AKADEMIA OBRONY NARODOWEJ

AON 5341/2001

Ppłk dr inż. Gabriel NOWACKI
Mjr dr inż. Waldemar SCHEFFS
Mjr mgr inż. Wiesław BŁAŻEJCZYK

ZAKŁÓCANIE INFORMACYJNE W WOJSKACH LĄDOWYCH

WARSZAWA 2001

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

AON 5341/2001

Ppłk dr inż. Gabriel NOWACKI
Mjr dr inż. Waldemar SCHEFFS
Mjr mgr inż. Wiesław BŁAŻEJCZYK

ZAKŁÓCANIE INFORMACYJNE W WOJSKACH LĄDOWYCH

Studium teoretyczne

WARSZAWA **2001**

Powielenie i oprawa: Akademia Obrony Narodowej – Wydział Wydawniczy, zam. nr 1120/2001

WPROWADZENIE

Po wojnie w rejonie Zatoki Perskiej zaczęto przywiązywać dużą wagę do nowych „środków przemocy", których zastosowanie w czasie wojny – i nie tylko – okazuje się wysoce skuteczne z punktu widzenia osiągnięcia zwycięstwa nad przeciwnikiem. Środki te nazywane są często „nieśmiercionośnym" arsenałem broni. Środki te powstały w wyniku notowanego w ostatnim czterdziestoleciu gwałtownego rozwoju elektroniki i nowoczesnych technik przekazywania danych. Sytuacja ta znalazła swoje odzwierciedlenie zarówno w architekturze jak i w stosowanych środkach walki. Do procesów rozpoznania, systemów uzbrojenia oraz do procedur planowania, organizowania i nadzorowania walki zbrojnej wprowadzono elektronikę. Wyposażenie wojsk wzbogacono w nowe rodzaje amunicji o cechach „inteligentnych". Udoskonalono środki przenoszenia broni oraz *de facto* zwiększono ich zasięg i skuteczność działania. Skrócono w sposób zasadniczy czas reakcji ogniowej i zwielokrotniono stopień manewrowości wojsk.

Znacząca miejsce w tym zakresie spełnia mikroelektronika. Jej rola i znaczenie nieustannie wzrasta, a dalszy rozwój będzie miał duży wpływ na unowocześnianie środków walki oraz na charakter, przebieg i rezultat prowadzonych działań bojowych.

Środki elektroniczne stają się swoistą „bronią", która umiejętnie wykorzystana może zdecydować o sukcesie na polu walki. Minione wojny i konflikty lokalne wykazały, że gdy technika elektroniczna decyduje o efektywności użycia środków walki i działania wojsk, w głównej sferze zainteresowania walczących stron znalazła się efektywność oddziaływania na nią, w celu obniżenia jej sprawności.

Oddziałując bezpośrednio na systemy informacyjne każda z walczących stron stara się zmniejszyć zdolność bojową strony przeciwnej, efektywność wykorzystania przez nią uzbrojenia, a tym samym obniżyć skuteczność działania. Ma to bezpośredni wpływ na jednoczesne poszukiwanie jak najlepszych rozwiązań organizacyjnych i technicznych mających na celu zabezpieczenie własnych systemy informacyjne przed oddziaływaniem coraz doskonalszych środków walki informacyjnej strony przeciwnej. Jest to jedna z ważniejszych płaszczyzn trwającego we współczesnych armiach wyścigu technologicznego. Kto go wygra zapewni sobie przewagę na przyszłym polu walki.

Potencjalny przeciwnik może zastosować narzędzia zakłócania informacyjnego, do których można zaliczyć: urządzenia wytwarzające impuls elektromagnetyczny[1] (wielkości walizki) projektowane w Laboratorium Narodowym Stanów Zjednoczonych w Los Alamos oraz specjalne „wirusy" „umieszczane" w systemach broni potencjalnego przeciwnika, powodujące ich dezorganizację i nieefektywność. Planuje się także wykorzystanie specjalnego rodzaju mikrobów, które mogą zniszczyć układy elektroniczne i izolacyjne w komputerach. Infradźwięki o częstotliwości 16 Hz używane przeciwko sile żywej powodują wzbudzanie wibracji w organach wewnętrznych, powstanie nudności, dolegliwości sercowych i zaburzeń równowagi. Zaletą tych rodzajów broni jest przede wszystkim łatwość przenikania przez struktury materii. Promienniki równokierunkowe (izotropowe) występujące w formie amunicji artyleryjskiej lub lotniczej, wytwarzają promieniowanie elektromagnetyczne o własnościach zbliżonych do laserowego. Ich działanie polega na krótkotrwałej emisji promieniowania elektromagnetycznego w zakresie od podczerwieni do nadfioletu w celu porażenia czujników, dezorientowania pilotów, czy nawet oślepienia żołnierzy. Wzrost roli czynników nieśmiercionośnych jest trendem rozwojowym, świadczącym o nowych możliwościach, jakie otwierają się przed pozazbrojnymi formami walki w działaniach wojennych.

Problematyka ta jest *sensu proprio* dostrzegana w wielu państwach na świecie. Najwyższą jednak rangę nadano jej w Stanach Zjednoczonych. W sierpniu 1996 r. Dowództwo Szkolenia i Doktryn (TRADOC — Trainining and Doctrine Command) opublikowało „Regulamin walki SL USA" (FM—100—6) zawierający doktrynę (koncepcję) operacji informacyjnych.

W kwietniu 1999 r. została przyjęta nowa Koncepcja Strategiczna NATO, w której podkreśla się znaczenie technologii informacyjnych na współczesnym polu walki. W części II, w punkcie „wyzwania i ryzyka polityki bezpieczeństwa", stwierdza się, że państwowi i niepaństwowi przeciwnicy mogą wykorzystywać wzrastające przez Sojusz zastosowanie systemów elektronicznych do prowadzenia operacji informacyjnych, których celem może być przeciwdziałanie wykorzystaniu tych systemów.

---

[1] Impuls elektromagnetyczny - impuls fal radiowych o czasie trwania rzędu tysięcznych części sekundy. Charakteryzuje się bardzo dużą amplitudą zmian natężenia pola elektrycznego i magnetycznego. Powoduje on zaindukowanie się prądów i napięć w obwodach urządzeń elektronicznych, co jest przyczyną niszczenia niektórych elementów półprzewodnikowych na skutek przeciążeń. Zasadniczymi obiektami oddziaływania impulsu elektromagnetycznego są środki radioelektroniczne.

W związku z nową Koncepcją Strategiczną NATO, Rosja opracowała nową Doktrynę Wojenną, w której w większym niż dotychczas zakresie podkreślono znaczenie bezpieczeństwa informacyjnego, którego jednym z zasadniczych elementów ma być prowadzenie wielopłaszczyznowej walki informacyjnej.

W tym kontekście treść poznawcza pracy została podporządkowana osiągnięciu głównego celu: *Zdefiniować i uporządkować podstawowe pojęcia zakłócania informacyjnego oraz określić metodykę cyklu decyzyjnego.*

Osiągnięcie głównego celu badań nastąpiło na drodze rozwiązania *głównego problemu badawczego*:

Na czym polega zakłócanie informacyjne i jak przebiega cykl decyzyjny jego przygotowania?

Z głównego problemu badawczego wyniknęły następujące *problemy szczegółowe*:

1. *Jakie są ogólne założenia zakłócania informacyjnego?*
2. *Jakie są rodzaje zakłócania informacyjnego?*
3. *Jak przebiega cykl decyzyjny przy planowaniu zakłócania informacyjnego?*

Praca składa się z trzech rozdziałów i zawiera wyniki badań, ujęte w formie teorii, oraz propozycje przyszłościowych rozwiązań dotyczących przygotowania i prowadzenia zakłócania informacyjnego.

W rozdziale pierwszym przedstawiono istotę i ogólne założenia zakłócania informacyjnego.

Zasadniczą treścią rozdziału drugiego jest klasyfikacja zakłócania informacyjnego.

W rozdziale trzecim scharakteryzowano ogólne zasady przygotowania zakłócania informacyjnego.

1. OGÓLNE ZAŁOŻENIA ZAKŁÓCANIA INFORMACYJNEGO

1.1. Istota zakłócania informacyjnego

Każda instytucja, organizacja, a także osoba fizyczna dysponuje różnymi informacjami, które są niezbędne do jej normalnego funkcjonowania. Należy zgodzić się z tezą, że informacja w każdym organizmie społecznym lub gospodarczym odgrywa taką samą rolę, jak krew w organizmie żywym[2], a obieg informacji można porównać do krwiobiegu. Rozszerzając to porównanie można stwierdzić, że podobnie jak organizm żywy umiera na skutek wykrwawienia lub zatrucia krwi, organizm gospodarczy lub społeczny może niedomagać lub zginąć, jeśli umożliwiająca mu funkcjonowanie informacja ulegnie zniszczeniu, przekłamaniu lub zostanie wykradziona, albo jeśli obieg tej informacji ulegnie zakłóceniu[3].

Zakłócanie informacyjne to wszelkie oddziaływanie na otoczenie (obszar zdobywania informacji — rejestratory danych, sygnały będące nośnikami informacji, zbiory danych, programy, biblioteki itp., które doprowadza do zaniku informacji pożądanej, jej deformacji lub wytwarzania informacji nieprawdziwych i przez to wpływa negatywnie na inne procesy pola walki.

Zakłócanie informacyjne jest jednym z elementów walki informacyjnej obok zdobywania informacji (rozpoznania) i obrony informacyjnej. Informacje z rozpoznania wpływają na precyzję rażenia, a zakłócanie i obrona informacyjna — na wyprzedzenie przeciwnika w użyciu celnego ognia. Środki i technologie informacyjne, stosowane w walce zbrojnej, mogą w znaczny sposób wprowadzić w błąd przeciwnika co do posiadanych sił i prowadzonych działań, zwiększając tym samym zdolność bojową wojsk własnych. Dowódcy zatem powinni mieć stworzone warunki do szybkiego podejmowania decyzji oraz sprawnego i skrytego wdrażania ich do realizacji.

---

[2]A. Z. Idźkiewicz: *„Ochrona informacji w procesie przetwarzania"*, Państwowe Wydawnictwo Ekonomiczne, Warszawa 1979, s.7.

[3]Zakłócenie to naruszenie ustalonego porządku, biegu spraw, dezorganizacja; niepożądany sygnał występujący jednocześnie z sygnałem użytecznym i pochodzący z innego źródła niż źródło sygnału użytecznego. *Leksykon techniczny*, op. cit., s. 624.

Zakłócanie informacyjne na polu walki prowadzi się w celu obniżenia efektywności funkcjonalnej systemu informacyjno-sterującego przeciwnika. Polega ono na zakłócaniu procesów rozpoznawczych przeciwnika, jego procesów dowodzenia i kierowania uzbrojeniem. Elementy zakłócania informacyjnego powinny koncentrować się na działalności umożliwiającej racjonalne modelowanie procesu przygotowywania wojsk do realizacji zadań bojowych w okresie zaistnienia konfliktu zbrojnego czy też wojny. Wiadomym jest, że szczególna rola w tym zakresie przypada rozpoznaniu. Znajomość planów przeciwnika stanowi inherentny element procesu przygotowania i prowadzenia zakłócania informacyjnego. Podmiot działań, wykorzystując wszelkie elementy rozpoznawcze zintegrowanego systemu rozpoznania sił zbrojnych zdobywając niezbędne dane dotyczące planowanych działań zbrojnych i niezbrojnych przeciwnika oraz realizowanych przez jego elementy rozpoznawcze przedsięwzięć, może przekazać przeciwnikowi specjalnie spreparowane dane, które spowodują podjęcie niekorzystnych dla niego decyzji oraz będą dla niego stanowić przyczynek podjęcia wymuszonych działań.

Zakłócanie informacyjne powinno być ukierunkowane na zwiększanie entropii informacyjnej u przeciwnika poprzez modyfikację komunikatów i destrukcję wszelkiej postaci nośników danych w systemach informacyjno sterujących.

Istotą zakłócania informacyjnego jest maksymalne ograniczenie napływu danych prawdziwych z jednoczesną dystrybucją danych fałszywych i powodowanie przez to zniekształcenia postrzeganego przez przeciwnika obrazu pola walki. Tak wytworzony fałszywy obraz będzie miał bezpośrednie przełożenie na podejmowanie decyzji oraz działanie środków ogniowych, wykonanie manewru, zaopatrzenie materiałowo-techniczne itp.

1.2. Zasady prowadzenia zakłócania informacyjnego

System zakłócania informacyjnego spełnia dwie zasadnicze funkcje. Jedną z nich jest szeroko rozumiana pozoracja (wprowadzanie w błąd przeciwnika). Jej celem jest udostępnienie przeciwnikowi takich postaci danych, które po przetworzeniu będą przedstawiać sytuację nierealną, nie mającą nic wspólnego z rzeczywistością. Sposoby i narzędzia wykorzystywane w prowadzeniu tych działań są bardzo złożone. Dlatego też należy wybierać takie formy działań, które stwarzać będą symptomy rzeczywistych sytuacji na polu walki. Muszą one być zsynchronizowane z obroną informacyjną i rozpoznaną już przez przeciwnika częścią działań i planów rzeczywistych. Oderwane

od siebie elementy działań pozorujących nie tylko nie wprowadzają przeciwnika w błąd, ale wręcz demaskują, że takie są prowadzone, co zmniejsza entropię informacyjną[4] i zwiększa stan uporządkowania wiedzy o otoczeniu.

Drugą funkcją jest fizyczna destrukcja nośników danych. Procedura destrukcyjnego oddziaływania na tor zdobywania danych (system rozpoznania) realizowana jest z zamysłem uniemożliwienia przeciwnikowi wykorzystania tych postaci danych, do których udało mu się zdobyć dostęp mimo stosowania obrony informacyjnej. Wykorzystując różne techniki energetycznego oddziaływani można niszczyć i czasowo uniemożliwiać pracę źródłom zdobywania danych, przetwornikom danych i sygnałów oraz układom odbierającym. Można także zmieniać strukturę nośników danych i nośników sygnałów, niszcząc tym samym lub zniekształcając zawarty w nich potencjał informacyjny. Zarówno jeden jak i drugi sposób działania zwiększa w torze zdobywania danych stan nieuporządkowania wiedzy o kooperancie negatywnym, tzn. zwiększa entropię informacyjną.

Proces zakłócania jest procesem zróżnicowanym zarówno w zakresie obszarów oddziaływania, jak i metod postępowania.

W walce zbrojnej proces zakłócania informacyjnego powinien obejmować czas przygotowania się do walki i okres jej prowadzenia. Czas przygotowania się do walki jest zwykle stosunkowo długi i charakteryzuje się niewielką dynamiką procesów informacyjnych. Okres walki cechuje się natomiast znacznie większą dynamiką, dlatego też zakłócanie informacyjne musi w tym wypadku musi być bardziej elastyczne.

Podczas realizacji zakłócania informacyjnego należy zawsze uwzględniać prowadzenie rozpoznania i obrony informacyjnej. Zdobywanie informacji jest w stosunku do zakłócania procesem pierwotnym. Procesy informacyjne są procesami bardzo skomplikowanymi, a ich zakłócanie może być spowodowane nie tylko przez działalność celowo zorganizowaną, ale może również wynikać z niedoskonałości poszczególnych układów. Zakłócanie celowe może być realizowane w każdym ogniwie procesu informacyjnego, stosownie do potrzeb i możliwości technicznych oraz

[4] Entropia informacyjna - miara nieokreśloności zdarzeń stanowiących źródła informacji przy określonym stanie niewiedzy o tych zjawiskach. Jest ona ściśle związana z ilością informacji prawdziwej zawartej w odebranym komunikacie, gdyż za miarę uzyskanej tą drogą przez odbiorcę ilości informacji przyjmuje się stopień zmniejszenia nieokreśloności. Dlatego entropia informacyjna, którą odbiorca przypisuje określonemu zjawisku, jest zawsze co najmniej równa entropii fizycznej tego zjawiska lub większej od niej. Tylko w przypadku, gdy odbiorca jest całkowicie poinformowany o statystycznej naturze zjawiska, wartość entropii fizycznej i informacyjnej pokrywają się (entropia fizyczna, to entropia będąca funkcją aktualnego stanu fizycznego określonego obiektu materialnego przy założeniu, że stan ten jest traktowany jako zmienna losowa).

dostępnego obszaru oddziaływania zakłócającego. Warunkiem nie tylko skuteczności ale i możliwości zakłócania jest wcześniejsze zdobycie niezbędnych danych o potencjalnym przeciwniku, terenie i panujących tam warunkach. Z kolei na polu walki i w jego otoczeniu w toku działań obiekty podlegające rozpoznaniu mogą zostać przez przeciwnika zamaskowane, dla szeroko rozumianych czujników informacyjnych pozornie obiekty te nie będą istniały. Ponadto w rozpoznawanej przestrzeni mogą zostać rozmieszczone obiekty fałszywe, które wysyłają identyczne sygnały jak prawdziwe. Może to spowodować, że do systemów logicznych (w tym dowódców i sztabów) napłyną dane niepełne lub niewłaściwie odzwierciedlające sytuację, wówczas błędnie mogą być podejmowane decyzje odnośnie zastosowania zakłócania informacyjnego.

W warunkach walki zbrojnej potok danych przetwarzany jest przez pojedyncze układy logiczne, takie jak: mózg człowieka czy komputer oraz przez układy złożone, jak sztaby i zespoły analityczne. Przy wykorzystywaniu sztucznych układów logicznych, istotny wpływ na ich funkcjonowanie mają programy, według których pracują. W wypadku czynnika ludzkiego — sprawność psychofizyczna.

