowych i technicznych.

Z rozpoznania operacyjnego wynika, że działania te

1/ "Instrukcja o organizacji pracy i ewidencjonowania w procesie elektronicznego przetwarzania danych w Siłach Zbrojnych", sygn. Sztab. Gen. 1133/83. Z uwagi na to, że stosunkowo szeroko są opisywane w ogólnodostępnej literaturze, odstąpiono od ich opisywania i rozwijania w omawianym zagadnieniu.

2/ Z. TOPOLEWSKI, Analiza i synteza ochrony informacji w procesach przetwarzania i teletransmisji danych - Wydawnictwo Politechniki Wrocławskiej, Wrocław 1985 r.

nie zapewniają pełnego zabezpieczenia danych, zwłaszcza w odniesieniu do środków wywiadu technicznego. Największe zagrożenia w tym względzie - związane są z emisją promieniowania elektromagnetycznego przez pracujący sprzęt komputerowy. Przeprowadzone pomiary wykazały, że stosowane obecnie metody ekranowania pomieszczeń nie eliminują w pełni tego zjawiska. Po części wynika to z faktu, iż brak jest praktycznych, ale opartych na naukowych podstawach, zasad wykonywania tego typu zabezpieczeń. Podejmowane rozwiązania uwarunkowane są też możliwościami finansowymi i lokalowymi poszczególnych komórek. Niektóre obiekty chronione są poprzez uplasowanie OPI w centrum zabudowań wojskowych w takiej odległości od ogólnie dostępnych dróg i zabudowań by uniemożliwić odbiór promieniowania.

Zagrożenia z tym związane będą narastać. Należy się liczyć, że wprowadzenie dużej ilości mini i mikrokomputerów stworzą nową jakościowo sytuację, wynikającą ze znacznego "rozproszenia" tego sprzętu i jego eksploatacji w pomieszczeniach niechronionych.

Podobnie wygląda sprawa z instalowaniem końcówek abonenckich^{1/} /terminali/.

Niemniej poważnym zagrożeniem jest naruszenie obowiązujących aktualnie przepisów.^{2/} Ustalenia operacyjne wskazują, że nadal powtarzają się przypadki nie respektowania zasad

1/ Powyższa problematyka była przedmiotem rozważań Rady Wojskowej MON w listopadzie 1986 r.

2/ Odprawa oficerów ochraniających kontrwywiadowczo OPI w Zarządzie III S.WSW w dniu 23.10.1984 r.

zabezpieczenia tajemnicy przez osoby odpowiedzialne za ochronę lub obsługę sprzętu. Stwierdza się nieprawidłowości w zabezpieczeniu pomieszczeń przed wejściem osób nieupoważnionych, w tym brak reakcji służb dyżurnych. Do uchybień należy zaliczyć brak opisu klauzuli tajności na dokumentach źródłowych i na tworzonych zbiorach z maszynowych nośników danych oraz przechowywania w wydziale eksploatacji systemów tajnych specjalnego znaczenia w szafach i skrzyniach łącznie z innymi systemami do których dostęp mają różni użytkownicy. Inne nieprawidłowości polegają na nie rejestrowaniu wydruków taśm, dysków magnetycznych oraz na wykorzystywaniu monitora ekranowego zamiast drukarki znakowo-mozaikowej, kopiowaniu zbiorów "TSZ" łącznie ze zbiorami o niższych klauzulach. Stwierdza się przy tym przypadki braku nadzoru ze strony osób funkcyjnych nad eksploatacją systemów o najwyższej klauzuli tajności, co występuje w większości ośrodków przetwarzania informacji. Notowano też fakty jednoosobowego odtwarzania jak i wywożenia taśm do instancji nadrzędnej bez odpowiedniego zabezpieczenia i listów przewozowych.

Ustalenia operacyjne są zbieżne z wynikami kontroli prowadzonych przez Zarząd XIV Sztabu Gen. WP.^{1/} Stwierdzono, że skuteczność systemów ochrony tajemnicy funkcjonujących w filiach WII jest niezadowalająca. Obok przedstawionych już nieprawidłowości wymieniano znaczną liberalizację wymagań w zakresie przestrzegania i znajomości przepisów dotyczących

1/ Załącznik nr 1 do pisma wchodz. 02352 z dn. 26.06.1984 r. - Wyciąg z Protokołu z kontroli stanu ochrony tajemnicy przeprowadzonej w filiach Wojskowego Instytutu Informatyki, wnioski i propozycje.

zasad ochrony informacji i ustalonego porządku technologicznego i organizacyjnego przepisów przetwarzania. Uznano za niewłaściwie realizowane - pod względem tematycznym i fachowym - szkolenia z zakresu omawianego problemu oraz brak działań w kierunku udoskonalenia istniejącego systemu ochrony między innymi drogą adaptacji nowoczesnych metod hardware'owo - software-owych. Nisko oceniono efektywność - w tym zakresie - pracy nieetatowych inspektorów d/s ochrony tajemnicy.

Praktyka dnia codziennego dostarcza szereg przykładów występowania przesłanek do naruszania tajemnicy. Przyczyny tego stanu rzeczy w większości przypadków mają charakter subiektywny. Rygorystyczne przestrzeganie przepisów niewątpliwie utrudnia pracę na sprzęcie. Obsługi, nie zawsze w pełni uświadamiają sobie realność zagrożeń wywiadowczych. Zaabsorbowane swoimi problemami, chęcią szybkiego i efektywnego wykonania zleconych prac - naruszenia przepisów tłumaczą potrzebami służbowymi, nadto tym, iż odstępstwa od określonych zasad nie wywołuje szkodliwych następstw.

W kontrwywiadowczej ochronie OPI duży nacisk trzeba położyć więc na niezwłoczne likwidowanie przesłanek do ujawniania tajemnicy. Skuteczność najlepiej nawet zaprojektowanych zabezpieczeń zależy od zawodności ludzi. Żaden system bezpieczeństwa nie broni się, jeśli człowiek zawiedzie zaufanie.^{1/} Wiele uwagi należy poświęcić na staranny dobór osób upoważnionych do tego charakteru prac i ich operacyjną ochronę.^{2/}

1/ Lance J. HOFFMAN, Poufność w systemach informatycznych, Wydawnictwo Naukowo-Techniczne, Warszawa 1982 r.

2/ Umownie należy przyjąć dobór kadr w ramach metod ochrony - jako metodę kadrową.

We wszystkich organach ZI musi być prowadzone szkolenie na temat obowiązujących zasad ochrony tajemnicy i zagrożeń wynikających z ich nieprzestrzegania. Sukcesywnie powinno powtarzać się sprawdziany ze znajomości przepisów. Na podstawie rozpoznania operacyjnego dokonywać okresowych weryfikacji osób posiadających upoważnienia do prac tajnych specjalnego znaczenia. W stosunku do osób nie reagujących na środki profilaktyczne - bezwzględnie cofać wydane uprzednio aprobaty. Mając na uwadze, że do prac w OPI upoważnia się osoby szczególnie starannie sprawdzone, ich kontrwywiadowczą ochronę należy organizować w ścisłym współdziałaniu z nimi. Po rozpoznaniu postaw i zachowań pracowników, systematycznie przypominać istniejące zagrożenia, wskazywać sposoby ich likwidowania bądź minimalizowania, zabiegać o stabilność kadrową zarówno wśród personelu jak i ochraniających oficerów KW. Do ochrony OPI należy kierować oficerów przeszkolonych w zakresie specyfiki tych obiektów, w miarę możliwości posiadających wykształcenie zbliżone do problematyki ochraniających obiektów, oraz legitymujących się już określonym stażem służbowym. Ułatwia to nawiązywanie kontaktów, zrozumienie wewnętrznych problemów tych kolektywów a także szukanie racjonalnych rozwiązań umożliwiających skuteczne zabezpieczenie. Wiąże się z tym konieczność dobrej znajomości sytuacji operacyjnej. Mówiąc o tym trzeba przede wszystkim dać odpowiedź na pytanie: jakie dane są zbierane oraz kto i w jakim zakresie ma do nich dostęp, jak dalece trzeba chronić każdy z rodzajów wiadomości, jakie są słabe punkty systemów informatycznych i zasobów, jakie jest ryzyko przypadkowego bądź intencjonalnego ujawnia-

nia, względnie zniszczenia informacji, jakich technologicznych zabezpieczeń użyto oraz z jakim efektem, a także jakie najczęściej występują naruszenia już obowiązujących przepisów /zabezpieczeń/. Te bowiem elementy determinują dobór sił i środków dla uzyskania skutecznego zabezpieczenia tajemnicy.

Tak jak w przypadku innych newralgicznych komórek wojska, działania operacyjne wkomponowane muszą być w całość systemu ochronnego. Ważną rolę spełnia również właściwie pojęte i realizowane współdziałanie zarówno z dowództwem jak i właściwymi organami SB zwłaszcza tam gdzie OPI świadczą usługi na rzecz instytucji cywilnych. Metody ochrony w systemie informatycznym bez teletransmisji ilustruje rysunek na stronie 186.

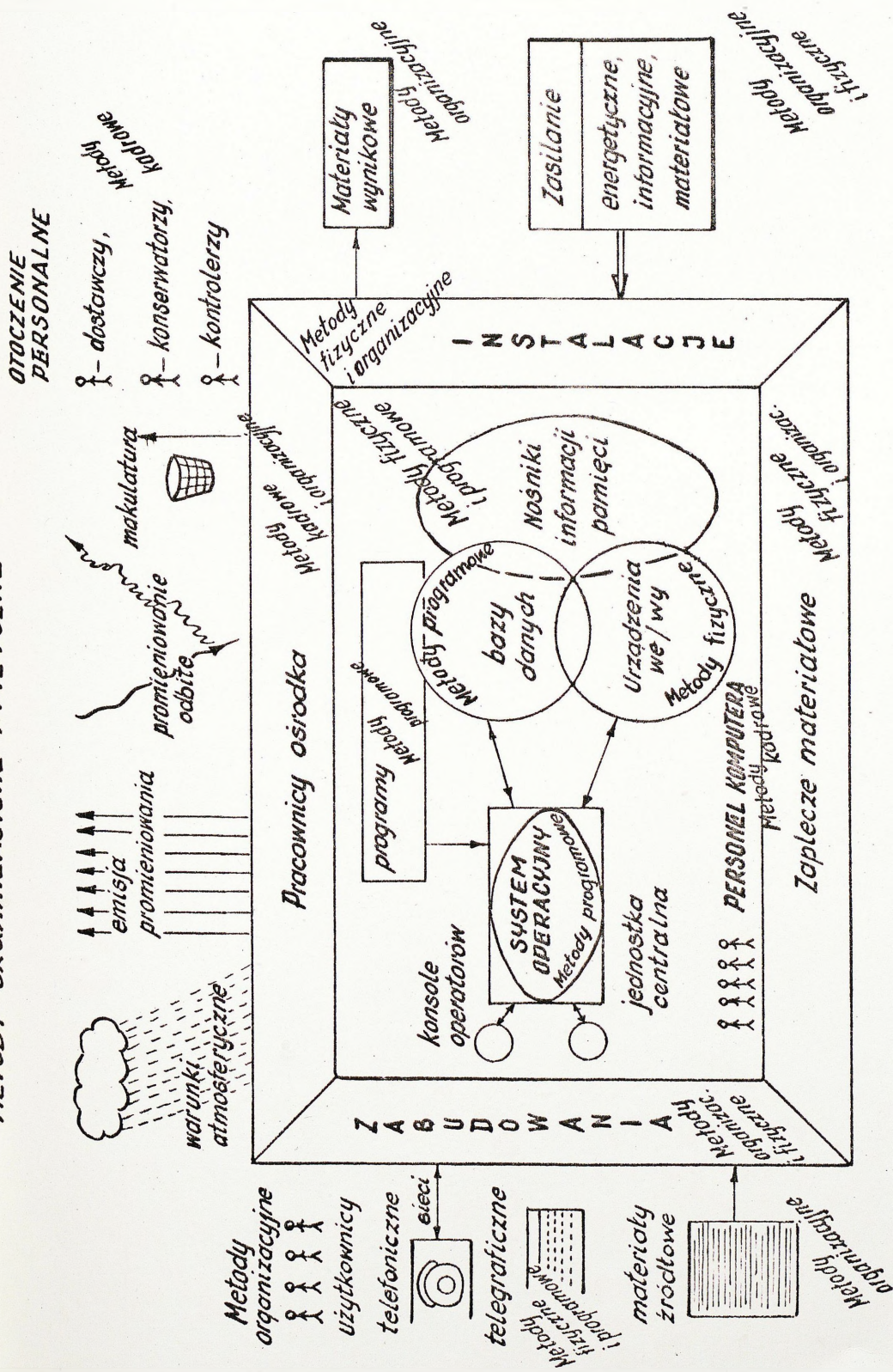
4. Przeciwdziałanie penetracji obiektów wojskowych przez dyplomatów i cudzoziemców oraz inne osoby

Jednym z elementów zabezpieczenia Sił Zbrojnych przed wywiadowczym rozpoznaniem ze strony służb specjalnych przeciwnika jest ochrona obiektów wojskowych przed penetracją.

