



AKADEMIA OBRONY NARODOWEJ

AON wewn. 5081/98

JAWNE

Do użytku służbowego

Egz. nr **50**

Płk dr inż. Józef JANCZAK

ANALIZA INFORMACJI O SIŁACH I ŚRODKACH PRZECIWNIKA W KONTEKŚCIE BUDOWY KOMPUTEROWEJ BAZY DANYCH

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. _____
51407

WARSZAWA

1998

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

KATEDRA ROZPOZNANIA WOJSKOWEGO I ARMII OBCYCH

PRZEKLASYFIKOWANO

AON wewn. 5081/98

Protokół Nr 54305

JAWNE

~~Do użytku służbowego~~

Egz. nr **50**

Plk dr inż. Józef JANCZAK

**ANALIZA INFORMACJI O SIŁACH
I ŚRODKACH PRZECIWNIKA
W KONTEKŚCIE BUDOWY KOMPUTEROWEJ
BAZY DANYCH**



Spis treści

Wstęp.....	5
I. Właściwości informacji o przeciwniku oraz wymagania stawiane przy jej pozyskiwaniu	7
II. Analiza struktur informacji o siłach i środkach przeciwnika	17
III. Analiza możliwości pozyskiwania informacji o siłach i środkach przeciwnika	31
IV. Formy informacji z rozpoznania gromadzonej w bazie danych na potrzeby militarne.....	54
1. Specyfika bazy danych na potrzeby militarne	54
2. Przykładowe formy informacji z rozpoznania niezbędnej na poszczególnych szczeblach dowodzenia.....	59
3. Współpraca użytkowników z bazą danych na potrzeby militarne	72
4. Dostępność do danych (do informacji wyjściowych) na różnych szczeblach dowodzenia.....	77
5. Bezpieczeństwo informacji w bazie danych na potrzeby militarne	78
Zakończenie.....	81
Bibliografia	82

WSTĘP

W przeszłości osiągnięcia technologiczne wykorzystywane były przede wszystkim w celu zwiększenia siły (mocy) i skuteczności rażenia wojsk oraz środków uzbrojenia. Obecny rozwój technologii sprawił, że dzięki zautomatyzowanym systemom dowodzenia i kierowania środkami walki, bazujących na ciągłym i szybkim dostępie dowództw i sztabów do aktualizowanych na bieżąco informacji - główny nacisk kładzie się na skoordynowanie i uelastycznienie działań zbrojnych. Teoretycy wojskowi przewidują, że przyszła wojna może przebiegać według scenariuszy podobnych do dziejszych wojennych filmów fantastycznych. *Jest prawdopodobne, że przywódcy zwaśnionych stron prowadzić będą wirtualne wojny zanim zdecydują się w ogóle na walkę.* Niektórzy futuryści w swoich przewidywaniach idą jeszcze dalej. Zakładają, że państwa będą toczyły symulowane wojny zamiast faktycznych bitew, a wojna będzie grą *wideo* bez konieczności zadawania bólu ludziom. W takiej sytuacji słuszną wydaje się teza, że *informacja stanie się czynnikiem kluczowym na przyszłym polu walki. Informacja w walce zbrojnej jest już dziś oraz będzie w przyszłości tym, czym był karabin maszynowy w pierwszej i czołg w drugiej wojnie światowej¹.* Aby zwyciężyć należy wygrać *walkę informacyjną.* Bez względu na charakter przyszłej wojny, *szybkie i sprawne zdobywanie (pozyskiwanie) dokładnych informacji o przeciwniku (typu rozpoznawczego) będzie w decydujący sposób wpływało na jej przebieg oraz rezultat końcowy.* Proces ten uzależniony będzie w dużej mierze od prawidłowego określenia struktur informacji o siłach i środkach przeciwnika oraz możliwości jej ciągłego i szybkiego pozyskiwania. Pozyskiwanie oraz efektywne wykorzystanie informacji wymaga wiedzy i umiejętności praktycznych w zakresie organizowania procesu rozpoznawczego oraz zapewnienia współdziałania ze sobą różnych organów sztabów i wojsk w złożonym

układzie techniczno-osobowym. Rozwiązywanie tego problemu przez zwiększanie ilości personelu w poszczególnych komórkach organizacyjnych należy już do przeszłości.

Zwiększenie efektywności procesu zbierania i przetwarzania informacji o siłach i środkach przeciwnika można osiągnąć odpowiednio wykorzystując możliwości współczesnych środków informatycznych. Analiza informacji o siłach i środkach przeciwnika oraz metod jej pozyskiwania w kontekście budowy komputerowej *bazy danych*² przedstawiona została w kolejnych rozdziałach pracy studyjnej.

PRZYPISY

¹ Tezę tę postawił adm. Wiliam Owens - zastępca przewodniczącego Kolegium Szefów Sztabu SZ USA.

² Teoria i praktyka tworzenia baz danych jest stosunkowo młodym, a zarazem burzliwie rozwijającym się działem informatyki. Pojęcie baza danych zostało wprowadzone do powszechnego użytku w latach sześćdziesiątych. Przedtem mówiło się o plikach i zbiorach danych. Wprowadzono je dlatego, gdyż zaistniała potrzeba wyróżnienia jedną nazwą zbiorów danych charakteryzujących się dużą ilością informacji, możliwością korzystania przez innych użytkowników a zarazem szybkim dostępem do poszczególnych danych oraz niezależnością od programów użytkowych.

I. WŁAŚCIWOŚCI INFORMACJI O PRZECIWNIKU ORAZ WYMAGANIA STAWIANE PRZY JEJ POZYSKIWANIU

Rezultaty walki zbrojnej zależą w znacznej mierze od informacji o przeciwniku. Stanowią one bowiem podstawę do analizy i oceny sytuacji, wypracowania i podjęcia decyzji oraz jej realizacji. Jednak nawet najlepsza informacja o przeciwniku staje się bezwartościowa, jeśli dotrze zbyt późno do adresata. Treść i terminowość jest znacznie ważniejsza od jej ilości. Autor doszedł do przekonania - po przestudiowaniu dostępnej literatury przedmiotu¹ - że analiza informacji o siłach i środkach przeciwnika powinna być poprzedzona naukowym wyjaśnieniem pojęcia „informacja”.

W rozumieniu potocznym pojęcie „informacja” oznacza wiadomość, wieść, nowinę, rzecz zakomunikowaną; miarę wiedzy o jakimś zdarzeniu². Informacja jest jednym z podstawowych pojęć w naukach teoretycznych i stosowanych. Trudno wskazać taki obszar zjawisk przyrodniczych lub taką gałąź techniki, w której nie byłoby do czynienia z przenoszeniem i przetwarzaniem informacji w procesach fizycznych. Jest to obiekt abstrakcyjny, który w postaci zakodowanej (dane)³ może być:

- pozyskiwany różnymi sposobami i metodami,
- na różne sposoby przesyłany na znaczne odległości, np. przy pomocy: fal elektromagnetycznych; sygnałów elektrycznych; umówionych sygnałów; głosu itp.,
- przechowywany na nośniku danych, np. taśmie magnetycznej, w pamięci rdzeniowej komputera, na dysku magnetycznym, na taśmie perforowanej itp.,
- przetwarzany i użyty do sterowania (np. komputerem steruje program będący zakodowaną informacją)⁴.

Informacjami mogą być dane których nośnikami są fale elektromagnetyczne oraz wszelkiego rodzaju uboczne efekty towarzyszące zbrojnym działaniom wojennym, na przykład: obrazy optyczne, dźwięki akustyczne (odgłosy pola walki), termiczne, sejsmiczne, magnetyczne, chemiczne itp. Źródłami informacji (rozpoznawczych) mogą być podające je obiekty. W tym aspekcie wyróżniane są źródła:

- binarne, podające jedną z dwóch możliwych wiadomości, np. element logiczny o 2 wyróżnionych stanach: „tak” i „nie”,
- ziarniste (dyskretne), podające jedną spośród skończonej liczby wiadomości,
- ciągłe, podające wiadomości różniące się między sobą dowolnie małą wielkością.

Należy nadmienić, że potrzeby nauki o ogólnych prawach pozyskiwania, odbierania, przesyłania lub przetwarzania informacji zrodziły się bardzo dawno. Początki sięgają starożytności. W poglądach filozofa greckiego Empedoklesa (V w. p.n.e.) wystąpiła już pierwsza próba wyjaśnienia mechanizmu postrzegania zmysłowego. Dowiódł on, że obiekt jest postrzegany przez narządy zmysłów kiedy „wpływy” są identyczne. Uogólniając można wnioskować, że nośnikiem informacji danej w doznaniach zmysłowych są pewne zjawiska fizyczne, które dziś zwykliśmy nazywać sygnałami. Z kolei Pitagoras i jego uczniowie odkryli, że nośnikiem doznań słuchowych są ruchy powietrza, a częstota tych ruchów ma bezpośredni związek z brzmieniem słyszalnego dźwięku.

W czasach nowożytnych wynalazki A. G. Bella (telefon - 1876 r.), S.F. Morse'a (telegraf elektromagnetyczny - 1838 r., alfabet - 1840 r.), T.A. Edisona (cewka indukcyjna, mikrofon węglowy, fonograf - 1877 r.), A.S. Popowa i G. Marconiego (antena, nadajnik, odbiornik radiowy - przełom XIX i XX w.) przyczyniły się do przedstawienia problemów przesyłania wiadomości na odległość w postaci sygnałów.

W latach dwudziestych naszego stulecia pojawiły się pierwsze rozważania teoretyczne H. Nyquista oraz R. V. L. Hartleya, w których dokonano próby rozgraniczenia między *sygnałem*, czyli określonym procesem fizycznym i tym, czym sygnał jest nacechowany, czyli *informacją*. Szczególne zasługi w rozwoju matematycznej teorii takich procesów położył uczony rosyjski A. Kołmogorow i dwaj uczeni amerykańscy: G. D. Birkhoff i N. Wiener.

Z cybernetycznego punktu widzenia: „informacja” - to każdy czynnik, dzięki któremu obiekt odbierający (człowiek, organizm żywy, organizacja, urządzenie automatyczne) może polepszyć swoją znajomość otoczenia i bardziej sprawnie przeprowadzić celowe działanie⁵.

W cybernetyce informacja stanowi jedno z podstawowych pojęć, którego desygnat jest nie w pełni definiowalny z uwagi na jego pierwotny i elementarny charakter⁶. W opisie procesów łączności i sterowania pojęcie informacja zajmuje podobną pozycję jak pojęcia masy i energii w fizyce. Wszystkie dotychczasowe próby zdefiniowania pojęcia informacja uważa się powszechnie za niezadowalające, a co najwyżej za ukazujące tylko niektóre aspekty informacji. Potwierdzeniem tej tezy są przytoczone poniżej poglądy niektórych autorytetów w tej dziedzinie.

Wiener określa informację jako *nazwę treści zaczerpniętej ze świata zewnętrznego, w miarę jak się do niego dostosowujemy i jak przystosowujemy doń swoje zmysły. Proces otrzymywania i wykorzystywania informacji jest procesem naszego dostosowywania się do różnych ewentualności środowiska zewnętrznego oraz naszego czynnego życia w tym środowisku.*

Couffignal twierdzi, że *w cybernetyce informacją nazywa się wszelkie działanie fizyczne, któremu towarzyszy działanie psychiczne.*

Według W. Głuszkowa, informacja to *wszelkie wiadomości o procesach i stanach dowolnej natury, które mogą być odbierane przez organy zmysłowe człowieka lub przez przyrodę.*

Według poglądów H. Greniewskiego, informacja to *stany wyróżnione wejść i wyjść układu*.

Zdaniem C. L. Shannona *informacją jest to wszystko, co nie jest ani energią, ani masą, czyli jest zasilaniem - jest to każde rozpoznanie stanu układu, odróżnialnego od innego stanu tego układu*⁷. Poza tym Shannon dowiódł⁸, że przesyłanie i odbiór informacji związane jest ze zmianą nieokreśloności u adresata. Według Shannona miarą nieokreśloności jest *entropia*, która wyraża się ilościowo jako średnia wartość funkcji prawdopodobieństw wszystkich możliwych realizacji doświadczenia:

$$H = - \sum_{i=1}^k p_i \log_2 p_i$$

gdzie:

p_i - oznacza prawdopodobieństwo i - tej informacji.

Źródłem nieporozumień dotyczących interpretacji pojęcia informacji przez różnych naukowców bywa często fakt, iż jest ono używane w cybernetyce w dwóch, nieco odmiennych znaczeniach, a mianowicie w odniesieniu do:

- układu na który informacja działa, czyli jest przez ten układ odbierana (zarówno przez organizm biologiczny, społeczeństwo, maszynę, jak też z pewnymi zastrzeżeniami przez przyrodę nieożywioną),

- miary zorganizowania układu, co jest związane z pojęciem entropii.

„Entropia” układu jest miarą chaosu, tj. wyraża stopień nieuporządkowania układu, natomiast informacja jest ilościową miarą zorganizowania układu. Często wyróżnia się entropię informacyjną oraz entropię fizyczną.

Entropia informacyjna - jest to entropia będąca miarą nieokreśloności zdarzeń stanowiących źródła informacji przy określonym stanie niewiedzy o tych zjawiskach. Jest ona ściśle związana z ilością informacji zawartej w odebranej komunikacie, gdyż za miarę uzyskanej tą drogą przez odbiorcę ilości informacji przyjmuje się stopień zmniejszenia nieokreśloności. W odróżnieniu od entropii fizycznej, która jest całkowicie określona przez

istniejący obiektywnie rozkład prawdopodobieństwa danego stanu, pojęcie *entropii informacyjnej* uwzględnia dodatkowo także i nieokreśloność spowodowaną niepełną wiedzą odbiorcy o statystyce zjawisk zachodzących w źródle informacji. Dlatego też entropia informacyjna, którą odbiorca przypisuje określonemu zjawisku, może być co najmniej równa entropii fizycznej tego zjawiska lub większa od niej. Tylko w przypadku, gdy odbiorca jest całkowicie poinformowany o statystycznej naturze zjawiska, wartość entropii fizycznej i informacyjnej pokrywają się. Ponieważ informacja przed podaniem jej przez źródło nie jest znana obiektowi przeznaczenia, traktuje się ją jako wielkość losową (prawdopodobieństwo, rachunek).

Miarą niewiedzy o tym, jaką konkretną wiadomość poda źródło ziarniste, jest entropia dyskretnej (nieciągłej) zmiennej losowej X_d , która charakteryzuje się ciągiem rozkładów:

$$P_k = P \{ X_d = x_k \}$$

dla $k = 1, 2, \dots, n$ i jest wyrażona zależnością:

$$H(X_d) = - \sum_{k=1}^n P_k \log_a P_k$$

gdzie:

P_k - prawdopodobieństwo k -tej realizacji dyskretnej zmiennej losowej,

x_k - k -ta realizacja zmiennej losowej X_d ,

a - podstawa logarytmu określająca jednostkę ilości.

W przypadku źródła binarnego, podającego informacje z jednakowymi prawdopodobieństwami - podstawą logarytmu będzie liczba „2”. Entropia równa jest jednostce, którą nazwano bitem⁹. Otrzymanie informacji jest związane ze zmniejszeniem entropii: - im większa jest niewiedza o tym, jaką wiadomość poda źródło, tym więcej informacji uzyskuje się otrzymując ze źródła konkretną wiadomość; - im bardziej prawdopodobny jest komunikat, tym mniej niesie informacji¹⁰.

Analiza dostępnej literatury pozwala postawić tezę, że informacja zaliczana jest do pojęć abstrakcyjnych. Jednak pojęciu temu często towarzyszą inne bardzo podobne określenia, np.: „dane”, „komunikat”, „wiadomość”, „sygnał”.

Dane są to informacje potencjalne, które po odpowiednim opracowaniu mogą stać się przydatnymi w działaniu celowym.

Komunikat stanowi pewną porcję informacji przekazanej adresatowi (do układu odbierającego) w czystej formie.

Wiadomość - to informacja specjalna opracowana na użytek konkretnego adresata (układu odbierającego - człowieka lub urządzenia technicznego). *Powszechnie wiadomo, że wiadomość może być przekazana w postaci komunikatu zawierającego pewną ilość informacji.*

W większości przypadków informacja nie jest ogólnie dostępna. Dotyczy to szczególnie sposobów użycia sił i środków potencjalnego przeciwnika na współczesnym polu walki. Przejawia się w postaci *nieskończonej liczby sygnałów*, które w rzeczywistości są nośnikami informacji. Mówiąc, że informacja zawarta jest w sygnale należy rozumieć, że niektóre cechy sygnału wpływające na jej postać nie należą do informacji, lecz należą do innych czynników. W skrajnym przypadku, gdy sygnał zależy tylko od informacji można go utożsamiać z informacją. *Zatem różnica między informacją a niosącą ją sygnałem jest w gruncie rzeczy w dużej mierze umowna.*

Współczesna walka zbrojna dostarcza ogromnych ilości informacji o przeciwniku, których pozyskiwaniem, opracowywaniem oraz szeroko pojętą dystrybucją zajmują się wyspecjalizowane komórki sztabowe wraz z podległymi im organami rozpoznawczymi. Tworzą one system informacyjny wojsk. *W systemie informacyjnym wojsk, tak źródła informacji, jak i układy odbierające dostosowane są nie tylko do spełniania swej roli w przestrzeni widma elektromagnetycznego. Dostosowywane są również do funkcjonowania w przestrzeni fal sprężystych, efektów magnetycznych*

i efektów chemicznych, przez pryzmat czego również możliwe jest identyfikowanie stanu aktualnego pola walki.

W takim ujęciu informacjami o przeciwniku są wszystkie te wiadomości, które mogą być wykorzystane w różnych przedziałach czasowych do prowadzenia wojny. Dotyczą one m.in.:

- sytuacji politycznej, gospodarczej i geostrategicznej, meteorologicznej, a także ich wzajemnych związków i zależności,

- możliwości operacyjno-technicznych sił i środków,

- cech charakterystycznych oraz sytuacji geograficznej, meteorologicznej, geologicznej, biologicznej, ekologicznej, chemicznej, medycznej oraz sposobów wykorzystania spektrum elektromagnetycznego,

- treści przekazów mówionych, obrazowych lub pisanych, tj. rozkazów, meldunków, wiadomości, informacji rozpowszechnianych przez środki masowego przekazu oraz sieci informatyczne o zasięgu globalnym (np. internet), krajowym, lokalnym lub resortowym,

- sposobów postępowania, z uwzględnieniem m.in. zasad dowodzenia i działania oraz przepisów, regulaminów a także innych reakcji, takich jak np. „warunkowe i bezwarunkowe odruchy” systemów broni,

- stanu i rozwoju właściwości fizycznych, psychicznych i moralnych,

- cybernetycznych współzależności pomiędzy informacjami pojedynczymi a dużą ilością danych (np. sytuacja).

O wartości informacji o przeciwniku w kontekście treści w niej zawartej, elementami decydującymi o jej wartości są:

- wiarygodność (prawdziwość),

- aktualność.

Obok informacji wiarygodnych o siłach i środkach przeciwnika występuje także duża ilość informacji dezinformujących, które mogą oddziaływać na procesy decyzyjne w postaci czynników zakłócających. Tak więc problem nie tkwi w braku czy niedostatku informacji, lecz w tym, że:

- nie zawsze istnieje możliwość dysponowania informacjami we właściwym czasie,
- informacji może być brak tam, gdzie są najbardziej potrzebne w danym momencie czasowym,
- informacje nie zawsze są pełne i często sprzeczne,
- do dyspozycji znajduje się tak duża ilość informacji, że tych naprawdę ważnych nie można we właściwym czasie z tej ilości wyselekcjonować.

Celem pozyskiwania informacji nie jest to, aby wszystko było wiadome, lecz to aby wiedzieć wystarczająco dużo, a przede wszystkim więcej niż przeciwnik. Przy czym często wystarczy, aby istotne informacje uzyskiwać wcześniej od innych. Niekiedy mówi się o tzw. „wyprzedzeniu informacyjnym”, które jest najczęściej równoznaczne z *posiadaniem przewagi czasowej*, natomiast rzadko stanowi to nadwyżkę informacji. Z tych też względów proces pozyskiwania informacji powinien być wyjątkowo starannie organizowany. W procesie tym należy kierować się następującymi zasadami:

- informacje powinny być uzyskiwane ze źródeł charakteryzujących się wysokim stopniem pewności,
- powinny być przekazane w ciągu określonego granicznego czasu a docelowo w czasie rzeczywistym,
- pozyskiwanie informacji powinno być starannie zaplanowane i przekazane do realizacji z możliwie dużym wyprzedzeniem czasowym,
- zaopatrywanie w informacje musi być tak organizowane, aby do dyspozycji znalazły się informacje pewne, we właściwym czasie i miejscu,
- powinno się prowadzić redukcję i kompresję informacji w celu dopasowania ich ilości do potrzeb odpowiednich szczebli dowodzenia i sprawności ich systemów przetwarzania, a także zapobieganie tworzeniu się tzw. „wąskich gardeł” przy przekazywaniu informacji. Należy jednak mieć na uwadze, by ilość informacji nie była w żadnym wypadku „obcinana” automatycznie oraz dostosowywana do możliwości (pojemności) środków przekazywania i przetwarzania informacji.