Zakłócanie informacyjne jest prowadzone przy zastosowaniu odpowiedniej techniki i metod postępowania. Najbardziej uniwersalnymi i skutecznymi są środki niszczenia, jednak mając na uwadze realia pola walki nie wszystko można będzie zniszczyć. Nie bez znaczenia są także koszty, które powinny być minimalizowane stosownie do osiąganych rezultatów. Niezbędnym jest więc posiadanie oprócz środków niszczenia również innych umożliwiających skuteczne prowadzenie zakłócania informacyjnego. Okoliczności te dyktują potrzebę posiadania środków maskowania, pozorowania, zakłócania elektromagnetycznego (aktywnego i pasywnego), środków umożliwiających ingerencję w systemy komputerowe i banki danych. Ilość oraz rodzaj czy proporcje tych środków należy dostosować do istniejących realiów pola walki. Metody przygotowania działań w zakresie zakłócania informacyjnego oraz metody użycia sił i środków należy wprowadzać i rozwijać stosownie do zmian zachodzących w środkach technicznych i metodach związanych z procesami informacyjno-sterującymi występującymi w walce zbrojnej. Należy kształtować właściwe proporcje posiadania sił i środków stosownie do istniejących i potencjalnych zagrożeń. Każda armia dysponuje określonym potencjałem bojowym[5], charakteryzującym się

[5] Określenie potencjał bojowy użyte jest w rozumieniu, że są to siły i środki przeznaczone do prowadzenia walki zbrojnej, której istotą jest rażenie przeciwnika.

jednoznacznymi wskaźnikami ilościowymi i jakościowymi. Z niego wynikają konkretne potrzeby w zakresie zakłócania, konieczne do uwzględniania w planowaniu działań, kierowaniu ruchem wojsk i sterowaniu środkami rażenia. Pomiędzy stanem posiadania a potrzebami zakłócania zachodzi związek zależności polegający na tym, że mniej doskonały potencjał bojowy wymaga bardziej doskonałego systemu zakłócania informacyjnego, który swoim działaniem może zdołać skompensować niedoskonałości manewrowe i ogniowe posiadanych środków bojowych.

Potencjał materialny zakłócania informacyjnego oraz sposoby jego prowadzenia muszą być kompatybilne do układu odniesienia (potencjalnego przeciwnika), charakteryzującego się zawsze takim, a nie innym uzbrojeniem i takimi, a nie innymi wzorcami wykorzystywania wojsk w walce. W tym zakresie najbardziej istotna jest jego technika i zasady prowadzenia walki informacyjnej. Dlatego też za odniesienie trzeba przyjmować stan materialny w otaczającej przestrzeni geometrycznej, niezależnie od tego czy panujące tam nastroje są nam przychylne czy też nie. Z drugiej zaś strony należy uwzględniać ograniczenia wynikające z istniejących założeń doktrynalnych. Zarówno procedury i techniki zakłócania informacyjnego jak również potrzeba ich ciągłego dostosowywania do zmieniających się warunków nie są aktualnie w pełni dostrzegane. Najczęściej problematyka ta identyfikowana jest tylko z aktywnym zakłócaniem technicznych torów transmisji danych i z dość prostymi formami generowania danych fałszywych. Zakłócanie informacyjne można jednak rozumieć i prowadzić w znacznie szerszym zakresie. Bowiem wszystko to co związane jest ze zwiększaniem entropii informacyjnej u przeciwnika jest z natury rzeczy zakłócaniem informacyjnym. Przy takim rozumieniu istoty zjawiska, do zakłócania informacyjnego można również zaliczyć niektóre formy maskowania (zarówno bezpośredniego jak i operacyjnego) i pozorowania. Wiele również można uczynić w zakresie zakłócania informacyjnego drogą destrukcyjnego oddziaływania na procedury przetwarzania i dystrybucji danych. Bardzo skutecznymi środkami mogą się tu okazać rozwiązania ulokowane w technice impulsowej, w sferze infradźwiękowej i w psychotronice.

1) *W procesie zakłócania informacyjnego niezwykle istotnym czynnikiem jest czas. Zakłócanie, aby spełniało zadania powinno w aspekcie czasu reakcji ciągle wyprzedzać funkcjonowanie procesów informacyjnych. Sprowadza się to do tego, że maskowanie i pozoracja w obszarze zbierania danych powinny zostać wykonane przed penetracją tego obszaru przez czujniki rozpoznawcze. Zakłócanie czujników należy realizować od chwili rozpoczęcia przez nie pracy. Sygnały w środkach*

transmisji danych należy zakłócać przed dotarciem do adresata. Niszczenie powinno być realizowane zaraz po wykryciu obiektu pracującego w systemie informacyjno - sterującym.

2) *W celu umożliwienia spełniania powyższych warunków należy dążyć do posiadania sprzętu maksymalnie ułatwiającego takie zachowanie. Ponadto proces zakłócania należy rozłożyć w czasie w taki sposób, aby u przeciwnika występowały różne stany, m.in. takie jak: okresowy zanik dopływu danych, opóźnienia lub brak zakłóceń, co w konsekwencji również może prowadzić do dezorganizacji procesów informacyjnych przy mniejszych reżimach czasu reakcji.*
3) *Skuteczność zakłócania jest uwarunkowana wieloma czynnikami, do których, miedzy innymi, należy zaliczyć:*
   — *posiadanie wiedzy o stanie i funkcjonowaniu procesów informacyjnych u przeciwnika, o wykorzystywanej przez niego technice, metodach zdobywania i gromadzenia informacji, o dowodzeniu itp. Wiedza ta jest niezbędna głównie po to, aby móc przygotować się pod względem technicznym, metodologicznym i organizacyjnym do realizacji procesu zakłócania;*
   — *dysponowanie środkami rozpoznania (w tym głównie środkami rozpoznania elektromagnetycznego), które będą zdobywały dane o funkcjonowaniu systemów informacyjnych przeciwnika, ich stanie oraz przebiegu procesów informacyjnych, w czasie niezbędnym na uruchomienie procesów zakłócających. Bez odpowiedniego poziomu informacji o pracy tych systemów i środków nie można podejmować przemyślanych i skutecznych zadań zakłócających, chociaż pewne działania profilaktyczne można podejmować na podstawie wiedzy zgromadzonej w bankach danych;*
   — *wyznaczenie i przygotowanie określonych organów, odpowiedzialnych za przygotowanie i prowadzenie procesu zakłócania. Związana jest z tym cała procedura przygotowania sztabów i wojsk do prowadzenia walki informacyjnej;*
   — *dysponowanie siłami i środkami technicznymi oraz materiałowymi, stosownie do stawianych przed zakłócaniem zadań. Możliwości techniczne tych środków powinny umożliwić wykonanie zadań, a zatem nie powinny odbiegać jakością od środków przeciwnika.*
4) *System informacyjny przeciwnika, który podlega zakłócaniu zmienia się poprzez eliminowanie lub dezorganizację poszczególnych jego ogniw oraz poprzez*

dokonywanie wewnętrznych zmian uodparniających go na oddziaływanie środków zakłócających. Wraz z tym zmieniają się warunki działania sił i środków na polu walki. Jest to proces dynamiczny przebiegający z różnym natężeniem w poszczególnych systemach. Procesowi temu powinno odpowiadać w działaniach zakłócających poszukiwanie optymalnych i skutecznych środków i metod postępowania. W takim działaniu należy unikać szablonów, wykorzystywać teren, istniejące warunki taktyczne i operacyjne. Należy dążyć do uzyskania zaskoczenia zarówno w obszarze jak i skali działania.

5) *Procesy informacyjne są nieodzowne w prowadzeniu walki zbrojnej, a zatem zakłócanie ich u przeciwnika prowadzi do obniżenia efektywności jego działań.*
6) *Pomimo że zakłócanie informacyjne może być realizowane w wielu punktach, powinno być postrzegane jako jeden obszar działania, jednolicie planowany pod kątem sposobu rozegrania walki przez dowódcę. Realizatorami zadań są wszyscy uczestnicy walki zbrojnej.*
7) *Procesy informacyjne, we współczesnej walce zbrojnej, w zdecydowanej większości są realizowane za pomocą środków elektronicznych, zatem spektrum elektromagnetyczne należy uznać za najważniejszy obszar w procesie zakłócania.*

Zakłócanie informacyjne powinno być: kompleksowe, celowe, wiarygodne, nieszablonowe, ciągłe, skryte, terminowe i elastyczne.

Kompleksowość przedsięwzięć odnosi się do stosowania jak najszerszego spektrum środków zakłócania (charakterystycznych dla określonego środowiska: elektromagnetycznego, akustycznego, magnetycznego, elektrycznego, chemicznego) z uwzględnieniem wszystkich rodzajów sił zbrojnych i instytucji cywilnych oraz sił paramilitarnych w strefie prowadzonych działań bojowych. Warunek kompleksowości dyktowany jest związkami funkcjonalnymi istniejącymi pomiędzy poszczególnymi elementami walki informacyjnej. Wszelkie działania z nią związane zawsze w finale sprowadzają się do jednego wspólnego celu - stwarzania sytuacji utrudniających przeciwnikowi: podejmowanie trafnych decyzji, wykonywanie sprawnych ruchów wojskami i precyzyjnych uderzeń ogniowych. Innymi słowy, ukierunkowane są na dezorientowanie przeciwnika w sytuacji pola walki, komplikowanie jego działań i w efekcie tego, zmuszanie go do podejmowania błędnych decyzji np. prowadzenia ognia do celów nie istniejących lub pustych miejsc. Dlatego też przedsięwzięcia z tym związane muszą być realizowane kompleksowo i według jednolitej koncepcji, ściśle

zsynchronizowanej z rzeczywistym i pozorowanym działaniem wojsk własnych oraz z ich maskowaniem. Wydaje się zatem, że najlepszym rozwiązaniem byłoby, aby cały potencjał zakłócania informacyjnego podporządkowany był tylko jednemu kierownictwu.

Celowość polega na ścisłej zgodności przedsięwzięć zakłócania informacyjnego z prowadzonymi działaniami bojowymi według zasady logicznego ciągu zdarzeń. Innymi słowy, zakłócanie informacyjne winno mieć cel tożsamy z celem prowadzonych działań bojowych, zarówno przy użyciu środków militarnych jak i pozamilitarnych.

Wiarygodność in praxi potencjalnie wyrażać się będzie w tym, by podmiot zakłócania informacyjnego i realizowane za jego pośrednictwem przedsięwzięcia były odczytywane przez przedmiot jako prawdopodobne lub prawdziwe na tle ogólnej sytuacji polityczno - militarnej.

Nieszablonowość realizacji przedsięwzięć wydaje się konieczna i celowa. Polegać ona może na nie powtarzaniu raz zastosowanych form zakłócania informacyjnego. Podmiot powinien dążyć do sytuacji, aby podejmowane przez niego działania nie zawierały wcześniej stosowanych sposobów działania i miały charakter nowatorskich rozwiązań w celu osiągnięcia efektu synergicznego w realizowanym całokształcie działań bojowych.

Ciągłość polega na realizowaniu zadań w sposób nieprzerwany, z intensywnością dostosowaną do potrzeb operacyjnych i bojowych. Zapewnia się ją przez właściwe zaplanowanie i ciągłe utrzymywanie sił i środków zakłócania w pełnej gotowości bojowej oraz stałym współdziałaniu z innymi rodzajami wojsk i służb.

Skrytość realizacji przedsięwzięć to warunek niezbędny dla prowadzenia jakichkolwiek działań w walce zbrojnej. Wydaje się celowe, by przedsięwzięcia zakłócania informacyjnego były planowane, organizowane i realizowane przez wyznaczone siły w ścisłej tajemnicy zarówno przed przeciwnikiem, jaki i przed wojskami własnymi, z wyjątkiem osób z kręgu planującego całokształt działań bojowych.

Terminowość niesie za sobą wymóg dostarczenia przeciwnikowi spreparowanych danych w takim czasie, by mógł on zareagować ale w sposób, który umożliwi osiągnąć cel wojskom własnym. Podjęcie przedsięwzięć zakłócania informacyjnego i wsparcie ich rzeczywistymi działaniami innych sił i środków, *ex ante* doprowadzi do podjęcia przez siły przeciwnika pożądanych postaw i zachowań.

Elastyczność opiera się na zasadzie szybkiej reakcji na zachodzące zmiany i stosowaniu takich sposobów zakłócania informacyjnego, które są w danej chwili najbardziej skuteczne ze względu na zaistniałą sytuację militarną i polityczną. W tym celu konieczne wydaje się permanentne analizowanie przez wydzielone siły, skuteczności prowadzonych oddziaływań skierowanych na wojska przeciwnika i jego ludność.

2. PODSTAWOWE RODZAJE ZAKŁÓCANIA INFORMACYJNEGO

W historii wojskowości znane są przypadki, kiedy dowódcy na polu walki próbowali uzyskać potrzebne dane i dzięki ich wykorzystaniu oddziaływać na przeciwnika w taki sposób aby najbardziej efektywnie wykorzystać własne siły zbrojne. Polegało to na wprowadzaniu przeciwnika w błąd, tak aby podejmował niekorzystne dla niego decyzje w stosunku do realnej sytuacji na polu walki. Ponieważ działalność ta była głównie skierowana na percepcję decydentów, strategię tą można nazwać *zakłócaniem percepcyjnym lub inaczej bezpośrednim.*

Obecnie systemy informacyjno — sterujące charakteryzujące się centralną bazą danych, zautomatyzowanym przekazywaniem i dystrybucją danych oraz dużym zasięgiem transmisji, umożliwiają bezpośrednie przesyłanie danych od źródła do miejsca przeznaczenia, co wskazuje na ich ogromne możliwości. Jednak stosowane technologie informacyjne nie gwarantują zabezpieczenia urządzeń transmisji danych przed zniszczeniem na tyle, aby atak stał się nierealny. Dlatego też możliwy jest inny rodzaj prowadzenia walki informacyjnej, który można nazwać *zakłócaniem technicznym lub pośrednim.*

Ze względu na kryterium dostępu do danych, zakłócanie informacyjne można podzielić na (rys. 2.1.):

— bezpośrednie;

— pośrednie.

2.1. Bezpośrednie zakłócanie informacyjne

Bezpośrednie zakłócanie informacyjne to zespół przedsięwzięć polegających na zdobywaniu danych o przeciwniku i rozpowszechnianiu odpowiednich już przetworzonych treści informacyjnych w jego wojskach w celu oddziaływania na morale (postawy, zachowania) i intencje, aby podjął niekorzystną dla siebie decyzję. Do tego zakresu przedsięwzięć zalicza się:

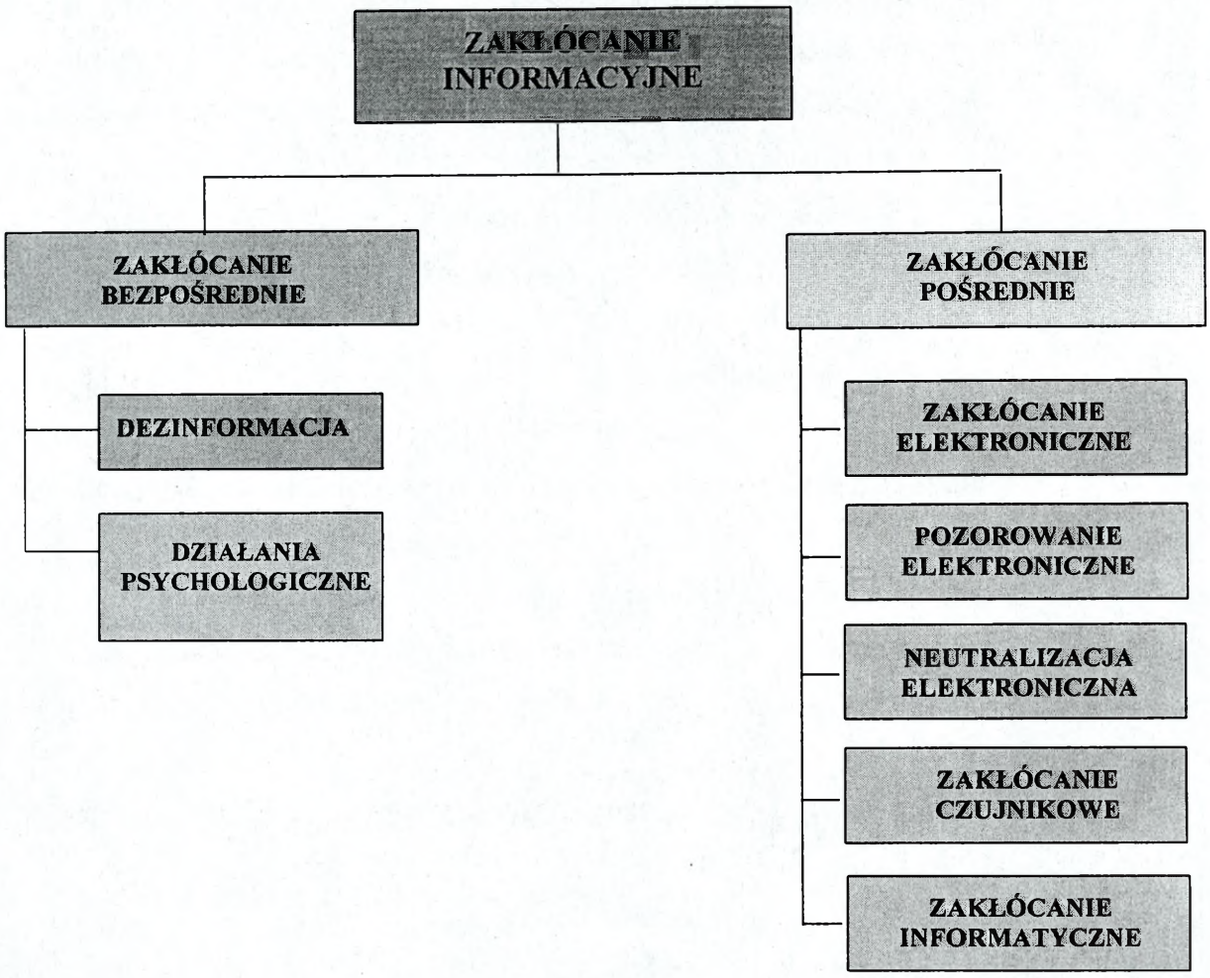
— dezinformację (wprowadzanie w błąd - Deception);

— działania psychologiczne (PSYOP — Psyhological Operations).

Dezinformacja to wprowadzanie w błąd przez podanie nieprawdziwych informacji[6]. W ujęciu wojskowym, to rozpowszechnianie nieprawdziwych wiadomości

[6] *Słownik języka polskiego*, t. II, op. cit., s.390.

i dokumentów dla wprowadzenia przeciwnika w błąd co do zamiaru, struktur organizacyjnych i prowadzenia operacji lub walki.