W myśl obowiązujących dokumentów normatywnych, penetracja obiektu wojskowego jest jedną z metod działalności wywiadowczej stosowaną przez dyplomatów i cudzoziemców z państw

METODY OCHRONY W SYSTEMIE INFORMATYCZNYM BEZ TELETRANSMISJI

METODY ORGANIZACYJNE I FIZYCZNE



OTOCZENIE PERSONALNE

- dostawczy, *Metody kadrowe*
- konserwatorzy, *Metody kadrowe*
- kontrolerzy, *Metody kadrowe*

makulatura
promieniowanie odbite

emisia promieniowania

warunki atmosferyczne

Metody organizacyjne

użytkownicy

telegraficzne

sieci

telegraficzne

Metody fizyczne i programowe

materiały źródłowe

Metody organizacyjne

Metody fizyczne i organizacyjne

Metody fizyczne i organizacyjne

Metody fizyczne i organizacyjne

Metody fizyczne i organizacyjne

Metody fizyczne i organizacyjne

Metody fizyczne i organizacyjne

Metody fizyczne i organizacyjne

Metody fizyczne i organizacyjne

kapitalistycznych bądź przez inne osoby, które poprzez obserwację /bezpośrednią lub przez użycie środków technicznych/, zbierają o tych obiektach informacje stanowiące tajemnicę państwową lub służbową.

W świetle dotychczasowych doświadczeń za prowadzącą penetrację należy uznać osobę, która w celu zdobycia informacji wywiadowczych:

- wtargnęła pieszo lub środkiem transportu na strzeżony lub oznaczony tablicami ostrzegawczymi teren wojskowy;
- w sposób otwarty lub skryty prowadziła bezpośrednią /lub przy użyciu środków technicznych/ obserwację wizualną obiektów wojskowych;
- dokonywała - wbrew zakazom - zdjęć fotograficznych lub filmowych, sporządzała szkice, rysunki obiektów wojskowych bądź nanosiła na mapę określone dane z obserwacji tych obiektów;
- nagrywała na taśmę magnetofonową lub w inny sposób dokumentowała wyniki swoich spostrzeżeń o obiektach wojskowych;
- pobierała próbki gruntu lub innych materiałów do badań i analiz;
- podejmowała inne działania rozpoznawcze.^{1/}

Jako zasadnicze cele penetracji należy przyjąć:

- rozpoznanie obiektu - szczególnie w przypadkach budownictwa specjalnego nowych inwestycji, rozformowania bądź przeobrażania jednostki;
- potwierdzenie lub pogłębienie danych pochodzących z wywiadu technicznego, bądź agenturalnych - głównie w przypadkach zaistnienia zmian w obiekcie lub jego otoczeniu.

1/ Zarządzenie Szefa WSW nr 04 z dn. 14.05.1981 r. w sprawie zadań i zasad postępowania organów WSW w zakresie kontrwywiadowczej ochrony obiektów wojskowych przed penetracją. Przepisy o ochronie tajemnicy w Siłach Zbrojnych PRL cz.I Wydawnictwo MON - 1987, rozdz.4 §24 - nakładają obowiązek na żołnierzy pełniący służbę wartowniczą lub patrolową zatrzymywania osób dokonujących wyżej opisane działania.

Penetracja może być również traktowana przez pracowników wywiadu jako kamuflaż zadań specjalnych wykonywanych w terenie dla odwrócenia uwagi kontrwywiadowczych służb, zamaskowanie zasadniczego celu wyjazdu /spotkanie z agentem, podjęcie materiału wywiadowczego, organizacja skrzynki kontaktowej/. Podejmowane czynności mają stworzyć wrażenie, iż pobyt w określonym rejonie podyktowany był wyłącznie chęcią rozpoznania obiektu wojskowego.

Zasadniczy udział w dokonywaniu penetracji mają pracownicy ambasad głównych państw NATO akredytowanych w Polsce, a szczególnie attache`s wojskowi.

Dla ujednoczenia poglądów, jak i wyostrenia czujności służb dyżurnych jednostek oraz stanów osobowych Wojskowej Służby Wewnętrznej generalnie przyjęto - na podstawie uzyskanych doświadczeń - że każdy przejazd dyplomaty drogą bezpośrednio przyległą do zabudowań koszarowych czy innych obiektów lub strzeżonych rejonów wojskowych, bez względu na to czy zostały naruszone obowiązujące w tym rejonie przepisy administracyjne, czy też nie - traktować należy jako penetrację.

Na przestrzeni ostatniego dziesięciolecia formy penetracji obiektów wojskowych przez przedstawicieli placówek dyplomatycznych akredytowanych w Polsce uległy wyraźnym zmianom. W latach 70-tych dyplomaci stosunkowo często naruszali obowiązujące w naszym kraju przepisy administracyjne, w ostatnim okresie przypadki tego charakteru należą do rzadkości. Stwarza to dodatkowe trudności w rozpoznaniu działalności dyplomatów i zabezpieczeniu obiektów wojskowych, ponieważ oczywiste naruszenie przepisów było stosunkowo łatwe w sensie

udokumentowania i podjęcia określonej interwencji.

Zmiana działań nie oznacza wcale, iż zmalało wywiadowcze zainteresowanie obiektami wojskowymi. Przeciwnie, według ustaleń, zarówno MSW jak i WSW, liczba wyjazdów penetracyjnych ciągle wzrasta. Aktualnie najczęściej spotykaną techniką penetracji jest bezpośrednia obserwacja wizualna lub z użyciem optycznych przyrządów rejestrujących, prowadzona z wnętrza samochodu poruszającego się na zmniejszonej szybkości drogami publicznymi obok obiektów, miejsc dyslokacji sprzętu lub kolumn wojskowych.^{1/}

Jednym ze sposobów jest też piesze penetrowanie rejonów przyległych, prowadzenie obserwacji wnętrza obiektów z dogodnie położonych punktów terenowych - bez naruszania przepisów administracyjnych.

Geografię penetracji obiektów wojskowych przedstawia zamieszczony na stronie 190 schemat.

Ustalenia operacyjne wskazują na ścisłą współpracę dyplomatów zachodnich w zakresie penetracji obiektów wojskowych. Rolę ośrodka wypracowującego i koordynującego na terenie naszego kraju wspólne działania spełnia attachat wojskowy USA. Wielokrotnie notowano wspólne wyjazdy wywiadowcze /np. Brytyjczyków z Kanadyjczykami - lata 1982-1983 i Duńczykami 1984 - 1985/.

1/ Charakterystycznym jest przykład zatrzymania w lutym 1985r. attache wojskowego USA - płk F. Meyera, który poruszając się na zwolnionej szybkości samochodem z duńską rejestracją cywilną, fotografował obiekty 2 prr i 20 OSSR w Przasnyszu. Po zatrzymaniu przez pracowników MSW, usiłował zniszczyć wykonane filmy. Mimo to ujawniono dwie klatki filmowe na których utrwalony był sprzęt wojskowy. Powyższe oraz inne materiały dowodowe stanowiły podstawę wydalenia wymienionego z Polski.

Dokładne dane liczbowe stwierdzonych faktów penetracji obiektów WP w latach 1981-85 obrazuje zestawienie wykonane na podstawie materiałów operacyjnych Szefostwa WSW.

Ostatnie lata tzn. rok 1987 i 1988 wskazują na znaczne uaktywnienie attachatów wojskowych małych krajów wchodzących w skład NATO. Dla przykładu attachat belgijski - praktycznie nie notowany dotychczas w wyjazdach penetracyjnych, wykonał w 1987 r. 56 tego charakteru podróży. Zauważalna jest również bliska współpraca attachatów Francji i Belgii - dowodem 8 wspólnych podróży penetracyjnych.^{1/}

Geografia ich wyjazdów jest w zasadzie w poszczególnych latach podobna. Stałymi rejonami wyjazdów są województwa północne i zachodnie kraju, zwłaszcza te, gdzie stacjonują pierwszorzutowe jednostki wojsk lądowych Śląskiego i Pomorskiego Okręgu Wojskowego oraz Wojsk Lotniczych i OPK wyposażone w nowy sprzęt.

W zespole ujawnionych penetracji stwierdzono pobyty dyplomatów w garnizonach, w których stacjonują jednostki o drugorzędnym znaczeniu, gdzie nie dokonywano żadnych zmian strukturalno-wyposażeniowych i nie było ruchu wojsk. Zakładamy, iż dyplomaci przejazdów tych dokonywali dla zakamuflowania rzeczywistych zainteresowań bądź zamierzeń. Częstym terenem ich pobytu są również poligony i miejsca przeprowadzania ćwiczeń. Jedną ze stereotypowych metod działania jest obserwacja wizualna przegrupowujących się drogami publicznymi bądź kolejami wojsk.

1/ Informacja i wytyczne dot. usprawnienia kontrwywiadowczego zabezpieczenia jednostek WP i AR z 31.05.1988 r. Dokument Wyzd. VI Dep. II MSW /bez numeru/.