Analizując właściwości informacji i wymagania stawiane przy ich pozyskiwaniu z wojskowego punktu widzenia, można zauważyć, że:

1. Bardzo często występuje tendencja do tego, aby możliwie dużo lub w ogóle wszystko wiedzieć. W związku z tym w wojskowych systemach wymiany informacji, często w obiegu występuje znacznie więcej informacji, niż jest to potrzebne. W praktyce dążenie to nie zawsze powinno być realizowane, ponieważ może doprowadzić do wywołania takiego napływu informacji, iż zostanie zablokowany proces decyzyjny.

2. Najczęściej występuje brak tych informacji, które są w danej chwili potrzebne. Wyływa stąd - być może najważniejszy wniosek, że w planie pozyskiwania informacji należy uwzględniać nie tylko siły i środki, lecz również obszar (względnie odległości), potrzeby czasowe oraz wydajność systemów dystrybucji informacji.

3. W systemie informacyjnym znajduje się bardzo duża ilość informacji, których jednak w razie potrzeby nie można wykorzystać. Z reguły wynika to z braku czasu na jej opracowanie i przekazanie.

4. Informacje istniejące (znajdujące się w dyspozycji) wykorzystywane są jako oczywiste. Zauważany jest dopiero ich brak. Jeżeli nie odczuwa się ich braku, oznacza to, że nie są one potrzebne.

5. Wiele spośród posiadanych informacji jest często niepotrzebnych. Dezaktualizują się, zanim zostaną przez kogokolwiek wykorzystane.

Z przedstawionych rozważań wynika, że problem pozyskiwania, przekazywania przetwarzania oraz dystrybucji informacji powinien być ujęty w odpowiednich planach, *a posługiwanie się nimi powinno być tak samo ćwiczone jak dzieje się to w przypadku użycia i działania wojsk*. W procesie zdobywania danych o siłach i środkach przeciwnika powinny być wykorzystane na szeroką skalę środki informatyczne, które - jak powszechnie wiadomo - umożliwiają tworzenie wielokryterialnych komputerowych baz danych. W bazach tych powinny być zawarte zbiory umożliwiające: tworzenie dowolnych kompilacji informacji (także w wypadku sytuacji nieprzewidzianej

nych), tworzenie prostego „dialogu” z bazą danych w systemie konwersacyjnym (tzn. pytanie - odpowiedź), graficzne zobrazowanie informacji o przeciwniku oraz komputerowe przetwarzanie i dystrybucję informacji w czasie zbliżonym do rzeczywistego.

Istotną rolę w przygotowaniu baz danych o przeciwniku ma przyjęcie odpowiednich kryteriów podziału informacji o jego siłach i środkach, tj. określenie odpowiednich struktur tej informacji. Sposób rozwiązania tego problemu przedstawiony zostanie w następnym podrozdziale.

PRZYPISY

¹ Wykaz literatury zamieszczony został w spisie bibliograficznym.

² W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Wiedza Powszechna, Warszawa 1980.

³ Dane - oderwana (nie mająca miana) forma informacji, do której przetworzenia (interpretacji) niezbędne jest ustalenie odpowiedniego „klucza” (określającego np. układ i znaczenie poszczególnych rubryk formularza użytego do zapisu danych). Niektórzy badacze traktują „dane” jako informację potencjalną.

⁴ *Encyklopedia powszechna PWN*, t. 2, Warszawa 1983, s. 281.

⁵ *Leksykon techniczny*, Wyd. NT, Warszawa 1983.

⁶ *Mały słownik cybernetyczny*, Warszawa 1973, s. 155.

⁷ Układ informacyjny to taki, który ma choć jedno wejście informacyjne oraz choć jedno wyjście informacyjne, a więc jest jednocześnie układem informującym i układem informowanym.

⁸ W pracy pt.: *Matematyczna teoria łączności* (1948).

⁹ Bit - najbardziej popularna jednostka ilości informacji, której nazwa pochodzi od ang. *binary information theoretical unit* = teoretyczna jednostka informacji binarnej lub binary digit = cyfra dwójkowa.

¹⁰ *Mały słownik cybernetyczny*, pod red. M. Kempisty, Wiedza Powszechna, Warszawa 1973, s. 155-157.

II. ANALIZA STRUKTUR INFORMACJI O SIŁACH I ŚRODKACH PRZECIWNIKA

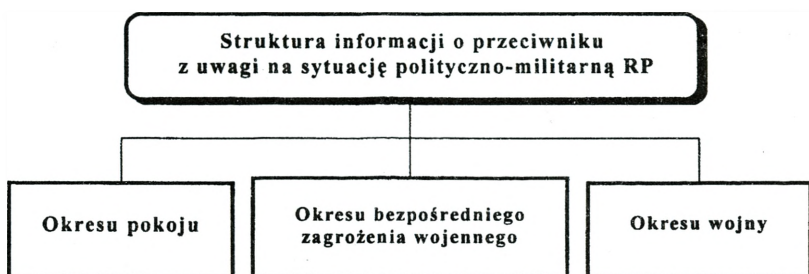
Złożoność procesów współczesnego pola walki powoduje, że decydenci żądają coraz większej ilości informacji, o coraz bardziej złożonej strukturze oraz szerszym zasięgu tematycznym. Wszystkie informacje dotyczące potencjalnego przeciwnika, jego sił zbrojnych, polityki, ekonomiki, infrastruktury, demografii, nastrojów, terenu, warunków hydrologicznych i meteorologicznych noszą nazwę *informacji rozpoznawczych*¹. Ważną rolę w procesie ich gromadzenia oraz przetwarzania stanowią komputerowe bazy danych.

Informacje wprowadzane do baz danych o siłach i środkach przeciwnika powinny być odpowiednio usystematyzowane oraz zgromadzone w odpowiednich, niezależnych zbiorach, uwzględniających wielokryterialne jej podziały.

Z uwagi na *sytuację polityczno-militarną RP* można wyróżnić trzy wzajemnie uzupełniające się zbiory informacji o siłach i środkach przeciwnika:

- zbiór okresu pokoju,
- zbiór okresu bezpośredniego zagrożenia wojennego,
- zbiór okresu wojny (początkowego okresu wojny).

W okresie pokoju powinna być gromadzona najliczniejsza baza danych o siłach i środkach potencjalnego przeciwnika². Szczególną uwagę należy zwrócić na te państwa, z którymi kraj nasz nie posiada sojuszy obronnych. Informacje powinny być gromadzone i weryfikowane koniecznie na bieżąco. Baza danych o siłach i środkach potencjalnego przeciwnika (*okresu pokojowego*) powinna obejmować zbiory informacji dotyczące:



- struktur organizacyjnych sił zbrojnych ww. państw: składu bojowego, organizacji, wyposażenia i dyslokacji poszczególnych rodzajów sił zbrojnych, ich sztabów, związków taktycznych, oddziałów oraz innych samodzielnych jednostek,

- rozwoju technicznego sił zbrojnych państw obcych, modernizacji poszczególnych rodzajów broni, wzrostu ich możliwości ogniowych i gotowości bojowej. szczególną uwagę należy zwrócić także na rozwój systemów rozpoznania i walki radioelektronicznej, dowodzenia, łączności i informatyki, obrony powietrznej oraz zabezpieczenia logistycznego,

- kierunków rozwoju strategii, sztuki operacyjnej i taktyki w poszczególnych państwach,

- systemów mobilizacyjnych oraz operacyjnego rozwijania sił zbrojnych, rodzajów wojsk, związków taktycznych i oddziałów, możliwych kierunków ich użycia oraz prawdopodobnych zadań,

- operacyjnego przygotowania teatrów działań wojennych i przewidywanych kierunków operacyjnych,

- przebiegu manewrów i ćwiczeń, procesów dydaktyczno-wychowawczych oraz zmian w koncepcjach ich prowadzenia oraz sposobach zabezpieczenia,

- przebiegu lokalnych konfliktów zbrojnych oraz taktyki użycia wydzielonych sił i środków państw obcych w misjach pokojowych,

- sylwetek ważniejszych dowódców, ich przebiegu służby wojskowej oraz stosowanych stylów i technik dowodzenia.

Struktura bazy danych *okresu bezpośredniego zagrożenia wojennego* powinna stanowić uzupełnienie (a niekiedy jedynie uaktualnienie) bazy okresu pokojowego i obejmować dane dotyczące:

- sygnałów alarmowych, zarządzeń oraz sposobów przechodzenia sił zbrojnych potencjalnego przeciwnika w stan pełnej gotowości bojowej,
- zakresu uruchomienia jego systemu mobilizacyjnego,
- zmian dyslokacji (bazowania), przegrupowania wojsk potencjalnego przeciwnika oraz operacyjnego rozwijania jego sił zbrojnych,
- stanu gotowości stacjonarnych oraz rozwijających się jego polowych systemów dowodzenia i łączności,
- rejonów rozmieszczenia ważnych obiektów przeciwnika,
- stanu ilościowego i ugrupowania wojsk przeciwnika w strefach przygranicznych oraz obszarach operacyjnego rozwijania jego sił zbrojnych a także możliwości narastania sił w wyniku mobilizacji lub przerzutów z innych kierunków operacyjnych,
- zmian operacyjnego przygotowania terenu w rejonach przygranicznych i na kierunkach planowanych przez niego działań,
- zakresu, kierunków i metod działalności psychologiczno-dywersyjnej przeciwnika.

Struktura bazy danych *okresu wojny (początkowego okresu wojny)* powinna stanowić uzupełnienie (a niekiedy uaktualnienie) poprzednich dwóch pierwszych baz oraz obejmować dane dotyczące:

- głównych zgrupowań uderzeniowych pierwszego rzutu operacyjnego przeciwnika, ich stanów ilościowo-jakościowych, kierunków działania oraz prawdopodobnych zadań,
- składu i rejonów rozmieszczenia drugich rzutów oraz odwodów, ich przegrupowań do obszaru zbrojnych działań wojennych, możliwych kierunków rubieży oraz terminów ich wprowadzenia do walki,

- możliwości i przebiegu formowania nowych związków, stopnia osiągania przez nie gotowości bojowej oraz prawdopodobnego czasu zdolności do działań,

- stanu i dyslokacji sił powietrznych, zmian bazowania lotnictwa oraz sposobów jego wykorzystania w ramach wsparcia i zabezpieczenia działań wojsk,

- zmian w rozmieszczeniu i działaniu sił morskich, sposobów ich użycia, wykorzystania baz morskich i portów do przerzutów wojsk i zaopatrzenia,

- stopnia przygotowania, czasu, kierunków i rejonów oraz celu użycia wojsk powietrzno-desantowych,

- zmian w strukturach organizacyjnych wojsk oraz w taktyce i sztuce operacyjnej,

- zmian w uzbrojeniu oraz w specjalistycznych środkach technicznych wprowadzanych do wyposażenia wojsk,

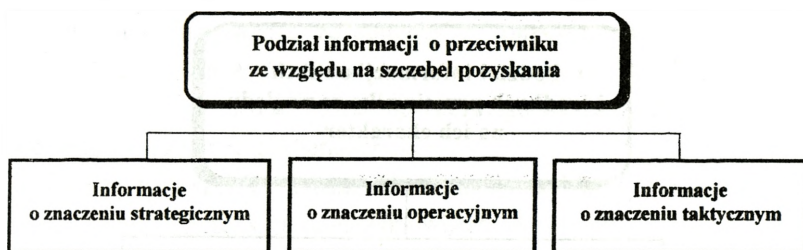
- skuteczności systemów bojowego oraz logistycznego zabezpieczenia zbrojnych działań wojennych,

- składu narodowościowego i społecznego wojsk przeciwnika, zdyscyplinowania, stanu moralnego i psychicznego żołnierzy oraz ich doświadczenia bojowego,

- zmian kadrowych, sylwetek nowych dowódców ich przebiegu służby wojskowej oraz stosowanych stylów i technik dowodzenia.

Informacje o siłach i środkach przeciwnika pozyskiwane są w wyniku prowadzonych działań rozpoznawczych przez etatowe, odpowiednio wyszkolone i wyposażone wojska rozpoznawcze, a także doraźnie przez wydzielone siły i środki z pododdziałów ogólnowojskowych oraz innych rodzajów wojsk na różnych szczeblach dowodzenia (strategicznym, operacyjnym i taktycznym). Podział ten powinien mieć również odzwierciedlenie w strukturze bazy danych o siłach i środkach przeciwnika.

Ze względu na *organ organizujący pozyskanie informacji*, a w ślad za tym ich charakter i wagę można wyróżnić trzy zasadnicze ich kategorie:

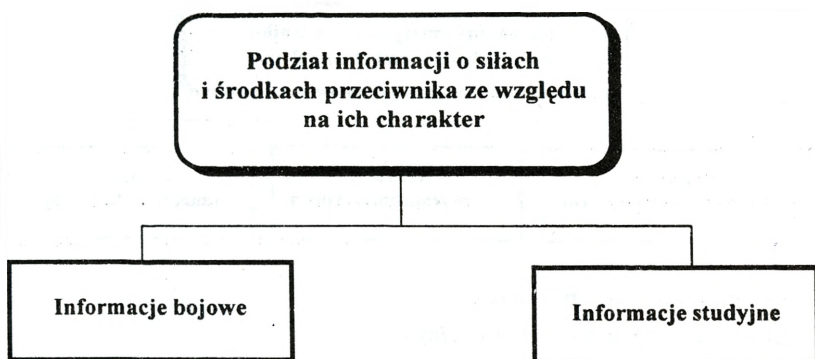


- informacje o znaczeniu *strategicznym*,
- informacje o znaczeniu *operacyjnym*,
- informacje o znaczeniu *taktycznym*.

Informacje o przeciwniku o znaczeniu strategicznym pozyskuje Sztab Generalny przy współudziale rodzajów sił zbrojnych. Ich treść powinna dotyczyć potencjalnego przeciwnika oraz teatrów działań wojennych, całokształtu życia politycznego, gospodarczego, naukowo - technicznego, wojskowego i innych ważnych dziedzin państwa (grupy państw) znajdującego się w zasięgu zainteresowania organów państwowych i wojskowych. Informacje te są niezbędne do planowania obrony narodowej w czasie pokoju oraz kierowania działaniami sił zbrojnych w okresie bezpośredniego zagrożenia oraz w czasie wojny. Powinny być pozyskiwane nieprzerwanie zarówno w czasie pokoju, jak i wojny.

Informacje o przeciwniku o znaczeniu operacyjnym powinny pozyskiwać dowództwa rodzajów sił zbrojnych oraz związków operacyjnych. Są one niezbędne do przygotowania i prowadzenia operacji. Należy pozyskiwać je wydzielonymi siłami i środkami w czasie pokoju oraz w pełnym zakresie w czasie wojny.

Informacje o przeciwniku o znaczeniu taktycznym pozyskiwane są przez dowództwa związków taktycznych, oddziałów i pododdziałów oraz dowódców (szefów) rodzajów wojsk. Mają one charakter informacji studyjnych bojowych dotyczących przeciwnika, terenu i warunków hydrometeorologicznych, niezbędnych do przygotowania i prowadzenia walki. W pełnym wymiarze pozyskuje się je w okresie zagrożenia wojennego i wojny.



Z przedstawionych rozważań jawi się następna kategoria podziału informacji o siłach i środkach przeciwnika. Są to *informacje bojowe i studyjne*³.

Informacje bojowe - to takie, które ze względu na stopień szczegółowości i wiarygodności mogą być bezpośrednio wykorzystywane do rażenia przeciwnika lub wykonania określonego manewru bez potrzeby ich opracowywania i uzupełniania. *Umieszczone w bazach danych powinny być dostępne dla odbiorców bez ograniczeń.*

Informacje studyjne - to takie, które z różnych względów nie mogą być bezpośrednio wykorzystane i wymagają dodatkowych analiz i opracowania przez sztabowe organa rozpoznawcze. Są one z reguły wykorzystywane w ogólnej ocenie sytuacji. Są to z reguły bardzo ważne informacje. *Umieszczenie ich w bazach danych powinno być związane z określeniem stopni ich dostępności dla różnych kategorii odbiorców.* Jednak w zależności od rozwoju sytuacji charakter tych informacji może ulec zmianie.

W procesie pozyskiwania, opracowywania i wykorzystywania informacji istnieje bowiem prawidłowość, iż ta sama informacja dla jednego odbiorcy jest informacją bojową, a dla drugiego studyjną. Informacje bojowe po wykorzystaniu stają się jednocześnie informacjami studyjnymi, a informacje studyjne po odpowiednim opracowaniu mogą się stać bojowymi.

Należy mieć na uwadze, że potrzeby informacyjne na poszczególnych szczeblach dowodzenia różnią się stopniem szczegółowości. Typowe zapotrzebowanie na informacje *związku operacyjnego lub taktycznego* (korpusu lub dywizji) ma zazwyczaj charakter ogólny.

Dowódcy tych szczebli potrzebują informacji studyjnych niezbędnych do podjęcia decyzji - poszukują zatem odpowiedzi na pytania:

- co?
- gdzie?
- kiedy?
- w jaki sposób?

Dlatego też działania rozpoznawcze na tych szczeblach dowodzenia powinny być ukierunkowane przede wszystkim na pozyskiwanie informacji niezbędnych do powzięcia decyzji, a szczególnie do wypracowania wniosków, jak ugrupować swoje siły i gdzie skupić główny wysiłek walki.

Dowódcy *oddziałów* (brygad, pułków) kierują bezpośrednio działaniami bojowymi na polu walki i określają główne cele do niszczenia (zwalczania). Stąd też potrzebują mniej więcej tyle samo informacji studyjnych co i bojowych.

Dowódcy *batalionów* natomiast potrzebują niewiele informacji studyjnych, ale za to dużo informacji bojowych o aktualnych ruchach wojsk i ważniejszych obiektach przeciwnika.

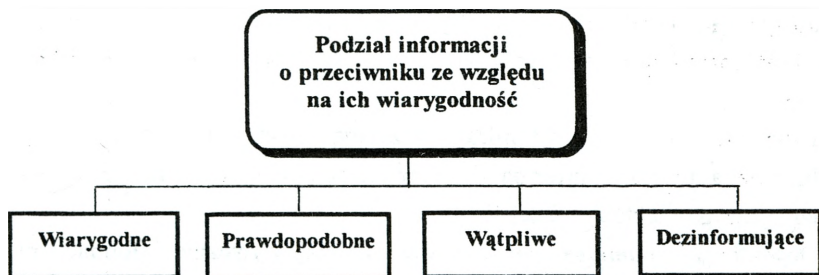
Dowódcy *kompanii* są zainteresowani niemal wyłącznie informacjami bojowymi, które muszą natychmiast wykorzystać, gdyż szybko się one dezaktualizują.

Budując bazy danych o siłach i środkach przeciwnika należy mieć na uwadze, iż przepływ informacji do różnych szczebli dowodzenia, komórek sztabowych, organów rodzajów wojsk i osób funkcyjnych winien być ujęty w sprawnie działający system obiegu informacji, organizowany i koordynowany przez szczebel nadrzędny. Jednostki niższego szczebla potrzebują mniej informacji studyjnych dotyczących oceny sytuacji a więcej informacji bojo-

wych wykorzystywanych do prowadzenia ognia i manewru wojskami, stosownie do szybko zmieniającej się sytuacji na polu walki. Dlatego też w ich działalności bojowej jest więcej meldowania, a mniej analizy. Natomiast związki wyższego szczebla, szczególnie korpus i w mniejszym zakresie - dywizja, opierają się głównie na analizach i ocenach. Zazwyczaj brygady, bataliony i kompanie przekazują informacje bojowe w górę, a otrzymują stamtąd opracowane informacje studyjne o przeciwniku i sytuacji na polu walki.

Pozyskiwane informacje o siłach i środkach przeciwnika mogą charakteryzować się różnymi stopniami **wiarygodności**. Budując bazy danych o siłach i środkach przeciwnika należy mieć na uwadze, że informacje te mogą być:

- wiarygodne,
- prawdopodobne,
- wątpliwe,
- dezinformujące.



Wiarygodne - to informacje z kilku źródeł lub z jednego pewnego źródła, w pełni odpowiadające istniejącej sytuacji bojowej i nie budzące żadnych wątpliwości.

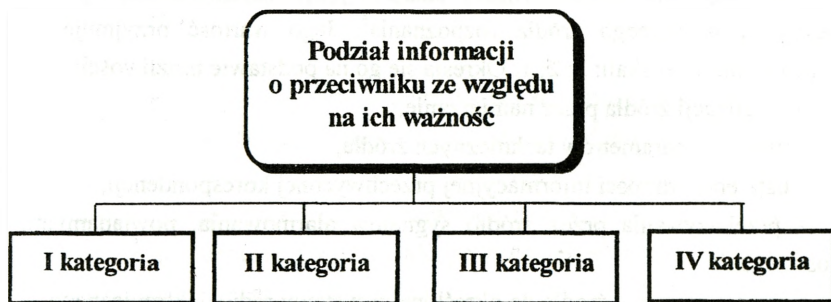
Prawdopodobne - to takie informacje, które odpowiadają aktualnej sytuacji bojowej, są zgodne z posiadanymi już informacjami, lecz wymagają sprawdzenia.