Rys. 2.1. Podstawowe rodzaje zakłócania informacyjnego

Uprawiana przez podmiot działań może potencjalnie stanowić *in praxi* jeden z głównych elementów wprowadzania w błąd żołnierzy i ludności cywilnej kraju przeciwnika oraz jego mniejszości narodowej. Dezinformacją będzie takie oddziaływanie podmiotu działań na wojska i ludność przeciwnika, które oparte na przekazie danych nieprawdziwych doprowadzi do wyciągnięcia takich wniosków i przekonań, jakie będą zgodne z celem prowadzonych działań. Dezinformacja *ex professo* stawia sobie za cel realizację konsekwentnego programu działania zmierzającego do zastąpienia w świadomości, w przekonaniach poglądów uznanych za niekorzystne dla podmiotu oddziaływań na takie, które są korzystne dla sił prowadzących działania bojowe.

W aspekcie stosowania dezinformacji niezbędne jest wyodrębnienie dwóch generalnych ograniczeń:

— *dezinformacja może być stosowana tylko wtedy, gdy istnieje pewna grupa — „masa krytyczna żołnierzy" lub ludności cywilnej przeciwnika już zdezorientowana lub podatna na wpływ;*

— *dezinformacji nie wolno stosować „pod prąd", to znaczy niecelowe jest przekazywanie informacji, które nie tylko, nie wywołają dezorientacji, ale nawet mogą wzbudzić sprzeciw. Dezinformacja może potencjalnie pobudzać aberracyjne trendy w celu zaognienia sytuacji w szeregach wojsk przeciwnika i jego społeczeństwie, de facto jednak potencjalnie skuteczna będzie wtedy, gdy wykorzysta już istniejące ogniska zapalne.*

Powyższe ograniczenia wypływają bezpośrednio ze specyfiki oddziaływań dezinformacyjnych, które to w swej istocie polegają nie na tym, by przedmiot uwierzył w coś, co podsuwa podmiot, lecz na zmodyfikowaniu jego postaw i zachowań.

Do form dezinformacji osobowej można zaliczyć pozorowanie i manipulację.

Pozorowanie polega na sztucznym tworzeniu „obrazu" (obiektu, czynności itp.) zbliżonego do rzeczywistego. Osiąga się je poprzez:

— tworzenie obiektów pozornych;

— pozorowanie innych form działań bojowych niż faktycznie prowadzone;

— stosowanie manewru pozornego oraz pozornych przedsięwzięć organizacyjnych;

— deformowanie obiektów rzeczywistych;

— tworzenie dowództw pozorujących istnienie nie istniejących oddziałów i związków taktycznych.

Celem działań pozornych jest okłamanie przeciwnika, czyli wprowadzenie go w błąd.

Działania pozorne należy zdefiniować jako kompleks organizacyjnych, materiałowych i praktycznych zadań, zgodnych z celem i zadaniami operacji, miejscem, czasem oraz sposobem działania wojsk, przedsięwzięć, mających na celu zmylenie przeciwnika co do przyjętego rzeczywistego zamiaru walczących sił, ich składu, stanów, prawdziwych zadań i przewidywanych przedsięwzięć w toku przygotowywania i prowadzenia operacji. Działania pozorne należą do tych czynności, które w sposób pośredni wywierają wpływ na przeciwnika. Oddziałują bowiem na wyniki jego rozpoznania jako główne źródło danych. Jeżeli zostaną uznane za działania prawdziwe, sprawią, że decyzje będą błędne, a wykorzystanie systemów uzbrojenia — niecelowe.

Chęć okłamania przeciwnika była, jest i pozostanie ważnym elementem przygotowania oraz prowadzenia walki i operacji. Będzie dowodem mistrzostwa dowódcy i jego zdolności narzucenia przeciwnikowi swej woli, przejęcia inicjatywy, zaskoczenia go, stworzenia jak najlepszych warunków własnym wojskom do osiągnięcia celu operacji. Dzięki prowadzeniu działań pozornych można osiągać wielkie sukcesy przy małych stratach stanów osobowych, niskim zużyciu materiałów i czasu. W tym sensie działania pozorne pozostaną ściśle związane z zasadami sztuki operacyjnej.

Drugą formą dezinformacji osobowej jest *manipulacja*. Termin ten nie jest jednoznaczny i trudny do zdefiniowania. Próby podejmowane na gruncie psychologii społecznej, socjologii i socjotechniki, nie dają jednoznacznych rezultatów[7]. Mówiąc o manipulacji, często *de facto* każdy człowiek otwiera usta po to tylko, by kimś manipulować. To właśnie instrumentalne podejście wydaje się być właściwe dla tego typu działań, ze względu na zadania, jakie realizuje podmiot tych oddziaływań i relacje, jakie zachodzą między podmiotem i przedmiotem tych działań. By zrozumieć istotę manipulacji, jej gnoseologiczne podstawy, celowe wydaje się rozpatrzenie tegoż pojęcia w kontekście wpływu społecznego i perswazyjnego oddziaływania na postawę i zachowanie człowieka. Każdy żołnierz, członek społeczności bezpośrednio lub pośrednio zaangażowanej w walkę zbrojną, podlega pewnemu wpływowi społecznemu. *Można wnioskować o różnego rodzaju percypowaniu wpływu manipulacji, a mianowicie:*

— *Po pierwsze — w zachowaniu osoby (lub grupy) zawarte są wyraźne wskazówki świadczące o tym, że osoba ta wywiera wpływ na inną osobę lub grupę w celu zmiany, modyfikacji postawy i zachowania.*

— *Po drugie — wskazówki świadczące o wywieranym wpływie są ukryte, lecz dostępne poznaniu osoby (grupy) będącej przedmiotem wpływu po dokonaniu przez nią odpowiedniej analizy zachowania lub intencji osoby wywierającej wpływ.*

---

[7]Maliszewski W.: *„Oddziaływanie psychologiczne w operacji obronnej"*. Rozprawa doktorska, AON, Warszawa 1998. Ponadto: M. Montana Czarnawska: *„Jak się bronić przed indoktrynacją"*, Warszawa 1997; K. Czuba: *„Media i władza"*, Warszawa 1995; G.H. Green, C.Cotter: *„Nie pozwól sobą manipulować"*, Warszawa 1997; P. Honey: *„Jak radzić sobie lepiej z ludźmi"*, Warszawa 1997; J. Kirschner: *„Manipulować – ale jak?"*, Warszawa 1994; R. Nawrat: *Manipulacja społeczna - przegląd technik i wybranych wyników badań.* W: *„Przegląd Psychologiczny"* 1/1989, s. 125 - 154; J.Reykowski: *„Osobowość a społeczne zachowanie się ludzi"*, Warszawa 1976.

— *Po trzecie, osoba (grupa) będąca przedmiotem wpływu, ani jej świadomość, nie zdaje sobie sprawy z wywieranego wpływu.*

— *Po czwarte —percepcja danych, jawnych bądź ukrytych, świadczy o tym, czy mamy do czynienia całkowicie lub częściowo z jawnymi metodami wpływu społecznego (wpływaniem na konformizm perswazją), czy też manipulacją.*

— *Po piąte — manipulacja odnosi się do trzeciego rodzaju percypowania wpływu — może być wykorzystywana jako technika wpływania na behawioralny komponent postawy*[8].

— *Po szóste — epistemologiczną istotą oddziaływania manipulacyjnego jest proces sterowania, który prowadzi do realizacji celów podmiotu działań — sprzecznych z celami i obiektywnym interesem własnych sił prowadzących działania bojowe. Innymi słowy manipulację można znaleźć tam, gdzie odpowiedni przekaz informacyjny (sterowanie) będzie modyfikował postawy i zachowania żołnierzy oraz ludności przeciwnika, tak że sterowana grupa społeczna (pododdział), nie urzeczywistni (poniecha lub zaniedba) jakichkolwiek starań ważnych dla własnej pomyślności, własnych interesów bądź celów tego, kto formalnie nią kieruje i dowodzi*[9]*. Manipulacją będą wiec takie działania, które zmuszają przedmiot do przyjmowania takich postaw i generowania zachowań, czynienia czegoś, czego przedmiot nie chce albo sobie nie życzy. Jest to wyrafinowane sterowanie świadomością przedmiotu działań przy wywoływaniu u nich wrażenia jakoby to, co czynią, wynikało z ich własnych planów i własnych wypracowanych decyzji.*

Manipulacja operuje uczuciami i wywołuje emocje. Wyznaczone siły, przekazując spreparowane dane, biorą pod uwagę to, iż działania te prowadzone są w gęstym otoczeniu społecznym, a przedmiot cierpi na tzw. głód informacyjny, są w stanie wywołać u przedmiotu szereg emocji i uczuć w celu sprowokowania określonych zachowań czynnościowych i werbalnych. Podmiot będzie w tym wypadku permanentnie dążył do uaktywnienia mechanizmu w celu ograniczenia bądź całkowitego zablokowania mechanizmów kontrolnych świadomości przedmiotu, który umożliwi narzucenie wzorców postaw i zachowań pochodzących od podmiotu.

---

[8]Por. R. Nawrat, op. cit., s.125 - 127.

[9]Por. P. Kołtunowski, op. cit., s. 180 -181.

Konkludując, pojmując emocje i ich efekt w postaci określonych postaw oraz zachowań, jako pewien proces kompensacji deficytu informacyjnego, można pokusić się o przedstawienie ich jako iloczynu motywu podjęcia określonego zachowania i różnicy danych niezbędnych do normalnego procesu decyzyjnego oraz danych posiadanych.

Najczęściej spotykanymi sposobami manipulowania procesem informacyjnym w celu kształtowania postaw i zachowań człowieka, są:

— *przekazywanie danych nieprawdziwych;*

— *preparowanie i przesyłanie do przedmiotu danych nieważnych lub mało ważnych z pominięciem najważniejszych;*

— *przekazywanie danych o dużym znaczeniu jako marginalnych;*

— *udostępnianie danych preparowanych w celu wywołania określonych interwencji;*

— *przesyłanie danych wieloznacznych, utrudniających zrozumienie;*

— *generowanie nadmiaru danych , by spowodować tzw. „chaos informacyjny".*

Pierwszy sposób polega, *exempli causa,* na podaniu przedmiotowi oddziaływań danych z gruntu nieprawdziwych, jednak takich, które w podświadomości tkwią jako możliwe do wystąpienia.

Drugi sposób odnosi się do przekazania danych skierowanych do żołnierzy wojsk przeciwnika i jego ludności na zasadzie przedstawienia rzeczywistego obrazu w krzywym zwierciadle.

Kolejna technika opiera się na założeniu, że każda postać danej, nawet sensacyjna, przekazana w dalszej kolejności całokształtu komunikatu informacyjnego staje się mniej ważną, nieznaczącą wiadomością, na którą przedmiot nie zwróci uwagi.

Czwarta technika *in praxi* może być sprowadzona do poruszania, wywoływania tzw. tematów dyżurnych. Permanentne przekazywanie danych (np. o mordowaniu ludności cywilnej) w tym wypadku może stanowić swoisty impuls do podjęcia działań interwencyjnych, to znaczy dociekania prawdy, ucieczki z pola walki i innych tego typu zachowań.

Przekazywanie danych wieloznacznych, stereotypowych może doprowadzić u ich odbiorcy (przedmiotu oddziaływań) do wytworzenia przekonania o tym, co ważne z punktu widzenia celu prowadzonych działań. Np. informacja o „pełnej izolacji strony przeciwnika w trakcie rozmów na forum ONZ" niesie za sobą treść z pewnością trafiającą do świadomości przedmiotu, że jego rząd, kraj i naród jest izolowany. Dane

o tym, że rozmowy na forum ONZ toczą się nadal, jest „rozmydlona" i *ex ante* nie dostrzegana przez przedmiot oddziaływań.

Ostatni sposób to przekazywanie danych w nadmiarze, prowadzące do „chaosu informacyjnego". Podmiot może zasypać przedmiot działań tak dużą ilością danych o faktach i zjawiskach pola walki, że spowoduje u niego brak wrażliwości na istotne i ważne wiadomości.

Jak wykazują doświadczenia z minionych konfliktów zbrojnych, szczególnie wojny w Zatoce Perskiej, dezinformacja realizowane ex professo i expedite wydają się być niezmiernie humanitarnym środkiem walki, umożliwiającym osiąganie celów politycznych i militarnych przy niewielkich kosztach rzeczowych i ludzkich. In abstracto oddziaływanie to można porównać do wysoce efektywnych systemów precyzyjnego rażenia.

Działania psychologiczne to zespół przedsięwzięć polegających na zdobywaniu danych o przeciwniku i rozpowszechnianiu odpowiednich wiadomości w jego wojskach w celu oddziaływania na postawy i zachowania żołnierzy oraz ludności strony przeciwnej. Na polu walki nazywane są często działaniami propagandowo — psychologicznymi ze względu na środki realizacji (słowo, dźwięk, obraz, gest, ruch czy światło).

Rola działań psychologicznych w walce zbrojnej polega na:

- ✓ kształtowaniu niekorzystnej sytuacji politycznej i militarnej do prowadzenia działań bojowych przez przeciwnika;
- ✓ stwarzaniu warunków mających wpływ na pomyślny przebieg działań bojowych wojsk własnych;
- ✓ bezpośrednim wspieraniu działań bojowych wojsk własnych w szczególnie sprzyjających sytuacjach.

Ich istota polega na powodowaniu negatywnych zmian w sferze psychicznej żołnierzy przeciwnika i jego ludności cywilnej, w celu ułatwienia wykonania zadań bojowych przez wojska własne. Głównym zadaniem działań psychologicznych jest osłabienie morale wojsk przeciwnika, a tym samym obniżenie jego zdolności bojowej i przez to wsparcie działań bojowych wojsk własnych.

Powodzenie zadania głównego zależy od wykonania na wszystkich szczeblach organizacyjnych szeregu zadań szczegółowych, zarówno w czasie pokoju jak i w czasie wojny.

Do zadań realizowanych w czasie pokoju należą:

- ✓ pozyskiwanie i gromadzenie danych o siłach zbrojnych państw obcych i na ich bazie, rozpoznawanie morale wojsk;
- ✓ prowadzenie prac studyjno - analitycznych w zakresie charakterystyki społeczno - demograficznej innych państw;
- ✓ poznawanie struktur działań psychologicznych innych państw oraz studiowanie ich doświadczeń;
- ✓ doskonalenie form i metod działania własnych pododdziałów działań psychologicznych;
- ✓ aktualizowanie danych o zasobach miejscowych (ośrodki RTV, punkty poligraficzne) pod kątem ich wykorzystania w ramach doraźnych świadczeń rzeczowych;
- ✓ systematyczne utrzymywanie rezerw osobowych w gotowości do prowadzenia działań psychologicznych.

Zadania realizowane w czasie wojny są między innymi następujące:

- ✓ kształtowanie i eksponowanie niekorzystnej dla przeciwnika sytuacji psychologicznej do prowadzenia działań bojowych;
- ✓ oddziaływanie nękające sferę psychiczną i system nerwowy żołnierzy przeciwnika oraz zakłócające rytm psychicznych i fizycznych czynności organizmu;
- ✓ potęgowanie zniechęcenia, poczucia stałego zagrożenia, wywołujących u żołnierzy przeciwnika stany beznadziejności, apatii i defetyzmu, osłabiające tym samym ich wolę walki;
- ✓ podrywanie zaufania do kierownictwa cywilnego i wojskowego oraz podważanie wiary w skuteczność prowadzonej wojny i możliwość osiągnięcia zwycięstwa;
- ✓ stymulowanie niezadowolenia wśród żołnierzy oraz osłabienie spoistości poszczególnych grup armii przeciwnika poprzez uwypuklanie sprzeczności i antagonizmów na tle narodowościowym, rasowym, politycznym, ekonomicznym i wyznaniowym;
- ✓ nakłanianie do zaniechania walki, wywoływanie zjawiska symulacji i osłabienia dyscypliny;
- ✓ umacnianie wpływu grup opozycyjnych w społeczeństwie przeciwnika;
- ✓ wspieranie działań bojowych wojsk własnych, poprzez oddziaływanie na zachowanie się ludności przeciwnika w rejonie walk.

Działania psychologiczne w działaniach wojennych zakładają osiągnięcie następujących celów:

- ✓ załamanie morale oraz zdolności bojowej wojsk przeciwnika;
- ✓ uodpornienie wojsk własnych i ludności, będącej w obszarze działań, na oddziaływanie informacyjno-psychologiczne sił i środków przeciwnika;
- ✓ współudział w skutecznym maskowaniu wojsk własnych.

Z analizy konfliktów zbrojnych wynika, że człowiek w dalszym ciągu będzie odgrywał dominującą rolę w walce zbrojnej. W czasie ewentualnego konfliktu zbrojnego, bez względu na jego zakres, szczególnego znaczenia nabiera czynnik psychiczny zarówno wśród uczestników walki, jak i ludności cywilnej. W warunkach dużej dynamiki działań, dążeń walczących stron do przejęcia inicjatywy, przy nagłych zmianach sytuacji i występowaniu niespodziewanych bodźców wzrokowych i słuchowych, ogromne obciążenie psychiczne i fizyczne żołnierzy będzie zjawiskiem powszechnym. Na przestrzeni dziejów stan psychiki oraz świadomość żołnierzy nigdy nie były obojętne dla wodzów i dowódców.

Wybór metod i form działań psychologicznych zależy od aktualnej sytuacji polityczno-militarnej, zadań wynikających z planów operacji, obiektów tegoż oddziaływania oraz możliwości technicznych. Należy także brać pod uwagę doświadczenia bojowe wojsk przeciwnika i efekty dotychczasowych działań psychologicznych.

W walce zbrojnej stosuje się głównie dwie metody prowadzenia działań psychologicznych – pośrednią i bezpośrednią.

Metoda pośrednia stanowi podstawowy sposób oddziaływania na wojska przeciwnika. Realizowana jest przy pomocy urządzeń technicznych, które przekształcają dane w postać odbieraną przez układ recepcyjny człowieka. Klasycznym tego przykładem może być telewizja, gdzie odbierany na wejściu sygnał elektromagnetyczny – nieodbierany bezpośrednio przez człowieka – przetwarzany jest w torze wizyjnym w konkretny obraz, a w torze fonicznym na konkretny głos, które człowiek jest już w stanie rejestrować. Ponadto metoda ta może być realizowana przy pomocy audycji radiowych oraz elektroakustycznych.

Metoda bezpośrednia stanowi pomocniczy sposób oddziaływania w odniesieniu do małych grup i pojedynczych osób. W tym wypadku oddziaływanie polega na przekazywaniu danych w formie bezpośrednio dostępnej dla człowieka, np. zawarte w paśmie promieniowania widzialnego, drgań akustycznych lub odbierane dotykowo, smakowo i przez powonienie.