Z E S T A W I E N I E

liczbowe stwierdzonych faktów penetracji
obiektów LWP w okresie 1981-1985

Państwa	Penetracja dokonana przez dyplomatów		Penetracje dokonane przez cudzoziemców przebywających w PRL.	Ogółem
	wojskowych	cywilnych		
W. Brytania	120	4	9	133
U. S. A	111	28	11	150
Kanada	44	-	1	45
Francja	79	17	21	117
R. F. N	-	11	241	152
Pozostałe państwa NATO	25	5	35	65
Inne państwa	24	31	51	106
Ogółem obcokrajowcy	403	96	396	868

Obywatele PRL	63
---------------	----

Ogółem penetracji	931
-------------------	-----

Z E S T A W I E N I E

liczbowe stwierdzonych faktów penetracji obiektów
LWP w okresie 1981 - 1985

Osoby dokonujące penetracji	1981	1982	1983	1984	1985
Dyplomaci państw NATO	14	23	98	154	155
Dyplomaci innych państw	-	5	9	24	17
Cudzoziemcy państw NATO	7	11	74	124	102
Cudzoziemcy innych państw	-	2	16	17	16
Obywatele PRL	7	7	12	18	19
OGÓLEM PENETRACJI	28	48	209	337	309

W ostatnich latach obserwuje się postępującą technizację metod pracy attache`s wojskowych państw kapitalistycznych. Podnoszona jest sprawność techniczna oraz udoskonalane systematycznie oprzyrządowanie samochodów wykorzystywanych do penetracji. Wyposażane są one w najnowsze urządzenia służące do prowadzenia nasłuchu radiowego, utrzymywania łączności z ambasadą oraz zapewnienia bezpieczeństwa przed rozpoznaniem organów MSW i WSW. Stwierdzono, że dyplomaci brytyjscy zostali wyposażeni w urządzenia elektroniczne do opracowywania - kodowania zdobytych informacji wywiadowczych.

Analiza operacyjna wskazuje, że około 25% stwierdzonych penetracji dyplomatów dokonanych zostało w czasie, gdy w jednostkach miały miejsce przedsięwzięcia nie wynikające z codziennego toku zajęć /ćwiczenia, przebazowanie, wprowadzenie podwyższonych stanów gotowości bojowej, wykonywanie lotów/. Wówczas intensywniej niż zwykle pracowały tam środki radiowe. Należy sądzić, że w oparciu o przechwycone przez przeciwnika drogą radiową informacje lub ustalenia wywiadu kosmicznego, dyplomaci otrzymali zadania udania się w określone rejony. W takich przypadkach, dyplomaci byli obecni w rejonie danej jednostki /rejonu ćwiczeń/ w kilka lub kilkanaście godzin po rozpoczętych tam przedsięwzięciach wojskowych, przy czym najczęściej zatrzymywali się w odległości 2-5 km od obiektu w miejscach ogólnodostępnych, skąd możliwe było ustalenie /potwierdzenie/ - poprzez nasłuch lub obserwację wizualną - interesujących ich zagadnień.

Można również z dużym prawdopodobieństwem przyjąć, iż pobyt dyplomatów w różnych garnizonach, w tym w niektórych

kilkakrotny, ma na celu wychwycenie wszelkich zmian tam zachodzących w zakresie budownictwa wojskowego, sprzętu, ochrony fizycznej i dyslokacji pododdziałów.

Dyplomaci zachodni - zwłaszcza Brytyjczycy - stosują już od kilku lat zasadę kilkudniowych podróży w teren,^{1/} z nocowaniem w uprzednio rezerwowanych pokojach hotelowych. W szeregu przypadkach stwierdzono, że dyplomaci mimo dokonanej rezerwacji w ogóle nie stawili się w oznaczonym czasie i miejscu, a noclegi organizowali we własnym zakresie.

Każdy wyjazd w teren jest przez nich dokładnie przygotowywany. Oprócz wspomnianego już sprzętu technicznego, dyplomaci wyposażeni są w wysokiej jakości sprzęt magnetofonowy, mapy planowanych rejonów wyjazdów. Wszelkie spostrzeżenia i ustalenia dokonywane w toku podróży, są dokumentowane już w czasie pobytu w terenie w formie zdjęć, zapisów magnetofonowych, notatek, bądź rysunków /szkiców/ na mapach. Posiadany sprzęt oraz torby z notatnikami są pilnie strzeżone, z reguły dyplomaci przez cały czas podróży noszą je przy sobie.

Mając świadomość, iż w czasie podróży podlegają kontroli operacyjnej, dyplomaci starają się zmylić czujność organów kontrwywiadowczych, próbują - jadąc na dużej szybkości oderwać się od obserwacji, ukryć w masywach leśnych

1/ Informacja Szefostwa WSW dla Ministra Obrony Narodowej nr DA-0139/10 z dn. 24.01.1986 r. dot. działalności penetracyjnej w 1985 r., w której podano, że w 1985 r. 36 pracowników attachatów z 8 ambasad państw NATO odbyło w celach wywiadowczych 188 podróży za Warszawę, przebywając w terenie łącznie 382 dni. W tym czasie 690 razy notowano ich pobyt w różnych garnizonach, z czego 140 uznano za ewidentne penetracje.

bądź też nadać wywiadowczym wyjazdom charakter weekendowy. Niejednokrotnie do działań wywiadowczych dyplomaci wykorzystują członków rodzin, zwłaszcza do ubezpieczania, bądź nadania większego prawdopodobieństwa oficjalnemu celowi wyjazdu.

Ośrodki wywiadowcze do działań penetracyjnych wykorzystują również korespondentów, przedstawicieli firm polonijnych, osoby przyjeżdżające do Polski służbowo, a także przywożących dary dla instytucji kościelnych.

Przede wszystkim jednak, jako bazę wywiadowczą należy traktować osoby przyjeżdżające do Polski w celach turystycznych. Szczególne zagrożenie ze strony tej kategorii osób dostrzegamy w turystach RFN. Na 369 ujawnionych w latach 1981-85 penetracji obiektów wojskowych przez cudzoziemców z KK - 241 dokonali obywatele RFN.

Wcześniej spotykanym sposobem penetracji było fotografowanie obiektów wojskowych, naruszanie przepisów drogowych: wjeżdżanie lub zatrzymywanie się w strefach zabronionych, lub wkraczanie pieszo w rejon obiektów. Podczas zatrzymań wyjaśniali, iż chcieli utrwalić miejsca z którymi byli związani rodzinie, bądź tłumaczyli się nieświadomością - iż postępowaniem swym naruszyli przepisy obowiązujące w naszym kraju.

Charakterystyczne dla penetracji dokonywanych przez obywateli RFN jest to, że w około 50% ujawnionych przypadków prowadzili je nie w docelowych miejscach podróży, lecz "niejako po trasie", bądź zbaczali z niej w rejony obiektów wojskowych.

Patrząc na problem perspektywicznie - na podstawie materiałów operacyjnych - należy się liczyć z dalszą eskalacją tej metody działań wywiadowczych i to zarówno ze strony zachodnich dyplomatów jak i cudzoziemców z KK przebywających czasowo na terytorium PRL.

Analiza materiałów operacyjnych za lata 1981 - 1988 świadczy o systematycznej eskalacji działań penetracyjnych. Możemy z dużym prawdopodobieństwem prognozować, że następować będzie dalsze narastanie tych działań, przy czym z uwagi na postępującą w kraju otwartość i jawność w zakresie obronności, formy penetracji mogą ulegać zmianom.

W dynamicznie zmieniających się warunkach istnieje pilna konieczność wypracowania nowych przedsięwzięć ochronnych. Potrzeby takie determinowane są również planowanymi przez Sztab Generalny WP zmianami w zakresie utajnienia poszczególnych jednostek. Naszym zdaniem fizyczna ochrona jednostek - w tym względzie - pozostać powinna bez zmian, tzn. służby i warty winny czuwać by osoby postronne nie przekraczały funkcjonujących aktualnie przepisów /zarówno wojskowych jak i administracyjnych/ szczególnie w zakresie bezprawnego wkraczania na teren wojskowy. Zabezpieczony powinien być tu również teren przyległy zwłaszcza w przypadkach uzyskania sygnału o pojawieniu się dyplomatów w danym rejonie. Widzimy celowość organizacji w wybranych punktach ZPO, dysponujących łącznością między sobą i oficerem dyżurnym, wystawianie patroli

1/ 1% jednostek planowany jest do pełnego utajnienia, 10% do wzmożonej ochrony, pozostałe praktycznie pozostają odkryte.

ruchomych do kontroli obrzeży, zwłaszcza w newralgicznych punktach, bądź miejscach szczególnie narażonych /bądź ułatwiających/ na penetrację. Doskonalić trzeba systemy powiadamiania o ruchach osób podejrzanych w rejonach zabezpieczanych. Przed osobami biorącymi udział w ochronie trzeba postawić konkretne zadania. O ile patrole mają nie dopuścić w zabezpieczany rejon osób niepożądanych, a więc będą to działania stricte oficjalne, to załogi ZPO powinny być przeinstruowane w zakresie skrytej obserwacji osób, które wkroczyły na ten teren zastrzeżony oraz dokumentowania ich zachowania /zdjęcia bądź filmowanie/, bez zdradzania swojej obecności. Załogi ZPO powinny mieć ustalone stałe składy, przeszkolone przez oficerów KW. Niezależnie od powyższego - w uzasadnionych przypadkach - można organizować zasadzki w celu ujęcia osoby penetrującej i przejęcia dowodów rzeczowych. Ten element łączy się jednak ściśle z pracą operacyjną i decyzje w tej sprawie powinny zapadać co najmniej na szczeblu Zarządu WSW OW/RSZ.

W nowych jakościowo warunkach muszą się zmieniać również formy pracy operacyjnej. Uważamy, że każdy ustalony przypadek penetracji - bez względu na obiekt powinien być dokumentowany operacyjnie i sygnalizowany centrali. W większości zdarzeń, tych zaistniałych przy jednostkach odkrytych - poza oczywiście szczególnymi charakterystycznymi faktami - nie należy podejmować innych działań. Wysiłek operacyjny natomiast powinien być skoncentrowany przy wybranych obiektach. Przede wszystkim pogłębienia wymaga praca rozpoznawcza w otoczeniu /idzie o ewentualną bazę, kontakty osoby penetrującej

z miejscowym środowiskiem/. Duży nacisk należy położyć na sprawdzenie czy w chronionym terenie nie zainstalowano tzw. "podrzutków" tj. urządzeń elektronicznych wychytujących promieniowanie, sygnały wychodzące z obiektu a następnie przekazujących je poprzez satelity, bądź urządzenia zainstalowane w samochodach dyplomatycznych.

Należy stwierdzić - na podstawie analiz wykonywanych przez Szefostwo WSW - że zabezpieczenie obiektów wojskowych przed penetracją wywiadowczą, jego skuteczność ulega systematycznej poprawie. Ustalenia na 1987 r. wskazują, że 75% penetracji ujawniono przez garnizonowe systemy przeciwpenetracyjne, około 12% przez załogi zakrytych punktów obserwacyjnych, 13% to efekt ustaleń środków pracy operacyjnej.

Do rzadkości należy zaliczyć przypadki niekontrolowanego pobytu dyplomatów w rejonach, gdzie prawidłowo funkcjonuje system powiadamiania. Stosowanie bardziej ofensywnych form pracy operacyjnej ukierunkowanych na przeciwdziałanie penetracji, harmonijne współdziałanie dowódców jednostek wojskowych z organami WSW, pogłębienie informacji o przeciwniku i dokładniejsze rozpoznanie jego aktualnych zainteresowań pozwalają prognozować dalsze zwiększenie efektywności zabezpieczenia wojsk przed próbami infiltracji wywiadowczej.

5. Rozpoznanie utrzymywanych przez kadre
i pracowników wojska kontaktów z krajami
kapitalistycznymi

Rozproszenie emigracyjne Polaków jest zjawiskiem powszechnym. Na podstawie dotychczas opracowanych danych statystycznych należy przyjąć, iż poza granicami kraju przebywa ponad 15 mln Polaków, w tym około 13 mln w krajach kapitalistycznych. Najliczniejszą część stanowią Polacy wywodzący się z emigracji przełomu XIX i XX wieku. Główne ich skupiska znajdują się na terenie Stanów Zjednoczonych AP, Francji, Belgii, Republiki Federalnej Niemiec i Brazylii. Emigranci ci oraz potomkowie utrzymują szerokie kontakty z Ojczyzną, uczestniczą - w zdecydowanej większości w kształtowaniu pozytywnej opinii o Polsce, wspomagają, często materialnie, ogólnopolskie inicjatywy społeczne.