Wątpliwe - to takie informacje, które zaprzeczają poprzednio uzyskanym informacjom z innych źródeł i wymagają sprawdzenia i potwierdzenia.

Dezinformujące - to takie informacje, które nie odpowiadają aktualnej sytuacji bojowej, a ich charakter został udowodniony na podstawie danych z innych źródeł rozpoznania. Mogą być wykorzystane do studiowania metod dezinformacji stosowanych przez przeciwnika.

Zdobyte informacje o siłach i środkach przeciwnika *posiadają różną wartość rozpoznawczą*. Mając na uwadze to kryterium podziału wyszczególnia się cztery kategorie ważności informacji⁴. Kryterium to ma swoje odzwierciedlenie przede wszystkim w rozpoznaniu radioelektronicznym.

W rozpoznaniu radioelektronicznym ważność informacji określa się na podstawie wartości rozpoznawczej ich źródeł. Z kolei wartość rozpoznawczą źródeł rozpoznania ustala się na podstawie znajomości organizacji łączności i systemów radiolokacyjnych przeciwnika oraz danych zdobytych o pracy źródeł w procesie wstępnego ich rozpoznania.



Wartość rozpoznawczą źródeł kształtują dwa współczynniki:

- roli źródła rozpoznania w zabezpieczeniu dowodzenia wojskami i kierowaniu uzbrojeniem,
- informatywności źródła rozpoznania.

Współczynnik roli źródła w zabezpieczeniu dowodzenia wojskami i kierowania uzbrojeniem przyjmuje się w trzystopniowej skali o wartościach: 3; 2; 1.

Wartość „3” stosuje się dla źródeł pracujących w następujących relacjach łączności radiowej lub systemach radiolokacyjnych:

- dowodzenia i kierowania strategicznymi siłami i środkami raketowymi,
- dowodzenia związkami operacyjnymi i taktycznymi,
- powiadamiania i alarmowania wojsk.

Wartość „2” stosuje się dla źródeł pracujących w następujących relacjach łączności radiowych lub systemach radiolokacyjnych:

- dowodzenia i kierowania ogniem artylerii klasycznej,
- tyłowych i zapasowych stanowisk dowodzenia,
- ośrodkach i posterunkach systemu obrony powietrznej,
- współdziałania lotnictwa taktycznego z wojskami lądowymi.

Wartość „1” stosuje się dla pozostałych źródeł rozpoznania.

Współczynnik informatywności charakteryzuje możliwość zdobywania danych z określonego źródła rozpoznania⁵. Jego wartość przyjmuje się w trzystopniowej skali: 3; 2; 1. Określa się go na podstawie możliwości:

- lokalizacji źródła przez namierzanie,
- ustalenia parametrów technicznych źródła,
- ustalenia wartości informacyjnej przechwyconej korespondencji,
- przekazywania przez źródło sygnałów alarmowania, powiadamiania i ostrzegania,
- przywiązywania źródła do określonego systemu radioelektronicznego,
- określenia działalności (zamiaru) obsługiwanego obiektu.

Wartość współczynnika „3” przyjmuje się dla źródeł spełniających co najmniej pięć z wyżej wymienionych czynników, wartość współczynnika „2” - dla źródeł spełniających co najmniej trzy czynniki, a wartość współczynnika „1” - dla źródeł spełniających co najmniej jeden współczynnik.

Na podstawie ww. współczynników można określić wartość rozpoznawczą źródła, która stanowi iloczyn obu współczynników. Tak więc wartość źródła rozpoznania może przyjąć wielkości: 9; 6; 4; 3; 2; 1. Na podstawie tak ustalonych wartości rozpoznawczych źródeł rozpoznania dokonuje się ich podziału na odpowiednie kategorie:

- I kategoria źródła rozpoznania o wartości rozpoznawczej „9”,
- II kategoria źródła o wartości rozpoznawczej „6”,
- III kategoria źródła rozpoznania o wartości „4” i „3”,
- IV kategoria źródła o wartości rozpoznawczej „2” i „1”.

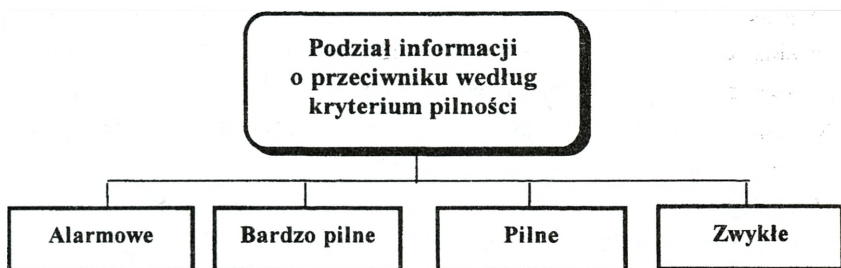
Zatem, budując bazę danych o źródłach radioelektronicznych przeciwnika należy uwzględnić 4 kategorie ich ważności.

Kolejnym kryterium podziału informacji o siłach i środkach przeciwnika w kontekście budowy baz danych jest ich **pilność**. Informacje o siłach i środkach przeciwnika w zależności od stopnia pilności dzieli się na:

- alarmowe,
- bardzo pilne,
- pilne,
- zwykle.

Informacje alarmowe - to dane o siłach i środkach przeciwnika, z których treści wynika, że natychmiast powinny być podjęte odpowiednie działania przez wojska własne. Czas ich dotarcia do odbiorcy - nie dłużej niż 2 minuty od chwili pozyskania przez źródło⁶ - powinien być w dobie obecnej skorygowany przez decydentów. Czas ten nie powinien przekraczać ułamka sekundy i zbliżać się do czasu rzeczywistego.

Informacje bardzo pilne - to dane dotyczące np. rejonów rozmieszczenia wojsk przeciwnika, jego stanowisk dowodzenia (węzłów łączności) oraz innych elementów ugrupowania operacyjnego (bojowego). Czas ich dotarcia do odbiorcy - nie przekraczający 5 minut⁷, powinien również być skorygowany przez decydentów.



Informacje pilne - to dane dotyczące np. zmian w ugrupowaniu przeciwnika, przerzutów wojsk, stanowisk dowodzenia (węzłów łączności) oraz innych elementów ugrupowania operacyjnego (bojowego). Czas ich dotarcia do odbiorcy - nie przekraczający 15 minut⁸, powinien również być zdecydowanie skorygowany przez decydentów.

Informacje zwykłe - to dane dotyczące np. działalności organizacyjno-szkoleniowej i administracyjnej rozpoznawanego przeciwnika. Czas ich przekazania - nie przekraczający 1 godziny⁹, powinien również być skorygowany przez decydentów.

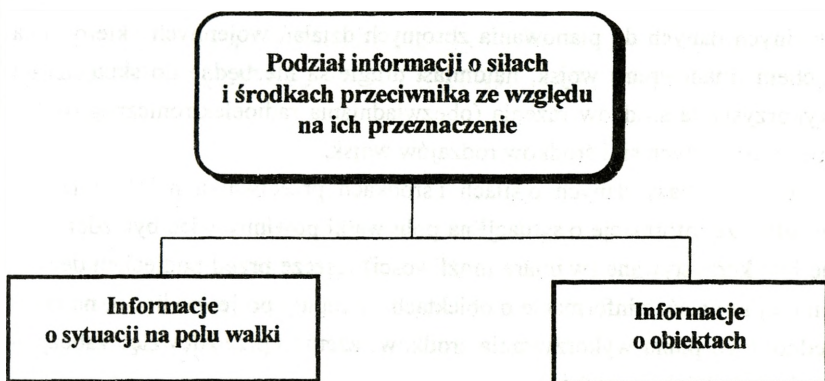
Autor jest zdania, że dowódca odpowiedniego szczebla dowodzenia, stawiając zadania do rozpoznania, każdorazowo powinien określać jakie informacje są dla niego najpilniejsze oraz w jakim czasie powinny docierać one do adresatów.

W zależności od *przeznaczenia* pozyskiwane informacje o siłach i środkach przeciwnika mogą służyć do:

- rozpoznania obiektów,
- rozpoznania sytuacji na polu walki¹⁰.

Informacje o sytuacji na polu walki dostarczają wiarygodnych danych o przeciwniku, terenie i warunkach hydrometeorologicznych, niezbędnych do przygotowania i prowadzenia zbrojnych działań wojennych.

Informacje o obiektach - to informacje bojowe o niezbędnym stopniu szczegółowości, konieczne do skutecznego niszczenia, obezwładniania



(w tym radioelektronicznego) i pokonywania obiektów przeciwnika lub tere-
nu. W wojskach posiadających środki rażenia ogniowego (obezwładniania
radioelektronicznego) są wykorzystywane do „wskazywania celów”,
a w pozostałych wojskach służą do technicznego rozpoznania obiektów.

Informacje o sytuacji na polu walki pozyskują przede wszystkim siły
i środki podległe dowódcom, natomiast informacje o obiektach - dostarczają
siły i środki rozpoznania rodzaju wojsk, zintegrowane z ich systemami
i środkami.

Należy jednak zaznaczyć, że informacje o sytuacji na polu walki oraz in-
formacje o obiektach w toku prowadzenia zbrojnych działań wojennych
nawzajem się uzupełniają. Informacje o obiektach są pozyskiwane na pod-
stawie informacji o sytuacji, natomiast dane z rozpoznania obiektów są wy-
korzystywane w ogólnej ocenie sytuacji.

Poza tym siły i środki przeznaczone do pozyskiwania informacji o sytu-
acji mogą być również wykorzystywane do pozyskiwania informacji o
obektach. W tym wypadku należy jednak liczyć się z faktem, iż korzystając
na dokładności pozyskanych informacji, traci się na ich ilości.

Różnica pomiędzy pozyskanymi informacjami o sytuacji a informacjami
o obiektach jest więc taka, iż pierwsze są pozyskiwane w celu zdobycia nie-

zbędnych danych do planowania zbrojnych działań wojennych i kierowania ruchem (manewrem) wojsk, natomiast drugie są niezbędne do skutecznego wykorzystania środków rażenia (obezwładniania radioelektronicznego) oraz specjalistycznych sił i środków rodzajów wojsk.

Budując bazy danych o siłach i środkach przeciwnika należy mieć na uwadze, że informacje o sytuacji na polu walki powinny więc być zdobywane i wykorzystywane (w miarę możliwości) jeszcze przed podjęciem decyzji i na jej korzyść, a informacje o obiektach - z reguły po jej podjęciu, na rzecz jednolitego planu wykorzystania środków rażenia i przedsięwzięć zabezpieczających działania wojsk¹¹.

Przedstawione kryteria podziału są odzwierciedleniem struktur informacji o siłach i środkach przeciwnika w różnych uwarunkowaniach pola walki. Mogą i powinny być uwzględnione podczas budowy komputerowych baz danych.

PRZYPISY

¹ Termin taki używany jest w Akademii Obrony Narodowej.

² W okresie pokojowym w bazie tej powinny być gromadzone przede wszystkim dane o siłach zbrojnych państw obcych sąsiadujących z RP.

³ Pogląd taki reprezentują pracownicy naukowcy Katedry Rozpoznania Wojskowego i Armii Obcych Akademii Obrony Narodowej.

⁴ *Organizacja i prowadzenie rozpoznania radioelektronicznego*, Podręcznik, Wyd. Szt. Gen. WP, 1979.

⁵ Cechy rozpoznawcze (informacyjne) występujące w pracy poszczególnych środków radioelektronicznych przedstawione są w literaturze specjalistycznej z tej dziedziny [13, 14].

⁶ *Organizacja i prowadzenie rozpoznania radioelektronicznego*, Podręcznik, Wyd. Szt. Gen. WP, 1979.

⁷ Tamże.

⁸ Tamże.

⁹ Tamże.

¹⁰ Podział ten ma istotne znaczenie w procesie planowania rozpoznania.

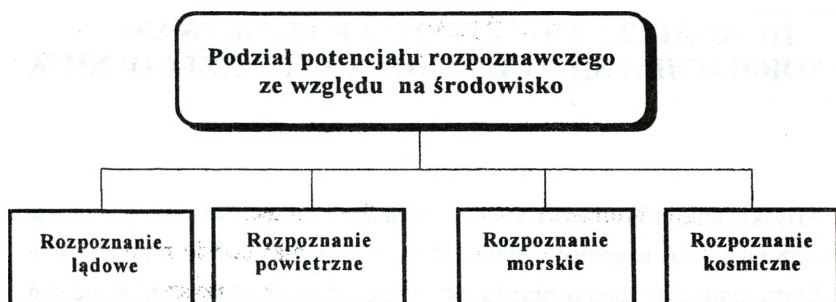
¹¹ W regulaminach NATO przyjmuje się, że rozkaz dla rozpoznania wydaje się jako rozkaz dla pojedynczego wykonawcy. Związane jest to z tym, iż rozkaz ten wydany jest wyprzedzająco w stosunku do przygotowania działań bojowych.

III. ANALIZA MOŻLIWOŚCI POZYSKIWANIA INFORMACJI O SIŁACH I ŚRODKACH PRZECIWNIKA

Pozyskiwanie informacji o siłach i środkach przeciwnika determinowane jest dążeniami do osiągnięcia stanu, który pozwalał będzie na dostarczanie użytkownikom dokładnego obrazu aktualnego stanu i przyszłych zachowań przeciwnika w czasie rzeczywistym lub maksymalnie zbliżonym do rzeczywistego. Osiągnięcie tego widziane jest przez pryzmat konstrukcji urządzeń dostosowanych technologicznie do automatycznego, ciągłego, wielofunkcyjnego¹ i wielospektralnego² postrzegania materii, energii, informacji i przestrzeni pola walki w sposób niedostrzegalny dla przeciwnika. Zdobyte tą drogą informacje o siłach i środkach przeciwnika noszą nazwę *działań rozpoznawczych*, które prowadzone są przez etatowe, odpowiednio wyszkolone i wyposażone wojska rozpoznawcze, a także wydzielane doraźnie siły i środki z pododdziałów ogólnowojskowych oraz innych rodzajów wojsk. Etatowe oraz doraźnie wydzielane siły i środki wojsk lądowych; wojsk lotniczych i obrony powietrznej (sił powietrznych) oraz marynarki wojennej tworzą zbiór nazywany *potencjałem rozpoznawczym*, który prowadzi swoją działalność w określonym środowisku. W zależności *od charakteru środowiska* w jakim jest prowadzone rozpoznanie oraz użytych do tego celu sił i środków wyróżnia się rozpoznanie:

- naziemne,
- powietrzne,
- morskie,
- kosmiczne.

Budując bazy danych o siłach i środkach przeciwnika należy mieć na uwadze, że najbardziej rozwinięte jest w Siłach Zbrojnych RP rozpoznanie lądowe oraz powietrzne, które wzajemnie się uzupełniają. W mniejszym stop-



niu rozwinięte jest rozpoznanie morskie, natomiast rozpoznanie kosmiczne dotychczas nie jest prowadzone.

Ze względu na *cechy wyróżnialności (kryteria rozstrzygalności)* odzwierciedlające, możliwe dziś i w perspektywie, sposoby walki o pozyskiwanie informacji o przeciwniku, potencjał ten powinien obejmować następujące rodzaje rozpoznania:

- rozpoznanie bezpośrednie³,
- rozpoznanie elektroniczne,
- rozpoznanie studyjne⁴.

Rozpoznanie bezpośrednie ma na celu zdobywanie oraz przetwarzanie tych informacji o przeciwniku, które znajdują się w zasięgu bezpośrednich możliwości recepcyjnych człowieka wspomaganych podręcznymi środkami technicznymi, np.: lornetką, aparatem podsłuchowym, kamerą, aparatem fotograficznym, magnetofonem itp.

Rozpoznanie bezpośrednie dzieli się na rozpoznanie: *agenturalne, specjalne i patrolowe*.

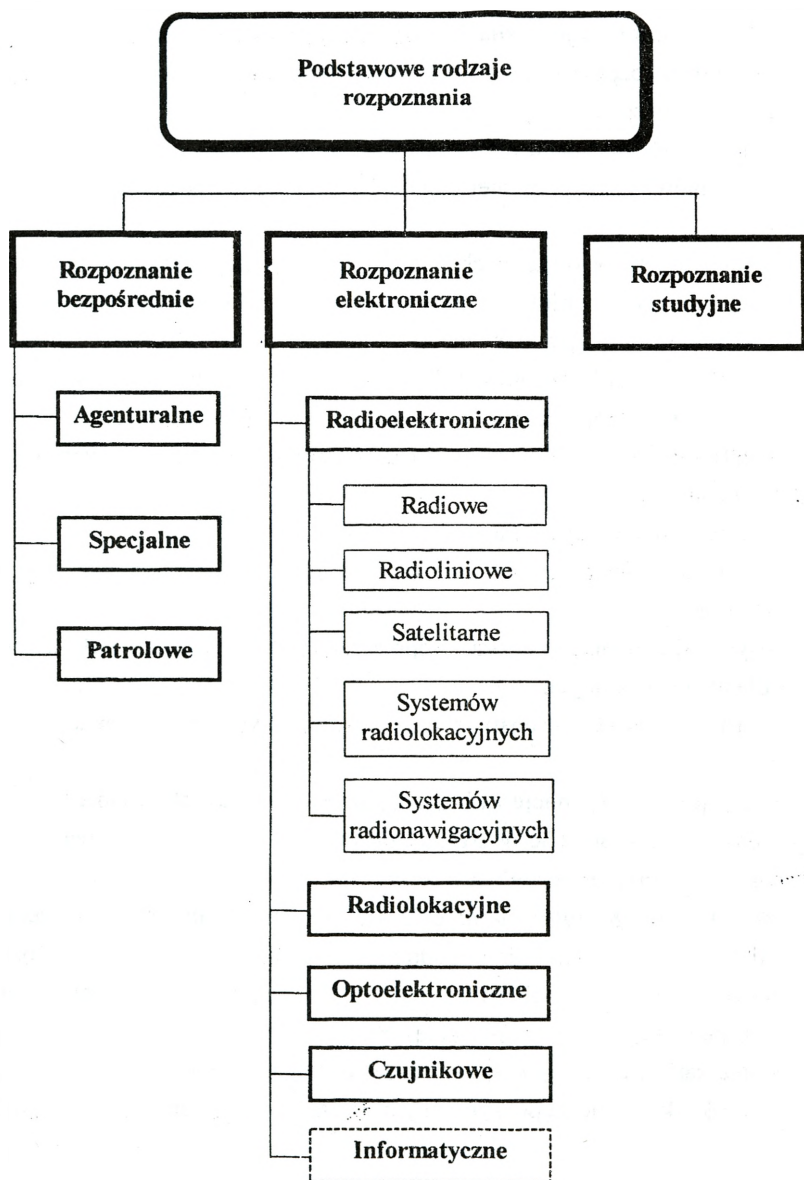
Rozpoznanie agenturalne jest przystosowane do zdobywania i przetwarzania informacji o przeciwniku drogą ściśle zakonspirowanych działań wywiadowczych (wywiad nielegalny) oraz legalnych działań wywiadowczych prowadzonych przez odpowiednie przedstawicielstwa dyplomatyczne. W okresie pokoju jest ono prowadzone na szczeblu strategicznym, a podczas wojny również na szczeblu operacyjnym. Pozyskiwane przez rozpoznanie

agenturalne informacje o siłach i środkach przeciwnika posiadają bardzo dużą wartość rozpoznawczą. Są to z reguły informacje o znaczeniu strategicznym i dotyczą m.in.:

- możliwości wybuchu wojny i jej charakteru,
- terminów osiągnięcia pełnej gotowości bojowej wojsk przeciwnika (agresora),
- dokładnych współrzędnych rejonów rozmieszczenia wojsk przeciwnika oraz jego środków ogniowych (stanowisk startowych rakiet operacyjno-taktycznych, lotnisk, magazynów amunicji, itp.),
- funkcjonowania systemów dowodzenia (od dywizji wzwyż), węzłów łączności oraz zabezpieczenia bojowego i logistycznego działań,
- przedsięwzięć mobilizacyjnych oraz przerzutu wojsk z innych terytoriów (regionów),
- stanu lotnictwa taktycznego,
- rozbudowy infrastruktury oraz nowych obiektów operacyjnego przeznaczenia terenu,
- sytuacji ekonomicznej oraz stopnia zaangażowania gospodarki narodowej dla celów wojennych,
- nastrojów w społeczeństwie oraz poziomu dyscypliny w siłach zbrojnych.