Ze względu na sposób przekazu treści wyróżnia się następujące rodzaje działań psychologicznych:

1. Rozpowszechnienie materiałów drukowanych;
2. Emitowanie audycji radiowych i telewizyjnych;
3. Emisje audycji elektroakustycznych.

Ad. 1. Materiały drukowane stosuje się powszechnie w oddziaływaniu na żołnierzy oraz ludność we wszystkich rodzajach działań bojowych, niezależnie od warunków terenowych, pory dnia i roku. Zaletami materiałów drukowanych są: znaczny stopień wiarygodności, duży zasięg oraz długotrwałość oddziaływania. W działaniach psychologicznych stosuje się najczęściej następujące formy materiałów drukowanych:

— ulotki;
— materiały poglądowe;
— falsyfikaty;
— druki zwarte.

Ulotki są najczęściej stosowanym materiałem drukowanym do oddziaływania na przeciwnika. Ze względu na treść i przeznaczenie ulotki dzielą się na: informacyjne, perswazyjne oraz nakazujące.

Ulotki informacyjne zawierają odpowiednio dobrane wiadomości polityczne i wojskowe, oparte na faktach, ukazujące sytuacje z dogodnego dla nas punktu widzenia.

Ulotki perswazyjne zawierają racjonalne argumenty, wynikające z faktów ukazywanych w taki sposób, aby odbiorcy byli przekonani o słuszności wysuwanych wniosków i byli skłonni do pożądanych przez nas zachowań.

Ulotki nakazujące zawierają wezwania i polecenia dowództwa wojsk własnych do zaniechania przez przeciwnika walki lub oporu, kapitulacji i poddania się. Ze względu na czas ich przygotowania dzielą się one na standardowe i sytuacyjne.

Ulotki standardowe to odpowiednio wcześniej przygotowane druki, zawierające ogólne odezwy, przeznaczone do wielokrotnego użycia. Mogą one być stosowane w szybko zmieniającej się sytuacji taktycznej, kiedy siły działań psychologicznych nie są w stanie przygotować ulotek odpowiadających aktualnemu położeniu bojowemu wojsk.

Ulotki sytuacyjne są przygotowane bezpośrednio przed akcją i zawierają specyficzne treści, odpowiednio do konkretnej sytuacji bojowej, jakich nie uwzględniały ulotki standardowe. Przeznaczone one są do jednorazowego użytku.

Materiały poglądowe są samodzielną lub uzupełniającą formą materiałów drukowanych, charakteryzują się sugestywnością i komunikatywnością. Najczęściej mają one charakter monotematyczny i przedstawiają treści za pomocą ilustracji. Do najczęściej stosowanych materiałów poglądowych zalicza się: zdjęcia, rysunki, schematy, plany, szkice, wykresy.

Falsyfikaty należą do materiałów stosowanych najczęściej w celu dezinformowania przeciwnika oraz zakłócania funkcjonowania jego zaplecza. Opracowanie falsyfikatów i sposób ich rozpowszechniania wymagają szczegółowego przygotowania. Do najczęściej stosowanych tego typu materiałów należy zaliczyć falsyfikaty: dokumentów bojowych, zarządzeń władz wojskowych i cywilnych, dokumentów, walut oraz prasy.

Druki zwarte to bogatsze od ulotek materiały drukowane, mające pogłębiać i utrwalać destrukcyjne nastroje oraz postawy określonych grup przeciwnika. Do druków zwartych należą m.in. odezwy, broszury, gazety, biuletyny. Materiały te muszą być dostarczone odbiorcy. Dlatego też rozpowszechnianie ich na terytorium zajętym przez przeciwnika stwarza pewne trudności.

Do rozpowszechniania ulotek i innych materiałów drukowanych wykorzystuje się przede wszystkim:

— w działaniach operacyjno-strategicznych – bomby i zasobniki przenoszone przez lotnictwo;
— w działaniach taktycznych – rakietowe pociski, a także zrzut ulotek ze śmigłowców, przenoszenie przez patrole rozpoznawcze i grupy wypadowe oraz pozostawianie podczas wycofania wojsk, w tym poprzez pomoc sektora pozamilitarnego.

Ulotki i inne materiały drukowane wykonywane są przez specjalistów sekcji poligraficznej grupy działań psychologicznych.

Ad.2. Audycje radiowe i telewizyjne stanowią jeden ze skuteczniejszych rodzajów działań psychologicznych, stosowanych w warunkach zagrożenia wojennego oraz we wszystkich rodzajach działań bojowych, a w szczególności w warunkach obrony własnego terytorium.

Zaletami przekazu radiowo-telewizyjnego są: duży zasięg oddziaływania, szybkość przygotowania i dotarcia audycji do odbiorców, łatwość percepcji oraz wysoka wiarygodność.

W działaniach psychologicznych stosuje się następujące formy przekazu radiowego i telewizyjnego:

— codzienne serwisy informacyjne z bieżących wydarzeń polityczno-wojskowych;
— komunikaty wojenne, zawierające opis zdarzeń z różnych kierunków działań bojowych, zgodne z oficjalną wykładnia dowództwa wojsk własnych;
— meldunki nadzwyczajne, informujące o szczególnych sukcesach bojowych wojsk własnych oraz niepowodzeniach strony przeciwnej;
— apele, wezwania i odezwy, zawierające polecenia i nakazy dowództwa wojsk własnych skierowane do żołnierzy przeciwnika, jak również do ludności;
— reportaże z frontów i obozów jenieckich;
— komentarze poświęcone sytuacji polityczno-militarnej oraz wydarzeniom wojennym;
— filmy i programy publicystyczne;
— wystąpienia i oświadczenia polityków, wyższych dowódców wojsk własnych oraz przedstawicieli strony przeciwnej;
— kroniki wojenne;
— materiały instruktażowe.

Na szczeblu operacyjnym audycje radiowo-telewizyjne przygotowywane są przez specjalistów sekcji nagrań grupy działań psychologicznych. Do ich emisji wykorzystuje się regionalne ośrodki RTV, w ramach doraźnych świadczeń rzeczowych i osobistych. Ponadto, do emisji określonych audycji mogą być wykorzystywane urządzenia pododdziałów walki elektronicznej, w ramach zakłócania i dywersji radiowej.

Ad. 3. Audycje elektroakustyczne są najskuteczniejszym rodzajem działań psychologicznych do wsparcia działań taktycznych, to jest w warunkach bezpośredniej styczności wojsk własnych z przeciwnikiem. Wymagają one ścisłej koordynacji z działaniami oddziałów i pododdziałów bojowych. Główną zaletą środków elektroakustycznych jest możliwość natychmiastowej reakcji na zmiany w sytuacji bojowej na polu walki.

Audycje elektroakustyczne dzielą się na: słowne, dźwiękowe i mieszane.

Audycje słowne opracowywane są w formie: komunikatu, odezwy, apelu, rozkazu, wezwania, polecenia i instrukcji. Audycje te wymagają od spikera doskonałej znajomości języka odbiorców. Służą one także do pozoracji ruchu wojsk.

Audycje dźwiękowe polegają na emisji określonych sygnałów dźwiękowych (np. o częstotliwości 2 – 15 Hz i poziomie głośności 115 – 155 dB), wywołujących i podtrzymujących stan stresu, a doprowadzających nawet do zaburzeń funkcjonowania organizmu. Stosowane są głównie w działaniach nękających i mają na celu zmniejszenie odporności psychicznej i fizycznej żołnierzy przeciwnika.

Audycje mieszane, w zależności od charakteru oraz relacji między słowem a sygnałami dźwiękowymi, służyć mogą wszystkim, wymienionym powyżej celom.

Audycje elektroakustyczne mogą być opracowywane i nagrywane przez grupę działań psychologicznych i dostarczane do odtworzenia do związków taktycznych (oddziałów).

Do rozpowszechniania audycji elektroakustycznych służą rozgłośnie elektroakustyczne, które dzielą się na; mobilne, montowane na pojazdach kołowych, gąsienicowych, środkach latających oraz plecakowe, przenoszone przez żołnierzy.

Działania psychologiczne w walce zbrojnej mogą zakończyć się sukcesem, jeżeli:

— personel będzie dysponował odpowiednią wiedzą, niezbędną przy tego typu działaniach;
— wszelkie oddziaływanie sił i środków tych działań będzie skoordynowane z planem i przebiegiem działań bojowych wojsk własnych;
— aktywa te zostaną użyte we właściwy sposób, przekazując i wykorzystując odpowiednio dobrane dane przy zastosowaniu efektywnych metod i technik oddziaływania;
— środki techniczne i materiałowe zapewnią możliwość sprawnego i elastycznego prowadzenia akcji z szerokim wykorzystaniem różnych torów transmisji danych.

2.2. Zakłócanie pośrednie

Zakłócanie pośrednie tworzy zespół skoordynowanych przedsięwzięć oraz sił i środków dostosowanych do zakłócania procesów informacyjno-sterujących przeciwnika poprzez oddziaływanie na jego urządzenia służące do zbierania, przetwarzania i dystrybucji danych w postaci niedostępnej bezpośrednio dla zmysłów

człowieka. W zakłócaniu pośrednim można wyróżnić (jak to przedstawiono wcześniej na rysunku 2.1):

- zakłócanie elektroniczne;
- pozorowanie elektroniczne;
- neutralizację elektroniczną;
- zakłócanie czujnikowe;
- zakłócanie informatyczne.

2.2.1. Zakłócanie elektroniczne

Zakłócanie elektroniczne jest jednym z ważnych elementów składowych walki elektronicznej. Powinno być ukierunkowane na dezorganizację tej części procesów informacyjnych przeciwnika, która oparta jest o wykorzystanie przestrzeni elektromagnetycznej.

Przedsięwzięcia zakłócania elektronicznego powinny zapobiegać lub ograniczać możliwości efektywnego wykorzystania przestrzeni elektromagnetycznej przez przeciwnika i w ten sposób wykluczyć lub ograniczyć jego możliwości dowodzenia i wykorzystania środków walki.

Zakłócanie elektroniczne może przyjmować formę *rażenia* lub *uderzenia elektronicznego* wyrażających zmasowane i kompleksowe użycie, w określonym czasie i miejscu, aktywnych środków walki elektronicznej w ścisłym powiązaniu z ogniowym rażeniem przeciwnika. Stanowi ono rodzaj aktywnych, ofensywnych działań elektronicznych, polegających na emitowaniu zakłócającej energii elektromagnetycznej na częstotliwościach pracy urządzeń odbiorczych przeciwnika.

Powinno być prowadzone na wszystkich szczeblach dowodzenia (w tym i na szczeblu taktycznym)we wszystkich rodzajach działań wojsk, w różnych warunkach terenowych i meteorologicznych, w stosunku do różnorakich środków elektronicznych, w które wyposażone są wojska przeciwnika.

Zasadniczymi obiektami zakłócania elektronicznego powinny być:

— w systemach łączności — różnego rodzaju urządzenie łączności radiowej UKF;
— w systemach radionawigacyjnych – pokładowe i naziemne urządzenia odbiorczo-wskaźnikowe i odbioru danych nawigacyjnych;
— w systemach radiolokacyjnych – naziemne stacje radiolokacyjne OP, OPL, rozpoznania pola walki, stacje kierowania ogniem oraz pokładowe stacje radiolokacyjne lotnictwa i sił morskich;

— w systemach samonaprowadzania – urządzenia odbiorcze pokładowych stacji radiolokacyjnych oraz urządzenia elektroniczne głowic samonaprowadzających się bomb, pocisków, rakiet, itp.;

— w systemach radiotelesterowania – różnego typu środki i urządzenia zapewniające zdalne sterowanie uzbrojeniem wojsk, samolotami bezpilotowymi oraz pociskami rakietowymi (przeciwpancernymi, przeciwlotniczymi itp.);

— w systemach optoelektronicznych – różnego typu urządzenia elektroniczne prowadzące rozpoznanie w ultrafiolecie, w zakresie promieniowania widzialnego oraz bliskiej, średniej i dalekiej podczerwieni;

— w systemach informatycznych – sieci informatyczne rozległe i lokalne oraz zautomatyzowane miejsca pracy na stanowiskach dowodzenia przeciwnika .

Ogólnie zakłócenia elektroniczne z uwagi na charakter ich powstawania podzielić można na zakłócenia przypadkowe[10] oraz celowe. Zakłócenia celowe są wytwarzane przez specjalne stacje (nadajniki) zakłócające lub pasywne retranslatory energii elektromagnetycznej. W teorii zakłóceń wyróżnia się zakłócenia celowe: aktywne, pasywne[11] i kombinowane (w przypadku jednoczesnego stosowania zakłóceń aktywnych i pasywnych).

Aktywne zakłócenia elektroniczne polegają na promieniowaniu przez urządzenie nadawcze zakłócającej energii elektromagnetycznej na częstotliwościach lub w paśmie pracy zakłócanych urządzeń odbiorczych. Mogą być emitowane przez stacje zakłócające stacjonarne i mobilne (polowe).

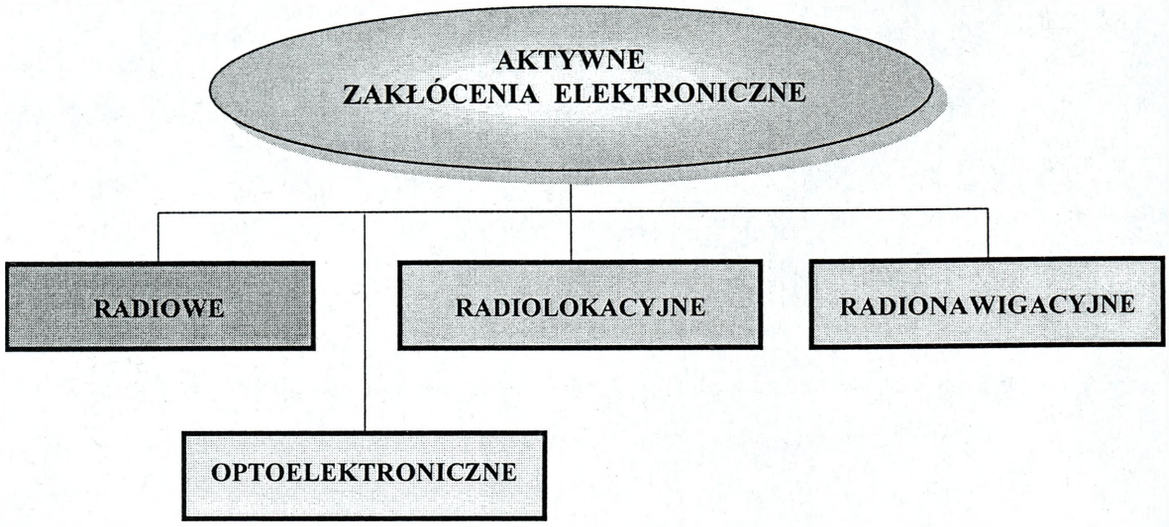
Aktywne, celowe zakłócenia elektroniczne charakteryzują się specyficznymi parametrami taktyczno.-.technicznymi dostosowanymi do konkretnych środków i systemów elektronicznych, przeciw którym mają działać. Zakłóceniami aktywnymi oddziałuje się na urządzenia odbiorcze poszczególnych środków elektronicznych. Wytwarzane one są na częstotliwościach roboczych, na których dokonywana jest transmisja danych i do których dokładnie dostrajane są nadajniki zakłócające. Wyróżnia

---

[10] Zakłócenia przypadkowe powstają w wyniku oddziaływania zjawisk przyrodniczych (naturalne) oraz urządzeń technicznych na urządzenia elektroniczne, najczęściej podczas wyładowań atmosferycznych, oddziaływania zorzy polarnej lub wybuchów słonecznych, opadów atmosferycznych, pracy urządzeń przemysłowych np. urządzeń spawalniczych, źle zabezpieczonych silników elektrycznych. Powstają również w rezultacie oddziaływania na środki elektroniczne polowych urządzeń elektrycznych, lub w wyniku nieumiejętnego rozmieszczenia środków elektronicznych na stanowiskach dowodzenia. Zakłócenia przypadkowe mogą być również pochodzenia kosmicznego oraz jako naturalne wewnętrzne szumy, powstające podczas pracy odbiorczych urządzeń elektronicznych. Zakłócenia przypadkowe mogą powstawać także wewnątrz aparatury.

[11] Zakłócenia pasywne szeroko wykorzystywane są w pozorowaniu elektronicznym.

się zakłócenia (rysunek 2.2.1.1): radiowe, radiolokacyjne, radionawigacyjne, optoelektroniczne i informatyczne.



Rys. 2.2.1.1 Podział aktywnych zakłóceń elektronicznych

Zakłócenia radiowe polegają na celowym promieniowaniu zakłócającej energii EM powodującej utrudnienie pracy elektronicznych środków radiowych przeciwnika. Zakłócenia radiowe mogą całkowicie zdezorganizować funkcjonowanie *systemów (sieci) łączności radiowej*. Mogą bowiem uniemożliwić odbiór sygnałów, pogorszyć słyszalność, spowodować nieprawidłowe działanie urządzeń końcowych, wprowadzić w błąd operatorów lub zwiększyć błędy urządzeń automatycznych. Przy pomocy zakłóceń radiowych można utrudnić lub uniemożliwić pracę jednego urządzenia, kilku lub kilkunastu, a nawet całego systemu łączności określonego szczebla dowodzenia. Zakłócenia radiowe są najbardziej ekonomicznym, a zarazem skutecznym sposobem zakłócania elektronicznego systemów łączności przeciwnika.

Zakłócenia radiowe mogą być również wykorzystane do dezorganizacji pracy urządzeń radiowych powodujących detonację bomb, rakiet i pocisków (radiozapalników). Mogą one spowodować przedwczesny wybuch lub niewybuch przez całkowite zablokowanie radiozapalnika.

Zakłócenia radiolokacyjne[12] to niepożądane sygnały zniekształcające lub zakłócające sygnały użytkowe na wejściu urządzeń odbiorczych, stanowiące nośniki danych w systemach radiolokacyjnych. Mogą być prowadzone przeciwko wszystkim rodzajom radiolokacyjnych urządzeń rozpoznawczych oraz przeciwko środkom

[12] Etatowe siły i środki zakłóceń radiolokacyjnych występują na szczeblu operacyjnym.

sterowania[13].

Zakłócenia radiolokacyjne powinno się szeroko wykorzystywać również w działaniach taktycznych wojsk lądowych z uwagi na pracę różnych stacji radiolokacyjnych przeciwnika w strefie taktycznej (do 20 km).