Drugą, znacznie mniejszą grupę stanowią osoby z tzw. emigracji politycznej. Tworzą ją ludzie, którzy pozostali na Zachodzie po II wojnie światowej oraz emigranci polityczni z lat 1945-1979, Najliczniejszą grupę emigrantów w latach powojennych utworzyły: wyjazdy emigracyjne do RFN i NRD - ponad 570 tys. osób oraz wyjazdy do Izraela - ponad 116 tys.^{1/}

Kolejną falę przemieszczeń emigracyjnych Polaków spowodowały wydarzenia lat 1980-1981. W okresie tym wyjechało na stałe do krajów kapitalistycznych ponad 81 tys. obywateli polskich, a ponadto około 80 tys. odmówiło powrotu z wyjazdów

1/ Rocznik statystyczny 1985 r. - Główny Urząd Statystyczny - Warszawa 1986 r.

służbowych i prywatnych.^{1/}

Środowiska emigracji politycznej, szczególnie z lat 1956-1958, 1968-1969, 1971-1979 oraz 1980-1981 odgrywają istotną rolę w działaniach dywersyjnych Zachodu, zwłaszcza Stanów Zjednoczonych, wobec naszego kraju. Część z nich stanowi również bazę aktywnie penetrowaną i wykorzystywaną przez zachodnie służby wywiadowcze, w tym wywiady wojskowe.

Liczba kadry i pracowników wojska utrzymujących kontakty z osobami zamieszkałymi w państwach kapitalistycznych kształtuje się na przestrzeni ostatniego pięciolecia na podobnym poziomie /ponad 6 tys.^{2/}/. W porównaniu do analogicznego okresu poprzedniego liczba osób posiadających kontakty z KK utrzymuje się w rzędzie tych samych wielkości. Około 85% kontaktów, kadra i pracownicy wojska utrzymują z krewnymi, pozostałe 15% to kontakty z przebywającymi na Zachodzie znajomymi. Charakter tych kontaktów - z uwagi na składane meldunki - znany jest z reguły dowództwu oraz rozpoznany przez Wojskową Służbę Wewnętrzną. W większości są to kontakty korespondencyjne, utrzymywane przeważnie okazjonalnie. Z dotychczasowych ustaleń nie wynika by stanowiły one większe zagrożenie dla Sił Zbrojnych. W stosunku do grupy osób, zwłaszcza dopuszczonych do prac tajnych specjalnego znaczenia /ok. 10%/, podejmowane są przedsięwzięcia profilaktyczne w ramach kontrwywiadowczej ochrony wojska.

Charakteryzując kontakty z KK utrzymywane przez śro-

1/ Migracje zewnętrzne 1983 i 1985, Informacja statystyczna, Ministerstwo Spraw Wewnętrznych, Biuro Paszportów, Warszawa 1984 i 1986.

2/ Dane statystyczne znajdują się w dyspozycji Zarządu III Szefostwa Wojskowej Służby Wewnętrznej.

dowiska wojskowe, należy również uwzględnić kontakty członków rodzin zamieszkałych w innych regionach kraju. Łącznie na przestrzeni ostatnich 5 lat, przeciętnie notuje się około 3 tys. takich przypadków. Jest to istotne między innymi dlatego, że w niektórych sytuacjach osoby te stanowią pośrednie ogniwo w łączności między kadrami /pracownikami wojska/ i krewnymi /znajomymi/ przebywającymi na Zachodzie.

Mimo generalnie pozytywnej oceny postaw kadry i pracowników wojska, utrzymujących kontakty z osobami mieszkającymi w państwach kapitalistycznych, należy stwierdzić, że mają również miejsce - odosobnione co prawda - przypadki pewnych nieprawidłowości, a mianowicie:

- niektóre osoby otrzymujące z Zachodu znaczne wsparcie materialne pod wpływem uzyskiwanej pomocy - prezentują postawy gloryfikujące zachodni styl życia, destrukcyjnie oddziałując na otoczenie;
- pewien - nieznaczny - procent kadry i pracowników wojska usiłuje ukryć przed przełożonymi utrzymywane kontakty, tłumacząc to niekiedy nieznaną przepisów. Praktycznie - jak wynika to z późniejszych wyjaśnień - kadra nie składa takich meldunków przeważnie w obawie o dalszy rozwój służby. Niejednokrotnie też obowiązek złożenia wyjaśnień związanych z utrzymywaniem kontaktu utożsamiany jest z ingerencją w życie prywatne lub dyskryminacją zawodową;
- żołnierze zawodowi bądź pracownicy wojska z reguły nie składają meldunków o spotkaniach z cudzoziemcami poza stałym garnizonem, bądź o zetknięciu się z tymi osobami u znajomych, nawet jeśli taki kontakt jest później podtrzymywany. Podobnie przedstawia się sprawa w odniesieniu do kontaktów utrzymywanych poprzez rodzinę;

- opóźnione w szeregu przypadków składanie meldunków przełożonym o nawiązaniu kontaktów z cudzoziemcami z państw kapitalistycznych.

W skali wojska co roku notowana jest znaczna liczba osób wyjeżdżających prywatnie na Zachód. W 1981 r. turystycznie lub na zaproszenie krewnych i znajomych, w ramach urlopów wyjeżdżało około 1500 /w tym 401 kadry/ osób, w 1982 liczba ta spadła do 100, a w latach następnych systematycznie wzrastała. W 1985 r. stwierdzono już ponad 1000 tego charakteru wyjazdów /kadry ponad 200/ i pracowników wojska. Ponadto w tym samym roku na Zachód wyjeżdżało prywatnie ponad 5 tys. osób ze środowiska rodzin kadry i pracowników wojska. Należy się liczyć, iż dalsza stabilizacja życia wewnętrznego kraju będzie sprzyjała wzrostowi wyjazdów. Ponadto w okresie 1981-85 na Zachód wyjeżdżały służbowo 5192 osoby w tym ponad 50% z grona kadry.^{1/}

Kadra i pracownicy wojska odwiedzani są też przez osoby zamieszkałe na stałe na Zachodzie. Średnio rocznie notuje się około 500 tego rodzaju przyjazdów. Nie we wszystkich przypadkach cudzoziemcy odwiedzają kadrę w miejscach zamieszkania, część spotkań odbywa się u krewnych zamieszkałych w innych miastach. Do kontaktów bezpośrednich dochodzi również w miejscowościach wczasowych, podczas urlopów, świąt i dni wolnych.

W Siłach Zbrojnych nowe - jakościowo - zjawiska zanotowano po 1980 r., kiedy to stosunkowo znaczna liczba krewnych, bądź bliskich znajomych kadry i pracowników wojska

^{1/} Cyfry przytoczone w oparciu o roczne zestawienie statystyczne Oddziału Wojskowych Spraw Zagranicznych.

wyjechała na Zachód i odmówiła powrotu do kraju. Na przestrzeni lat 1981-85 odmówiło powrotu ogółem ponad 900 osób, z czego ponad 700 - to członkowie rodzin kadry. Część żołnierzy zawodowych utrzymujących kontakty z tą kategorią osób, dopuszczona jest do prac tajnych specjalnego znaczenia, bądź pełni służbę w jednostkach specjalnych.^{1/}

O ile - jak wynika z ustaleń operacyjnych - utrzymywane przez kadrę i pracowników wojska kontakty z krewnymi zamieszkałymi od lat w państwach kapitalistycznych nie stanowią większego zagrożenia dla Sił Zbrojnych, to zupełnie inaczej przedstawia się problem osób - powiązanych ze środowiskami wojskowymi - które po 1980 r. odmówiły powrotu do kraju.

Przede wszystkim należy przypomnieć, że w nowej sytuacji społeczno-politycznej jaka wytworzyła się po wydarzeniach lata 1980 r., służby wywiadowcze i ośrodki dywersji ideologicznej głównych państw NATO zintensyfikowały swoją działalność skierowaną na wojsko. Stąd wszystkie osoby związane /nawet pośrednio/ z kadrą, które pozostawały na Zachodzie traktowane są przez przeciwnika jako potencjalna baza werbunkowa. Podejmowane są więc zróżnicowane przedsięwzięcia, by decyzją pozostania na Zachodzie zdyskontować dla potrzeb wywiadowczych. Idzie głównie o uzyskanie informacji /charakterystyk/ o osobach wojskowych, danych o znanych obiektach wojskowych, potencjale obronnym kraju. Prowadzona jest w tym środowisku wzmożona działalność wywiadowcza poprzez próby werbunku, różnego rodzaju przesłuchania i inda-

1/ Dane statystyczne Zarządu III S.WSW.

gacje w obozach przejściowych, urzędach policji. Stosuje się często metodę uzależniania - w różnej postaci - osób ubiegających się o prawo stałego pobytu na Zachodzie, w celu późniejszego wykorzystania ich w działalności politycznej przeciwko Polsce. Szantaż, bądź prowokacja, nie jest odosobnioną formą działania służb specjalnych.^{1/}

Jest faktem, że wiele osób wyjeżdżających za granicę nie ma świadomości, iż podczas pobytu - zwłaszcza w głównych państwach NATO - narażone mogą być na różnego rodzaju indagacje a nawet prowokacje. Do rzadkości należy by wyjeżdżający otrzymał wcześniej wyczerpujący instruktaż, by uprzedzono go jak się ma zachować w przypadku stosowania prowokacji np. podczas zwiedzania miasta, zakupów w supermarkiecie itp. Część wyjeżdżających z kolei traktuje udzielone "rady" z przysłowiowym "przymrużeniem oka", uznając je za przerosty ostrożności.

W sprawach wyjaśniania i oceny kontaktów z KK, musi być widoczny udział wszystkich ogniw dowódczych oraz partyjnopolitycznych. Rzecz idzie bowiem o zjednywanie wojsku ludzi, a nie stwarzanie atmosfery podejrzliwości i wzajemnej wrogości. Kadrze trzeba uświadomić istniejące zagrożenia - przekonać, iż jest współodpowiedzialna za ich likwidację bądź minimalizację. Wymaga to działań nie kampanijnych, lecz podejmowanych na co dzień w warunkach wzajemnego zrozumienia i zaufania.

1/ Dla przykładu w 1986 r. ujawniono 200 prób werbunku Polaków przebywających za granicą, z czego 80% podejmowanych było przez CIA i BND na terytorium RFN i Berlina Zachodniego - dokument MSW nr ODP-7/0164/88 z dn.17.10.88r

6. Ocena skuteczności aktualnie realizowanych
działań na rzecz kontrwywiadowczej ochrony
tajemnicy

Zasadnicza część rozdziału oparta została na ustaleniach operacyjnych związanych z bieżącą ochroną tajemnicy w Siłach Zbrojnych WP. Zebrane tą drogą doświadczenia upoważniają do sprecyzowania ocen i wniosków. Generalnie patrząc na problem należy stwierdzić, że skuteczność ochrony zasadniczych elementów tajemnicy jest zadowalająca. Powoli lecz systematycznie podnoszone są wymagania w zakresie zabezpieczenia tajemnicy, notuje się wzrost poczucia odpowiedzialności kadry za powierzone jej wiadomości niejawne.