Uznając ww. informacje za bardzo ważne autor nie jest w stanie na obecnym etapie badań określić *w jaki sposób i w jakim charakterze powinny one docierać do komputerowych baz danych.*

Rozpoznanie specjalne ma na celu prowadzenie działań rozpoznawczych siłami niewielkich grup lub pododdziałów na terenie zajmowanym przez przeciwnika i w ten sposób zdobywania o nim informacji. Elementy rozpoznania specjalnego (grupy specjalne, grupy specjalne pływonurków, grupy specjalne kadrowe, grupy rozpoznawcze) działają zwykle na tych obszarach przeciwnika, które nie są pokryte innymi rodzajami rozpoznania, lub są po-

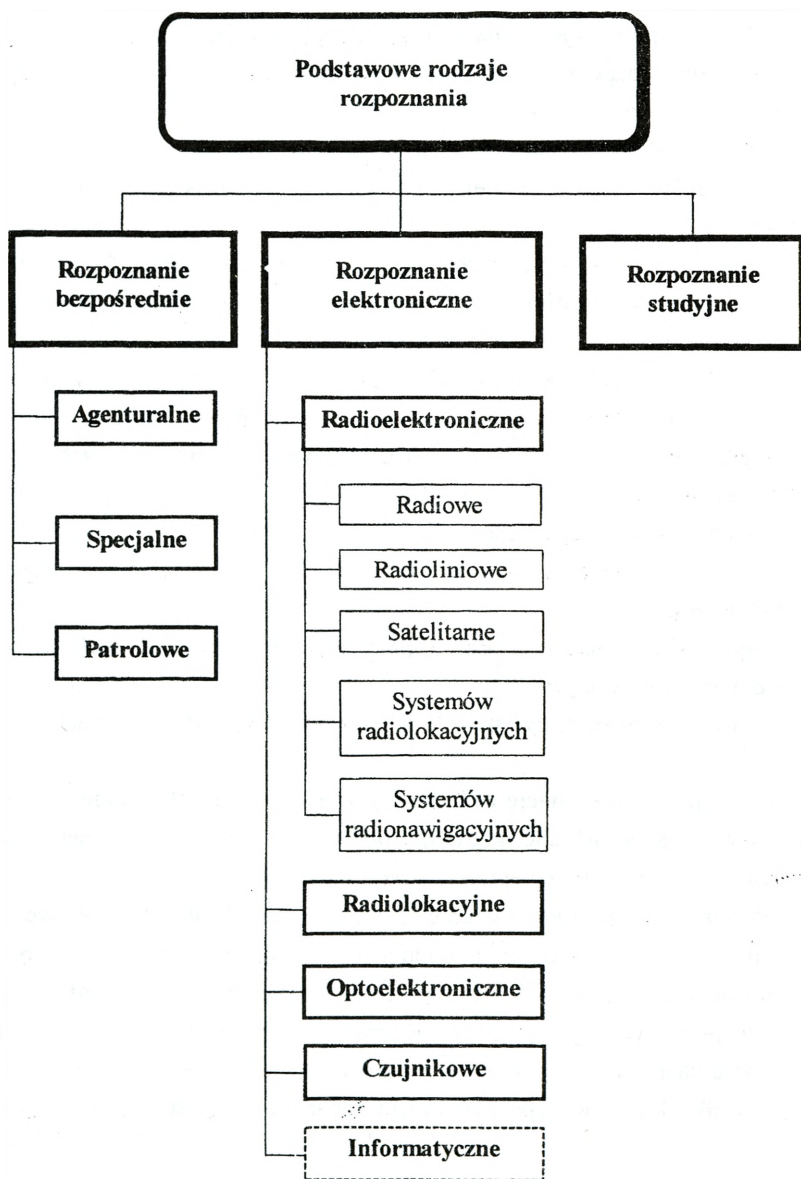


kryte, ale w taki sposób, że wiarygodność zdobywanych informacji o przeciwniku jest za mała aby skutecznie kierować wojskami i środkami rażenia. Doświadczenia wojen lokalnych wykazują na wzrost znaczenia tego rodzaju rozpoznania. Głębokość usytuowania obszarów rozpoznania specjalnego może być różna, ale zawsze warunkowana jest możliwościami przerzutu (przenikania) i przetrwania elementów ugrupowania rozpoznawczego.

Siły i środki rozpoznania specjalnego mogą pozyskiwać bądź potwierdzać informacje zdobyte przy pomocy innych źródeł, bez względu na warunki (pogodę, porę roku, doby, itp.) i stopień zamaskowania obiektów. Są one w stanie określić rodzaj, charakter, stan i gotowość bojową przeciwnika, a nade wszystko określić dokładne współrzędne wykrywanych obiektów.

W konkretnej sytuacji pola walki, pozyskiwane przez rozpoznanie specjalne informacje o siłach i środkach przeciwnika powinny dotyczyć:

- ważnych środków ogniowych przeciwnika, ich systemów kierowania, składów i punktów amunicji specjalnej oraz symptomów świadczących o przygotowaniu do ich użycia,
- składu i rozmieszczenia systemów dowodzenia i węzłów łączności,
- rozmieszczenia środków rozpoznania radioelektronicznego, powiadamiania i naprowadzania,
- urządzeń i obiektów obrony przeciwlotniczej i przeciwrakietowej,
- rejonów ześrodkowania wojsk oraz kierunków ich przegrupowania,
- rozmieszczenia lotnisk, lądowisk, portów, baz morskich, obiektów obrony wybrzeża oraz urządzeń zabezpieczających ich funkcjonowanie,
- danych o obiektach komunikacyjnych oraz systemach logistycznego zabezpieczenia wojsk,
- danych o systemach zapór inżynierskich, szerokich przeszkodach wodnych, stanie urządzeń hydrotechnicznych itp.,
- form i zasad oddziaływania propagandowego i psychologicznego w stosunku do wojsk i ludności cywilnej.



kryte, ale w taki sposób, że wiarygodność zdobywanych informacji o przeciwniku jest za mała aby skutecznie kierować wojskami i środkami rażenia. Doświadczenia wojen lokalnych wykazują na wzrost znaczenia tego rodzaju rozpoznania. Głębokość usytuowania obszarów rozpoznania specjalnego może być różna, ale zawsze warunkowana jest możliwościami przerzutu (przenikania) i przetrwania elementów ugrupowania rozpoznawczego.

Siły i środki rozpoznania specjalnego mogą pozyskiwać bądź potwierdzać informacje zdobyte przy pomocy innych źródeł, bez względu na warunki (pogodę, porę roku, doby, itp.) i stopień zamaskowania obiektów. Są one w stanie określić rodzaj, charakter, stan i gotowość bojową przeciwnika, a nade wszystko określić dokładne współrzędne wykrywanych obiektów.

W konkretnej sytuacji pola walki, pozyskiwane przez rozpoznanie specjalne informacje o siłach i środkach przeciwnika powinny dotyczyć:

- ważnych środków ogniowych przeciwnika, ich systemów kierowania, składów i punktów amunicji specjalnej oraz symptomów świadczących o przygotowaniu do ich użycia,
- składu i rozmieszczenia systemów dowodzenia i węzłów łączności,
- rozmieszczenia środków rozpoznania radioelektronicznego, powiadamiania i naprowadzania,
- urządzeń i obiektów obrony przeciwlotniczej i przeciwrakietowej,
- rejonów ześrodkowania wojsk oraz kierunków ich przegrupowania,
- rozmieszczenia lotnisk, lądowisk, portów, baz morskich, obiektów obrony wybrzeża oraz urządzeń zabezpieczających ich funkcjonowanie,
- danych o obiektach komunikacyjnych oraz systemach logistycznego zabezpieczenia wojsk,
- danych o systemach zapór inżynieryjnych, szerokich przeszkodach wodnych, stanie urządzeń hydrotechnicznych itp.,
- form i zasad oddziaływania propagandowego i psychologicznego w stosunku do wojsk i ludności cywilnej.

W szczególnych sytuacjach siły rozpoznania specjalnego mogą być wykorzystywane do wykonywania zadań: dywersyjnych, sabotażowych, psychologiczno-propagandowych, terrorystycznych i szturmowych, a na własnym terytorium - zadań antyterrorystycznych i przeciwdywersyjnych.

Ranga i znaczenie informacji pozyskiwanych przez rozpoznanie specjalne wymaga szczególnych zabiegów (stosowanie urządzeń utajnających z gwarantowaną mocą kryptograficzną) w toku ich przekazywania do organów nadrzędnych oraz do odpowiednich baz danych.

Rozpoznanie patrolowe ma na celu zdobywanie informacji o przeciwniku drogą fizycznej (optycznej i akustycznej) penetracji terenu (obszaru) zajmowanego przez przeciwnika. Rozpoznanie patrolowe prowadzą nie tylko etatowe siły i środki, ale i inne rodzaje wojsk, stosownie do potrzeb oraz posiadanych możliwości. Do elementów ugrupowania patrolowego i elementów patrolowych zalicza się: patrol rozpoznawczy, wóz patrolowy, posterunek obserwacyjny (różnego rodzaju), samolot. Prowadzone jest przede wszystkim na szczeblu taktycznym.

Dostarcza bieżącej informacji rozpoznawczej o siłach i środkach przeciwnika wykonujących zadania bojowe w określonych rejonach. *Informacje te powinny docierać do baz danych w jak najkrótszym czasie (zbliżonym do rzeczywistego), celem ich uaktualnienia.*

Rozpoznanie elektroniczne to kolejny rodzaj rozpoznania wojskowego. Ma na celu zdobywanie i przetwarzanie tych informacji o przeciwniku, których nośnikami są fale elektromagnetyczne oraz inne efekty uboczne towarzyszące działaniom bojowym. Postęp naukowo-techniczny pozwolił już na konstruowanie wielu takich urządzeń. Między innymi opracowano całą rodzinę urządzeń pozwalających na postrzeganie pola walki poprzez widmo promieniowania elektromagnetycznego, fale sprężyste (akustyczne i sejsmiczne) oraz przez pole magnetyczne i skład chemiczny środowiska. Rejestracja nośników informacji o przeciwniku odbywa się za pomocą odpowiednio skonstruowanych urządzeń elektronicznych.

Rozpoznanie elektroniczne prowadzi się we wszystkich warunkach atmosferycznych, czasowych oraz usytuowania i nie powoduje to istotnego źródnicowania wartości uzyskiwanych efektów (wyników rozpoznania). Jest to najszybszy, najtańszy, najbardziej manewrowy i skryty oraz najbezpieczniejszy rodzaj rozpoznania wojskowego. Do mankamentów zalicza się natomiast wrażliwość na zakłócenia i dezinformację.

Rozpoznanie elektroniczne dzieli się na:

- rozpoznanie radioelektroniczne,
- rozpoznanie radiolokacyjne,
- rozpoznanie optoelektroniczne,
- rozpoznanie czujnikowe,
- rozpoznanie informatyczne.

Rozpoznanie radioelektroniczne ma na celu zdobywanie i przetwarzanie tych informacji o przeciwniku, których nośnikami są fale elektromagnetyczne (wraz z informacją w nich zawartą) wypromieniowane przez źródła przeciwnika. W widmie promieniowania elektromagnetycznego szczególnie wykorzystywana jest druga połowa pasma niższych częstotliwości - od nadfioletu aż do dolnej granicy promieniowania radiowego. Do pracy w paśmie promieniowania radiowego⁵ skonstruowano różnego rodzaju urządzenia radiowe⁶, radioliniowe⁷ radionawigacyjne⁸, radiolokacyjne⁹ i sonarowe¹⁰.

Według dotychczas obowiązujących poglądów w Siłach Zbrojnych RP rozpoznanie radioelektroniczne dzieli się na rozpoznanie: *radiowe, radioliniowe, satelitarne, systemów radiolokacyjnych i systemów radionawigacyjnych*. Należy mieć na uwadze, że współczesne środki rozpoznania radioelektronicznego przystosowane są zarówno do odbioru fal elektromagnetycznych emitowanych przez te źródła jak i do prowadzenia analizy technicznej. Wartość rozpoznawczą poszczególnych źródeł określa się na podstawie określonych w procesie rozpoznania radioelektronicznego ich cech rozpoznawczych (informacyjnych). Klasyfikacja i podział cech informacyjnych w pracy środków radioelektronicznych przedstawiona jest obszernie w literaturze facho-

wej, dotyczącej rozpoznania radioelektronicznego¹¹. *Budując bazy danych o siłach i środkach przeciwnika należy mieć na uwadze, że informacje pozyskiwane przez rozpoznanie radioelektroniczne są dwójakiego rodzaju.*

Pierwszy rodzaj obejmuje wiadomości dotyczące *rozwoju sytuacji radioelektronicznej* o siłach zbrojnych przeciwnika pozyskiwanych na podstawie analizy charakterystyk częstotliwościowych i czasowych sygnałów radiowych, radiolokacyjnych oraz radionawigacyjnych, według których możliwe jest określenie:

- typów środków radioelektronicznych oraz ich identyfikację,
- składu i charakteru funkcjonowania systemów radioelektronicznych, a w ślad za tym systemów dowodzenia, systemów wykrywania i naprowadzania a także pokładowych systemów radiolokacyjnych przeznaczonych do obserwacji pola walki i kierowania uzbrojeniem.

Drugi rodzaj obejmuje informacje związane z *rozwojem sytuacji wojskowo-politycznej*. Z uwagi na fakt, że środki rozpoznania radioelektronicznego same nie promieniują energii elektromagnetycznej (z tego względu określa się je jako grupę rozpoznawczych środków pasywnych, zachowujących bardzo dużą skrytość działania) możliwe jest prowadzenie rozpoznania radioelektronicznego zarówno w okresie pokoju jak i wojny.

W okresie pokoju rozpoznanie radioelektroniczne powinno dostarczać - na podstawie analizy pracy środków radioelektronicznych przeciwnika - informacji dotyczących:

- symptomów świadczących o podwyższaniu stanów gotowości bojowej wojsk, uruchamianiu systemów mobilizacyjnego oraz operacyjnego rozwijania jego sił zbrojnych,
- nowych oraz potwierdzenia istniejących rejonów rozmieszczenia ważnych środków ogniowych,
- przegrupowujących się wojsk, a zwłaszcza sztabów i jednostek rakietowych,
- działalności szkoleniowej wojsk na podstawie ćwiczeń oraz manewrów,

- systemów dowodzenia i łączności,
- działalności rozpoznawczej przeciwnika.

W okresie bezpośredniego zagrożenia oraz w początkowym okresie wojny pozyskiwanie informacji o siłach i środkach przeciwnika powinno być ukierunkowane na wykrywanie i ustalenie:

- rejonów rozmieszczenia środków ogniowych, stanowisk dowodzenia oraz punktów kierowania środkami walki,
- ewentualnych symptomów świadczących o przygotowaniach przeciwnika do użycia broni jądrowej,
- rejonów ześrodkowania wojsk oraz kierunków ich przegrupowania,
- nowych środków radioelektronicznych przeciwnika oraz sposobów ich wykorzystania w systemach dowodzenia i kierowania środkami walki,
- aktualnego stanu wojsk przeciwnika oraz jego zamiarów.

Rozpoznanie radiolokacyjne¹² - będące w swej istocie elementem rozpoznania elektronicznego - ma na celu zdobywanie oraz przetwarzanie tych informacji o przeciwniku, których nośnikami są fale elektromagnetyczne wypromieniowane przez własne urządzenia rozpoznawcze (stacje radiolokacyjne) i odbite od obiektów przeciwnika. Współczesne rozpoznanie radiolokacyjne obejmuje: systemy rozpoznania obszaru powietrznego, systemy nadzorowania pola walki, systemy kierowania ogniem, systemy obrony przeciwlotniczej, systemy rozpoznania powierzchni ziemi SLAR i in. Prowadzone jest przez samoloty rozpoznawcze wyposażone w stacje radiolokacyjne obserwacji bocznej oraz naziemne, brzegowe okrętowe stacje radiolokacyjne w różnych zakresach częstotliwości.

Informacje pozyskiwane przez te urządzenia w kontekście budowy baz danych powinny dotyczyć:

- radiolokacyjnych obrazów odpowiednich sektorów przestrzeni powietrznej, terenu (lądu) oraz akwenów morskich,
- tras przelotu samolotów oraz miejsc rozmieszczenia celów ruchomych (czołgów, transporterów opancerzonych, samochodów, pododdziałów oraz

pojedynczych żołnierzy w warunkach braku widoczności (noc, mgła, opady atmosferyczne, zadymienie, kurz) itp.,

- współrzędnych tych celów.

Rozpoznanie optoelektroniczne - jako nowy rodzaj rozpoznania elektronicznego - ma na celu zdobywanie oraz przetwarzanie tych informacji o przeciwniku, których nośnikami są fale elektromagnetyczne pasma optycznego¹³. Do pracy w tym paśmie skonstruowano całą rodzinę urządzeń optoelektronicznych¹⁴ pozwalających na prowadzenie rozpoznania w ultrafiolecie, w zakresie promieniowania widzialnego oraz w zakresie bliskiej, średniej, dalekiej i skrajnej podczerwieni. Należą do nich m.in. urządzenia: telewizyjne¹⁵, termowizyjne¹⁶, noktowizyjne¹⁷, laserowe¹⁸.

Budując komputerowe bazy danych o siłach i środkach przeciwnika należy mieć na uwadze, że informacje pozyskiwane w wyniku rozpoznania optoelektronicznego mają charakter obrazowy. Mogą zatem być szeroko wykorzystywane do monitorowania pola walki, a w tym funkcjonowania sił i środków przeciwnika.

Rozpoznanie czujnikowe - również jako nowy rodzaj rozpoznania elektronicznego - ma na celu zdobywanie oraz przetwarzanie informacji o przeciwniku, których nośnikami są fale sprężyste, tj. zakresu promieniowania innego niż radiowe (np. infradźwięki¹⁹, ultradźwięki²⁰) oraz wszelkiego rodzaju uboczne efekty towarzyszące działaniom bojowym, na przykład: akustyczne, termiczne, sejsmiczne, naciskowe, magnetyczne, chemiczne, zapachu itp. Do postrzegania materii pola walki, przez pryzmat fal sprężystych oraz w zakresie efektów magnetycznych i chemicznych środowiska, skonstruowano całą rodzinę urządzeń czujnikowych z szerokim zastosowaniem elektronicznej przemiany rejestrowanych efektów. Pozyskiwane informacje o siłach i środkach przeciwnika w wyniku prowadzonego rozpoznania czujnikowego powinny dotyczyć:

- nadzorowania aktywności przeciwnika w wybranych rejonach, w których rozmieszczone zostały odpowiednie czujniki,

- nadzorowania natężenia ruchu i poziomu aktywności przeciwnika wzdłuż wybranych tras,

- nadzorowania aktywności przeciwnika w rejonach rozmieszczenia własnych zapór i pól minowych,

- nadzorowania aktywności przeciwnika w rejonach przepraw rzecznych, mostów i brodów,

- nadzorowania rejonów zaplanowanych do jako strefy lądowania lub zrzutu własnych wojsk desantowoszturmowych,

- rejestracji zmian w funkcjonowaniu wybranych elementów ugrupowania przeciwnika, ich stanowisk dowodzenia, punktów zaopatrywania, itp.,

- wskazywania celów do szczegółowego rozpoznania.

Rozpoznanie czujnikowe jest perspektywicznym rodzajem rozpoznania na szczeblach taktycznych. Umożliwia bowiem pozyskiwanie informacji rozpoznawczych z najbardziej niedostępnych stref²¹ w czasie zbliżonym do rzeczywistego.

Rozpoznanie informatyczne²² jako również perspektywiczny rodzaj rozpoznania elektronicznego - powinno być prowadzone z uwagi na masowy rozwój sieci informatycznych o zasięgu globalnym oraz lokalnym. Sieci informatyczne są bogatymi źródłami informacji o siłach i środkach przeciwnika. Pozyskiwanie tych informacji jest stosunkowo łatwe. Poza tym nie wymaga się ani skomplikowanych urządzeń ani też specjalistycznego przygotowania załóg. Przykładem w tym zakresie mogą być międzynarodowi piraci komputerowi (ang. *hackers*), którzy bez większych przeszkód włamują się do odpowiednio zabezpieczonych systemów komputerowych m in. Pentagonu. Nie trzeba zatem „być wielkim i bogatym” aby skutecznie prowadzić rozpoznanie informatyczne. *Przebogate i niezmiernie wartościowe informacje dla rozpoznania ulokowane są również w promieniowaniu komputerowym.* Te nowe stosunkowo źródła są jeszcze mało dostępne dla organów rozpoznawczych naszych sił zbrojnych. Należy jednak uczynić wszystko aby barierę tę jak najszybciej pokonać od strony technologicznej i organizacyjnej.

Budując zatem bazy danych o siłach i środkach przeciwnika należy obowiązkowo uwzględnić możliwość pozyskiwania różnorodnej informacji, szczególnie w okresie pokoju przez rozpoznanie informatyczne.

Rozpoznanie studyjne - będące ważnym rodzajem rozpoznania wojskowego - ma na celu gromadzenie, analizowanie i przetwarzanie wszelkich informacji rozpoznawczych pozyskanych przez inne rodzaje rozpoznania wojskowego (najczęściej fragmentarycznych) i na tej podstawie opracowywanie (wytworzenie) informacji nowych o znacznie większej wartości użytkowej. Rozpoznanie studyjne prowadzi się głównie w dowództwach i komórkach rozpoznawczych. Niezależnie od uwarunkowań sytuacyjno-czasowych ma ono charakter ciągły. Typowym efektem (wynikiem) studyjnej działalności rozpoznawczej jest ocena przeciwnika (przewidywane warianty działań przeciwnika) przedstawiana dowódcy w procesie wypracowywania decyzji. W wyniku rozpoznania studyjnego powstają wszelkiego rodzaju opracowania, komunikaty, meldunki, wnioski, zestawienia, wykresy itp., zawierające określone zbiory odpowiednio opracowanych informacji rozpoznawczych. Informacja studyjna o siłach i środkach przeciwnika powinna być wprowadzana do baz danych *również w postaci wzorców doktrynalnych*²³.