Zakłócenia radionawigacyjne obejmują środki i systemy radionawigacyjne (w tym bliskiej radionawigacji oraz systemy globalne) i mają na celu uniemożliwienie lub utrudnienie obiektom ruchomym przeciwnika określenie swojego miejsca położenia w przestrzeni. Zakłócenia radionawigacyjne szczególnie systemów bliskiej radionawigacji powinny być wykorzystywane w przyszłości również w działaniach taktycznych wojsk lądowych.

Zakłócanie optoelektroniczne służy do zakłócania pracy lub niszczenia aparatury rozpoznania pola walki i naprowadzania pocisków na cel. Działanie tej broni opiera się na emisji promieniowania elektromagnetycznego o długości fali i natężeniu wiązki zdolnej do (najczęściej do czasowego) zakłócania pracy czujników lub porażenia wzroku żołnierza obsługującego broń.

Do tej grupy należą:

— broń laserowa małej mocy;

— promienniki kierunkowe;

— generatory promieniowania mikrofalowego dużej mocy.

Broń laserowa małej mocy może być stosowana we wszystkich rodzajach sił zbrojnych. W siłach lądowych może występować jako środek przenośny (zestawy indywidualne lub podwieszane pod karabinkiem) lub przewoźny.

W laserach małej mocy wykorzystuje się promieniowanie o różnej długości fali, co zwiększa skuteczność jego działania. Najczęściej stosowane jest promieniowanie ultrafioletowe, czerwone, niebieskie i żółte.

Urządzenia impulsowego promieniowania laserowego są również stosowane do wytwarzania plazmy i fali uderzeniowej, służących do niszczenia czujników i porażenia załóg wozów bojowych. Wykorzystuje się zjawisko ablacji, zachodzące w wypadku uderzenia promienia laserowego w atakowaną powierzchnię oraz tworzenie fali uderzeniowej i powstawanie odłamków z materiału pancerza. Plazma może uszkodzić czujniki, układy kontrolno-pomiarowe i obserwacyjne.

---

[13] Środki sterowania obejmują urządzenia sterowania uzbrojeniem, samosterujące oraz sygnały sterujące różnorodną techniką wojskową (rakietami, środkami bezpilotowymi, systemami rozpoznania itp.).

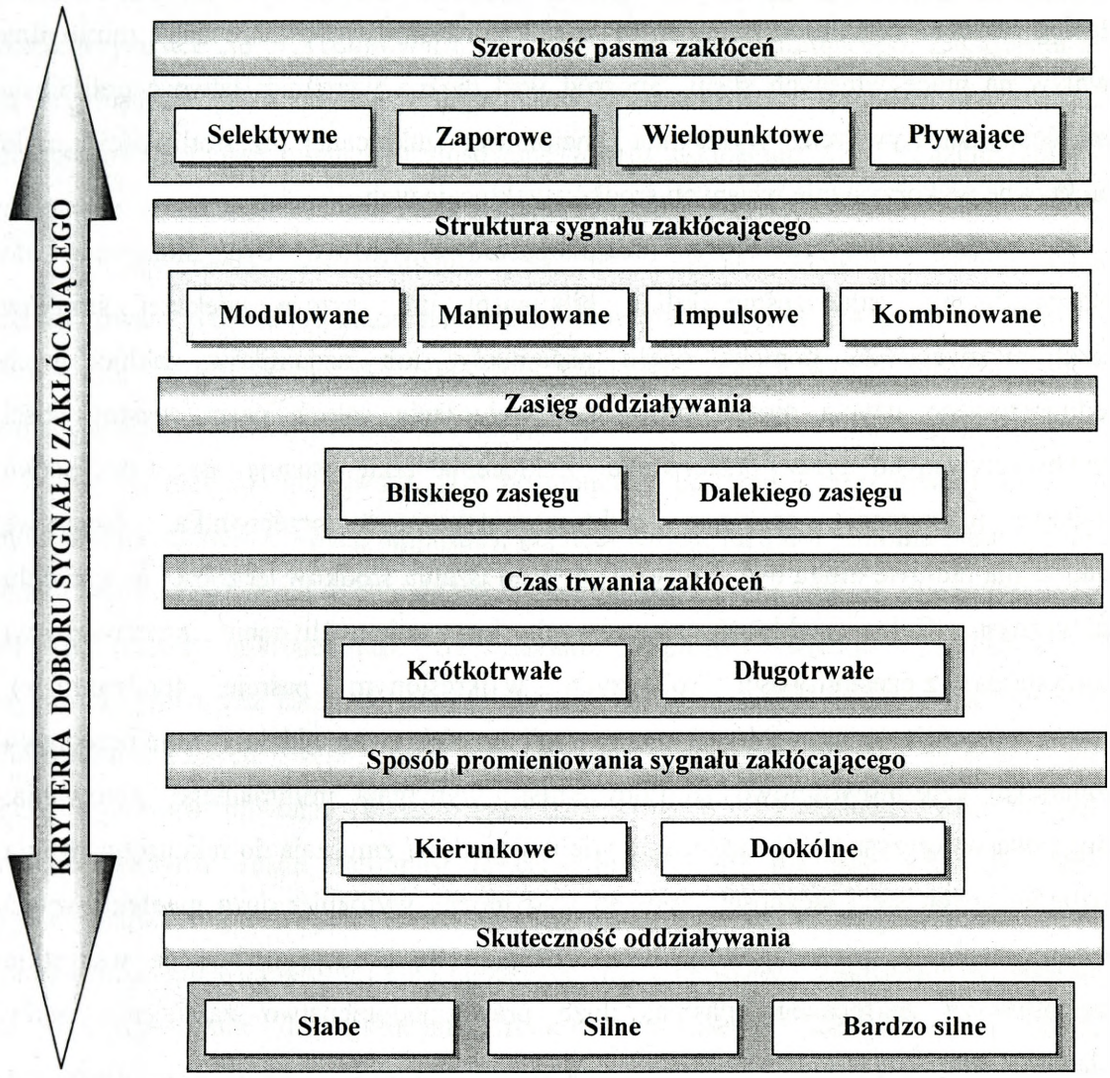
Broń tego typu może być wykorzystana między innymi do obezwładniania lekko opancerzonych wozów bojowych.

Promienniki równokierunkowe lub izotropowe wykorzystywane do celów wojskowych występują w formie amunicji artyleryjskiej lub lotniczej, wytwarzającej promieniowanie elektromagnetyczne o własnościach zbliżonych do laserowego. Ich działanie polega na krótkotrwałej emisji promieniowania elektromagnetycznego w zakresie od podczerwieni do nadfioletu oraz na porażeniu czujników i oczu żołnierzy przeciwnika. Źródłem promieniowania jest plazma powstała z gazu szlachetnego. Do rozgrzania gazu i doprowadzenia go do stanu plazmy wykorzystuje się energię detonacji materiału wybuchowego w kształcie stożka wypełnionego gazem szlachetnym. Najczęściej stosowanymi gazami są: neon, argon lub ksenon.

Promienniki kierunkowe, w odróżnieniu od równokierunkowych, są dodatkowo wyposażone w urządzenia ukierunkowujące strumień promieniowania. Pod względem konstrukcyjnym różnią się też umiejscowieniem ładunku wybuchowego. Charakteryzują się one większą sprawnością i mniejszym prawdopodobieństwem przypadkowego porażenia celów własnych.

Największą efektywność zakłócania elektronicznego można osiągnąć w wyniku kompleksowego wykonywania różnego rodzaju oddziaływań elektronicznych w stosunku do najważniejszych środków i obiektów elektronicznych przeciwnika w sposób zmasowany, niespodziewanie, na głównych kierunkach i w decydujących etapach taktycznych.

W praktyce zakłócanie elektroniczne polega na celowym (rozmyślnym) promieniowaniu, energii elektromagnetycznej w celu osłabienia efektywności użycia odbiorczych urządzeń (systemów) elektronicznych wykorzystywanych przez przeciwnika. Zakłócanie elektroniczne wnosi do relacji informacyjnych przeciwnika dodatkowe wartości energetyczne, które powodują dezorganizację ich pracy. Osiąga się je przez stosowanie nadajników, emitujących aktywne sygnały zakłócające o strukturze zbliżonej do sygnałów użytecznych przeciwnika. Jak już wspomniano wcześniej, bardzo ważną rolę w procesie zakłócania elektronicznego odgrywa *dobór sygnału zakłócającego do sygnału zakłócanego.* Powinien on być dokonywany - według następujących kryteriów (rysunek 2.2.1.1):



Rys. 2.2.1.1. Kryteria doboru sygnałów zakłóceń elektronicznych

1. Ze względu na szerokość zakłócanego pasma:

– *zakłócenia selektywne (wąskopasmowe, punktowe)*. Zakłócenia te odznaczają się dużą dokładnością dostrojenia urządzeń stacji zakłócającej do częstotliwości roboczej zakłócanego środka elektronicznego. Przy stosowaniu tych zakłóceń nadajnik promieniuje sygnał zakłócający o szerokości pasma optymalnej do zakłócanego urządzenia. Zasadniczym zaś warunkiem, pozwalającym na realizację zakłóceń wąskopasmowych, jest dokładna znajomość częstotliwości roboczych poszczególnych środków elektronicznych przeciwnika. W działalności bojowej tego rodzaju zakłócenia stosuje się głównie w systemach łączności wąskopasmowego emisji radiowych (A1A,

A2A, F1A), radionawigacji oraz systemach sterowania. Dokładność dostrojenia do częstotliwości nośnej emisji wąskopasmowych nie powinna być gorsza niż 15-30 Hz. Do podstawowych zalet zakłóceń wąskopasmowych można zaliczyć: maksymalny zasięg zakłóceń (cała moc zakłóceń przypada na częstotliwość zakłócaną); minimalny wpływ na pracę własnych stacji. Spośród wad można wyróżnić: łatwość uniknięcia zakłóceń selektywnych; wymagana znajomości zakłócanej częstotliwości; mało efektywne wykorzystanie własnych środków zakłócających.

- *zakłócenia zaporowe* (szerokopasmowe). Mogą być stosowane do obezwładniania jednocześnie kilku, kilkunastu lub jeszcze większej środków elektronicznych. Za pomocą wielu nadajników lub nadajników zakłócających jednorazowego użycia można prowadzić zagłuszanie całych pasm częstotliwości wykorzystywanych przez przeciwnika. Zakłócenia takie stosuje się w przypadku słabego rozpoznania spektrum elektromagnetycznego przeciwnika. Zaporowe zakłócenia radiowe mogą być stosowane do zagłuszania środków łączności na szczeblu taktycznym. Celem zakłóceń zaporowych jest uniemożliwienie przeciwnikowi korzystania z częstotliwości roboczych w określonym paśmie (podzakresie). Podstawowymi zaletami zakłóceń zaporowych są: efektywne oddziaływanie przeciwko zmiennym częstotliwościowo źródłom emisji; wymagają minimalnego sterowania; mogą być wykorzystane do zakłócania wielu sygnałów; zmuszają do rekonfigurowania rozbudowanych sieci łączności. Spośród wad można wyróżnić: duża nieefektywność wykorzystania mocy nadajników, która rozkłada się proporcjonalnie na wszystkie częstotliwości zakłócanego pasma; duże prawdopodobieństwo zakłócenia pracy własnych stacji.

– *zakłócenia wielopunktowe.* Polegają na zakłócaniu pojedynczych częstotliwości. Ich główną zaletą jest zwiększona efektywność zakłócania w porównaniu z zakłócaniem selektywnym (punktowym).

– *zakłócenia pływające.* Polegają na punktowo-zaporowym przemieszczaniu (przemiataniu) energii zakłócającej na zakłócanych częstotliwościach. Podstawowymi zaletami zakłóceń pływających są: efektywne użycie zakłóceń przeciwko sieciom wieloczęstotliwościowym; cała moc sygnału zakłócającego jest skupiona w danej chwili na jednej częstotliwości; maksymalny zasięg zakłóceń; możliwość sterowania własnymi stacjami w celu uniknięcia zakłóceń wzajemnych. Spośród wad można wyróżnić: skomplikowane technicznie urządzenia.

2. Ze względu na strukturę sygnału zakłócającego:

– *zakłócenia modulowane (szumowe)*. Są to drgania wielkiej częstotliwości modulowane amplitudowo, częstotliwościowo lub fazowo. Najbardziej rozpowszechnionym rodzajem zakłóceń modulowanych są zakłócenia szumowe, charakteryzujące się przypadkowymi zmianami napięcia modulującego. Zakłócenia te są otrzymywane przez modulację drgań wielkiej częstotliwości sygnałem szumowym. Zakłócenia szumowe mogą być stosowane w celu zakłócenia wielu rodzajów pracy radiostacji, a przede wszystkim pracy fonicznej.

– *zakłócenia manipulowane*. Są to drgania wielkiej częstotliwości manipulowane ręcznie lub automatycznie amplitudowo, częstotliwościowo lub fazowo. Stosowane są najczęściej do zakłócania wąskopasmowych emisji telegraficznych z manipulacją amplitudy lub częstotliwości.

– *zakłócenia impulsowe*. To postępujące po sobie krótkotrwałe impulsy modulowane czasem trwania, amplitudą, częstotliwością, fazą lub kilkoma parametrami jednocześnie. Zakłócenia te charakteryzują się bardzo krótkim czasem promieniowania energii (rzędu mikrosekund). Są ciągami impulsów wielkiej częstotliwości, wytworzonymi przez nadajnik zakłócający na częstotliwościach zakłócanych środków radioelektronicznych. Jeśli częstotliwość powtarzania zakłóceń pokrywa się z częstotliwością powtarzania zakłócanej stacji, mamy do czynienia z zakłóceniami synchronicznymi. Jeżeli natomiast te częstotliwości się nie pokrywają, mówimy o zakłóceniach impulsowych nie synchronicznych. Zakłócenia te mogą być odzewowe (jednokrotne lub wielokrotne) albo niezależne (nie odzewowe). Zakłócenia impulsowe są wykorzystywane do zakłócania środków pracujących impulsowo, np. stacji radiolokacyjnych, stacji radioliniowych, urządzeń radiotelesterowania rakietami itp.

– *zakłócenia kombinowane*. To drgania wielkiej częstotliwości modulowane i manipulowane równocześnie kilkoma sposobami, na przykład impulsowe zakłócenia radiowe w połączeniu z modulacją szumami. Tego rodzaju zakłócenia stosowane są głównie do naruszania pracy środków radioliniowych oraz radiotelegrafii z przesuwem częstotliwości.

3. Ze względu na zasięg działania:

– *zakłócenia bliskiego zasięgu* zapewniają skuteczne zagłuszanie i dezorganizację pracy środków elektronicznych przeciwnika na odległość do 10 km od miejsca pracy nadajnika lub stacji zakłócającej. Występują one podczas użycia nadajników zakłócających jednorazowego użycia, autonomicznych środków

zakłócających oraz niektórych środków wykorzystywanych na szczeblach taktycznych.

– *zakłócenia dalekiego zasięgu* zapewniają skuteczne zagłuszanie i dezorganizację pracy środków elektronicznych przeciwnika na odległość powyżej 10 km (nawet do kilkuset kilometrów). Taki zasięg zakłóceń uzyskuje się wykorzystując naziemne i powietrzne stacje dużej mocy.

4. Ze względu na czas trwania:

– *zakłócenia* krótkotrwałe. Prowadzone są w czasie równym a nawet krótszym od czasu nadawania jednego lub kilku sygnałów przeciwnika.

– *zakłócenia* długotrwałe. Polegają na zakłócaniu pracy elektronicznych środków elektronicznych w czasie od kilkunastu minut do kilku godzin. Stosowane są przy wykorzystaniu nadajników jednorazowego użytku.

5. Ze względu na sposób promieniowania:

– *zakłócenia dookólne* prowadzi się gdy promieniowanie anteny odbywa się we wszystkich kierunkach z jednakową mocą. Stosuje się je, wówczas gdy są nieznane miejsca rozmieszczenia zakłócanych środków. Ponadto w nadajnikach zakłócających jednorazowego użytku i często w stacjach pracujących w ruchu. Ujemną cechą zakłóceń dookólnych jest stosunkowo niski stopień wykorzystania energii wynikający ze znacznego jej rozproszenia.

– *zakłócenia kierunkowe.* Występują wtedy, gdy energia EM jest promieniowana przez antenę stacji zakłócającej w kierunku zakłócanego środka elektronicznego przeciwnika. Uzyskuje się to przez stosowanie dobranych anten o charakterystyce kierunkowej. Dzięki kierunkowości anten istnieje możliwość uzyskania w punkcie odbioru większego strumienia zakłócającej energii elektrycznej. Stosując tego typu zakłócenia należy częściowo znać miejsca rozmieszczenia zakłócanego środka lub środek elektroniczny musi się znajdować w sektorze pracy stacji zakłócającej. Zakłócenia kierunkowe zwiększają efektywność wykorzystania mocy nadajnika. Stosowanie takich zakłóceń jest konieczne w przypadku zagłuszania urządzeń o dużej kierunkowości anten oraz skomplikowanych strukturach sygnału.