Te pozytywne trendy wynikają przede wszystkim z konsekwencji kierownictwa służbowego MON, którego nakazy obligują do sukcesywnych ocen stanu ochrony tajemnicy, nowelizacji - w zależności od potrzeb - dokumentów normatywnych oraz wzrostu efektywności nadzoru służbowego jak również poszukiwania coraz doskonalszych form ochrony.

Dokonana w ostatnim okresie nowelizacja "Przepisów o ochronie tajemnicy w Siłach Zbrojnych" stanowi kolejny krok na drodze zabezpieczenia wojska przed wrogim rozpoznaniem zwłaszcza agenturalnym.

Nie oznacza to wcale, iż w zakresie ochrony tajemnicy osiągnięto poziom w pełni zadowalający. Nadal w codziennym życiu występuje szereg - i to niekiedy poważnych - przesłanek do ujawniania istotnych informacji. Część kadry, zwłaszcza na niższych szczeblach, nie zawsze dostrzega istniejące realne

zagrożenia. W wyniku niedbalstwa i wygodnictwa naruszane są zasady pracy przy dokumentach niejawnych, lekceważy się niekiedy reżimy zabezpieczenia obiektów /pomieszczeń, dokumentów, sprzętu/. Łamane są przepisy korzystania z technicznych środków łączności. O problemach niejawnych, niefrasobliwie dyskutuje się w otoczeniu osób postronnych. Wiele do życzenia pozostawia jeszcze nadzór służbowy, zbyt dużo jeszcze w tym względzie formalizmu i tolerancji.

Miernikiem skuteczności ochrony tajemnicy jest - między innymi - liczba utraconych dokumentów zawierających tajemnicę państwową. W omawianym okresie liczba ta systematycznie malała. Stwierdzono zagubienie jednego dokumentu o klauzuli "Tajne specjalnego znaczenia" oraz 151 tajnych. Dla porównania w latach 1976-1980 dopuszczono do utraty 5 dokumentów TSZ i 220 tajnych. Tendencje malejące zauważalne są w okresie pięciolecia, wskazują na to cyfry: 38 utraconych dokumentów tajnych w 1981, 23 w roku 1985. Mimo zauważalności wzrostu skuteczności ochrony, liczba utraconych wydawnictw nadal jest niepokojąco wysoka. Nie udało się wyeliminować powtarzających się stosunkowo często zarówno przyczyn jak i okoliczności utraty dokumentów. Materiały znajdujące się w posiadaniu Oddziału V Sztabu Generalnego oraz Szefostwa WSW wskazują, że powodem takiego stanu pozostaje przede wszystkim nieprzestrzeganie przez wykonawców i ich przełożonych postanowień zawartych w "Przepisach o ochronie tajemnicy w Siłach Zbrojnych PRL" a w szczególności:

- nierzetelna kontrola i samokontrola oraz przekazywanie dokumentów niejawnych z pominięciem kancelarii tajnej lub bez pokwitowania;

- niewłaściwe zabezpieczenie dokumentów i pomieszczeń w których je przechowywano;
- brak poczucia odpowiedzialności za ochronę powierzonych dokumentów podczas podróży służbowych, ćwiczeń, odpraw i szkoleń, w tym spożywania alkoholu w trakcie ich przenoszenia /dysponowania, przewożenia/.

Każdy przypadek utraty dokumentów niejawnych był przedmiotem szczegółowych wyjaśnień. Niezależnie od działań ukierunkowanych na odzyskanie dokumentów, dążono do ustalenia kręgu osób, które mogłyby się zapoznać z treścią niejawną,^{1/} jak również starano się ustalić okoliczności w jakich nastąpiła utrata. Znamienne, że jeśli idzie o przesłanki towarzyszące zdarzeniu, w szeregu przypadkach stan nieprzestrzegania przepisów - bo w tym główna przyczyna - trwał przez dłuższy czas i nie zwracali na to uwagi ani przełożeni jak i oficerowie KW. Problemom tym nadawano stosowną rangę dopiero po zaginięciu dokumentu.

Z ogólnej liczby 537 utraconych dokumentów niejawnych prawie połowa stanowią pisma korespondencyjne. Utracie tych pism sprzyja, że w skali całych Sił Zbrojnych w codziennym obiegu znajduje się ich około 70.000 a w skali roku przeszło 4 miliony.

W omawianym okresie utracono w Siłach Zbrojnych 379 arkuszy map. W porównaniu do minionego pięciolecia nie notowano zasadniczych zmian w stanie ochrony wydawnictw kartograficznych. Zaginęło dużo map technicznych w skali

1/ Dokonane w takich sytuacjach ustalenia w większości wykluczały możliwości zapoznania się z treścią przez osoby do tego nieupoważnione.

1: 500 000 a więc obejmujących obszar kraju, oraz map w skali 1:200 000 i mniejszych pokrywających tereny zachodniej, północno-zachodniej i północno-wschodniej Polski, a więc terenów na których rozmieszczona jest znaczna liczba garnizonów i poligonów wojskowych.

Na dobrym generalnie poziomie kształtował się stan ochrony tajemnicy w informatyce. Wpływ na poprawę ochrony miały badania przeprowadzone w 1984 r., przy użyciu specjalnej aparatury w Wojskowym Instytucie Informatyki. Stwierdzone wówczas nieprawidłowości stanowiły podstawę do wydania przez Sztab Generalny WP określonych poleceń dla OW i RSZ a równolegle znowelizowano przepisy dotyczące zasad ochrony tajemnicy podczas projektowania i eksploatacji systemów informatycznych w warunkach stacjonarnych jak i polowych, jak również wprowadzono ograniczenia w dostępie osób do ośrodków przetwarzania informacji.

Prawidłowo organizowano ochronę tajemnicy i właściwie przestrzegano przepisy w wojskowych drukarniach i innych komórkach poligraficznych. Praktycznie w okresie analizowanego pięciolecia nie stwierdzono istotnych naruszeń tajemnicy. Aktualnie funkcjonujące przepisy zapewniają właściwe działanie tych komórek.^{1/}

Ujawnienie tajemnicy - to nie tylko utrata dokumentów i wydawnictw kartograficznych. Do powtarzających się zagrożeń należy przede wszystkim ujawnianie - w różnych okolicznościach i formie - wiadomości stanowiących tajemnicę służbową a nie-

1/ Zarządzenie MON nr 43 z 10.07.85 r. w sprawie działalności poligraficznej prowadzonej przez jednostki /instytucje/ wojskowe oraz przedsiębiorstwa państwowe podległe MON.

kiedy i państwową przez żołnierzy i pracowników cywilnych w obecności osób nieupoważnionych. Zdarzenia tego charakteru miały miejsce zarówno na terenie wojskowym - szczególnie w okresach ćwiczeń wojskowych, inspekcji oraz zmian kadrowych - jak i w miejscach publicznych /restauracje, kawiarnie, punkty zaopatrzenia/. W ramach tak zwanego gadulstwa niejednokrotnie też przenikały na zewnątrz informacje o bieżących zamierzeniach jednostek, charakterystyki dowódców, kadry.

W ostatnich latach - mimo funkcjonujących obostrzeń - nie zdołano w pełni wyeliminować przypadków przekazywania wiadomości stanowiących tajemnicę podczas wykorzystywania radiowych i radioliniowych środków łączności. W samym tylko 1985 r. drogą wyrywkowych kontroli urządzeń radioliniowych i radiostacji UKF w okresie ćwiczeń "RUBIN", "GRANIT" i "PRZYJAZN" ujawniono 31 zdarzeń o charakterze niejawnym przez nieutajnione środki. Z reguły dotyczyło to wymieniania stopni, nazwisk oraz stanowisk służbowych osób funkcyjnych. Przekazywano również terminy niektórych zamierzeń, miejsca dyslokacji, trasy przemarszu wojsk, nazwy sprzętu. Łącznie w omawianym pięcioleciu wykryto 307 naruszeń dyscypliny radiowej. W zdecydowanej większości w naruszeniach tych nie stwierdzono ujawnienia tajemnicy państwowej lub służbowej.

Do przesyłania informacji niejawnych - w polowych i stacjonarnych systemach łączności wszystkich szczebli - używano wyłącznie środków łączności szyfrowej, utajnionej i kodowej. Środki te zapewniały sprawny i terminowy obieg informacji niejawnych i ich należyłą ochronę.

Obieg informacji w codziennej działalności służbowej

dowództw i sztabów zapewniono poprzez techniczne środki łączności i pocztę specjalną. W tym zakresie nie ujawniono poważniejszych zaniedbań.

Prawidłowo na ogół zabezpieczone były dokumenty szyfrowe i kodowe, dobrze organizowana była ochrona sprzętu. Z tych też powodów nie doszło do istotnych w skutkach naruszeń. Miały jednak miejsce odosobnione przypadki zagubienia dokumentów ręcznego kodowania i ujawniania treści tabel kryptonimów.

Lata 1981-85 to również działania mające na celu doskonalenie systemu ochrony terenów i obiektów wojskowych. Podejmowane przedsięwzięcia ukierunkowane zostały na wzmocnienie bezpośredniej ochrony fizycznej obiektów wojskowych a zwłaszcza obiektów specjalnych. Z materiałów zebranych przez Wojskową Służbę Wewnętrzną wynika, iż w okresie tym nastąpiła widoczna poprawa w ochronie obiektów wojskowych. Ujawnione jeszcze niedociągnięcia wynikały głównie z niedopracowań organizacyjnych niektórych dowódców jak i przyczyn obiektywnych w tym: naturalnego zużycia elementów ochrony fizycznej, rozmyślnego niszczenia przez żołnierzy i okoliczną ludność ogrodzeń, znaków, tablic ostrzegawczych.

Podstawowym normom - w większości obiektów - odpowiada ogrodzenie a ich stan techniczny nie budzi poważniejszych zastrzeżeń. Tym niemniej w niektórych jednostkach występują znaczne ubytki na skutek korozji siatki i drutu kolczastego oraz wyłomy w ogrodzeniach spowodowane przez żołnierzy służby zasadniczej oraz ludność cywilną zamieszkałą w pobliżu

jednostek. Podobnie kształtowała się sytuacja w odniesieniu do znaków drogowych i tablic ostrzegawczych wystawionych w bezpośredniej bliskości obiektów i terenów wojskowych.

Prawidłowo na ogół wyznaczone były i funkcjonowały strefy ochronne w rejonach wybranych obiektów wojskowych.^{1/}

Czynnikiem osłabiającym ochronę wyznaczonych stref była znaczna awaryjność jak i wadliwe funkcjonowanie zainstalowanych systemów alarmowych. Duża ich liczba znajdowała się w remoncie a częste awarie lub fałszywe sygnały obniżały czujność wart i służb.^{2/}

Służby i warty nadal stanowiły jeden ze słabych elementów systemu ochrony. W minionym pięcioleciu stwierdzono w tym zakresie szereg nieprawidłowości. W niektórych jednostkach zwłaszcza WL i OPK rozmieszczenie posterunków było za rzadkie w stosunku do ochraniających obszarów. Zagrożenia wynikały również z nieregularnego pełnienia służby wartowniczej oraz braku należytej kontroli ze strony osób funkcyjnych. Problem stanowiło również niezdiscyplinowanie części wartowników cywilnych, ich niska sprawność fizyczna oraz występujące przypadki spożywania alkoholu przed lub na służbie.

Ujawnione przez Wojskową Służbę Wewnętrzną nieprawidłowości były na bieżąco sygnalizowane dowództwu jednostek. Reakcje na ogół prawidłowe - wpływały na poprawę stanu ochrony obiektu. Wobec winnych wykroczeń stosowano kary dyscyplinarne

1/ Strefy ochronne istnieją tam, gdzie nie zachowano niezbędnych norm lokalizacyjnych przy projektowaniu samych obiektów jak też inwestycji cywilnych wznoszonych w ich bezpośrednim sąsiedztwie.