Uzupełnieniem rozpoznania typu ogólnego jest **rozpoznanie rodzaju wojsk**. Poszczególne rodzaje wojsk, wchodzące w skład ogólnowojskowych związków operacyjnych (taktycznych) mają możliwość - wykorzystując swoje specjalistyczne etatowe i nieetatowe siły i środki rozpoznania - pozyskiwania informacji o siłach i środkach przeciwnika, które do tej pory były z reguły wykorzystywane na ich korzyść. Do rozpoznania rodzaju wojsk zalicza się:

- rozpoznanie artyleryjskie,
- rozpoznanie skażeń,
- rozpoznanie inżynieryjne,
- rozpoznanie przeciwlotnicze.

Rozpoznanie artyleryjskie ma na celu wykrycie i określenie położenia z wymaganą dokładnością obiektów (celów) niezbędnych do planowania i wykonywania własnych uderzeń ogniowych, a także do korygowania startu rakiet i ognia artylerii. Prowadzone jest przy pomocy środków rozpoznania wzrokowego, dźwiękowego, radiolokacyjnego oraz optoelektronicznego. Pozyskiwane przez nie informacje powinny dotyczyć:

- wykrywania i określenia współrzędnych stanowisk startowych (ogniowych) środków napadu jądrowego, pododdziałów artylerii, moździerzy oraz innych środków ogniowych przeciwnika,
- wykrywania i określania położenia punktów dowodzenia, punktów oporu, ustalenia charakteru i systemu pozycji (rubieży) urządzeń obronnych przeciwnika oraz umocnień i przeszkód,
- rozpoznania bezpośredniego obiektów (celów) przeciwnika na rzecz wykonania własnych uderzeń ogniowych,
- rozpoznania odwodów przeciwnika, dróg ich marszu oraz rubieży rozwinięcia,
- obserwacji pola walki.

Rozpoznanie inżynierskie ma na celu zdobywanie niezbędnych informacji o terenie, obiektach obronnych przeciwnika oraz jego uzbrojeniu inżynierskim. Pozyskiwane przez nie informacje powinny dotyczyć:

- składu, wyposażenia i możliwości wojsk inżynierskich przeciwnika,
- wpływu warunków terenowych na działanie przeciwnika,
- rodzaju i typu urządzeń inżynierskich, systemów zapór inżynierskich,
- stanu technicznego dróg, mostów, wiaduktów i innych obiektów komunikacyjnych oraz warunków ich eksploatacji,
- możliwości pokonania lub obejścia rejonów trudno dostępnych przez przeciwnika,
- charakteru przeszkód wodnych oraz możliwości ich pokonania przez przeciwnika.

Rozpoznanie przeciwlotnicze ma na celu wykrycie w odpowiednim czasie działania środków napadu powietrznego przeciwnika oraz dostarczenie niezbędnych danych do ich zwalczania. Pozyskiwane przez nie informacje powinny dotyczyć:

- składu, wyposażenia i możliwości wojsk napadu powietrznego przeciwnika,
- taktyki działania sił napadu powietrznego,
- systemów naprowadzania sił napadu powietrznego,
- kierunków zagrożeń środków napadu powietrznego przeciwnika,
- rejonów oraz rubieży rozmieszczenia sił i środków napadu powietrznego przeciwnika.

Rozpoznanie skażeń ma na celu pozyskiwanie i dostarczanie w odpowiednim czasie informacji o miejscach i stopniu skażenia terenu, wody i powietrza. Pozyskiwane przez nie informacje powinny dotyczyć:

- składu, wyposażenia oraz możliwości wojsk chemicznych przeciwnika,
- stopnia przygotowania oraz czasu wykonania uderzeń bronią masowego rażenia oraz prawdopodobnych zagrożeń,
- prognoz meteorologicznych w związku z możliwością użycia broni masowego rażenia,
- rodzajów zapór chemicznych oraz rejonów ich rozmieszczenia,
- stref skażeń oraz możliwości ich pokonania lub obejścia.

Analiza możliwości pozyskiwania informacji o siłach i środkach przeciwnika przez autonomiczne siły i środki rodzajów wojsk pozwala postawić tezę, że informacje te stanowią istotne uzupełnienie rozpoznania studyjnego prowadzonego przez organa rozpoznawcze dowództw. Oznacza to, że informacje pochodzące od autonomicznych środków rozpoznania rodzajów wojsk powinny być bezwzględnie wykorzystywane w zintegrowanym rozpoznaniu studyjnym. Powinny mieć odzwierciedlenie w odpowiednich zbiorach bazy danych o siłach i środkach przeciwnika.

Rozpoznanie powietrzne jest podstawowym rodzajem rozpoznania szczebla operacyjnego. Prowadzone jest również na szczeblu taktycznym. Ma na celu zdobywanie informacji o przeciwniku, terenie (w tym akwenów morskich) i pogodzie, realizowanych za pomocą techniki zamontowanej na różnych aparatach latających. *Współczesne lotnictwo rozpoznawcze powinno posiadać duże możliwości w zakresie szybkiego przenikania w głąb terytorium przeciwnika, prowadzenia rozpoznania dużych rejonów w stosunkowo krótkim czasie, określania współrzędnych wykrytych obiektów oraz natychmiastowego przekazywania danych bezpośrednio z pokładów samolotów do odpowiednich baz danych wojsk oraz ich organów dowodzenia.* Rozpoznanie powietrzne wykonuje swoje zadania zarówno w okresie pokoju jak i wojny.

W okresie pokoju prowadzone jest z nad własnego terytorium, z nad własnych wód przybrzeżnych oraz w obszarach wód neutralnych. Pozyskiwane tą drogą informacje powinny dotyczyć:

- systemów radiolokacyjnych sił powietrznych przeciwnika oraz obrony powietrznej potencjalnego przeciwnika,
- zmian w wykorzystywanej przez potencjalnego przeciwnika sieci lotniczej,
- przebiegu ćwiczeń sił powietrznych i morskich potencjalnego przeciwnika,
- identyfikacji okrętów i statków oraz rozpoznawanych baz i portów morskich,
- działalności okrętów potencjalnego przeciwnika na własnych wodach przybrzeżnych oraz obszarach wód neutralnych,
- wykorzystania powietrznych sił i środków rozpoznawczych przeciwnika oraz sposobów ich działania.

W okresie bezpośredniego zagrożenia oraz wojny intensywność rozpoznania powietrznego powinna wzrosnąć. Pozyskiwane przez nie informacje powinny dotyczyć:

- rejonów mobilizacji i ześrodkowania głównych zgrupowań wojsk i odwodów oraz kierunków ich przegrupowania i operacyjnego rozwijania,
- potwierdzenia stanu i rejonów bazowania lotnictwa taktycznego,
- wykrywania oraz kontroli systemów dowodzenia i OPL przeciwnika oraz zachodzących w nich zmian,
- rozpoznania infrastruktury przeciwnika, a zwłaszcza w zakresie możliwości pokonywania przez niego przeszkód wodnych, zapór inżynieryjnych, portów morskich itp.,
- wykrywania składów i baz materiałowo-technicznego zabezpieczenia, ze szczególnym uwzględnieniem punktów zaopatrywania w amunicję specjalną,
- rozpoznania rejonów w których planuje się wysadzenie własnych desantów powietrznych (morskich).

Rozpoznanie morskie ma na celu zdobywanie informacji o siłach morskich i powietrznych przeciwnika oraz warunkach hydrometeorologicznych, realizowanym za pomocą nawodnych i podwodnych jednostek pływających oraz urządzeń brzegowych. Charakter i możliwości pozyskiwanych przez nie informacji - w kontekście budowy komputerowych baz danych - są zbliżone do tych, które pozyskuje rozpoznanie powietrzne.

Rozpoznanie kosmiczne ma w celu zdobywanie informacji o przeciwniku, warunkach terenowych i meteorologicznych, za pomocą urządzeń rozpoznawczych zainstalowanych na sztucznych satelitach ziemi i aparatach operujących w przestrzeni kosmicznej. Obecnie ten rodzaj rozpoznania nie jest wykorzystywany w Siłach Zbrojnych RP.

Potrzeba pozyskiwania precyzyjnych, wiarygodnych oraz aktualnych informacji o siłach i środkach przeciwnika stała się głównym stymulatorem postępu w dziedzinie rozwoju różnorodnych **systemów rozpoznania wojskowego**. Analiza współczesnych systemów rozpoznania wojskowego najbogatszych państw świata pozwala sformułować następujące wnioski i uogólnienia:

1. System rozpoznania (pozyskiwania) informacji powinien terminowo zasilać procesy analityczne, decyzyjne i kontrolne (ocenowe) wszechstronnymi informacjami źródłowymi o sytuacji na polu walki - położeniu, działalności bojowej przeciwnika, stanie jego sił i środków, a także o terenie oraz warunkach atmosferycznych.

2. Współczesny system rozpoznania powinien zapewnić:

- wykrywanie, identyfikowanie, lokalizowanie i ciągłe monitorowanie wszystkich istotnych elementów ugrupowania bojowego przeciwnika oraz obiektów terenu z dokładnością stosowną do przeznaczenia informacji,

- pokrycie polem widzenia całego obszaru zainteresowania dowódców poszczególnych szczebli dowodzenia,

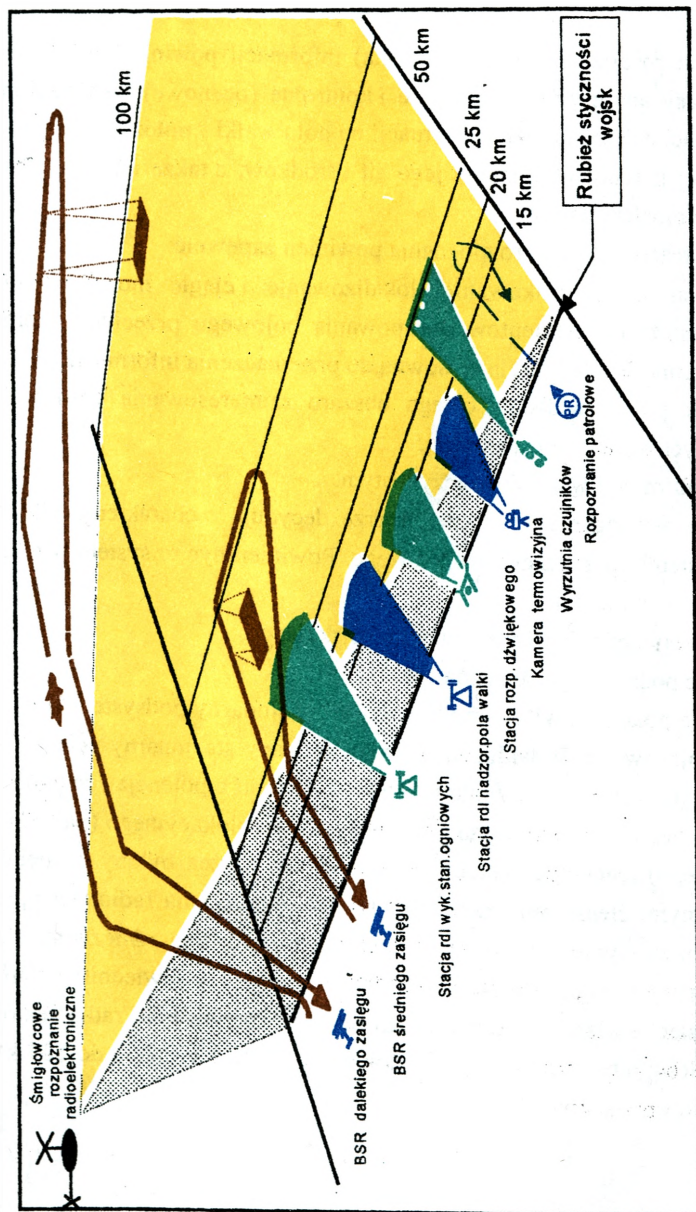
- obieg informacji w czasie rzeczywistym.

Powyższe wymagania w istotnej mierze decydują o charakterze współczesnego systemu rozpoznania wojskowego. Powinien być to system w pełni zintegrowany i obejmować:

- stacjonarny podsystem rozpoznania wojskowego,

- mobilne podsystemy rozpoznawcze.

W okresie pokoju powinien funkcjonować stacjonarny podsystem rozpoznania wojskowego. W takim ujęciu zintegrowany stacjonarny podsystem rozpoznania mógłby już dziś funkcjonować w oparciu o potencjał: rozpoznania agenturalnego oraz rozpoznania radiowego i radiolokacyjnego (pasywnego i aktywnego) dalekiego zasięgu. W przyszłości można byłoby uzupełnić go powietrznymi elementami dopplerowskiego rozpoznania radiolokacyjnego, jak również wyniesionymi ponad ziemię, w pasie nadgranicznym, elementami horyzontowego rozpoznania radiowego. Przy odpowiednim skonfigurowaniu sieci i właściwie dobranej trasy lotu, rozpoznanie radioelektroniczne mogłoby nieprzerwanie i dość dokładnie śledzić sytuację do 500 km wzdłuż granicy państwowej.



Mobilne systemy rozpoznawcze związków operacyjnych, taktycznych oraz oddziałów i pododdziałów powinny funkcjonować na wypadek zagrożenia i wojny. W ich skład powinny wchodzić:

- bezzałogowe samoloty rozpoznawcze (bsr) dalekiego, średniego i bliskiego zasięgu, dostosowane do zdobywania informacji w technice tele- i termowizyjnej, z automatyczną transmisją danych,

- stacje radiolokacyjne kierowania ogniem,
- polowe radiolokacyjne stacje wykrywania,
- akustyczne stacje wykrywania,
- kamery termowizyjne z wysięgnikami,
- wyrzucane zestawy rozpoznania czujnikowego,
- śmigłowcowe zestawy rozpoznania radioelektronicznego,
- patrolowe elementy rozpoznania osobowego.

Odpowiednio zorganizowany zintegrowany system rozpoznania wojkowego powinien umożliwiać prowadzenie wieloprzestrzennego penetrowania stosownych stref odpowiedzialności i zainteresowania wojsk oraz dostarczać wiarygodnej i terminowej informacji o siłach i środkach przeciwnika do komputerowych baz danych.

PRZYPISY

¹ Postrzeganie wielofunkcyjne to dostosowanie do zbierania informacji w różnych technikach - w różnych przestrzeniach informacyjnych.

² Postrzeganie wielospektralne to dostosowanie do jednoczesnego zbierania informacji w kilku różnych zakresach widma elektromagnetycznego.

³ Płk L. Ciborowski w swoim opracowaniu *Organizacja rozpoznania w sztabach*, AON wewn. 4315/91 - określa je jako „osobowe”.

⁴ Dotychczas określane w wojskach i literaturze przedmiotu jako „praca informacyjna”.

⁵ Widmo radiowe obejmuje promieniowanie elektromagnetyczne, którego długość fal mieści się w przedziale od 1000µm aż do rzędu kilometrowego. Widmo to dzielone jest na 6 następujących podzakresów: 1) fal długich 1-30km; 2) fal średnich 100-1000m; 3) fal krótkich 10-100m; 4) fal ultrakrótkich 1-10m; 5) pasma UHF 0,1-1m; 6) mikrofal 0,0001-0,1m.

⁶ Środki radiowe to potoczna nazwa wszelkich urządzeń nadających (nadawczych) i odbierających (odbiorczych) fale elektromagnetyczne w celu przekazywania i przechwytywania sygnałów mowy (dźwiękowych), obrazów itp. oraz innych rodzajów informacji.

⁷ Środki radioliniowe to odmiana środków radiowych. Ich wyróżnienie wynika z tego, że emisja sygnałów elektromagnetycznych odbywa się tylko w wąskich wiązkach.

⁸ Środki radionawigacyjne to urządzenia kierowania obiektami, które do tego celu wykorzystują fale radiowe. W metodach określania położenia i parametrów ruchu obiektów wykorzystuje się informacje zawarte w parametrach odbieranych sygnałów radiowych. Parametry odbieranych sygnałów - amplituda, faza, częstotliwość i czas - są związane funkcjonalnie z wielkościami geometrycznymi (kątem, odległością i różnicą odległości), charakteryzującymi położenie obiektu względem punktów nawigowania oraz parametrami ruchu.

⁹ Środki radiolokacyjne przeznaczone są do wykrywania i określania położenia obiektów za pomocą fal radiowych. Termin radiolokacja pochodzi od łacińskich słów *radius* (promień) i *locus* (miejsce), jego zaś odpowiednik *RADAR* od angielskiego określenia: *Radio Aids for Defence and Reconnaissance* (radiowe pomoce do obrony i rozpoznania) i amerykańskiego - *Radio Detection and Ranging* (wykrywanie i namierzanie za pomocą radia). Ze względu na sposób uzyskiwania sygnału różni się radiolokację: 1) aktywną - z pasywną lub aktywną odpowiedzią; 2) półaktywną, 3) pasywną.

¹⁰ *SONAR* (*Sonic Navigation and Ranging*) to urządzenie echolokacyjne służące do penetrowania hydrosfery.

¹¹ M.in. w *Poradniku oficera rozpoznania radioelektronicznego wojsk OPK*, Wyd. OP, Warszawa 1990 oraz w podręczniku *Organizacja i prowadzenie rozpoznania radioelektronicznego*, Wyd. Szt. Gen. WP, Warszawa 1979.

¹² Chociaż występowało już od czasów II wojny światowej, nie ujmowane jest w podręcznikach jako oddzielny rodzaj rozpoznania. Często utożsamiane jest często z rozpoznaniem radiotechnicznym.

¹³ Pasmo optyczne (zakres optyczny) widma elektromagnetycznego stanowią promieniowania: ultrafioletowe (długość fali: 0,01-0,38 μm), widzialne (długość fali: 0,38-0,76 μm) i podczerwone (długość fali: 0,76-1000 μm).

¹⁴ Optoelektronika - to dział elektroniki, którego przedmiotem jest łączne wykorzystanie optycznego jak i elektrycznego sposobu przetwarzania i przekazywania sygnałów. Podstawą optoelektroniki są fizyczne procesy warunkujące przetwarzanie sygnałów elektrycznych na optyczne i sygnałów optycznych na elektryczne oraz procesy wytwarzania, przesyłania, przetwarzania i magazynowania informacji niesionych przez światło.

¹⁵ Telewizja to dział telekomunikacji zajmujący się przekazywaniem na odległość, za pomocą elektrycznego kanału łączności, obrazów ruchomych wraz z towarzyszącym dźwiękiem. W celu przetworzenia obrazu optycznego na sygnał elektryczny wykorzystuje się zjawisko fotoelektryczne, natomiast dla odwrotnego przetworzenia wykorzystuje się zjawisko katodoluminescencji. System telewizyjny działa w nastę-

pujący sposób: przekazywana scena projektowana jest za pomocą obiektywu kamery telewizyjnej na światłoczułą powierzchnię lampy analizującej (w kamerze studyjnej jest to zazwyczaj superortikon) i w niej w procesie skanowania zostaje zamieniona na ciąg impulsów elektrycznych odpowiednio uporządkowanych, o amplitudach zależnych od jaskrawości poszczególnych punktów przekazywanego obrazu. Impulsy te, stanowiące sygnał wizyjny modulują napięcie częstotliwości nośnej nadajnika i za pomocą anteny nadawczej promieniowane są w przestrzeń. Sygnały telewizyjne odbierane przez antenę odbiorczą, po odpowiednim wzmacnieniu i przekształceniu sterując ruchem i jaskrawością plamki świetlnej na ekranie kineskopu, tworząc obraz. Plamka świetlna porusza się na ekranie z taką samą prędkością i w taki sam sposób jak strumień elektronów podczas analizowania obrazu w nadajniku.

¹⁶ Termowizja - to postrzeganie obrazów w widmie promieniowania podczerwonego (aktualnie wykorzystywane są tylko dwa pasma tego widma: 3-5 μm i 10-13 μm). Termowizja, w istocie wykorzystywanego zjawiska, podobna jest do noktowizji pasywnej. Różnica polega na tym, że termowizja posiada jeszcze urządzenie skanujące zamieniające obraz widziany w podczerwieni na ciąg impulsów elektrycznych (noktowizor pasywny z urządzeniem skanującym można nazywać termowizorem). Ponadto w termowizji technika przetwarzania sygnału zbliżona jest do techniki stosowanej w telewizji.

¹⁷ Noktowizja to dziedzina zastosowań techniki optoelektronicznej umożliwiającej widzenie w widmie promieniowania o długości 0,76-1000 μm . Zakres ten podzielono na podczerwień bliską 0,76-1,5 μm , średnią 1,5-5,6 μm i daleką 5,6-1000 μm - w dolnym paśmie podczerwieni dalekiej wyróżniony jest również zakres zwany podczerwienią skrajną). Obserwacja różnych obiektów w podczerwieni może być realizowana przez wykorzystywanie ich promieniowania własnego (wszystkie ciała, których temperatura jest wyższa od zera bezwzględnego, wysyłają własne niekoherentne promieniowanie podczerwone) lub odbitego. W związku z tym przyrządy noktowizyjne dzieli się na pasywne i aktywne.