6. Ze względu na skuteczność działania:

– *zakłócenia słabe*. Są to takie zakłócenia, przy których natężenie pola elektrycznego sygnału zakłócającego (Ez) w punkcie odbioru u przeciwnika, jest większe od natężenia sygnału użytecznego (Es) i wynosi średnio 3-5% *(Ez>ES - średnio o 3-5%)*. Przy tego rodzaju zakłóceniach poziom zakłóceń w punkcie odbioru

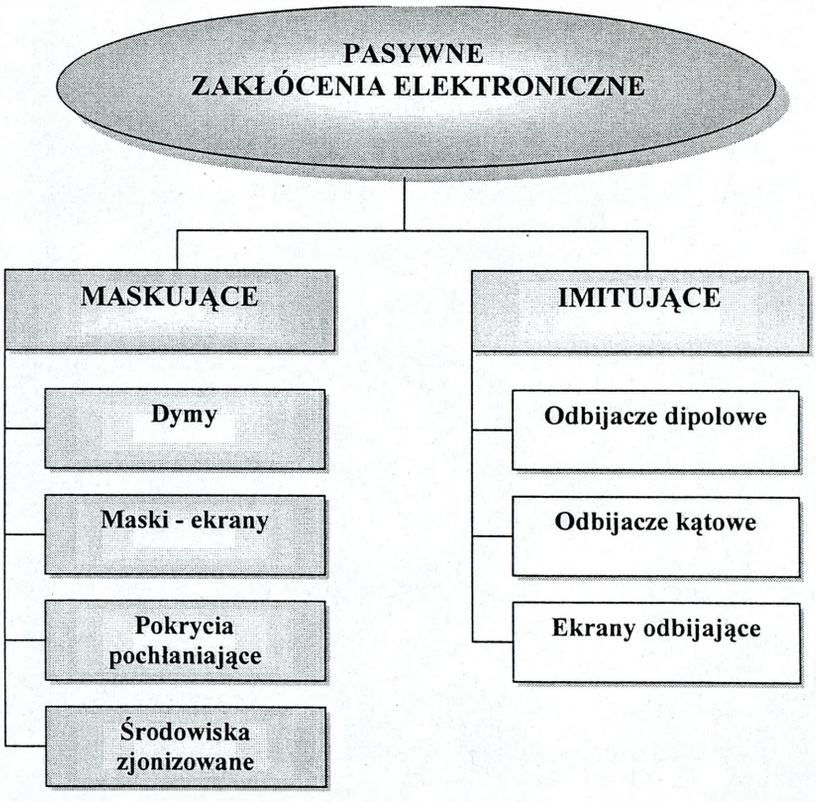
sygnału użytecznego powoduje utratę lub obniżenie wiarygodności przesyłanych danych w granicach 5-15%. Oznacza to, że w wypadku stosowania słabych zakłóceń występują tylko pewne zniekształcenia przekazywanych danych. W relacjach łączności utrudniony jest odbiór telegramów lub prowadzenie bezpośrednich rozmów. W zasadzie w większości wypadków odbiór jest możliwy przez doświadczonego operatora (oficera sztabu) przygotowanego do pracy w warunkach zakłóceń. Istnieje potrzeba powtarzania transmisji w granicach 10-15%. W urządzeniach radiolokacyjnych występują utrudnienia w odróżnieniu celu.

– *zakłócenia silne*. To takie zakłócenia, przy których natężenie pola elektrycznego sygnału zakłócającego w punkcie odbioru po stronie przeciwnika jest większe o 5-15% od natężenia pola elektrycznego sygnału użytecznego środka elektronicznego przeciwnika *(Ez>ES o 15-50%)*. Tego typu zakłócenia powodują utratę lub obniżenie wiarygodności danych od 15 do 50%. Oznacza to, że w relacjach łączności będzie poważnie utrudniony odbiór, a nawet utrata jej znacznej części danych. W najnowszych systemach może dojść do zerwania synchronizacji ich pracy. W systemach radiolokacyjnych na ekranach wskaźników w znacznym stopniu będzie ograniczona widzialność i rozróżnialność celów. Zamiast celów rzeczywistych mogą pojawiać się cele pozorne, nieczytelne sektory i pasy, obejmujące do 50% ekranu.

– *zakłócenia bardzo silne zakłócenia* (tłumiące). To takie zakłócenia, przy których natężenie pola elektrycznego sygnału zakłócającego w punkcie odbioru po stronie przeciwnika jest znacznie większe, ponad 50% wyższe od natężenia pola elektrycznego sygnału użytecznego *(Ez>Es ponad 50%)*. Przy tego rodzaju zakłóceniach poziom zakłóceń w punkcie odbioru jest tak wysoki, że powoduje całkowitą utratę danych.

Pasywne zakłócenia elektroniczne polegają na wtórnym promieniowaniu, odpromieniowaniu, odbijaniu, rozpraszaniu lub wchłanianiu energii elektromagnetycznej przez środki nie dysponujące generatorem energii EM w celu zmylenia systemów elektronicznych i odwrócenia uwagi przeciwnika. Zakłócenia pasywne dotyczą najczęściej środków radiolokacyjnych, środków pracujących w podczerwieni oraz urządzeń laserowych. Wytwarzane są przez sztuczne zmiany właściwości elektromagnetycznych środowiska rozprzestrzeniania się fal. Ze względu na sposób oddziaływania na zakłócane urządzenia rozróżnia się zakłócenia *maskujące i imitujące* (rysunek 2.2.1.2).

Zakłócenia maskujące utrudniają lub uniemożliwiają przeciwnikowi wykrycie i obróbkę sygnału użytecznego. Urządzenia rozpoznania elektronicznego przeciwnika rejestrują niepełny i niezgodny z rzeczywistością obraz pracy naszych środków elektronicznych. Analiza oparta na niepełnych i niezgodnych z rzeczywistością danych może doprowadzić do wyciągnięcia fałszywych wniosków. Dla uzyskania efektu zakłóceń maskujących wykorzystuje się dymy metalizowane, ekrany maskujące, pokrycia przeciwradiolokacyjne, a także środowisko zjonizowane. Zastosowanie środków wywołujących lokalną jonizację przestrzeni powoduje zmianę właściwości elektromagnetycznych ośrodka, podobnie jak różnego rodzaju przeciwradiolokacyjne pokrycia maskujące. W przypadku ich użycia wyklucza się możliwość wykorzystania fal elektromagnetycznych do wszelkiego rodzaju pomiarów i przekazywania danych. Pasywne zakłócenia mogą być też wywołane przez naturalne czynniki, takie jak deszcz, śnieg, gęstą mgłę itp.



Rys. 2.2.1.2 Rodzaje zakłóceń pasywnych

Zakłócenia imitujące wprowadzają do zakłócanego systemu dane fałszywe. Za ich pomocą można wytworzyć np. na ekranie wskaźnika stacji radiolokacyjnej zobrazowanie celu na takim azymucie i odległości, gdzie nie ma celów rzeczywistych.

Zastosowanie tych zakłóceń dezorientuje przeciwnika oraz utrudnia podjęcie właściwych decyzji. Jako środki do wytwarzania imitujących zakłóceń pasywnych stosowane są odbijacze kątowe[14], odbijacze dipolowe[15], wszelkiego rodzaju pułapki i fałszywe cele radiolokacyjne.

Zakłócanie elektroniczne (zarówno aktywne, jak i pasywne) stanowi bardzo skuteczny sposób dezorganizacji pracy i działania różnorakich środków i systemów elektronicznych wykorzystywanych w dowodzeniu wojskami i kierowaniu środkami walki przeciwnika. Ogranicza ono zakres i możliwości wykorzystania ww. systemów przez poszczególne dowództwa i sztaby a ponadto, mimo że nie powodują bezpośrednich materialnych zniszczeń, to jednak w wielu sytuacjach są przyczyną powstających u przeciwnika znacznych strat w sile żywej i sprzęcie bojowym.

W rezultacie zakłócania elektronicznego środków i systemów elektronicznych przeciwnika następują zmiany w ilości danych przesyłanych do poszczególnych dowództw i sztabów oraz do wojsk wykonujących określone zadania bojowe. Często, mimo sprawności technicznej środków elektronicznych w wielu ogniwach dowodzenia wystąpić może całkowita lub częściowa utrata danych albo opóźnienie w przekazywaniu wiadomości bojowych. Poza tym przekazywane dane mogą być zniekształcone w znacznym stopniu, zamazywane i deformowane. Występować może zmniejszenie ich ilości lub też zwiększenie w drodze imitowania. Do dowództw i sztabów, na stanowiska dowodzenia, do wojsk i środków walki docierać będą dane niepełne, wątpliwe, odznaczające się niskim stopniem wiarygodności. Przekaz danych może być też na pewien okres czasu całkowicie przerwany. Brak danych lub niski stopień ich wiarygodności uniemożliwia lub utrudnia realizację terminowego, skoordynowanego i operatywnego dowodzenia wojskami i kierowania środkami walki.

---

[14] *Odbijacze kątowe* dzięki zwiększonemu odbijaniu energii elektromagnetycznej są używane do pozorowania obiektów rzeczywistych w otaczającym je tle. Wielkość odbijanej energii zależy od kształtu i rozmiarów odbijaczy. Specjalna konstrukcja odbijaczy kątowych powoduje znaczne odbicia energii przy stosunkowo niewielkich wymiarach.

[15] *Odbijacze dipolowe*, to najczęściej metalizowane włókna szklane i poliamidowe lub metalizowana, odpowiednio cięta folia. Długość tych elementów z reguły odpowiada długości 1/2 λ. Środki dipolowe są przeznaczone do zakłócania stacji radiolokacyjnych, pozorowania obiektów i maskowania rzeczywistych obiektów. Dipole można wyrzucać w określonych odstępach czasowych, na dużych przestrzeniach.

Obniża to sprawność bojową wojsk, ich siłę uderzeniową i skuteczność działań, uniemożliwia terminowe wykonanie zadań bojowych oraz bardzo często prowadzi do znacznych strat w sile żywej i sprzęcie bojowym.

Należy mieć na uwadze, że efekty zakłócania elektronicznego wzrastają w przypadku silnej koordynacji działań elektronicznych z oddziaływaniem ogniowym na wybrane obiekty elektroniczne. Czas zakłócania elektronicznego powinien być podporządkowany potrzebom wykonania zadań ogniowych i manewrowych. Szczególnie jest to widoczne w walce z systemami obrony powietrznej i systemami dowodzenia wojsk lądowych.

Zakłócanie elektroniczne może być prowadzone selektywnie na wybranych obiektach i środkach elektronicznych lub w sposób zmasowany na środkach elektronicznych w wybranych rejonach. Wówczas wszystkie środki elektroniczne przeciwnika w obszarze walki podlegają obezwładnieniu.

Zakłócanie elektroniczne powinno obejmować odpowiednie działania, zmierzające do zapobiegania lub zredukowania efektywnego użycia przez przeciwnika widma elektromagnetycznego poprzez użycie energii elektromagnetycznej przez własne środki.

Doktryna Działań Powietrzno – Lądowych obliguje do umiejętnego użycia środków wykrywania i namierzania celów oraz systemów kierowania broni. Realizacja powyższego wymaga współdziałania pomiędzy rodzajami sił zbrojnych i służb. Niezbędna w tym zakresie staje się łączność, jej brak może spowodować duże problemy w wykonaniu zadania bojowego.

Doktryna Walki Elektronicznej określa konieczność integracji zakłócania elektronicznego z kolejnymi fazami działań taktycznych. Zakłócanie narusza łączność przeciwnika lub uniemożliwia mu przekazywanie kluczowych danych, w wyniku czego jego działania stają się nieefektywne. Skuteczne zakłócanie może spowodować, że przeciwnik będzie zmuszony zmienić częstotliwości, ustalić nowe dane radiowe lub zwiększyć moc nadajników.

Planowanie zakłócania wymaga dużej ilości danych o przeciwniku, które są uzyskiwane głownie z rozpoznania radioelektronicznego, a także z innych źródeł.

Decyzja dowódcy do zakłócania zależy od wielu czynników. Kluczowym czynnikiem jest czas. Rozpoznanie i zakłócanie nie może być prowadzone jednocześnie przeciwko tym samym węzłom łączności przeciwnika. Ponadto zbyt duża moc własnych stacji zakłóceń może spowodować ich lokalizację przez przeciwnika.

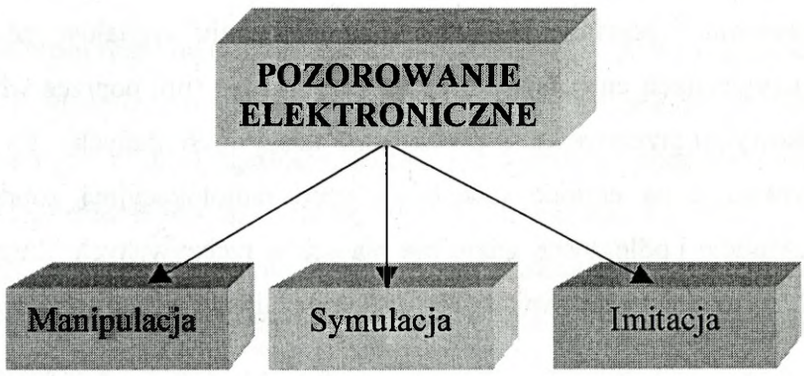
Dowódca ZT musi decydować o priorytetach czasowych zakłócania, rozpoznania, rażenia ogniowego i innych aspektów działań taktycznych.

2.2.2. Pozorowanie elektroniczne

Pozorowanie elektroniczne to zespół przedsięwzięć i działań ukierunkowanych na ukrywanie rzeczywistych zamiarów wojsk własnych. Polega na użyciu energii elektromagnetycznej do emisji fałszywych danych i sygnałów elektromagnetycznych maskujących sygnały użyteczne oraz na odpowiednim odbijaniu lub tłumieniu sygnałów wejściowych w sposób mający na celu zmylenie przeciwnika w zakresie wykorzystania danych pozyskanych przez jego systemy elektroniczne. W pozorowaniu elektronicznym wykorzystuje się w szerokim zakresie pasywne zakłócenia elektroniczne.

Pozorowanie elektroniczne stanowić powinno część ogólnego planu wprowadzania przeciwnika w błąd. Wymaga zwykle scentralizowanej koordynacji i kierowania. Dlatego w działaniach taktycznych wojsk lądowych, działania pozorujące powinny mieć zastosowanie w ograniczonej skali i w wybranych kluczowych okresach walki.

Wybrane elementy pozorowania elektronicznego w działaniach taktycznych WL należy realizować poprzez (rysunek 2.2.2.1):



Rys. 2.2.2.1. Sposoby pozorowania elektronicznego

- manipulację;
- symulację;
- imitację.

Manipulacja[16] powinna polegać na zmianie profili elektronicznych rozmieszczenia własnych środków elektronicznych w celu uniemożliwienia przeciwnikowi rozpoznania ich sygnałów, np. poprzez emisję fałszywych danych we własnych relacjach łączności oraz tworzenie pozornych relacji łączności. Stosując manipulację należy mieć na uwadze zmiany parametrów technicznych urządzeń oraz naruszenia zasad wymiany radiowej (wyłomy, przekroczenia, naruszenia, przekazywanie spreparowanych danych związanych z działaniami bojowymi lub etapami walki).

Realizacja przedsięwzięć w zakresie manipulacji wymaga studiowania oraz odpowiedniej zmiany własnego elektronicznego rozkazu bojowego. Powinna być ostrożnie planowana i realizowana tylko wtedy, kiedy przeciwnik będzie działał tradycyjnie przeciwko naszym wojskom[17].

Symulacja[18] powinna polegać na elektronicznej reprezentacji własnych sił (całych lub części systemów elektronicznych) w innych miejscach niż znajdują się one w działaniach rzeczywistych (w trakcie trwania tzw. „ciszy radiowej"). Jej celem jest przeciwdziałanie rozpoznaniu elektronicznemu przeciwnika w określaniu ugrupowania wojsk własnych, ich rozmieszczenia, potencjalnych możliwości oraz zamiarów. Do prowadzenia symulacji niezbędne są dodatkowe siły i środki elektroniczne, jeżeli przeciwnik posiada wystarczające środki do ich wykrycia. Głównymi cechami symulacji zatem są: fałszywa lokalizacja obiektów, tzw. obiektów pozornych; zmiana własnego elektronicznego rozkazu bojowego i in.

Imitowanie[19] powinno polegać na upodobnieniu sygnałów zakłócających do sygnałów użytecznych emitowanych przez przeciwnika (np. poprzez włączanie się do relacji radiowych przeciwnika i przesyłania fałszywych danych). Za jego pomocą można wytworzyć na ekranie wskaźnika stacji radiolokacyjnej zobrazowanie celu w takim azymucie i odległości, gdzie nie ma celów rzeczywistych. Zastosowanie tych zakłóceń dezorientuje użytkownika oraz utrudnia podjęcie właściwych decyzji.

---

[16] Dotychczas w SZ RP w odniesieniu do systemów łączności i radionawigacyjnych używano pojęcia „dezinformacja radiowa".

[17] Należy mieć na uwadze, że potencjalny przeciwnik zawsze studiuje wiadomości o emisjach elektromagnetycznych w czasie pokoju i obserwuje każdą z nich oddzielnie podczas różnych specjalistycznych ćwiczeń. Jego analitycy poszukują zmian w akceptowanych typach i poziomach ruchu i sugerują wykorzystanie ich w charakterze wskazówek do określenia naszych przyszłych zamiarów.

[18] Dotychczas w SZ RP wykorzystywano pojęcie „mylenie radioelektroniczne".

[19] W teorii walki elektronicznej w SZ RP imitowanie w odniesieniu do środków łączności i radionawigacji utożsamiane było z dywersją elektroniczną, którą uznawano za specyficzną formę obezwładniania elektronicznego, polegającą na przekazywaniu danych przeciwnikowi w taki sposób, aby odbierający nie zorientował się, że pochodzi ona ze stacji przeciwnika, zaś przekazaną treść przyjął jako prawdziwą.

2.2.3. Neutralizacja

Neutralizacja powinna polegać na celowym użyciu energii elektromagnetycznej o dużej gęstości mocy do chwilowego uszkodzenia, jak i stałego zniszczenia tych urządzeń elektronicznych przeciwnika[20], których działanie opiera się na wykorzystaniu mikroelektroniki.

Badania nad wzbudzaniem silnych impulsów EM (niszczących) środkami klasycznymi wskazują, że należy zwrócić szczególną uwagę na ten problem. Impuls EM powoduje krótkotrwałe wzbudzenie dużych napięć i prądów w aparaturze elektronicznej, powodując uszkodzenie (przegrzewanie) wrażliwych elementów tej aparatury: układy scalone, tranzystory, cewki itp. Przyszłe bomby impulsowe charakteryzować się będą zatem dużymi mocami promieniowania, ponad tysiąc razy większymi niż generują klasyczne środki WE.

Środkami niszczącymi przy użyciu energii EM dużej gęstości mocy mogą być zarówno urządzenia mikrofalowe jak i laserowe o dużej mocy. Można je wykorzystywać do niszczenia środków elektronicznych, szczególnie czułych na to zjawisko systemów termowizyjnych i czujników laserowych, a także innej wrażliwej na takie oddziaływanie aparatury.

Energia wiązkowa (Directed Energy - DE) to skoncentrowana (skupiona) energia elektromagnetyczna wypromieniowana w celu zniszczenia lub uszkodzenia obiektu.

Działanie broni wiązkowej *(Directed Energy Weapon - DEW)* polega na tym, że wygenerowany i odpowiednio uformowany strumień fal elektromagnetycznych lub cząstek elementarnych o dużej gęstości energii bezpośrednio oddziałuje na obiekt, powodując jego zniszczenie lub uszkodzenie, bądź wyeliminowanie z walki.