2/ Ocena stanu ochrony tajemnicy w resorcie Obrony Narodowej za lata 1981-1985 oraz wnioski do działalności na lata 1986-1990. Materiał Sztabu Generalnego WP na posiedzenie Rady Wojskowej MON w dniu 28.04.1986 r.

a w sporadycznych - poważniejszych przypadkach sprawców pociągano do odpowiedzialności karnej.^{1/}

Istotnym wzmocnieniem systemu ochrony obiektów i terenów wojskowych były patrole i zakryte punkty obserwacji. W zakresie ich działania nie stwierdzono poważniejszych niedociągnięć. Organizowane były z uwzględnieniem warunków terenowych i sytuacji, zwłaszcza w okresie ćwiczeń wojskowych, alarmów lub intensyfikacji szkolenia.

Szereg innowacyjnych rozwiązań spowodował poprawę w działaniu systemu przepustkowego. Między innymi o 70% ograniczono liczbę wydanych przepustek uprawniających osoby ze szczebli nadrzędnych do wejścia na teren jednostek. Ujednolicono zasady wydawania przepustek zezwalających na wstęp do obiektów specjalnych. Podjęto też próbę unifikacji formy przepustek, mającą na celu ułatwienie kontroli osób przez wartowników. Założenia tych modyfikacji zostały pozytywnie ocenione przez zespół fachowców. Występujące nadal niedostatki to głównie nieprzestrzeganie obowiązujących przepisów. Stwierdzono przypadki nie kontrolowania bądź pobieżnego sprawdzania osób wchodzących na teren jednostek jak i wystawiania przepustek dla grup osób na nazwisko jednej z nich, bez odnotowywania w ewidencji danych personalnych pozostałych. Przykładem nieprawidłowej pracy biura przepustek było wpuszczenie na teren dwóch jednostek obywateli Berlina Zachodniego.

Na niezmiennym, przeciętnym poziomie kształtował się w omawianym okresie stan zabezpieczenia pomieszczeń służbowych.

1/ Patrząc na problem z perspektywy czasu - należy stwierdzić, iż konsekwencja działania dowódczego zaczyna owocować. W 1986 r. liczba wykroczeń ze strony wartowników cywilnych była znacznie mniejsza niż w latach ubiegłych.

Mimo zaostżonego nadzoru słuźbowego, w dalszym ciągu występowały przypadki pozostawiania pomieszczeń z dokumentacją niejawną w czasie pracy bez nadzoru wykonawców oraz brak niezbędnego zabezpieczenia ich po godzinach słuźbowych. Do istotnych uchybień należało zatrudnianie żołnierzy słuźby zasadniczej do prac niejawnych bez nadzoru kadry zawodowej, zwłaszcza w okresach poprzedzających ćwiczzenia, kontrole i inspekcje.

Nie budzi większych zastrzeżeń stan maskowania wydzielonych obiektów. Wytyczne Sztabu Generalnego WP były w tym zakresie realizowane i przestrzegane. Również ochrona, maskowanie i eksploatacja techniki awangardowej była właściwa - zgodnie z obowiązującym zarządzeniem Szefa Sztabu Generalnego WP.

Na właściwym poziomie organizowano kontrwywiadowcze zabezpieczenie ćwiczzeń, przemarszów i zgrupowań wojsk.

W zarysowanym skrótowo stanie ochrony tajemnicy w Siłach Zbrojnych, celowo eksponowaliśmy występujące jeszcze nieprawidłowości zwłaszcza te, które powtarzają się na przestrzeni analizowanego pięciolecia. Mimo bowiem niewielkiej - jak na skalę wojska - ilości naruszeń zasad ochrony, zagrożenia wynikające z tego tytułu są znaczne i niezmiennie.

Pozytywnym zjawiskiem wynikającym z analizy, jest fakt powolnego ale systematycznego zmniejszania się przypadków ujawniania tajemnicy i naruszeń przepisów ochrony. Miał też ciężar gatunkowy zdarzeń. Godzi się podkreślić, że

w postępowaniu sprawców w toku prowadzonych wyjaśnień nie dopatrzono się elementów celowego działania czy złej woli. Z reguły naruszenia zasad ochrony tajemnicy były wynikiem niedbalstwa i lekkomyślności. W tych warunkach istniała możliwość dużego zróżnicowania środków przeciwdziałania. Za przewinienia tego charakteru, prowadzonych było 79 postępowań karnych.^{1/} Dotyczyły one przede wszystkim osób, które utraciły dokumenty niejawne. Większość z nich zakończyła się warunkowym umorzeniem z powodu późniejszego obniżenia klauzuli tajności utraconych dokumentów jak i dobrych opinii sprawców.

Zaostrzona została natomiast poważnie wymagalność wobec osób odpowiedzialnych za ochronę tajemnicy. Tego charakteru tendencje spowodowały - w porównaniu do poprzedniego pięciolecia - znaczny wzrost ilości kar dyscyplinarnych. Łącznie wymierzono ich około 5 tys. - mimo generalnie zdecydowanej poprawy w latach 1981-85 stanu zabezpieczenia tajemnicy. Liczba wymierzanych kar w miarę upływu czasu w pięcioleciu zmalała.

Tam gdzie działania profilaktyczne nie dawały zadowalających efektów, stosowano przeniesienie na mniej odpowiedzialne stanowiska. W odniesieniu do pracowników cywilnych - represją było odsunięcie od prac niejawnych bądź zwolnienie z pracy. W przypadkach mniejszej wagi prowadzone były rozmowy profilaktyczno-ostrzegawcze. W ramach przedsięwzięć zapobiegawczych, systematycznie prowadzone były ze stanami osobowymi

1/ Dane statystyczne przedstawiono graficznie na podstawie materiałów S. WSW /Informacja dot. oceny zagrożenia wywiadowczego Sił Zbrojnych PRL w latach 1981-1985, zał. do pisma nr DA-089/16 z dn. 16.01.1986 r./.

**WYKAZ POSTĘPOWAŃ KARNYCH PROWADZONYCH
W STOSUNKU DO OSÓB UWANNIAJĄCYCH TAJEMNICĘ**

LATA	Ilość postępowań karnych	SPRAWCY					Sposób zakonczenia			Rodzaj przestępstwa	
		ofic.	chor.	podofic. zaw.	zahn.	prof. cyw.	akt. oskarż.	war. umarz.	utrata dokum.	inne	
1981	21	13	1	-	1	-	3	12	12	3	
1982	25	13	6	5	3	-	6	21	23	4	
1983	8	6	-	1	1	-	4	4	7	1	
1984	9	10	1	2	1	-	1	13	13	1	
1985	13	9	1	4	1	-	5	8	11	2	
Razem	76	51	9	12	7	-	19	58	66	11	

wojska szkolenia i pogadanki. W tych formach profilaktyki aktywnie uczestniczyli oficerowie kontrwywiadu. W tym dziale pracy kładziono znaczny nacisk na uzyskiwanie informacji wyprzedzających,^{1/} o występujących niedomaganiach w systemie ochrony tajemnicy. W skali roku dowódcom różnych szczebli przekazywano około 2,5 tys. informacji. W większości przypadków umożliwiało to dowódcom podejmowanie trafnych i skutecznych przedsięwzięć zabezpieczających tajemnicę.

Elementy zagrożeniogenne w ujęciu statystycznym w pięcioleciu 1981-1985:

- wyjazdy do KK ze środowisk wojskowych	- służbowo 5192 - prywatnie 15000	
- utrzymywane kontakty	- kadra, prac. cywil. rodziny	6000 3000
- przyjazdy cudzoziemców	-	2500
- odmówiło powrotu, pozostało w KK	-	900
<hr/>		
- penetracje	-	934
- utrata dokumentów niejawnych	-	537
- utrata map	-	379
- naruszenia reżimów łącności	-	307
<hr/>		

Istnieje ponadto tzw. "czarna liczba" - zdarzenia ujemnie wpływające na stan ochrony tajemnicy, których rozmiary nie są w pełni ustalone: np. gadulstwo, zatrudnianie przy pracach

^{1/} Pod pojęciem tym rozumiemy uzyskiwanie danych o zamiarach /planach/ przestępczych, przygotowaniach do tego rodzaju działalności, jak i nieprawidłowościach w systemie zabezpieczenia, których nie usunięcie grozi utratą sprzętu /jego zniszczeniem/ względnie ujawnieniem chronionych wiadomości.

niejawnych osób nie posiadających stosownych upoważnień, czasowa utrata kontroli nad dokumentami niejawnymi, nieszczelność systemów przepustkowych, fluktuacja kadr.

Występujące niedomagania w zakresie ochrony tajemnicy w Siłach Zbrojnych PRL wynikają nie tylko ze złej woli sprawców ale przede wszystkim z braku wyrobionych nawyków, niskiej świadomości prawnej, niepełnej znajomości przepisów instrukcyjnych. W tym stanie rzeczy, szczególnego znaczenia nabierają działania profilaktyczne, a przede wszystkim profilaktyka kreatywna ukierunkowana na:

- ujawnianie zagrożeń zwłaszcza wewnętrznych i skutków lekceważenia przepisów;
- systematyczne ujawnianie przesłanek i zagrożeń w celu współdziałania z dowództwem w podejmowaniu skutecznych przeciwdziałań;
- położenie większego niż dotąd akcentu na szkolenie kontrwywiadowcze kadry zawodowej Sił Zbrojnych w celu ukazania faktycznych zagrożeń i uczulenia na niefrasobliwość, lekkomyślność i niedbalstwo jako przyczyny łamania elementarnych zasad ochrony tajemnicy.

Te elementy profilaktyki kreatywnej włączone w system kontrwywiadowczej ochrony sztabów wyższego szczebla oraz instytucji centralnych MON dają już wymierne efekty.

WNIOSKI KONCOWE

Analiza podjętej w niniejszej pracy problematyki kontrwywiadowczej ochrony tajemnicy wskazuje nie tylko na złożoność jej uwarunkowań ale przede wszystkim na potrzebę dostrzegania jej dynamizmu, a więc koncentrowania uwagi nie tylko na potrzebach dnia dzisiejszego ale przede wszystkim na przewidywanych trendach rozwojowych w najbliższej perspektywie.

Oznacza to, że na modelowe doskonalenie systemu kontrwywiadowczej ochrony tajemnicy istotny wpływ wywierać będzie podejmowana na czas działalność identyfikacyjna form i sposobów rozpoznawania destrukcyjnego oddziaływania służb specjalnych państw NATO na moc obronną Sił Zbrojnych PRL.

Z całą pewnością można postawić tezę, że przeciwnik w swych działaniach wykorzystywać będzie współczesną wiedzę socjotechniczną, wiedzę z zakresu psychologii społecznej, cybernetyki oraz teorii informacji. Wykorzystywana będzie niewątpliwie nowoczesna technika informacyjna, a przede wszystkim, technika informatyczna i telekomunikacyjna oraz telewizja satelitarna.

Nowoczesna technika, technologia i wiedza społeczna wykorzystywane będą zarówno do zbierania informacji, jak i do oddziaływania na społeczeństwo naszego państwa. Formy i intensywność tych oddziaływań będą różnicowane w zależności od obiektu, warstw i grup społecznych będących w zainteresowaniu służb specjalnych, a głównie instytucji wywiadowczych.