¹⁸ Laser - to optyczny generator kwantowy lub generator światła spójnego, czy też źródło monochromatycznych fal elektromagnetycznych w zakresie optycznym (promieniowanie monochromatyczne to promieniowanie elektromagnetyczne o ustalonej długości fali). Nazwa lasera została utworzona z liter początkowych słów: Light Amplification by Stimulated Emission of Radiation (wzmacniacz światła z wymuszoną emisją promieniowania). Głównymi cechami laserowego promieniowania są: koherencja przestrzenna - istnienie przestrzeni, na których amplitudy fali są w pełni określone w funkcji czasu (koherencja to spójność światła polegająca na zgodności między fazami w różnych punktach wiązki światła lub w różnych wiązkach światła - w wąskim znaczeniu rozumie się to zjawisko jako zdolność do interferencji), koherencja czasowa (istnienie korelacji pomiędzy amplitudą fali w danym punkcie przestrzeni i czasem) nazywana też monochromatycznością fali (fala jednobarwna), polaryzacja i wielka, nie spotykana zarówno w przyrodzie, jak i w innych zwykłych sztucznych źródłach, gęstość widma mocy. Z koherencji przestrzennej wynika właściwa tylko wiązkom promieniowania laserowego znikoma rozbieżność, pozwalająca na skupienie ich w plamkę o teoretycznej średnicy rzędu długości fali. Dzięki kohe-

rencji czasowej promieniowanie może być poddawane procesowi modulacji (amplitudy, częstotliwości, fazy i impulsowej) i wykorzystywane przy odbiorze heterodynowym. Gęstość mocy promieniowania, nawet bez skupiania, jest niezwykle duża (do kilkuset megawatów na centymetr kwadratowy). Ponadto promieniowanie laserowe ma wszystkie właściwości typowych, klasycznie wytwarzanych fal radiowych, zaś różni się od nich jedynie długością fali. Podstawowymi elementami każdego lasera są: ośrodek laserujący, rezonator optyczny oraz źródło energii wraz z odpowiednim urządzeniem umożliwiającym dostarczanie jej, w odpowiedniej formie i ilości, do ośrodka (materiału) laserującego. Materiałem (ośrodkiem) laserującym może być ciało stałe, gaz lub ciecz. Elementem czynnym w materiale laserującym są atomy, jony lub molekuly (nazywane również mikrocząstkami materii), często stanowiące w nim tylko domieszkę o odpowiedniej koncentracji. Mikrocząsteczki te mogą znajdować się tylko w określonych stanach stacjonarnych, którym odpowiadają określone dyskretne stany energetyczne, czyli wartości energii układu atomowego. Przejście między stanami energetycznymi może nastąpić w wyniku emisji lub absorpcji promieniowania w postaci fali elektromagnetycznej lub w wyniku przeniesienia energii do innego układu. Przejście między stanami jest nazywane kwantowym, gdyż częstotliwość promieniowania pochłanianego lub emitowanego jest określona prawem Bohra: $h\nu = E_1 - E_2$, gdzie E_1 i E_2 oznaczają energie stanów, pomiędzy którymi zachodzi przejście, h - stała Plancka = $6,22 \cdot 10^{-27}$ erg s., ν - częstotliwość kwantu pochłoniętego lub wysłanego. Proces przenoszenia mikrocząsteczek materiału laserującego na wyższe (wzbudzone) poziomy energetyczne jest nazywany pompowaniem. Realizuje się go na przykład przez naświetlanie bardzo silnym strumieniem światła (pompowanie optyczne), przez zderzenia z szybkimi elektronami, przez zderzenia z pobudzonymi atomami lub w inny sposób. W procesie pompowania oraz generacji może być wykorzystane kilka poziomów energetycznych - zwykle trzy lub cztery. Promieniowanie jest zatem generowane z jedną częstotliwością (gdy przejście emisyjne odbywa się między jedną parą poziomów) lub z kilkoma częstotliwościami (przy korzystaniu z większej liczby poziomów). Emisja promieniowania z materiału laserującego ma charakter spontaniczny (wytwarzane fale nie są wówczas koherentne) lub wymuszony (stymulowany). W drugim wypadku emitowane kwanty są koherentne i zgodne z wymuszającym polem elektromagnetycznym, pochodzącym od tych kwantów emisji spontanicznej, których kierunek propagacji zgodny jest z osią rezonatora optycznego (interferometru). Dzięki dwóm równoległym zwierciadłom wiązka promieniowania odbija się kilkakrotnie i ulega wzmocnieniu przechodząc przez materiał laserujący. Warunkiem wystąpienia emisji wymuszonej jest dostarczenie dużej wartości wzmocnienia. Powstająca w rezonatorze fala spójnego promieniowania wyprowadzana jest na zewnątrz układu dzięki odpowiedniej konstrukcji rezonatora.

¹⁹ Infradźwięki - fale sprężyste o częstotliwościach mniejszych niż 16 Hz, a więc leżące poniżej zakresu ludzkiej słyszalności. Fale te są słabo tłumione i dlatego rozprzestrzeniają się na duże odległości od źródła. Mogą być wykorzystane do rejestracji efektów sejsmicznych oraz eksplozji na polu walki.

²⁰ Ultradźwięki - drgania i fale sprężyste o częstotliwościach większych niż 20 kHz, a więc leżące powyżej zakresu ludzkiej słyszalności. Mogą być wykorzystane do rejestracji efektów akustycznych (odgłosów) pola walki.

²¹ W przyszłości może być wysyłane w powietrze lub rozmieszczane na lądzie tysiące małych czujników. Miniaturowe czujniki zapachu mogą nawet wyczuć przeciwnika, bowiem unoszące się w powietrzu biosensory będą mogły śledzić żołnierzy na podstawie ich oddechów lub potu.

²² W USA jest jednym z elementów wojny informacyjnej.

²³ Wzorce takie szeroko wykorzystywane są podczas informacyjnej preparacji pola walki w państwach NATO.

IV. FORMY INFORMACJI Z ROZPOZNANIA GROMADZONEJ W BAZIE DANYCH NA POTRZEBY MILITARNE

1. Specyfika bazy danych na potrzeby militarne

Wielokryterialny wymiar współczesnego pola walki oraz złożoność procesów zachodzących w toku działań wojennych nakłada na jego uczestników obowiązek przetwarzania ogromnej ilości informacji, o coraz bardziej złożonej strukturze oraz szerszej rozpiętości problemowej. Obserwuje się również potrzebę systematycznego skracania czasu na jej opracowanie i racjonalne wykorzystanie. Rozwiązywanie tego problemu przez zwiększanie ilości personelu w poszczególnych komórkach organizacyjnych należy już do przeszłości. Bardziej skutecznym sposobem zwiększenia efektywności analizy informacji oraz procesu podejmowania decyzji jest odpowiednie wykorzystanie środków informatycznych w których priorytetową rolę stanowią - jak wcześniej sygnalizowano - bazy danych. Tworzenie baz danych jest zatem obecnie żywotną koniecznością dla prawidłowego funkcjonowania naszych Sił Zbrojnych zarówno w czasie pokoju, ewentualnego okresu zagrożenia lub wojny. Należy jednak mieć na uwadze, że baza danych budowana na potrzeby militarne znacznie różni się od powszechnie występujących w chwili obecnej w otaczającej nas rzeczywistości, np. na potrzeby finansów, księgowości, ewidencji materiałowej, turystyki itp. Również informacje gromadzone w bazie danych na potrzeby militarne mają inny charakter, gdyż:

- są zróżnicowane w strukturze, formie i treści, tj. całkowicie odmienne niż w powszechnie stosowanych systemach,
- charakteryzują się różnym stopniem wiarygodności, tzn. mogą być nawet niepełne, niepewne, zdezaktualizowane, o różnym stopniu wiarygodności (szczególnie o przeciwniku),

- są wykorzystywane w dwustronnym systemie destrukcyjnym (zarówno wojsk własnych jak i przeciwnika), czyli takim, który jest nastawiony na niszczenie a nie na tworzenie, w wyniku czego w toku działań bojowych ogólna liczba informacji może być zmienna, a wiele z nich będzie się szybko dezaktualizować,

- bardzo często są wykorzystywane w skrajnie krótkich przedziałach czasowych,

- są odpowiednio usystematyzowane pod względem dostępności na różnych szczeblach dowodzenia z uwzględnieniem zaostrożonych wymagań w zakresie bezpieczeństwa ich przechowywania.

W bazie danych na potrzeby militarne powinny być gromadzone informacje operacyjno-techniczne niezbędne do funkcjonowania Sił Zbrojnych RP w okresie pokoju, stanu zagrożenia oraz wojny (początkowego okresu wojny). Wykorzystanie ww. bazy w procesie wspomagania dowodzenia wojskami i kierowania środkami pozwala na:

- gromadzenie elementarnych danych i informacji,

- agregowanie danych w bardziej złożone obiekty, którymi posługują się osoby funkcyjne podczas działalności służbowej,

- parametryzowanie funkcji ocenowych, planistycznych i monitorowanie czynności,

- wspaganie decydentów w zakresie rozszerzania jego możliwości do interpretacji działań alternatywnych w kategorii celów, które należy osiągnąć.

Istotą projektowania baz danych, jak i użytkowej ich eksploatacji jest między innymi to że:

- treść i struktura wykorzystywanych zbiorów informacji powinna być formułowana zarówno w kategoriach taktycznych, jak i informatycznych,

- wartość informacji opisujących modelowane obiekty (np. teren, warunki atmosferyczne, przeciwnik, a nawet sąsiedzi) ulega częstym zmianom,

- objętość przetwarzanych zbiorów informacji jest bardzo duża i porównywalna z istniejącymi w tym zakresie potrzebami systemów dowodzenia,

- treść i struktura wykorzystywanych zbiorów informacji jest bardzo zróżnicowana, a proces ich przygotowania wymaga znacznego czasu i współdziałania wielu specjalistów.

Prawidłowe funkcjonowanie bazy danych związane jest zatem ze zbieraniem i przetwarzaniem dużych zbiorów informacji. Architektura bazy danych na potrzeby militarne, jak każdej nowoczesnej bazy danych powinna być trójpoziomowa i obejmować:

- poziom fizyczny,
- poziom pojęciowy,
- poziom prezentacji.

Poziom fizyczny powinien określać sposób przechowywania danych w pamięci zewnętrznej komputerów. Na poziomie fizycznym powinny być gromadzone dane w plikach (zbiorach) danych o określonych strukturach. Zarówno z punktu widzenia projektanta, jak też użytkownika systemu, poziom ten nie powinien wpływać na sposób pracy, jednak powinien wpływać na ostateczne działanie poszczególnych aplikacji.

Poziom pojęciowy powinien być odwzorowaniem poziomu fizycznego przy pomocy języka definicji danych (ang. *data definition language - DDL*). Reprezentantami fizycznie istniejących danych powinny być abstrakcyjne pojęcia oraz relacje między nimi.

Zapewnienie użytkownikowi możliwości operowania danymi właśnie za pomocą pojęć abstrakcyjnych, pomijając całkowicie - jeśli to możliwe - fizyczny sposób przechowywania danych przez komputery, powinno należeć do zadań systemu zarządzania bazą danych.

Na poziomie prezentacji zawartość bazy danych powinna być odwzorowywana w sposób czytelny dla użytkownika, np. w postaci tabel, schematów, rysunków, wydruków itp.

Projektując bazę danych na potrzeby militarne należy uwzględnić następujące założenia i ograniczenia:

- struktura organizacji danych w każdej tablicy bazy danych powinna być uniwersalna, tzn. mieć możliwość zdefiniowania jej na poziomie dowolnego systemu zarządzania bazą danych w dowolnym środowisku operacyjnym,
- struktura organizacji danych w tablicach powinna być pozbawiona redundancji¹,
- struktura organizacji danych w tablicach bazy danych powinna zapewniać integralność danych,
- baza danych powinna funkcjonować w środowisku sieci komputerowej,
- dane przechowywane na poziomie fizycznym bazy danych powinny być utajnione.

W celu zrealizowania pierwszego z założeń należy przyjąć standardowe typy danych dla definiowanych pól tablic tak, aby ich strukturę organizacyjną można było wprowadzić przy pomocy dowolnego systemu zarządzania bazą danych. Należy zwrócić uwagę na redundancje danych. Można i należy eliminować ją na etapie projektowania tablic bazy danych. Jednym ze sposobów unikania redundancji jest odpowiednie wiązanie tablic relacjami.

Integralność bazy danych złożonej z tablic powiązanych relacjami powinna być kolejnym jej założeniem. Zapewnienie integralności powinno polegać na takim zarządzaniu danymi, aby po wykonaniu dowolnej operacji na bazie danych, została zachowana pełna odpowiedniość pomiędzy jej elementami i obiektami świata rzeczywistego, których atrybuty te elementy reprezentują. Odpowiedniość ta powinna być zapewniana przez wewnętrzne mechanizmy systemu zarządzania bazą danych.

System zarządzania bazą danych powinien zapewniać niejawnosć danych na poziomie fizycznym. Niejawnosć ta powinna być zapewniona przez wewnętrzne mechanizmy systemu zarządzania lub też przez specjalnie zaprojektowane procedury np. szyfracji i deszyfracji.

Baza danych powinna składać się - na poziomie fizycznym - z plików danych, które tworzone są na dysku, natomiast na poziomie logicznym - elementami bazy danych powinny być tablice złożone z pól reprezentujących informacje, którymi posługują się dowódcy i osoby funkcyjne mające do niej dostęp.

Ważną rolę w procesie gromadzenia i przetwarzania informacji odgrywają odpowiednie *źródła jej pozyskiwania*. Informacje przechowywane w bazach danych powinny tworzyć następujące zbiory:

a) zbiory informacji wejściowych względnie stałych, aktualizowanych z reguły co pół roku przez poszczególne dowództwa rodzajów sił zbrojnych RP oraz odpowiednie komórki sztabów związków operacyjnych, związków taktycznych i oddziałów na poszczególnych szczeblach dowodzenia, np:

- dane o strukturach organizacyjnych wojsk i wybranych elementach ugrupowania operacyjnego (bojowego),
- dane o terenie przewidywanych działań bojowych,
- parametry i normy taktyczno-techniczne środków walki,
- dane o środkach radioelektronicznych, ze szczególnym uwzględnieniem cech demaskujących ich pracę,
- słowniki nazw elementów ugrupowania operacyjnego i bojowego, ZO, ZT, oddziałów i pododdziałów oraz środków walki,
- inne;

b) zbiory informacji wejściowych zmiennych, aktualizowanych na bieżąco:

- dane pomiarowe, badawcze, uzyskiwane w toku działań jednostek specjalnych,
- dane agenturalne,
- inne;

c) zbiory informacji wynikowych, dostępnych na poszczególnych szczeblach dowodzenia, np:

- dane stanowiące treść meldunków o stanie, położeniu i działaniu wojsk,
- dane stanowiące treść doraźnych komunikatów i meldunków,

- graficzny obraz sytuacji (stan, położenie i działanie wojsk),
- dane informujące o dynamice działań - o powstałych stratach, tempie natarcia i potencjałach walczących stron,
- parametry techniczno-operacyjne środków walki i uzbrojenia,
- wybrane cechy demaskujące pracę środków i systemów radioelektronicznych,
- sylwetki dowódców,
- inne.

2. Przykładowe formy informacji z rozpoznania niezbędnej na poszczególnych szczeblach dowodzenia

W podrozdziale tym zaprezentowano najbardziej reprezentatywne- zdaniem autorów - formy informacji z rozpoznania niezbędnej na różnych szczeblach dowodzenia w kontekście budowy komputerowych baz danych na potrzeby militarne. Bliska perspektywa przystąpienia SZ RP do NATO oraz konieczność zapewnienia interoperacyjności z wojskami Sojuszu skłoniła autorów do posiłkowania się metodologią pracy sztabów państw NATO² w zakresie informacyjnego (rozpoznawczego) przygotowania pola walki³.

Pierwszoplanową rolę w tym procesie odgrywają *informacje o obszarze działań (terenie), obiektach taktycznych oraz warunkach atmosferycznych*. Są one ściśle związane z lokalizacją przestrzenną a tym samym z mapą. Dlatego też forma informacji zamieszczanych w bazie danych powinna odpowiadać niektórym cechom map topograficznych oraz map pogody. Jednak informacje o obszarze działań (terenie) przedstawiane na typowych mapach topograficznych są trudne do wykorzystania w komputerowych bazach danych. Można wprowadzać współrzędne prostokątne obszaru odpowiedzialności do odpowiednich tablic, np.: „PARAMZO”, „PARAMZT” o następującej strukturze informacyjnej:

- współrzędnych prostokątnych czterech wierzchołków prostokąta określającego obszar odpowiedzialności na danym szczeblu dowodzenia,
- szerokości obszaru,
- głębokości obszaru.

Wprowadzając współrzędne dwóch wierzchołków prostokąta należy wybrać położone najbliżej linii frontu oraz głębokość obszaru. Jeśli dwa pozostałe wierzchołki prostokąta położone są w punktach o współrzędnych X , Y większych od dwóch wprowadzonych punktów, należy wprowadzić głębokość obszaru ze znakiem ujemnym (przypadek, gdy przeciwnik znajduje się na kierunku południowym). Szerokość obszaru, jak również dwa pozostałe wierzchołki prostokąta obliczane mogą być automatycznie.

Istnieje pilna potrzeba by informacje przedstawiane na mapach topograficznych przedstawić w postaci dostępnej dla bazy danych (na nośniku informacji typowym dla komputerów). W opracowywanej komputerowej bazie danych na potrzeby militarne należy korzystać (o ile będzie to możliwe) z cyfrowych map terenu. Mapy cyfrowe powinny zapewnić komputerowy zapis i elektroniczne zobrazowanie wybranych elementów topograficznych oraz obszarów działań wojennych na różnych szczeblach dowodzenia. Z punktu widzenia użytkownika mapa cyfrowa powinna mieć budowę warstwową. Poszczególne jej warstwy powinny zawierać:

- mapę wysokościową terenu,
- naturalne pokrycie terenu,
- szlaki komunikacyjne,
- miejscowości,
- charakterystyczne budowle, linie wysokiego napięcia, mosty, wiadukty itp.

Punktowe obiekty terenowe powinny być wprowadzane do dwóch tablic: „**MIASTA**” i „**OBIEKTY**”. W tablicy „**MIASTA**” przechowywane powinny być nazwy i współrzędne prostokątne miejscowości. Nazwy te mogą być wprowadzone w fazie przygotowania systemu do pracy, ale również w innych, późniejszych fazach. Tablica powinna być zaprojektowana w celu

ułatwienia wprowadzania położenia obiektów, stanowisk dowodzenia i węzłów łączności istotnych dla struktury organizacyjnej.

Tablica „**OBIEKTY**” powinna posiadać strukturę informacyjną zawierającą następujące elementy:

- typ obiektu,
- nazwa obiektu,
- nazwa miejscowości,
- współrzędne prostokątne obiektu,
- opis obiektu.

Wyróżnić należy następujące typy obiektów terenowych:

- zakłady przemysłowe istotne z punktu widzenia funkcjonowania systemu łączności, warsztaty remontowe, składnice sprzętu łączności itp. - *typ 1*,
- lotniska i lądowiska - *typ 2*.

Konieczne jest aby treści topograficzne mogły być uzupełniane treściami taktycznymi (zasadnicze elementy ugrupowania wojsk własnych i przeciwnika)⁴.

Informacje o warunkach atmosferycznych (o pogodzie) powinny mieć swoje odzwierciedlenie również w odpowiednich, cyfrowych mapach pogody. Dane o pogodzie wybranego obszaru powinny być dostępne co najmniej z pięciu ostatnich lat.

Informacje o wojskach innych państw, (potencjalnego przeciwnika) powinny obejmować dane co do ilości (zestawienia w formie tabelarycznej) jak i struktury wojsk (w formie graficznej). W zależności od szerebła dowodzenia powinna być różna objętość tych informacji oraz stopień szczegółowości. Celowe wydaje się podzielić je na trzy grupy:

- szczebel strategiczny (informacje o siłach zbrojnych),
- szczebel operacyjny (informacje o związkach operacyjnych),
- szczebel taktycznych (informacje o związkach taktycznych, oddziałach i pododdziałach).

Elementy systemu walki armii państw obcych (potencjalnego przeciwnika) wprowadzane powinny być do odpowiedniej tablicy, np. „**UGRUP-PRZECIWNIA**” o następującej strukturze informacyjnej:

- kraj,
- nazwa elementu ugrupowania,
- grupa elementów ugrupowania,
- szczebel,
- parametry taktyczno-operacyjne,
- dotychczasowe wzorce doktrynalne,
- uwagi.

Dane te powinny być gromadzone dla każdego elementu ugrupowania na danym szczeblu dowodzenia w danym kraju.

Pole „**GRUPA ELEMENTÓW UGRUPOWANIA PRZECIWNIA**” powinna umożliwiać dokonanie podziału elementów ugrupowania operacyjnego (taktycznego) na grupy. Powodem podziału powinna być potrzeba uporządkowania elementów ugrupowania i zapewnienia szybszego dostępu do wyróżnionego rodzaju ugrupowania. Należy predefiniować następujące rodzaje ugrupowań zawarte w tablicy „**RODZUGRUPOWAN**”:

- ugrupowania szczebla strategicznego (centralnego),
- związki operacyjne,
- związki taktyczne,
- oddziały,
- jednostki dowodzenia i łączności,
- jednostki WRe,
- jednostki radiotechniczne,
- inne.