Broń tego typu jest w stanie zniszczyć lub uszkodzić elementy uzbrojenia przeciwnika, bądź obezwładnić siłę żywą. Wiązkową broń energetyczną można podzielić na trzy rodzaje:

— broń częstotliwości radiowych;

— broń laserową,

— broń cząstek elementarnych.

---

[20] Ta forma oddziaływania była dotychczas rozpatrywana w sytuacji użycia broni jądrowej, gdzie przy wybuchach część energii zamieniała się w impuls EM.

W związku z prowadzonymi na świecie badaniami nad tymi rodzajami broni, szczególnie w Stanach Zjednoczonych (program HAARP) oraz w Rosji (program SURRA) proponuje się interpretować termin *Directed Energy* jako energia kierowana, a *Directed Energy Weapon* jako broń energii kierowanej. W tej sytuacji oprócz już wymienionych trzech rodzajów tej broni podział obejmowałby również:

— broń ekstremalnie niskich częstotliwości - *Extremely Low Frequency Weapon*;

— broń infradźwiękową - *Infrasonic Weapon*;

— broń impulsową na ekstremalnie wysokich częstotliwościach (promieniowanie gamma) - *Extremely High Frequency Pulse Weapon (Gamma Radiation)*.

Broń fal elektromagnetycznych, obok broni laserowej i wiązkowej, zaliczana jest do broni energii bezpośredniej. Wykorzystują ją specjalistyczne urządzenia zdolne wysyłać w kierunku celu, z bardzo dużą prędkością, energię niszczącą.

Broń laserowa i wiązkowa opiera się na zasadzie wysyłania wiązki skoncentrowanej energii świetlnej (laser) i cząstek elementarnych (broń wiązkowa). Można nią niszczyć selektywnie wybrane cele, również radioelektroniczne, na różnych odległościach – w zależności od mocy urządzenia. Bardziej zaawansowane są prace nad bronią laserową, której różne odmiany wprowadza się już na uzbrojenie wojsk.

Problemy przy konstruowaniu broni wiązkowej związane są z propagacją wiązki. Z uwagi na istnienie silnych zewnętrznych pól elektrycznych i magnetycznych, może występować zjawisko rozogniskowania wiązki. Tego typu negatywne zjawiska nie występują w przypadku wykorzystania cząstek neutralnych, głównie atomów wodoru. Problem stanowi nadanie tym cząstkom odpowiedniej energii w celu kierowania wiązki na duże odległości. Przeprowadzone dotychczas doświadczenia z nad wykorzystaniem broni cząstek elementarnych wykazały, że może ona okazać się o wiele skuteczniejsza od broni laserowej. Cząstki elementarne przenikają bowiem przez obudowę urządzeń, powodując uszkodzenie układów elektronicznych, eksplozję ładunku wybuchowego głowicy lub zapłon paliwa napędowego, przy czym nie wymaga to długiego utrzymywania wiązki na celu, tak jak ma to miejsce w przypadku lasera.

Przedstawioną powyżej broń laserowa i wiązkowa, ze względu na sposób jej działania i możliwości użycia, zaliczyć można również do środków rażenia.

W definicji środków zakłócania niszczącego (neutralizacji) mieści się również *broń fal elektromagnetycznych*. Obecnie trwają intensywne prace nad jej skonstruowaniem. Badania koncentrują się głównie na *broni mikrofalowej, generatorach impulsów elektromagnetycznych i broni modulowanych sygnałów*

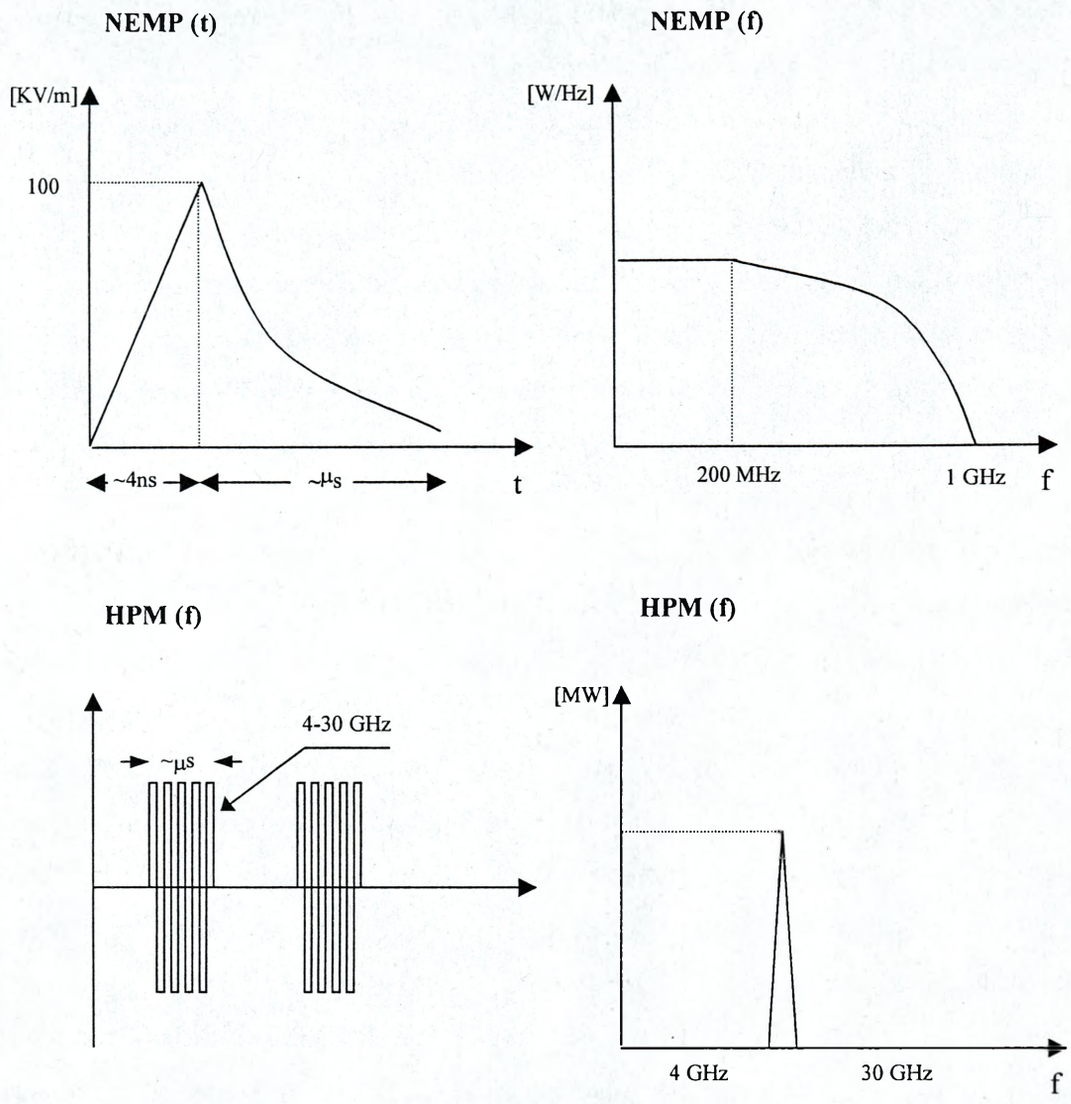
impulsowych. Każdy z tych rodzajów broni będzie miał inne przeznaczenie i będzie selektywnie oddziaływał na ściśle określone cele.

Broń mikrofalowa będzie przeznaczona głównie do zakłócania pracy urządzeń radiowych i radiolokacyjnych, podobnie jak czynią to współczesne środki walki radioelektronicznej. Różnica polega jednak na zastosowaniu ogromnej mocy promieniowania (tysiące razy większej niż stosowana jest obecnie przez środki WRE), przez co często określa się tę broń mianem środka superzakłócającego. Emitowane sygnały mikrofalowe mogą mieć również moc wystarczającą do niszczenia układów elektronicznych, a także innych elementów i mechanizmów środków bojowych, powodując ich przegrzanie oraz samozapłon. Broń ta może być zastosowana do zwalczania celów wykonanych w technice „stealth". Zastosowane do maskowania radiolokacyjnego tych środków bojowych specjalne materiały pochłaniające energię elektromagnetyczną, mogą powodować przegrzanie się pokrycia i w konsekwencji uszkodzenie, a nawet zniszczenie takiego celu.

Impuls mikrofalowy HPM (ang. High Power Microwave) ma charakter pojedynczego impulsu lub ciągu impulsów wielkiej częstotliwości. Są to impulsy wąskopasmowe o częstotliwości środkowej z zakresu 4-30 GHz i o mocy w impulsie do 100 MW. Przewiduje się, że już wkrótce możliwa będzie generacja impulsu o mocy rzędu giga i nawet terawatów.

W dziedzinie czasu impuls NEMP (rys. 2.2.3.1.) charakteryzuje się czasem narastania rzędu 3-10 ns i czasem opadania rzędu milisekund. W szczycie impulsu składowa elektryczna pola może osiągnąć wartość ok. 50 kV/m. Natomiast sygnał HPM ma postać impulsu (ciągu impulsów) o czasie trwania rzędu mikrosekundy, wypełnionego sygnałem sinusoidalnym o częstotliwości 4-30 GHz. Moc w impulsie może osiągnąć 100 MW, ale można spotkać informacje o badaniach nad impulsem o mocy rzędu giga i nawet terawatów.

W dziedzinie częstotliwości sygnał NEMP ma widmo ciągłe o szerokości listków około 1 GHz. Główna część energii tego impulsu jest zgromadzona w zakresie do 200 MHz. Natomiast sygnał HPM ma postać sygnału wąskopasmowego (praktycznie pojedynczego prążka). Częstotliwość środkowa tego sygnału zależy od przyjętych rozwiązań technologicznych i jak już wcześniej podano, jest zwykle wybierana z zakresu częstotliwości 4-30 GHz.



Rys. 2.2.3.1. Parametry widmowe i czasowe impulsów NEMP i HPM

Przy obecnym stanie rozwoju urządzeń HPM wykorzystuje się dwa mechanizmy generacji impulsu:

- generacja eksplozyjna (wybuchowa);
- elektroniczny układ generacji

W zależności od mocy i częstotliwości powtarzania impulsu, urządzenia HPM mogą być montowane na pojazdach, samolotach, w rakietach i pociskach. Mogą być także wykonane w wersji przenośnej w postaci walizki. Szczegóły techniczne rozwiązań takich urządzeń nie są publikowane. Wiadomo jedynie, że w ostatnich latach są prowadzone intensywne badania nad doskonaleniem technologii generacji impulsu oraz nad miniaturyzacją i elastycznością (możliwość generacji ciągu impulsów, zmiany częstotliwości pracy itp.) rozwiązań.

Przewiduje się, że urządzenia HPM mogą znaleźć zastosowanie w następujących obszarach:

- ✓ pole walki (akcje ofensywne i obronne) - zwalczanie pocisków i rakiet, obrona strefy powietrznej, biologiczna degradacja siły żywej przeciwnika;
- ✓ walka elektroniczna - niszczenie elementów sieci łączności i informatyki, stacji radiolokacyjnych, elektronicznych urządzeń sterowania środkami walki itp.;
- ✓ sabotaż i akcje dywersyjne.

Mechanizm wnikania sygnału HPM do obiektów elektronicznych jest podobny jak dla sygnału NEMP. Różnice dotyczą skuteczności stosowanych zabezpieczeń i skutków oddziaływania, co wynika z różnicy parametrów elektrycznych tych sygnałów. Podstawowe drogi wnikania i sposób oddziaływania sygnału HPM na różne obiekty przedstawia tabela 3.

Tabela 2.2.3.2

Drogi wnikania i sposób oddziaływania sygnału HPM

Obiekt rażenia	Drogi wnikania	Skutki oddziaływania
Obiekty łączności i informatyki	- anteny; - kable i przewody metalowe; - otwory i nieciągłości w ekranach elektromagnetycznych	- spalenie układów elektronicznych; - kasowanie pamięci; - zapłon materiałów (izolacji, obudowy itp.)
Paliwa i materiały wybuchowe	- otwory w konstrukcjach metalowych; - przewody metalowe.	- zapłon i detonacje
Organizmy żywe (ludzie)	- wnikanie i propagacja wzdłuż wewnętrznych organów ciała; - wzbudzanie prądów wirowych w małych przedmiotach metalowych stanowiących elementy ubioru lub wyposażenia.	- spalenie elementów ubrania lub wyposażenia (przy rażeniu ciągiem impulsów); - degradacja biologiczna trwała (przy gęstości energii 20-100 J/cm^2) lub przejściowa (do 100 mJ/cm^2)

Generalnie, ochrona obiektów elektronicznych przed oddziaływaniem HPM jest organizowana według ogólnych zasad kompatybilności elektromagnetycznej, zwłaszcza ekranowania i filtracji. Wymagana jest jedynie znacznie większa dbałość o jakość wykonania zabezpieczeń. Wynika to z bardzo wielkiej częstotliwości sygnału HPM, a więc małej długości fali: 1-10 cm, dzięki czemu może on przenikać przez niewielkie otwory i nieciągłości ekranu. Ekrany skutecznie zabezpieczające przed

sygnałem NEMP mogą nie stanowić żadnej przeszkody dla sygnału HPM, a przewód łączący ekran z obudową złącza może być dla tego sygnału doskonałą anteną odbiorczą. Ponadto korozja, a nawet migracja materiałów w uszczelkach mogą powodować miniaturowe nieciągłości, prze które może wniknąć sygnał HPM.

Ochrona urządzeń elektronicznych przed sygnałem HPM może polegać na:

- ✓ stosowaniu w jak największym stopniu kabli optycznych zamiast metalowych;
- ✓ ekranowaniu przewodów i złączy;
- ✓ bardzo dokładnym, dookólnym łączeniu ekranu przewodów z obudową złącza;
- ✓ umieszczaniu urządzeń elektronicznych w ekranowanych pomieszczeniach, kabinach lub obudowach;
- ✓ stosowaniu filtrów w przewodach sieciowych i sygnałowych.[21]

Omówiona nowa broń, polegająca na wykorzystaniu sygnału HPM znajduje się w początkowej fazie rozwoju. Dotyczy to zarówno rozwiązań technologicznych jak i jej wykorzystania na polu walki. W niedalekiej przyszłości broń ta może okazać się jednym z najbardziej skutecznych środków obezwładniania radioelektronicznego, szczególnie w stosunku tych urządzeń, które posiadają skuteczne zabezpieczenia przed innymi środkami i metodami obezwładniania.

Ocenia się, że prawdopodobieństwo użycia takiej broni może być dużo większe niż NEMP. Dotyczy to szczególnie rozwiązań w postaci przenośnych, walizkowych urządzeń, które mogą być wykorzystane przez grupy sabotażowe lub terrorystyczne. Przy pomocy takiego przenośnego urządzenia, z niewielkiego wzniesienia, można spowodować całkowite spustoszenie w pamięci komputerów tak dużego miasta jak Nowy Jork.

Generatory impulsów elektromagnetycznych (wykorzystujących inne zakresy częstotliwości niż generatory mikrofalowe) mają być wykorzystywane do zakłócania, powodowania uszkodzeń lub niszczenia środków łączności, komputerów, czułych elementów sterowania siecią energetyczną itp. Dobór odpowiednich parametrów generowanych impulsów może zapewnić selektywne oddziaływanie na określony rodzaj urządzeń.

---

[21] Aloksa W. "Impuls mikrofalowy dużej mocy"

Broń modulowanych sygnałów impulsowych będzie oddziaływać wyłącznie na organizmy żywe. Odpowiednio dobrany co do częstotliwości, kształtu, czasu narastania i czasu trwania impulsów, specjalnie zmodulowany sygnał impulsowy może spowodować zaburzenia w pracy mózgu, paraliż, a nawet śmierć ludzi. Sygnał ten może również powodować zaburzenia w pracy poszczególnych organów wewnętrznych, np. serca, nerek lub wątroby, a także powodować przegrzewanie się stawów lub innych części ciała wrażliwych na zmiany temperatury. Ten rodzaj broni zaliczany jest do broni masowego rażenia, gdyż sposób jej oddziaływania jest podobny do niektórych czynników rażenia broni jądrowej lub chemicznej.[22]

2.2.4. Zakłócanie czujnikowe

Zakłócanie czujnikowe polega na obezwładnianiu poszczególnych detektorów lub uniemożliwianiu ich pracy drogą dostarczania energii zakłócającej odpowiadającej parametrami sygnałom bodźcowym, charakterystycznym dla danego środowiska — akustycznego, magnetycznego, elektrycznego, chemicznego.

W zakresie fal sprężystych stosowane są *generatory infradźwięków* do czasowego obezwładniania siły żywej dzięki wytwarzaniu i emitowaniu fal akustycznych o bardzo małej częstotliwości.

Działanie infradźwięków polega na wykorzystaniu zjawiska wzbudzania wibracji materiałów na skutek oddziaływania fal o długości zbliżonej do fizycznych rozmiarów opromieniowywanego obiektu. Przy wystarczającej intensywności i czasie ekspozycji można spowodować wibrację i zniszczenie trwałych struktur budownictwa lądowego. Natomiast infradźwięki o częstotliwości 16 Hz używane przeciwko sile żywej powodują wzbudzanie wibracji w organach wewnętrznych, powstanie nudności, dolegliwości sercowych i zaburzeń równowagi. Zaletą tych rodzajów broni jest przede wszystkim łatwość przenikania przez struktury materii.

W zakresie środowiska magnetycznego wykorzystuje się *generatory impulsów elektromagnetycznych* bardzo dużej mocy, które wytwarzają bardzo wysokie pole magnetyczne, które indukuje prąd elektryczny we wszelkiego rodzaju urządzeniach elektronicznych, co jest przyczyną niszczenia niektórych elementów półprzewodnikowych na skutek przeciążeń. Obecnie generatory tego typu mogą być instalowane w pociskach rakietowych, bombach lotniczych i sztucznych satelitach.

---

[22] Tendencje rozwojowe w technice bojowej głównych państw zachodnich, MON, Warszawa 1991, s. 306

W zakresie środowiska elektrycznego wykorzystuje się *środki do uszkadzania linii energetycznych* (EPDM - Electronical Power Distribution Munition). Jest to amunicja zawierająca bardzo lekkie włókna węglowe przewodzące prąd elektryczny, oplątujące linie przesyłowe oraz stacje rozdzielcze i wywołujące spięcie. Zastosowane podczas działań w Iraku wykazały wysoką skuteczność. Wywołane awarie powtarzały się przez dłuższy czas.