Należy zatem liczyć się z selektywnym wykorzystywaniem wyrafinowanych form i technik destrukcyjnego oddziaływania na funkcjonujący system bezpieczeństwa państwa a w tym również i jego Sił Zbrojnych.

Zjawiska te nabierać będą szczególnego znaczenia w warunkach "otwartego" funkcjonowania społeczeństwa polskiego w systemie pluralistycznym, swobodnego przepływu informacji i intensyfikacji wzajemnego komunikowania się. Trzeba się liczyć z większym niż dotychczas wykorzystywaniem w walce informacyjnej prowadzonej przez wyspecjalizowane struktury służb specjalnych państw NATO teorii informowania i dezinformowania oraz parainformowania. W tych nowych warunkach rozwoju cywilizacyjnego trzeba bezwzględnie dostrzegać potrzebę badań nad zachodzącymi zmianami w formach i środkach działalności rozpoznawczej i destrukcyjnego oddziaływania służb specjalnych NATO.

W tej sytuacji kontrwywiad WSW, dla podniesienia skuteczności swoich działań powinien część sił i środków przeznaczyć na systemową działalność analityczną, prognozowanie trendów rozwojowych aby stawiane diagnozy realistycznie odzwierciedlały sytuację operacyjną, możliwe zagrożenie i na tej podstawie dawały szansę poszukiwania bardziej efektywnych, systemowych rozwiązań na rzecz kontrwywiadowczej ochrony Sił Zbrojnych, a w szczególności ochrony tajemnicy.

W pełni celowe i uzasadnione wydaje się utworzenie w Szefostwie WSW komórki, która bazując na możliwościach wprowadzanego systemu informatycznego, dysponując nie tylko bazą danych, ale także bazą wiedzy i doświadczeń różnych

specjalistów przyczyniałyby się do wspomagania procesu decyzyjnego kierownictwa Szefostwa WSW. Tworzenie takiego systemu ekspertowego dla wspomagania procesu decyzyjnego w działaniach kontrwywiadowczych należy uznać za rozwiązanie odpowiadające celom i roli kontrwywiadu wojskowego XXI wieku.

W procesie kształcenia kadr kontrwywiadu wojskowego i ich późniejszego doskonalenia w systemie kształcenia ustawicznego należy tak dobierać treści kształcące oraz metodykę nauczania aby ukształtować ważną cechę oficera kontrwywiadu jaką jest antycypacyjność, czyli zdolność przewidywania zjawisk odległych w czasie. Zdolność ta powinna być kształtowana ze szczególną intensywnością metodą analizy wielu różnych wariantów sytuacji alternatywnych.

Kształcenie umiejętności antycypacyjnych oficerów kontrwywiadu wojskowego winno dać w efekcie takie wartości jak śmiałość i odwagę w podejmowaniu przez nich działań uprzedzających, które w rozumieniu profilaktyki kreatywnej ukierunkowane powinny być nie na walkę ze skutkami oddziaływań przeciwnika, a przede wszystkim na walkę z przyczynami skutków.

Ten proponowany styl pracy operacyjnej charakteryzuje się ukierunkowaniem działań uprzedzających na walkę z przyczynami skutków może upowszechniać się pod warunkiem zmiany w sposobie myślenia oficerów kontrwywiadu. Myślenie operacyjne współczesnego oficera kontrwywiadu powinno charakteryzować:

- myślenie perspektywiczne, czyli umiejętność przewidywania odległych skutków działań, antycypowanie przyszłości i tworzenie racjonalnych scenariuszy przyszłych stanów zjawisk, które będą wymagały operacyjnych interwencji;

- myślenie alternatywne, ułatwiające poszukiwanie nowych konkurencyjnych rozwiązań, które byłyby lepsze od już istniejących;
- myślenie probabilistyczne, czyli umiejętność operowania niepewnością i prawdopodobieństwami, a więc umiejętność podkreślania nie tego, co się pewno wydarzy, ale tego, co może się zdarzyć.

Przedstawione kierunki kształcenia nowego stylu myślenia operacyjnego oficerów kontrwywiadu mogą mieć istotny wpływ na skuteczność ich działań praktycznych w proponowanym przez autorów systemie kontrwywiadowczej ochrony tajemnicy.

Z analizy wybranych teoretycznych aspektów cybernetycznego modelu systemowego kontrwywiadowczej ochrony tajemnicy wynika, że skuteczność działalności usprawniającej funkcjonowanie kontrwywiadu wojskowego zależy od poziomu wiedzy oficerów kontrwywiadu.

Do tego nie wystarcza już tylko wiedza specjalistyczna, potrzebna jest zatem wiedza będąca syntezą różnych dyscyplin naukowych. Oficerom kontrwywiadu WSW nie powinna być obca wiedza, której dostarczają takie dyscypliny jak:

- prakseologia, badająca zasady spornego działania;
- cybernetyka, a w szczególności cybernetyka społeczna, badająca procesy sterowania i komunikowania;
- socjologia i psychologia społeczna, badająca zachowanie społeczne pod wpływem różnorodnych bodźców;
- teoria informacji - ilościowa i jakościowa - dająca podstawy naukowej analizy procesów informacyjnych;
- analiza systemowa, pozwalająca na ocenę efektywności różnych wariantów działania;

- informatyka, pozwalająca racjonalnie posługiwać się nowoczesną techniką komputerową.

Podjęta próba przedstawienia systemu kontrwywiadowczej ochrony tajemnicy, jako systemu informacyjnego rozwijającego się wskazuje na wyraźną zależność sprawności jego funkcjonowania nie tylko od wysokiej pojemności i sprawności informacyjnej ale również od właściwie dobranej struktury organizacyjnej, której charakterystyczną cechą jest elastyczność.

Elastyczne struktury systemów, a w tym systemu kontrwywiadowczej ochrony tajemnicy odpowiadają nowym sytuacjom, nowym warunkom działania przez to, że zapewniają:

- wysoką gotowość systemu, czyli szybkie podjęcie realizacji nowych zadań i ich sprawne wykonanie w pożądanym czasie;
- wysoką adaptacyjność, czyli zdolność przystosowania się do nowych, zmiennych warunków działania;
- wysoką żywotność, czyli odporność na wszelkie formy destrukcyjnego oddziaływania przeciwnika .

Aby zatem sprostać zadaniom jakie najbliższa perspektywa przyszłości postawi przed organami kontrwywiadu wojskowego, trzeba już dzisiaj myśleć o zastąpieniu struktur sztywnych, "ociężałych", łatwo poddających się biurokracyzacji, strukturami nowoczesnymi, a więc elastycznymi, odpowiadającymi nowym sytuacjom i nowym warunkom działania przez to, że pozwolą wyzwolić inicjatywę i podnieść wymagania funkcjonalne.

Podjęta w niniejszej pracy problematyka niektórych aspektów współczesnej walki informacyjnej w układzie wywiad - kontrwywiad pozwala na wyprowadzenie wniosku ogólnego, że

w procesie organizacji systemu kontrwywiadowczej ochrony tajemnicy należy zwrócić szczególną uwagę na te zagrożenia, z których mogą wynikać realne możliwości niszczenia informacyjnego przez przeciwnika stosowanego przez nas systemu kontrwywiadowczej ochrony. Należy zatem wypracować stosownie do możliwych zagrożeń metody przeciwdziałania dywersyjnym działaniom informacyjnym jakie może zastosować wobec nas przeciwnik.

Przeprowadzona w rozdziale III analiza wywiadowczej działalności głównych państw NATO, ukierunkowanej na osłabianie mocy obronnej Sił Zbrojnych PRL, wskazuje, że mimo postępującego procesu odprężeniowego w relacjach Wschód - Zachód w działalności służb specjalnych nie należy spodziewać się osłabienia aktywności, a wręcz przeciwnie, sytuacja polityczna w naszym kraju i wynikające z niej konsekwencje stanowić będzie okazję do zdynamizowania wywiadowczej penetracji. Należy liczyć się z tym, że zachwiania w świadomości społecznej oraz funkcjonowanie realnej opozycji politycznej zostanie wykorzystane przez służby specjalne państw NATO. Przedstawiona prognoza uzasadnia potrzebę aktywnego zajęcia się przez służbę kontrwywiadu WSW, rozpoznaniem bieżących i perspektywicznych zagrożeń wywiadowczych godzących w moc obronną Sił Zbrojnych PRL.

Podjęta w niniejszej pracy próba wypracowania praktycznego modelu kontrwywiadowczego zabezpieczenia ważnych nośników informacji, w oparciu o zdobycze współczesnej nauki, a głównie teoretycznych podstaw ogólnej teorii systemów i cybernetyki oraz dotychczasowe doświadczenia praktyczne daje podstawę do postawienia tezy, że w zainteresowaniu oficera

kontrwywiadu, podejmującego działania wynikające z kontrwywiadowczej ochrony tajemnicy, powinny znaleźć się przede wszystkim te informacje, które ujawniają faktyczne naruszenie reżimów ochrony lub mogą wskazywać na możliwość wywiadowczej infiltracji chronionego obiektu.

Usprawnianie kontrwywiadowczej ochrony tajemnicy w warunkach obowiązującej doktryny obronnej i odtajnienia danych o mocy obronnej Sił Zbrojnych PRL wymaga nowelizacji przepisów o ochronie tajemnicy, a w szczególności cz. II Instrukcji o ochronie tajemnicy w Siłach Zbrojnych PRL.

Przedstawione w niniejszej pracy teoretyczne i praktyczne aspekty budowy i funkcjonowania systemu kontrwywiadowczej ochrony tajemnicy - chociaż nie wyczerpują całokształtu możliwych rozwiązań - to jednak wskazują na główny kierunek innowacyjnych działań usprawniających w zakresie ochrony tajemnicy, w aktualnych i prognozowanych uwarunkowaniach wynikających z przyjętej doktryny obronnej, zagrożeń ze strony służb specjalnych NATO, złożonej sytuacji politycznej w naszym kraju oraz procesów odprężeniowych w relacji Wschód - Zachód.

B I B L I O G R A F I A

A. WYKAZ AKTÓW NORMATYWNYCH DOT. OCHRONY

TAJEMNICY W SIŁACH ZBROJNYCH PRL

1. Ustawa z dnia 14.12.1982 r. o ochronie tajemnicy państwowej i służbowej - Dz.U. z dn. 18.12.1982 r. nr 40, poz. 271
2. Zarządzenie nr 29/MON z dn. 27.05.1983 r. w sprawie ochrony tajemnicy państwowej i służbowej w resorcie Obrony Narodowej, Dz.Rozk. MON z 1983 r., poz.35
3. Zarządzenie Szefa WSW nr 010 z dn. 20.09.1985 r. w sprawie stosowania przedsięwzięć radiokontrywiadowczych.
4. Zarządzenie Szefa Sztabu Generalnego WP nr PF-10/Sztab z dn. 14.04.1986 r. wprowadzające do użytku "Przepisy o ochronie tajemnicy w Siłach Zbrojnych PRL. Część I. Zasady ogólne".
5. Zarządzenie Ministra Obrony Narodowej nr PF-7/MON z dnia 12.09.1983 r. w sprawie szczegółowych zasad i sposobu postępowania z wiadomościami stanowiącymi tajemnicę państwową o szczególnie ważnym znaczeniu dla obronności Państwa i Sił Zbrojnych PRL.
Dziennik Rozkazów Tajnych MON 1983 r., poz. 15.
6. Zarządzenie Szefa WSW nr 06 z dn. 10.07.1985 r. w sprawie kontrywiadowczej ochrony tajemnicy w Siłach Zbrojnych PRL
7. Rozkaz MON 018/MON z 17.12.1987 r. w sprawie doskonalenia systemu ochrony baz, składnic, lotnisk, dywizjonów rakietowych i technicznych WOPK, portów wojennych MW, wojskowych jednostek badawczo-rozwojowych, wojskowych zakładów remontowo-produkcyjnych i obiektów koszarowych jednostek.
8. Instrukcja pracy sztabowo-biurowej w Siłach Zbrojnych PRL wprowadzona Zarządzeniem Szefa Sztabu Generalnego WP nr 39/Sztab z dn. 28.07.1987 r., sygn. 1306/87
9. Informacja S.WSW o niektórych problemach zagrożeń gotowości bojowej oraz skuteczności przeciwdziałania im przez organy WSW w 1987 r. - pismo S. WSW nr DA-04631 z dnia 11.05.1988 r. /dot. penetracji/.
10. Informacja Szefostwa WSW nr DB-01414/35 z dn. 27.06.1985r.