Wprowadzanie elementu ugrupowania operacyjnego (taktycznego) poprzedzone powinno być wyborem grupy elementów ugrupowania, do którego dany element zostanie zaliczony. Wprowadzający powinni mieć możliwość tworzenia własnych podziałów elementów ugrupowań na grupy. Obie wy-

mienione tablice powinny współpracować ze sobą. Możliwość usuwania grupy w wypadku, gdy zaliczony będzie do niej jakikolwiek element ugrupowania powinna być zablokowana.

Pole „UWAGI” powinno służyć do wprowadzenia informacji ważnych dotyczących danego elementu ugrupowania.

Stanowiska dowodzenia - funkcjonujące na poszczególnych szczeblach dowodzenia - powinny być wprowadzane do tablicy „STANDOWO”, o następującej strukturze informacyjnej:

- rodzaj stanowiska dowodzenia,
- nazwa stanowiska dowodzenia,
- element ugrupowania, do którego należy stanowisko dowodzenia,
- rejon rozmieszczenia (miejscowość, współrzędne prostokątne położenia)

stanowiska dowodzenia,

- środki i sposoby automatyzacji dowodzenia,
- uwagi.

Pole „RODZAJ STANOWISKA DOWODZENIA” powinno umożliwiać dokonanie podziału stanowisk dowodzenia na grupy. Powodem podziału powinna być potrzeba uporządkowania stanowisk dowodzenia i zapewnienia szybszego dostępu do wyróżnionego rodzaju stanowisk dowodzenia. Należy predefiniować poszczególne rodzaje stanowisk dowodzenia i umieścić je w tablicy „RODSTAN”:

- stanowiska dowodzenia szczebla strategicznego (centralnego),
- stanowiska dowodzenia związku operacyjnego,
- stanowiska dowodzenia związków taktycznych,
- stanowiska dowodzenia oddziałów ogólnowojskowych,
- stanowiska dowodzenia jednostek WRe,
- stanowiska dowodzenia jednostek radiotechnicznych,
- inne.

Wprowadzanie stanowiska dowodzenia poprzedzone powinno być wyborem jego rodzaju. Wprowadzający powinien mieć możliwość tworzenia wła-

snych podziałów stanowisk dowodzenia. Obie wymienione tablice powinny współpracować ze sobą. Możliwość usuwania rodzaju stanowisk dowodzenia w przypadku, gdy już zaliczono do tej grupy jakiegokolwiek stanowisko dowodzenia powinna być zablokowana. Pole "UWAGI" powinno służyć do wprowadzenia ważnych informacji, które dotyczą danego stanowiska dowodzenia.

Nazwy osób funkcyjnych powinny być gromadzone w tablicy „OSFUNK” w odniesieniu do poszczególnych stanowisk dowodzenia. Tablica ta powinna posiadać następującą strukturę informacyjną:

- nazwa osoby funkcyjnej,
- funkcja,
- element ugrupowania,
- węzeł łączności, na którym osoba przebywa,
- miejsce pracy osoby funkcyjnej,
- krótka charakterystyka osobowa wraz ze zdjęciem (dotyczy dowódców i innych ważnych osób funkcyjnych),
- uwagi.

Nazwa osoby funkcyjnej powinna być złożona z dwóch członów: funkcji sprawowanej przez osobę oraz elementu ugrupowania, do którego dana osoba funkcyjna należy. Wprowadzenie nazw osób funkcyjnych wymaga więc wypełnienia tablicy funkcji „FUNKCJE” oraz tablicy „ELUGR”. Bardzo istotne jest wprowadzenie danych o miejscu pobytu osoby funkcyjnej na danym stanowisku dowodzenia oraz jego nazwisku (jeżeli jest znane).

Węzły łączności szczebla strategicznego, operacyjnego (taktycznego) przeciwnika, powinny być wprowadzane do tablicy „WĘZŁY” o następującej strukturze informacyjnej:

- nazwa węzła łączności,
- rodzaj węzła łączności,
- miejscowość,
- współrzędne prostokątne położenia węzła łączności,
- stanowisko dowodzenia, jeśli dany węzeł jest węzłem łączności SD,
- kryptonim węzła łączności,

- adres radiowy węzła łączności,
- inne.

Pole „**RODZAJ WĘZŁA ŁĄCZNOŚCI**” powinno umożliwiać dokonanie podziału węzłów na grupy. Powodem takiego podziału jest potrzeba uporządkowania węzłów i zapewnienie szybszego dostępu do wyróżnionego ich rodzaju. Powinny być predefiniowane poszczególne rodzaje węzłów łączności i umieszczone w tablicy „**RODWĘZ**”:

- WŁ SD szczebla strategicznego (centralnego),
- WŁ SD związków operacyjnych,
- WŁ SD związków taktycznych,
- WŁ SD oddziałów łączności i oddziałów bezpośredniego podporządkowania,
- WŁ SD ugrupowań sąsiednich,
- podstawowe węzły sieciowe (PWS),
- stacje bazowe lądowej radiokomunikacji ruchomej (SB LLR),
- stacjonarne WŁ MON (garnizonowe węzły łączności),
- stacjonarne WŁ Ministerstwa Łączności,
- stacje wzmacniakowe,
- inne.

Wyróżnienie węzłów łączności systemu stacjonarnego wynika z faktu, że informacja zarówno o polowych węzłach łączności, jak i o węzłach łączności systemu stacjonarnego powinna być gromadzona w tej samej tablicy „**WĘZŁY**”.

Wprowadzanie węzła łączności poprzedzone powinno być wyborem rodzaju węzłów, do którego dany węzeł zostanie zaliczony. Mogą być tworzone własne podziały węzłów łączności. Obie wymienione tablice powinny współpracować ze sobą. Usuwanie określonego rodzaju węzłów łączności w przypadku, gdy zaliczono do niego jakikolwiek węzeł, powinno być zablokowane. Podczas wprowadzania rodzaju węzłów łączności należy określić, czy obejmuje on węzły łączności stanowisk dowodzenia czy nie.

Informacje o sieci łączności radioliniowo-przewodowej zorganizowanej przez dany związek strategiczny, operacyjny (taktyczny) lub oddział wojsk przeciwnika, powinny być wprowadzane do odpowiednich tablic „**SRLPRZ**” o następującej strukturze informacyjnej:

- numer kierunku,
- typ kierunku,
- środek łączności,
- początkowy i końcowy węzeł łączności,
- typ stacji radioliniowej,
- długość kierunku radioliniowego,
- uwagi.

Dodatkowo należy dokonać podziału na następujące grupy:

- kierunki szczebla strategicznego (centralnego),
- kierunki związków operacyjnych,
- kierunki w stacjonarnym systemie łączności,
- kierunki w sieci podstawowej,
- dowiązania węzłów łączności stanowisk dowodzenia do sieci podstawowej.

W tej samej tablicy powinny być przechowywane dane o kierunkach radioliniowych, przewodowych i troposferycznych, rozróżniane przy pomocy pola „**ŚRODEK ŁĄCZNOŚCI**” Długość toru radioliniowego powinna być obliczana automatycznie na podstawie współrzędnych położenia początkowego i końcowego węzłów łączności tworzących linię łączności.

Dane dotyczące rodzajów sieci radiowych powinny być gromadzone w tablicy „**RODZSIECI**” o następującej strukturze informacyjnej:

- nazwa rodzaju sieci radiowych,
- szczebel (strategiczny, operacyjny, taktyczny).

Nazwa rodzaju sieci radiowych powinna określać grupę sieci radiowych wyróżnioną przez wprowadzającego do bazy danych. Należy wprowadzić to wyróżnienie w celu zwiększenia czytelności danych na ekranie i operowania mniejszymi porcjami danych. Dodatkowo powinno się określić:

- numer sieci radiowej,
- rodzaj sieci radiowej,
- nazwa sieci radiowej,
- urządzenie utajniaszące,
- typy radiostacji sieciowych,
- rodzaje emisji,
- częstotliwości robocze i zapasowe w dwóch kolumnach dla sieci radiowych (w przypadku radiostacji należy przewidzieć pozyskiwanie odpowiednich systemów kodowania),
- inne.

Dane dotyczące składu korespondentów w sieciach radiowych gromadzone powinny być w tablicy „**KORESPONDENCI**”. Tablica ta powinna mieć strukturę informacyjną złożoną z następujących elementów:

- numer sieci radiowej,
- osoba funkcyjna,
- typ radiostacji,
- inne.

Wprowadzenie do tablicy korespondentów sieci radiowej uzależnione powinno być uprzednim wprowadzenia sieci i zaliczeniem jej do jednego ze zdefiniowanych wcześniej rodzajów sieci radiowych.

Zasoby środków łączności przeciwnika, z wyszczególnieniem ich parametrów taktyczno-technicznych należy gromadzić w odpowiednich tablicach:

- środki łączności radiowej,
- środki łączności radioliniowej,
- środki łączności radiotelefonicznej,
- środki łączności kablowej (przewodowej, światłowodowej),
- inne.

Środki łączności radiowej powinny być gromadzone w tablicy „**RDSTACJE**”. Z uwagi na gromadzone o nich informacje w bazach danych istotne są następujące dane o typach radiostacji:

- typ radiostacji,

- zakres pracy radiostacji: UKF lub KF,
- moc radiostacji: duża, średnia, mała,
- moc wyjściowa nadajnika [W],
- typ anteny (wybierany z tablicy rodzajów anten),
- struktura widma,
- inne cechy demaskujące ich pracę.

Środki łączności radioliniowej powinny być gromadzone w tablicy „**RDLN**”. Z uwagi na gromadzone o nich informacje w bazach danych istotne są następujące dane o typach radiolinii:

- typ radiolinii,
- moc sygnału na wyjściu odbiornika [W],
- typ anteny (wybierany z tablicy rodzajów anten),
- rodzaj emisji (wybierany z tablicy rodzajów emisji),
- struktura widma,
- inne cechy demaskujące ich pracę.

Środki łączności radiotelefonicznej gromadzone powinny być w tablicy „**TYPYRTL**”, która powinna posiadać następującą strukturę informacyjną:

- typ środka łączności radiotelefonicznej,
- moc nadajnika pokładowego [W],
- moc nadajnika osobistego [W],
- wysokość anteny radiotelefonu pokładowego [m],
- wysokość anteny radiotelefonu osobistego [m],
- wysokość anteny stacji bazowej [m],
- struktura widma,
- inne cechy demaskujące ich pracę.

Środki łączności kablowej gromadzone powinny być w tablicy „**KABL**”. Z uwagi na gromadzone o nich informacje w bazach danych istotne są następujące dane:

- typ środka,
- podstawowe parametry techniczne,
- zakres wykorzystania na poszczególnych szczeblach dowodzenia,

- czasy rozwijania odcinków fabrycznych,
- inne.

Dane o siłach i środkach WRe przeciwnika na poszczególnych szczeblach dowodzenia powinny być gromadzone w odpowiednich tablicach.

Tablica „**SILYWRE**” powinna zawierać następujące informacje:

- nazwa i rodzaj jednostki WRe,
- podstawowe wyposażenie,
- element ugrupowania, do którego należy jednostka WRe,
- rejon rozmieszczenia (miejscowość, współrzędne prostokątne położenia),
- dotychczasowe wzorce doktrynalne,
- możliwości taktyczno-operacyjne,
- uwagi.

Tablica „**ŚRODEKWRE**” powinna zawierać następujące informacje:

- typ środka WRe,
- kategoria środka (naziemny lub powietrzny),
- rodzaj pracy (wykrywanie, namierzanie, obezwładnianie zakłóceniami),
- położenie środka (współrzędne prostokątne),
- strefa dyżurowania w [km] dla środków powietrznych,
- typy anten,
- rodzaje pracy,
- moc nadajników,
- struktura widma,
- dane dotyczące skuteczności zakłóceń (pozyskiwane przy pomocy wewnętrznych kalkulatorów bazy danych),
- inne cechy demaskujące pracę środków WRe.

Obiekty WRe powinny być wprowadzane w dwóch głównych kategoriach: naziemne i powietrzne.

Dane o siłach i środkach radiolokacyjnych przeciwnika na poszczególnych szczeblach dowodzenia powinny być gromadzone w odpowiednich tablicach.

Tablica „**SILYRLS**” powinna zawierać następujące informacje:

- nazwa i rodzaj elementu,
- podstawowe wyposażenie,
- przynależność do elementu ugrupowania ogólnowojskowego,
- rejon rozmieszczenia (miejscowość, współrzędne prostokątne położenia),
- dotychczasowe wzorce doktrynalne,
- możliwości taktyczno-operacyjne,
- uwagi.

Tablica „**ŚRODEKRLS**” powinna zawierać następujące informacje:

- typ środka radiolokacyjnego,
- kategoria środka (naziemny lub powietrzny),
- rodzaj pracy,
- położenie środka (współrzędne prostokątne),
- strefa dyżurowania w [km] dla środków powietrznych,
- typy anten,
- rodzaje pracy,
- moc nadajników,
- struktura widma,
- inne cechy demaskujące ich pracę środka.

Obiekty radiolokacyjne powinny być wprowadzane w dwóch głównych kategoriach: naziemne i powietrzne.

Dane o siłach i środkach radionawigacyjnych przeciwnika na poszczególnych szczeblach dowodzenia powinny być gromadzone w odpowiednich tablicach.

Tablica „**SIŁYRNW**” powinna zawierać następujące informacje:

- nazwa i rodzaj elementu,
- podstawowe wyposażenie,
- przynależność do elementu ugrupowania ogólnowojskowego,
- rejon rozmieszczenia (miejscowość, współrzędne prostokątne położenia),
- dotychczasowe wzorce doktrynalne,

- możliwości taktyczno-operacyjne,
- uwagi.

Tablica „**ŚRODEKRNW**” powinna zawierać następujące informacje:

- typ środka radionawigacyjnego,
- kategoria środka (naziemny lub powietrzny),
- rodzaj pracy,
- położenie środka (współrzędne prostokątne),
- typy anten,
- rodzaje pracy,
- moc nadajników,
- struktura widma,
- inne cechy demaskujące ich pracę środka.

Obiekty radionawigacyjne powinny być wprowadzane w dwóch głównych kategoriach: naziemne i powietrzne.

Dane o innych obiektach radioelektronicznych przeciwnika na poszczególnych szczeblach dowodzenia powinny być gromadzone w odpowiednich tablicach.

Tablica „**SIŁYREL**” powinna zawierać następujące informacje:

- nazwa i rodzaj elementu,
- podstawowe wyposażenie,
- przynależność do elementu ugrupowania ogólnowojskowego,
- rejon rozmieszczenia (miejscowość, współrzędne prostokątne położenia),
- dotychczasowe wzorce doktrynalne,
- możliwości taktyczno-operacyjne,
- uwagi.

Tablica „**ŚRODEKREL**” powinna zawierać następujące informacje:

- typ środka radionawigacyjnego,
- kategoria środka (naziemny lub powietrzny),
- rodzaj pracy,
- położenie środka (współrzędne prostokątne),
- strefa dyżurowania w [km] dla środków powietrznych,

- typy anten,
- rodzaje pracy,
- moc nadajników,
- struktura widma,
- inne cechy demaskujące ich pracę środka.

Obiekty radioelektroniczne powinny być wprowadzane w dwóch głównych kategoriach: naziemne i powietrzne.

3. Współpraca użytkowników z bazą danych na potrzeby militarne

Ważną rolę w procesie korzystania z bazy danych odgrywać powinien *interfejs użytkownika*. Umożliwia on współpracę człowieka z komputerem. Współpracę tę określa się w teorii systemów wspomagania podejmowania decyzji terminem *dialog*, który można zdefiniować jako: *wymianę symboli i działań między komputerem a człowiekiem*. Symbolami w tym sensie są wyrazy języka naturalnego, wyrażenia matematyczne i obrazy graficzne. W skład interfejsu użytkownika powinien wchodzić sprzęt i oprogramowanie, które umożliwiają podjęcie i kontynuowanie dialogu oraz wykonywanie innych niezbędnych działań w procesie przetwarzania informacji. Sposoby i metody podejmowania działań przez użytkownika określane są terminem *język komunikacji*.

Użytkownik powinien mieć możliwość posługiwania się następującymi obiektami na ekranie monitora komunikując się z systemem:

1) PRZYCISK

Na ekranie przycisk powinien być widoczny jako prostokąt z cieniem, we wnętrzu którego powinien znajdować się napis określający rodzaj działania, jakie zostanie podjęte przez system, jeśli użytkownik dokona wyboru i zatwierdzenia działania (opcji). Wyboru działania (opcji) można będzie dokonać przy pomocy klawiatury lub myszy. Przyciski powinny być niezbędnymi

obiektami na ekranach prezentujących listy wyboru opcji (menu), gdzie powiązane powinny być z nazwami procedur, które zostaną wykonane po zatwierdzeniu przycisku. We wszystkich pozostałych typach procedur przyciski powinny być podobne w celu zachowania uniwersalności obsługi systemu. Wybranie przycisku „WSTAW” oznaczać powinno wybór działania, które będzie polegało na wprowadzaniu nowych danych. Wybór przycisku „ZMIANA” oznaczać powinno podjęcie akcji modyfikacji danych. Wybór przycisku „USUŃ” powinno być równoznaczne z podjęciem akcji usunięcia wskazanych wcześniej danych. Wybranie przycisku „ZATWIERDZENIE” lub „OK” powinno spowodować przyjęcie wprowadzonych przez użytkownika danych i ich zapis do pamięci zewnętrznej, natomiast naciśnięcie przycisku „REZYGNACJA” powinno uruchomić działanie odwrotne: odwołanie wprowadzonych danych i przyjęcie ich poprzednich wartości. Oprócz wspomnianych przycisków, które powinny być uniwersalne w całym systemie, należy wprowadzić w zależności od potrzeb inne przyciski.

2) OBIEKTY WYBORU

Obiekty te pozwolą użytkownikowi wybrać jedną spośród kilku opcji, przy czym zwykle będą to parametry podejmowanych działań. Do obiektów stosowanych w bazie danych mogą należeć: *radio button*, *checkbox*, *option box*, *list box*, *combo box*. itp.

3) OKNA KOMUNIKATÓW

W momencie, gdy aplikacja ma umożliwić użytkownikowi wykorzystanie informacji, powinno otworzyć się okno i wyświetlić się odpowiedni komunikat. Nie zawsze komunikat ten może dotyczyć błędów wykrytych w czasie pracy użytkownika z systemem, czasem system zwyczajnie powinien poinformować użytkownika, jakie działania podejmie. Do zjawisk, mogących powodować wyświetlanie komunikatów o wykrytych błędach przez system będą należały:

- kolizje sieciowe użytkowników - wtedy komunikat będzie wyjaśniał powody kolizji i sposób ich rozwiązania,

- wprowadzenie nieprawidłowej danej przez użytkownika tzn. danej o niewłaściwym typie od wymaganego lub danej spoza dziedziny dla niej określonej,

- wprowadzenie danej, która będzie zakłócać integralność bazy np. duplikacja danych, na podstawie których zbudowane będą główne klucze indeksowe (ang. *primary keys*) dla danych zgromadzonych w pliku bazy danych,

- uszkodzenia fizyczne zbiorów bazy danych, które uniemożliwiają zapis i odczyt danych,

- brak pamięci dla przetwarzania danych,

- brak możliwości zrealizowania transakcji, a ściślej - złożonego procesu aktualizacji danych, który obejmie dwa lub więcej plików bazy danych powiązanych relacjami.

4) KURSOR

Kursor powinien być wskaźnikiem pozycji wprowadzanych znaków na ekranie i pojawiać się w odpowiednich polach zawsze wtedy, gdy użytkownik będzie wprowadzał dane. Naciśnięcie klawisza na klawiaturze powinno powodować zobrazowanie znaku na ekranie w pozycji kursora i przesunięcie kursora w prawo. Innym wskaźnikiem, który widoczny powinien być na ekranie to wskaźnik myszy. Jego zadaniem powinno być wskazywanie obiektów ekranowych przy pomocy tego urządzenia.

Dla wszystkich operacji ekranowych, jakie użytkownik będzie wykonywał, należy przyjąć model obsługi nazywany interfejsem SAA/CUA (ang. *System Application Architecture / Common User Access*). Standaryzuje on działania użytkownika w zakresie obsługi klawiatury i myszy.

Prezentacje odbierane przez użytkownika powinny być graficzną reprezentacją danych przetwarzanych w bazie danych. Podstawowym medium prezentacyjnym powinien być ekran monitora, gdzie informacje mogą być odbierane i analizowane przez użytkownika. Szczególnymi prezentacjami powinny być raporty, które standardowo odbierane będą przez użytkownika na papierze drukarki (plottera).

Interfejs użytkownika powinien być obsługiwany znormalizowanymi schematami obrazowania działania procedur. W praktyce oznacza to, że z punktu widzenia użytkownika każda procedura, która przetwarza dane w podobny sposób, powinna posługiwać się tymi samymi obiektami na ekranie w celu obrazowania jej działania.

Z punktu widzenia użytkownika na ekranie monitora mogą pojawiać się następujące *obiekty do prezentacji danych*:

- okna prezentacji tablic,
- pola do wprowadzania danych z informacjami opisowymi,
- pola do wyświetlania danych z informacjami opisowymi,
- pola do wprowadzania szablonów w celu wyszukiwania danych.

Podstawową formą przeglądania danych powinny być tabele prezentacji danych. Powinny umożliwiać one wyświetlanie dowolnych schematów danych (tzw. perspektyw) z różnych plików, o ile powiązane będą one relacjami. Znaczenia prezentowanych danych powinny być opisane nad tablicą tworząc nagłówki kolumn. Na ekranie, w obrębie tablicy, powinien znajdować się pasek w innym kolorze, który zwykle określać się terminem „**PODŚWIETLENIE**”. Powinien wskazywać ono rząd (rekord) danych, które mogą podlegać przetwarzaniu. W tablicy wyświetlane powinno być tyle rzędów danych, ile się zmieści. Przemieszczanie kolejnych porcji (rekordów) danych wymuszane powinno być przesuwaniem podświetlenia, co realizować powinny klawisze sterujące na klawiaturze. U dołu lub/i z boku tablicy powinny pojawić się wskaźniki sygnalizujące możliwy kierunek przemieszczania w niej danych - poziomy lub pionowy. Wskaźniki te powinny pokazywać jednocześnie względną pozycję podświetlenia w zbiorze prezentowanych danych.

Obsługa wprowadzania danych przez użytkownika powinna być jednolita w całym systemie. Wprowadzanie danych powinno obejmować ich dopisywanie, zmianę i usuwanie. Pole, w którym użytkownik będzie dokonywał operacji wprowadzania wyświetlone powinno być w innym kolorze niż oto-

czenie, w polu pojawiać się powinna dotychczasowa wartość edytowanej danej oraz kursor, przy pomocy którego można wprowadzać kolejne znaki z klawiatury.

Niektóre pola przeznaczone do wprowadzania danych powinny być uzupełnione symbolem „>”. Oznaczać to powinno, że wprowadzane do pola wartości będą podlegać ścisłej kontroli. W wypadku wprowadzenia nieprawidłowej danej wywoływana powinna być tablica danych, z której użytkownik może wybrać daną prawidłową.

Niektóre pola powinny mieć częściowo lub całkowicie zablokowaną możliwość wprowadzania danych, czego powodem jest zagrożenie zaburzenia integralności danych. Pola te zatem powinny wyświetlać jedynie wartości, które mogą być potrzebne użytkownikowi.

Wyszukiwanie danych realizowane powinno być dwoma sposobami:

Pierwszy sposób powinien polegać na stosowaniu pomocniczych tablic wyboru w celu selekcji danych w tablicy głównej. Pojemność danych może być dzięki temu zawężona do takiej ich ilości, której skontrolowanie nie sprawia trudności.

Drugi sposób powinien polegać na wykorzystaniu mechanizmu o nazwie „LOKATOR”. Lokator jest polem na ekranie, do którego wprowadza się szablony, według którego nastąpi przeszukanie tablicy danych (może to być np. pierwsza litera szukanej nazwy). Kursor w tabeli danych zostaje ustawiony na początku grupy danych spełniających podany warunek.

4. Dostępność do danych (do informacji wyjściowych) na różnych szczeblach dowodzenia

Dostępność do danych to możliwość uzyskania wszystkich potrzebnych informacji w jak najkrótszym czasie. Jedną z ważniejszych przyczyn, dla których tworzy się bazy danych jest zwiększenie dostępności do danych w wyniku zmniejszenia czasu dostępu oraz zwiększenie asortymentu dostęp-

nych danych. Problem dostępności do danych (do informacji wyjściowych) należy ujmować wieloaspektowo.

Po pierwsze - istotny jest czas i miejsce dostępu do zbiorów informacji. Projektując bazy danych należy zapewnić do nich wielopoziomowy dostęp:

- w wojskach lądowych - dowódcom i oficerom sztabu do szczebla batalionu włącznie,

- w innych rodzajach wojsk (w siłach powietrznych, w marynarce wojennej) - dowódcom pojedynczych środków walki (samolotów, okrętów).

Po drugie - należy uwzględnić, przy uzyskanym już dostępie do bazy danych czas dostępu (zobrazowania, szukania) do określonego rodzaju informacji. Czas ten uzależniony jest jakością łącz transmisyjnych i bywa niekiedy bardzo długi⁵.

Po trzecie - ważny jest dostęp pod względem objętości informacji to znaczy czy użytkownik ma możliwość jednoczesnego dostępu do wszystkich dostępnych informacji, czy zmieszczą się one na ekranie monitora, lub czy rozdzielczość urządzeń wyjściowych umożliwi zobrazowanie wszystkich szczegółów.

Konieczne jest zatem określenie dostępności przy pomocy ww. parametrów. Należy mieć na uwadze, że jeżeli skracać będzie się czas dostępu to i liczba dostępnych informacji będzie niewielka.

5. Bezpieczeństwo informacji w bazie danych na potrzeby militarne

Bazy danych na potrzeby militarne powinny charakteryzować się dużą wiarygodnością informacji oraz odpowiednią jej ochroną przed ujawnieniem, zmianą lub zniszczeniem, tj. odpowiednim bezpieczeństwem. Bezpieczeństwo informacji jest cechą trudną do ilościowego wyrażenia i zmierzenia. Sam fakt stosowania różnych zabezpieczeń, charakterystycznych dla cywil-

nych baz danych nie stanowi o dużej wartości współczynnika bezpieczeństwa informacji.

W tej sytuacji należy zwrócić szczególną uwagę na *szyfrowanie* danych na poziomie fizycznym. Oznaczać powinno to, że teoretycznie nie będzie mogła odczytać ich osoba niepowołana przy pomocy programów narzędziowych. Mechanizm szyfrowania powinien być następujący: każda tablica danych powinna otrzymać klucz szyfrowy, który powinien szyfrować wprowadzane do niej dane. Klucz ten powinien być jednocześnie hasłem, dzięki któremu możliwy byłby dostęp do plików danych przy pomocy np. menadżera plików bazy danych. Dane przekazywane między serwerem a stacjami roboczymi powinny być również zaszyfrowane, co zwiększyć powinno ich bezpieczeństwo, a w konsekwencji doprowadzić do minimalizacji przechwyty danych podczas ich transmisji.

Przedstawiony mechanizm może ograniczyć nie tylko możliwość przechwyty danych, ale praktycznie pozbawi sensu celowe kopiowanie ich na dyskietkę w celu odczytu na komputerze zewnętrznym. Odszyfrowanie danych z około 100 plików, z których każdy posługuje się innym kluczem szyfrowym, jest wyjątkowo trudnym i czasochłonnym zadaniem. Z kolei odczytanie danych z kilku plików nie da jakiegokolwiek wyobrażenia o elementach strukturalnych i funkcjonalnych zaplanowanego systemu łączności.

Należy nadmienić, że zapewnienie poufności obowiązuje przede wszystkim ludzi, którzy mają dostęp do poufnych informacji. Komputer nie może zabronić człowiekowi przekazania dalej informacji, którą mu udostępnia, nie może więc - z natury - stanowić antidotum na całościowe rozwiązanie tego problemu. Można jednak wprowadzić pewne mechanizmy, które - przy możliwości fizycznego dostępu do urządzeń komputerowych lub sieci transmisyjnej - ograniczą lub praktycznie wyeliminują dostęp osób niepowołanych do przetwarzanych danych.

Poza wymienionymi sposobami ochrony danych użytkownicy mogą i powinni stosować inne metody, przede wszystkim organizacyjno-administracyjne np.:

- stałą kontrolę techniczną sieci komputerowej ze szczególnym uwzględnieniem nie rejestrowanych zmian w konfiguracji sieci,
- fizyczny, wysoce fachowy nadzór nad ekipami serwisowymi,
- zabezpieczenie przed awariami instalacji elektrycznej,
- stosowanie programów antywirusowych,
- archiwizowanie danych na innych nośnikach informacji (np. dyskietki, streamery),
- zgodne z przepisami przechowywanie dokumentów powstających w wyniku działania aplikacji,
- rejestrowanie osób przybywających z zewnątrz do miejsc pracy osób funkcyjnych, posługujących się systemem informatycznym lub dokumentami w nim wytwarzanymi;
- rejestrowanie drukowanych dokumentów,
- wydzielenie odpowiednich, zamkniętych pomieszczeń dla przechowywania nośników informacji i wydruków,
- zakaz wykonywania czynności serwisowych przez jedną osobę.

W bazie danych na potrzeby militarne należy przewidzieć dodatkowe zabezpieczenia. W tym celu proponuje się przyjęcie pięciostopniowej skali bezpieczeństwa informacji:

- stopień I - brak zabezpieczeń - dotyczy informacji ogólnych, ujmowanych w przepisach o ochronie tajemnicy wojskowej jako „jawne”,
- stopień II - zabezpieczenie przed przypadkowymi zdarzeniami, tj. zabezpieczenie przed nieumyślnym zniszczeniem informacji, tj. informacje określane w przepisach o ochronie tajemnicy wojskowej jako „do użytku służbowego”,
- stopień III - zabezpieczenie przed działaniem typowego użytkownika, tj. informacje określane w przepisach o ochronie tajemnicy wojskowej jako „poufne”,

- stopień IV - zabezpieczenie przed działaniem specjalisty informatyka, tj. informacje strategicznego i operacyjnego przeznaczenia, określane w przepisach o ochronie tajemnicy wojskowej jako „tajne”,

- stopień V - zabezpieczenie przed działaniem wyspecjalizowanych szpiegowskich służb informatycznych, tj. informacje strategicznego i operacyjnego przeznaczenia, określane w przepisach o ochronie tajemnicy wojskowej jako „tajne specjalnego znaczenia”.

Oczywiste jest, że uzyskanie najwyższego stopnia zabezpieczenia wymaga zastosowania specjalistycznego sprzętu komputerowego i oprogramowania.

PRZYPISY

¹ Terminem *redundancji danych* określa się sposób ich organizacji, w którym dane są niepotrzebnie powielane.

² *Regulamin walki NATO: ATP -35 B.*

³ *Ang. EPB - Intelligence Preparation of the Battlefield.*

⁴ W państwach NATO analiza terenu realizowana jest przez wyspecjalizowane komórki sztabowe już na szczeblu dywizji wykorzystujące wyspecjalizowane komputerowe systemy wspomagające proces wartościowania terenu pod względem taktyczno-ogniowym. Uwzględnia się następujące aspekty: warunki prowadzenia obserwacji optycznej i elektronicznej, możliwość prowadzenia ognia na wprost i z zakrytych stanowisk ogniowych, warunki maskowania przed obserwacją optyczną i elektroniczną, charakterystykę naturalnych przeszkód terenowych, charakterystykę wybudowanych obiektów terenowych, charakterystykę terenów kluczowych, których opanowanie pozwoli na uzyskanie przewagi nad przeciwnikiem, rejonu o dużych oraz małych możliwościach manewrowych, drogi marszu oraz korytarze manewru. W toku planowania działań wojennych wykonuje się odpowiednie oleaty IPB (*Intelligence preparation of the battlefield, Staff College, Intelligence Handbook*).

⁵ W chwili obecnej problem ten jest widoczny podczas pozyskiwania danych z sieci Internet.

ZAKOŃCZENIE

Wprowadzenie na uzbrojenie wojsk jakościowo nowych środków walki i związane z tym zmiany w sposobach prowadzenia współczesnych działań wojennych wywierają istotny wpływ na formy i metody zbierania, gromadzenia i przetwarzania informacji. Obecny rozwój technologii sprawił, że dzięki zautomatyzowanym systemom dowodzenia i kierowania środkami walki, bazujących na ciągłym i szybkim dostępie dowództw i sztabów do aktualizowanych na bieżąco informacji rozpoznawczych, - główny nacisk kładzie się na skoordynowanie i uelastycznienie działań zbrojnych. Ważną rolę w tym względzie mają do spełnienia komputerowe bazy danych. Ich przydatność w sztabach w okresie pokoju oraz w razie konieczności na polu walki staje się w obecnych czasach bezdyskusyjna. Należy dołożyć wszelkich wysiłków aby powstała ona również w SZ RP. Potrzeba ta staje się nakazem zapewnienia interoperacyjności naszych sztabów i wojsk z wojskami NATO.

Bibliografia

- [1] *Regulamin walki państw NATO ATP 35-B (ang. Land Force Tactical Doctrine)*
- [2] Ciborowski L.: *Organizacja rozpoznania w sztabach*. AON, Warszawa 1991
- [3] Ciborowski L.: *Informacyjna preparacja pola walki*. Referat w materiałach III KNTWRE'97. Wyd. WAT, Żegiestów 1997
- [4] Ciborowski L., Nowacki G.: *Walka informacyjna*. Referat w materiałach III KNTWRE'97. Wyd. WAT, Żegiestów 1997
- [5] *Encyklopedia powszechna*. Wyd. PWN, Warszawa 1983
- [6] Kopaliński W.: *Słownik wyrazów obcych i zwrotów obcojęzycznych*. Wyd. Wiedza Powszechna, Warszawa 1980,
- [7] Kwećka R., Nowak A.: *Budowa modelu systemu rozpoznania wojskowego w aspekcie organizacyjnym i informacyjnym*. Rozprawa doktorska. AON, Warszawa 1994
- [8] Janczak J.: *Wybrane problemy walki radioelektronicznej*. Wyd. WSOWŁ, Zegrze 1996
- [9] Łokociejewski M.: *Ogólne założenia rozpoznania wojskowego*. Artykuł w Zeszytach Naukowych AON nr 4, Warszawa 1996
- [10] *Leksykon techniczny*. Wyd. NT, Warszawa 1983
- [11] *Mały słownik cybernetyczny*. Wyd. Wiedza Powszechna, Warszawa 1973
- [12] *Organizacja i prowadzenie rozpoznania na szczeblach taktycznych. Zasady ogólne*. Podręcznik. ASG WP, Warszawa 1985
- [13] *Organizacja i prowadzenie rozpoznania operacyjnego*. Podręcznik. Wyd. Szt. Gen. WP, Warszawa 1981

[14] *Organizacja i prowadzenia rozpoznania radioelektronicznego*. Podręcznik. Wyd. Szt. Gen. WP, Warszawa 1979

[15] *Poradnik oficera rozpoznania radioelektronicznego wojsk OPK*. Wyd. OPK, Warszawa 1989

[14] Organizacja i prowadzenie rozpoznania radiologicznego. Warszawa 1972
 [15] Poradnik oficera rozpoznania radiologicznego wojsk. Warszawa 1983



Wyd. OPK, Warszawa 1983
 [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67] [68] [69] [70] [71] [72] [73] [74] [75] [76] [77] [78] [79] [80] [81] [82] [83] [84] [85] [86] [87] [88] [89] [90] [91] [92] [93] [94] [95] [96] [97] [98] [99] [100] [101] [102] [103] [104] [105] [106] [107] [108] [109] [110] [111] [112] [113] [114] [115] [116] [117] [118] [119] [120] [121] [122] [123] [124] [125] [126] [127] [128] [129] [130] [131] [132] [133] [134] [135] [136] [137] [138] [139] [140] [141] [142] [143] [144] [145] [146] [147] [148] [149] [150] [151] [152] [153] [154] [155] [156] [157] [158] [159] [160] [161] [162] [163] [164] [165] [166] [167] [168] [169] [170] [171] [172] [173] [174] [175] [176] [177] [178] [179] [180] [181] [182] [183] [184] [185] [186] [187] [188] [189] [190] [191] [192] [193] [194] [195] [196] [197] [198] [199] [200] [201] [202] [203] [204] [205] [206] [207] [208] [209] [210] [211] [212] [213] [214] [215] [216] [217] [218] [219] [220] [221] [222] [223] [224] [225] [226] [227] [228] [229] [230] [231] [232] [233] [234] [235] [236] [237] [238] [239] [240] [241] [242] [243] [244] [245] [246] [247] [248] [249] [250] [251] [252] [253] [254] [255] [256] [257] [258] [259] [260] [261] [262] [263] [264] [265] [266] [267] [268] [269] [270] [271] [272] [273] [274] [275] [276] [277] [278] [279] [280] [281] [282] [283] [284] [285] [286] [287] [288] [289] [290] [291] [292] [293] [294] [295] [296] [297] [298] [299] [300] [301] [302] [303] [304] [305] [306] [307] [308] [309] [310] [311] [312] [313] [314] [315] [316] [317] [318] [319] [320] [321] [322] [323] [324] [325] [326] [327] [328] [329] [330] [331] [332] [333] [334] [335] [336] [337] [338] [339] [340] [341] [342] [343] [344] [345] [346] [347] [348] [349] [350] [351] [352] [353] [354] [355] [356] [357] [358] [359] [360] [361] [362] [363] [364] [365] [366] [367] [368] [369] [370] [371] [372] [373] [374] [375] [376] [377] [378] [379] [380] [381] [382] [383] [384] [385] [386] [387] [388] [389] [390] [391] [392] [393] [394] [395] [396] [397] [398] [399] [400] [401] [402] [403] [404] [405] [406] [407] [408] [409] [410] [411] [412] [413] [414] [415] [416] [417] [418] [419] [420] [421] [422] [423] [424] [425] [426] [427] [428] [429] [430] [431] [432] [433] [434] [435] [436] [437] [438] [439] [440] [441] [442] [443] [444] [445] [446] [447] [448] [449] [450] [451] [452] [453] [454] [455] [456] [457] [458] [459] [460] [461] [462] [463] [464] [465] [466] [467] [468] [469] [470] [471] [472] [473] [474] [475] [476] [477] [478] [479] [480] [481] [482] [483] [484] [485] [486] [487] [488] [489] [490] [491] [492] [493] [494] [495] [496] [497] [498] [499] [500] [501] [502] [503] [504] [505] [506] [507] [508] [509] [510] [511] [512] [513] [514] [515] [516] [517] [518] [519] [520] [521] [522] [523] [524] [525] [526] [527] [528] [529] [530] [531] [532] [533] [534] [535] [536] [537] [538] [539] [540] [541] [542] [543] [544] [545] [546] [547] [548] [549] [550] [551] [552] [553] [554] [555] [556] [557] [558] [559] [560] [561] [562] [563] [564] [565] [566] [567] [568] [569] [570] [571] [572] [573] [574] [575] [576] [577] [578] [579] [580] [581] [582] [583] [584] [585] [586] [587] [588] [589] [590] [591] [592] [593] [594] [595] [596] [597] [598] [599] [600] [601] [602] [603] [604] [605] [606] [607] [608] [609] [610] [611] [612] [613] [614] [615] [616] [617] [618] [619] [620] [621] [622] [623] [624] [625] [626] [627] [628] [629] [630] [631] [632] [633] [634] [635] [636] [637] [638] [639] [640] [641] [642] [643] [644] [645] [646] [647] [648] [649] [650] [651] [652] [653] [654] [655] [656] [657] [658] [659] [660] [661] [662] [663] [664] [665] [666] [667] [668] [669] [670] [671] [672] [673] [674] [675] [676] [677] [678] [679] [680] [681] [682] [683] [684] [685] [686] [687] [688] [689] [690] [691] [692] [693] [694] [695] [696] [697] [698] [699] [700] [701] [702] [703] [704] [705] [706] [707] [708] [709] [710] [711] [712] [713] [714] [715] [716] [717] [718] [719] [720] [721] [722] [723] [724] [725] [726] [727] [728] [729] [730] [731] [732] [733] [734] [735] [736] [737] [738] [739] [740] [741] [742] [743] [744] [745] [746] [747] [748] [749] [750] [751] [752] [753] [754] [755] [756] [757] [758] [759] [760] [761] [762] [763] [764] [765] [766] [767] [768] [769] [770] [771] [772] [773] [774] [775] [776] [777] [778] [779] [780] [781] [782] [783] [784] [785] [786] [787] [788] [789] [790] [791] [792] [793] [794] [795] [796] [797] [798] [799] [800] [801] [802] [803] [804] [805] [806] [807] [808] [809] [810] [811] [812] [813] [814] [815] [816] [817] [818] [819] [820] [821] [822] [823] [824] [825] [826] [827] [828] [829] [830] [831] [832] [833] [834] [835] [836] [837] [838] [839] [840] [841] [842] [843] [844] [845] [846] [847] [848] [849] [850] [851] [852] [853] [854] [855] [856] [857] [858] [859] [860] [861] [862] [863] [864] [865] [866] [867] [868] [869] [870] [871] [872] [873] [874] [875] [876] [877] [878] [879] [880] [881] [882] [883] [884] [885] [886] [887] [888] [889] [890] [891] [892] [893] [894] [895] [896] [897] [898] [899] [900] [901] [902] [903] [904] [905] [906] [907] [908] [909] [910] [911] [912] [913] [914] [915] [916] [917] [918] [919] [920] [921] [922] [923] [924] [925] [926] [927] [928] [929] [930] [931] [932] [933] [934] [935] [936] [937] [938] [939] [940] [941] [942] [943] [944] [945] [946] [947] [948] [949] [950] [951] [952] [953] [954] [955] [956] [957] [958] [959] [960] [961] [962] [963] [964] [965] [966] [967] [968] [969] [970] [971] [972] [973] [974] [975] [976] [977] [978] [979] [980] [981] [982] [983] [984] [985] [986] [987] [988] [989] [990] [991] [992] [993] [994] [995] [996] [997] [998] [999] [1000]