11. Informacja Szefostwa WSW nr DB-00220/3 z dn. 10.02.1986 r.
12. Informacja Szefostwa WSW nr DB-001921/35 z dn. 14.11.1983r.
13. Informacja MSW nr 00604/84 - dot. działalności agentów CIA, Jurzaka i Adamaschka.
14. Informacja Szefostwa WSW nr DB-0720/3 z dn. 10.04.1987 r. dot. form i metod działalności CIA.
15. Informacja Zarządu III Szefostwa WSW nr DB-01342/35 z dn. 14.06.1985 r.
16. Informacja Zarządu III Szefostwa WSW nr DB-0321/5 z dnia 24.02.1982 r.
17. Informacja Zarządu III Szefostwa WSW nr DB-0752/35 z dnia 11.05.1984 r.
18. Informacja Zarządu III Szefostwa WSW nr DB-2701/5 z dnia 23.12.1981 r.
19. Informacja Zarządu III Szefostwa WSW nr DB- PF-1103/3 z dn. 30.06.1987 r.
20. Informacja Zarządu III Szefostwa WSW nr DB-0936/2 z dnia 14.05.1983 r.
21. Informacja Zarządu III Szefostwa WSW nr DB-01817/3 z dnia 5.09.1985 r.
22. Informacja Szefostwa WSW nr DB-0686/3 z dnia 29.03.1985 r.
23. Informacja Szefostwa WSW nr DB-PF-1184/35 z dnia 21.05.85 r.

B. LITERATURA

1. Ch. AILLERET "Francuska przygoda atomowa"
Wyd. MON, Warszawa 1979 r.
2. Z. BAKO "Wojna ekonomiczna", Wyd. MON,
Warszawa 1983 r.
3. J. BRONISŁAWSKI "Szpiegostwo, wywiad, paragrafy",
Wyd. Iskry, Warszawa 1979 r.
4. W. BIAŁOWĄS "Pojęcie i istota motywów zachowań
ludzkich", Zeszyty Naukowe ASW, nr 19,
Warszawa 1978 r.
5. F. BIELAK "Służby wywiadowcze Republiki
Federalnej Niemiec", Wyd. MON,
Warszawa 1985 r.
6. L. BERTELANFFY "Ogólne teorie systemów", Wyd. PWN,
Warszawa 1984 r.
7. Z. BRONIAREK "Źródła spirali zbrojeń", Wyd. MON,
A. KARKOSZKA Warszawa 1985 r.
8. E. BUŁA "Praktyczne wskazówki do pracy
z zakresu profilaktyki kontrwywia-
dowczej", Ośrodek Nauk Społecznych
i Wojskowych Śląskiego Okręgu
Wojskowego, Wrocław 1975 r.
9. E. BUŁA "Węzłowe problemy profilaktyki
kontrwywiadowczej", Oddział Propa-
gandy Zarządu Politycznego, Ośrodek
Nauk Społecznych i Wojskowych SOW,
Wrocław 1974 r.
10. B. CHOCHA "Wojna i doktryna wojenna", Wyd. MON,
J. KACZMAREK Warszawa 1980 r.
11. M. DANILUK "Gospodarka pokojowa a wojna", Wyd.
MON, Warszawa 1984 r.
12. J. DOŁGOPOŁOW "Wojna bez linii frontu", Wyd. MON
Warszawa 1985 r.
13. W. DRUŻYNNIN "Idea, algorytm, decyzja", Wyd. PWN,
D. KONTOROW Warszawa 1975 r.

14. W. FILAR
A. BARTCZAK "Symulacja i gry komputerowe w zastosowaniach wojskowych", Wyd. MON, Warszawa 1985 r.
15. R. FRELEK "Historia zimnej wojny", Wyd. MON, Warszawa 1971 r.
16. J. GAJEWSKI "Canaris", Wyd. KiW, Warszawa 1987r.
17. Z. GOŁĄB "Wojna a system obronny państwa", Wydanie MON, Warszawa 1984 r.
18. J. GOLEC "Rola kompleksu wywiadowczo-analitycznego CIA", Zeszyty Naukowe WOS nr 1 1988 r.
19. L. GONDEK "Działalność Abwechry na terenie Polski 1933-1939", Wyd. MON, Warszawa 1974 r.
20. Cz. GOLISZEWSKI "Wojna w wojnie", Wyd. KAW, Warszawa 1979 r.
21. S. HIPSZ
Z. KAROLAK "Jak powstaje technika wojskowa", Wyd. MON, W-wa 1981 r.
22. J. HABR "Systemowa analiza i synteza", Wyd. PWE, Warszawa 1976 r.
23. A.Z. IDZKIEWICZ "Ochrona informacji w procesie przetwarzania", Wyd. PWE, Warszawa 1979 r.
24. R. KILARSKI "Organizacje wywiadowcze Reinkarde Gehlena", Wyd. MON, Warszawa 1978 r.
25. S. KENT "Wywiad strategiczny", tłumacz., Szefostwo WSW, Warszawa 1962 r.
26. W. KOZACZUK "Bitwa o tajemnice", Wyd. KiW, Warszawa 1977 r.
27. W. KOZACZUK "Wojna w eterze", Wyd. RiTV, Warszawa 1977 r.
28. J. KOSSECKI "Cybernetyka kultury", Wyd. PIW, Warszawa 1974 r.
29. J. KOSSECKI "Tajniki sterowania ludźmi", Wyd. KAW, Warszawa 1984 r.

30. J. KOSSECKI "Cybernetyka społeczna", Wyd. PWN, Warszawa 1981 r.
31. P.W. KOSTIN "FBI - amerykańska tajna policja", Wyd. KiW, Warszawa 1971 r.
32. A.K. KOŹMIŃSKI "Analiza systemowa organizacji", Wyd. PWE, Warszawa 1976 r.
33. A.K. KOŹMIŃSKI "Zarządzanie systemowe", Wyd. PWE, Warszawa 1973 r.
34. J. KONIECZNY "Cybernetyka walki", wyd. PWN, Warszawa 1970 r.
35. J. KONIECZNY "Inżynieria systemów działania", Wyd. WNT, Warszawa 1984 r.
36. T. KOTARBIŃSKI "Traktat o dobrej robocie", Wyd. Ossolineum 1969 r.
37. J. KAMIŃSKI "Nauka i doktryna wojenna", Wyd. MON, Warszawa 1980 r.
38. S. LEWICKI "Szpiegzy Kajzera i Hitlera", Wyd. KAW, Warszawa 1978 r.
39. W. ŁUKÓW "O niektórych psychologicznych i społecznych aspektach czujności obywatelskiej", Zeszyty Naukowe ASW nr 28, Warszawa 1981 r.
40. J. MAZUR "Profilaktyka kontrwywiadowcza" Szefostwo WSW, Warszawa 1985 r.
41. M. MAZUR "Cybernetyczna teoria układów samodzielnych", Wyd. PWN, Warszawa 1966 r.
42. M. MAZUR "Pojęcie systemu i rygory jego stosowania", Wyd. PWN, Warszawa 1976r.
43. D.D. MEADOWS "Granice wzrostu", Wyd. PWE, Warszawa 1973 r.
44. L. MICHNOWSKI "Istota nowoczesnej wojny informacyjnej", Wyd. WSNS, Warszawa 1984 r.

45. J. MASTERMAN "Brytyjski system podwojonych agentów", Wyd. MON, Warszawa 1974 r.
46. A. NAGORNYJ "Jestem z kontrwywiadu", Wyd. MON, Warszawa 1983 r.
47. E.K. NOWAK "Za parawanem służb specjalnych RFN", Wyd. MON, Warszawa 1981 r.
48. K. NOŻKO "Walka o przewagę", Wyd. MON, Warszawa 1985 r.
49. E. NORD "Za parawanem służb specjalnych", Wyd. MON, Warszawa 1981 r.
50. M. POPIOLEK "Amerykańska wojna specjalna", Wyd. MON, Warszawa 1968 r.
51. A. RAMME "Służba bezpieczeństwa SS", Wyd. MON, Warszawa 1984 r.
52. M. RENIAK "Kulisy, fakty, dokumenty", Wyd. MON, Warszawa 1984 r.
53. F. RYSZKA "Polityka i wojna", Wyd. PiW, Warszawa 1975 r.
54. A. ROGUCKI "Analiza systemów w planowaniu obrony", Wyd. MON, Warszawa 1975 r.
55. S. SAWICKI "Attache`s wojskowi w systemie służby dyplomatycznej oraz w strukturze sił zbrojnych i służb wywiadowczych głównych państw NATO", Wyd. Zeszyty Naukowe ASW nr 6 - 1985 r.
56. P. SIENKIEWICZ "Inżynieria systemów", Wyd. MON, Warszawa 1983 r.
57. P. SIENKIEWICZ "Inżynieria systemów kierowania", Wyd. PWE, Warszawa 1988 r.
58. P. SIENKIEWICZ "Teoria efektywności systemów", Wyd. Ossolineum 1987 r.
59. Z. TOPOLEWSKI "Analiza i synteza informacji w procesach przetwarzania i teletransmisji danych", Wyd. PW - Wrocław 1985 r.

60. W. WIENER "Cybernetyka i społeczeństwo",
Wyd. PWN, Warszawa 1961 r.
61. L.N. WOŁGIN "Problema optimalności w teoreti-
czeskiej kibernetike", Moskwa 1968r.
62. B. WOŹNIECKI "NATO lat osiemdziesiątych", Wyd.
MON, Warszawa 1982 r.
63. J. WIATR "Socjologia wojska", Wyd. MON,
Warszawa 1987 r.
64. J. ZIELENIEWSKI "Organizacja i zarządzanie", Wyd.
PWN, Warszawa 1969 r.
65. E.M. ZACHARIAS "Tajne misje - zapiski oficera
wywiadu", Wyd. Szefostwa WSW,
Warszawa 1962 r.
66. "Inżynieria systemów w rozwoju
społeczno-ekonomicznym i obronnym
kraju", Materiały z kolokwium
w ASG WP, Warszawa 1985 r.
67. "Poradnik kontrwywiadu armii
Stanów Zjednoczonych", Przekład
z angielskiego, Wyd. WOS MSW,
Warszawa 1986 r.
68. "Zasady pracy wywiadowczej przeciwko
NATO", /tłumaczenie z języka rosyjs-
kiego/, Wyd. MON - Sztab Gen. WP
wewn. 4/189/87, Warszawa 1987 r.

Wydrukowano w 1 egz.
Powielono w 4 egz.

Druk A.S.
Dnia 20.05.1989 r.
Nr 082/K