Chemiczne środki wykorzystuje się np. do uszkadzania elektrowni wodnych. Dodane do wody powodują wzrost jej lepkości, a jeśli są to nici polimerowe, to owijają się wokół turbin i powodują niszczenie układów elektrowni.

Poza tym mogą być wykorzystywane *bakterie o dużej aktywności,* które są zdolne do niszczenia urządzeń wykonanych z tworzyw sztucznych, betonu i metali. Ich przedostanie się do stacji uzdatniania wody może również stanowić duże zagrożenie dla ludzi i środowiska.

Zakłócanie pracy czujników jest procesem skomplikowanym ze względu na dużą ilość i różnorodność tego typu środków na polu walki oraz ich odporność na oddziaływanie przeciwnika.

2.2.5. Zakłócanie informatyczne

Przedmiotem zakłócania informatycznego są komputery, jak też programy i zbiory danych. Zakłócanie to może być realizowane przy wykorzystaniu różnorodnych „programów złośliwych", które powodują wymazanie w krótkim czasie dużej liczby zbiorów danych, spowalniające pracę programów użytkowych. Programem złośliwym nazywa się kod wyrządzający szkody. Niektórzy również posługują się określeniem *malware* (zlepek z ang. *malicious software* - oprogramowanie złośliwe)[23]. Do programów tych należy zliczyć: „wirusy", „konie trojańskie", „bomby logiczne", „robaki komputerowe", „bakterie i króliki" oraz wiele im podobnych.

Koncepcja zastosowania *wirusów komputerowych* wprowadzonych do systemów komputerowych przeciwnika (CVW — Computer Virus Weapon) w celu zakłócenia pracy systemów dowodzenia i kierowania po raz pierwszy została sprawdzona w czasie wojny w rejonie Zatoki Perskiej.

[23] S. Garfinkel, G. Spafford: *„Bezpieczeństwo w Unixie i Internecie"*, Warszawa 1997, s. 31.

Niektóre *wirusy* podejmują działania natychmiast po wprowadzeniu do systemu, a niektóre wprowadzone są w postaci zaszyfrowanej lub upakowanej. Charakteryzują się tym, że po wprowadzeniu do systemu komputerowego podejmują jedynie działania mające na celu samoreplikację i dotarcie do najistotniejszych elementów systemu. Sygnałem do podjęcia działań destrukcyjnych jest samoistna lub zdalna aktywacja po określonym czasie lub zajściu określonych warunków w systemie. Celami dla tego rodzaju *wirusów* są urządzenia komputerowe pracujące w sprzęcie bojowym i elementach zabezpieczenia logistycznego, ich uruchamianie może nastąpić np. za pomocą sygnału radiowego.

Konie trojańskie otrzymały swoją nazwę ze względu na analogię ze znanym mitem greckim. Są one podprogramami, które (wmontowane np. w oryginalne programy użytkowe, np. gry, arkusze kalkulacyjne czy edytory) mogą na określony sygnał lub komendę wymazywać bazy danych, formatować dyski itp. Użytkownik może na przykład myśleć, że program jest grą. W czasie gdy na ekranie monitora wyświetlany jest komunikat o tym, że komputer aktualizuje bazy danych, bądź zadawane jest pytanie w stylu „jaki wybierasz poziom zaawansowania?", program może w tym czasie faktycznie usuwać pliki, formatować dysk czy w inny sposób modyfikować wiadomości.

Bomby logiczne są zazwyczaj podkładane w programach przez informatyków, którzy mają legalny dostęp do systemu. Impulsem wyzwalającym „wybuch bomby" może być obecność określonych plików, pewien dzień tygodnia czy jakiś użytkownik uruchamiający aplikację. Odpalona bomba logiczna może zniszczyć lub zniekształcić dane, spowodować zatrzymanie pracy komputera lub w inny sposób zniszczyć system. Bomby mają podobne działanie jak konie trojańskie, mogą np. uniemożliwiać korzystanie z zakupionego oprogramowania z chwilą utraty ważności licencji użytkownika.

Robaki komputerowe to programy, które mogą działać samodzielnie, a których zadaniem jest podróżowanie z komputera na komputer za pośrednictwem połączeń sieciowych. Może mieć miejsce taka sytuacja, gdzie wiele części jednego robaka będzie działać w różnych komputerach. Same robaki nie zmieniają innych programów, ale mogą przenosić kod, który to robi. Wypełniają one pamięć komputera taką ilością zupełnie przypadkowo generowanych danych, że prowadzi to do istotnego spowolnienia pracy komputera lub wręcz do jego zatrzymania.

Bakterie, zwane również *królikami*, to programy, które nie uszkadzają plików wprost. Ich jedynym zadaniem jest rozmnażanie. Typowy program — bakteria lub program — królik może nie robić nic innego niż dzielić się na dwie kopie i uruchamiać je w środowisku wielozadaniowym. Może też tworzyć dwa nowe pliki, z których każdy jest kopią programu wyjściowego. Oba nowe programy będą się następnie dalej mnożyły, tworząc kolejne „potomstwo". Bakterie reprodukują się wykładniczo i zajmują ogromną ilość czasu procesora, pamięci, przestrzeni dyskowej i innych zasobów, przez co użytkownik nie może z nich dalej korzystać.

Zakłócanie informatyczne będzie jednym z najważniejszych sposobów walki informacyjnej w XXI wieku. Przekonały się o tym Stany Zjednoczone, których komputery, zarówno w sferze cywilnej jak i wojskowej są wrażliwe na atak informatyczny. Systemy komputerowe Departamentu Obrony USA stają się coraz częściej celem „hackerów", którzy włamując się do komputerów Pentagonu mają dostęp do informacji zastrzeżonych. Hackerzy dokonują każdego roku około 250 tysięcy włamań, z czego 65% kończy się powodzeniem. Departament Obrony Stanów Zjednoczonych przeprowadził badania, w ramach których przeprowadzono 8932 próby penetracji na systemy komputerowe. 88% prób penetracji powiodło się. Tylko 320 włamań zostało wykrytych, a 22 zostały zgłoszone przez system. Włamywacze dostają się do komputerów, ponieważ potrafią ominąć specjalne zabezpieczenia. Najczęściej monitorują wybraną sieć, a następnie podszywają się pod jakiś zaufany komputer w tej sieci i przechwytują informacje, na podstawie których otwierają sobie drzwi do systemu informacyjnego. Włamywacze nie muszą korzystać wyłącznie z luk w systemach bezpieczeństwa. Mają możliwość „podglądania" interesującej ich sieci dzięki urządzeniom wbudowanym w sprzęt komputerowy. Mogą także analizować emisję pola elektromagnetycznego generowanego przez monitor (np. głównego komputera w sieci) i na tej podstawie odtwarzać informacje wyświetlane na ekranie komputera.

Jim Settle, konsultant ds. bezpieczeństwa FBI, jest przekonany, że przyszła wojna będzie polegać na blokowaniu dostępu do informacji i wprowadzaniu w błąd strony przeciwnej. W odróżnieniu od zasobów nuklearnych, środki walki informacyjnej (zakłócania informatycznego) są osiągalne prawie dla każdego. Celem tej walki będzie zarażenie wirusem programów komputerowych przeciwnika, tak aby był niezdolny do podejmowania jakichkolwiek działań. Skoro systemy obrony większości krajów oparte są na systemach komputerowych, wystarczy zakłócić pracę tego systemu, aby przeprowadzić skuteczny atak. Wpadli na to Amerykanie podczas wojny z Irakiem. Pół

roku wcześniej sprzedali do Iraku drukarki komputerowe, których odbiorcą było wojsko. Wewnątrz drukarek były zainstalowane specjalne mikronadajniki, które codziennie podawały swoją pozycję do satelity. W ten sposób można było zlokalizować cele wojskowe w Iraku. Lotnictwo amerykańskie bombardowało te pozycje, na których znajdowały się drukarki.

3. METODYKA I TREŚĆ PRACY W CYKLU DECYZYJNYM DO ZAKŁÓCANIA INFORMACYJNEGO

Cykl decyzyjny do zakłócania informacyjnego jest nierozerwalnie związany z procesem dowodzenia i przygotowania działań wojsk lądowych. Jest realizowany przez sztab korpusu (dywizji), gdzie najważniejsze zadania realizują oddziały G2 i G3. Celem przygotowania zakłócania informacyjnego jest określenie kolejności, sposobów i terminów wykonania zadań z zakresu zakłócania przez ZT, oddziały oraz specjalistyczne pododdziały WE, rozwiązanie problemów współdziałania i zabezpieczenia walki oraz organizacji dowodzenia.

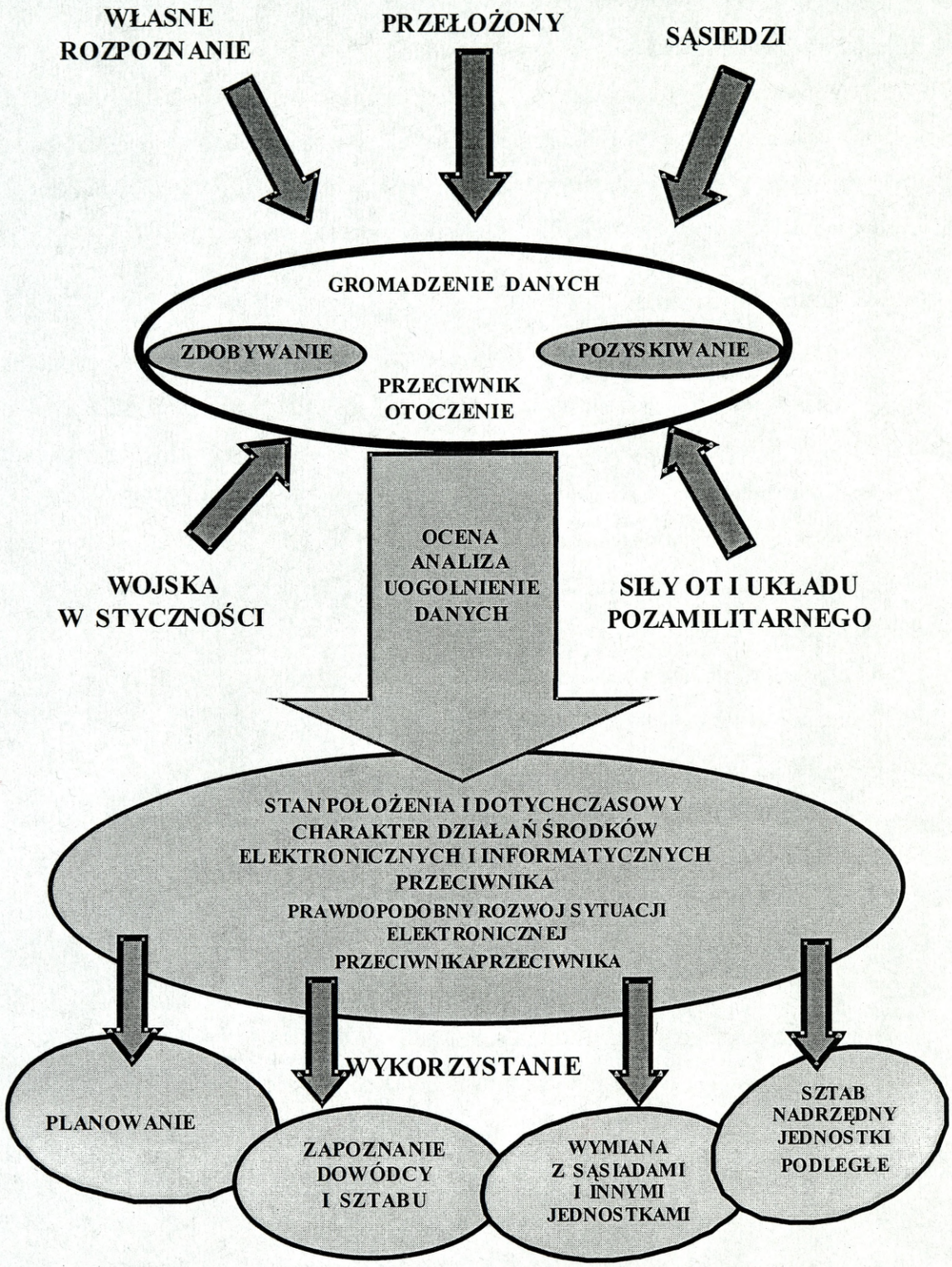
3.1. W fazie ustalania położenia

Podczas analizy zadania prowadzonej przez dowódcę z udziałem szefa sztabu, oficera G2 i G3 dokonywana jest wstępna analiza położenia sił i środków (elektronicznych) przeciwnika, wojsk własnych, właściwości środowiska, w którym będzie rozegrana walka.

Celem ustalenia położenia z punktu widzenia potrzeb procesu zakłócania informacyjnego jest zebranie, uporządkowanie, a następnie zobrazowanie danych o położeniu i ukompletowaniu elektronicznym przeciwnika, jego dotychczasowych działaniach, otoczeniu pola walki (teren, pogoda, warunki demograficzne itp.) a także o położeniu i realizowanych zadaniach przez potencjał rozpoznania wojsk własnych. Dane są pozyskiwane przez systemy rozpoznawcze z obszaru *odpowiedzialności rozpoznawczej*, a za dostarczanie informacji z obszaru *zainteresowania rozpoznawczego* odpowiedzialny jest przełożony .

Podstawę do ustalenia położenia przeciwnika stanowią meldunki wojsk w styczności, rozkazy operacyjne i komunikaty szczebla nadrzędnego, meldunki o własnym potencjale rozpoznania (o ile był lub jest w działaniu), informacje uzyskane od sąsiadów, sił Obrony Terytorialnej, układu pozamilitarnego.

Położenie własnych sił i środków rozpoznania jest z kolei ustalane na podstawie meldunków od podwładnych. Zebrane dane są porządkowane i ewidencjonowane oraz poddawane wstępnej analizie, ocenie i uogólnieniu. Tak „obrobione" stają się materiałem wyjściowym dla procesu planowania zakłócania informacyjnego. Zasilane są nimi również podległe wojska, sąsiedzi, szefowie rodzajów wojsk i służb oraz inni uprawnieni zainteresowani.



Rys. 3.1.1. Przebieg fazy ustalania położenia

Ocena posiadanych danych rozpoznawczych pozwala również na określenie luk w wiedzy o przeciwniku i terenie oraz ukierunkowanie na nie cyklu rozpoznawczego zgodnie z zadaniami postawionymi przez dowódcę.

Właściwością procesu zakłócania informacyjnego w fazie ustalania położenia jest to, że ma on charakter działania ciągłego, podczas którego dane szczątkowe i rozpoznawcze poddaje się stałej weryfikacji. Jest przez to możliwa ich aktualizacja, uwiarygodnianie oraz poszerzanie obszaru wiedzy (rozpoznania).

3.2. W fazie planowania

W fazie planowania oficerowie oddziału G2 i G3 wypracowują ogólną koncepcję prowadzenia zakłócania informacyjnego oraz ustalają potrzeby niezbędne do jej realizacji. Koncepcja prowadzenia zakłócania informacyjnego w każdym przypadku podporządkowana jest zadaniom jakie otrzymał ZO (ZT) oraz celowi i decyzji dowódcy. Jest ściśle skoordynowana z prowadzeniem rozpoznania wojskowego oraz oddziaływaniem ogniowym.. Po wypracowaniu decyzji następuje etap jej wdrażania, tj. stawiania zadań i organizowania działań bojowych.

Proces wypracowania decyzji w zakresie użycia sił i środków walki elektronicznej realizowany jest w wydziale rozpoznawczym (G2) sztabu dywizji i nazywany jest etapem wypracowania koncepcji prowadzenia WE.

Wypracowanie decyzji rozpoczyna się po otrzymaniu rozkazu operacyjnego dowódcy korpusu (niekiedy poprzedzony jest on zarządzeniem przygotowawczym albo wstępnym zarządzeniem operacyjnym). Po otrzymaniu takiego dokumentu oficerowie G2 z sekcji (komórki) walki elektronicznej (WE), którzy przeprowadzają analizę zadania pod kątem prowadzenia działań elektronicznych i przystępują do rozpoczęcia procesu elektronicznego przygotowania pola walki.

Przygotowanie zakłócania informacyjnego to proces, do którego realizacji wymagana jest rozległa widza aby poprawnie i ze znawstwem wykonać pracę jaka w obecnych warunkach ciąży na sekcji walki elektronicznej. Rozszyfrowanie danych o przeciwniku stawia przed rozpoznaniem elektronicznym najwyższe wymagania. Poprawnie wykonana prognoza zagrożenia elektronicznego to połowa sukcesu, gdyż nie zawsze dysponuje się wystarczającą ilością czasu oraz możliwościami zapewniającymi kontrolę całego obszaru odpowiedzialności rozpoznawczej.

Proces przygotowania zakłócania informacyjnego integruje doktrynalne zasady działania sił i środków elektronicznych i informatycznych przeciwnika z pogodą

i terenem oraz wiąże te czynniki z zadaniem i sytuacją na polu walki. W ten sposób daje podstawę do oceny możliwości działania tych sił i środków przeciwnika (wskazuje wrażliwe miejsca i prawdopodobną strategię działania) oraz planowania użycia własnych jednostek elektronicznych i ich prawidłowego ugrupowania na polu walki. Oficerowie komórki walki elektronicznej z G2 rozpoczynają powyższy proces z chwilą otrzymania zadania, ale czas jego rozpoczęcia jest uzależniony do ewentualnych zmian na polu walki[24]. Dane na temat potencjalnego przeciwnika (sił i środków elektronicznych oraz zasad użycia), strefy odpowiedzialności rozpoznawczej (SOR), terenu i pogody gromadzone są już w czasie pokoju (w bankach danych). Wykorzystując odpowiednie programy komputerowe i bazy danych (o dużej pojemności przechowywania) istnieje możliwość analizy terenu oraz prognozy pogody w obszarze operacji, co znacznie skraca czas pracy komórki i całego wydziału rozpoznawczego – G2. Wnioski w tym zakresie przedstawia się w postaci opisowej i graficznej na oleatach.

Istotą procesu przygotowania zakłócania informacyjnego jest analiza danych, której wynikiem będzie redukcja niepewności (wątpliwości) dotyczących działania sił elektronicznych i informatycznych przeciwnika, pogody i przeszkód terenowych w strefie odpowiedzialności rozpoznawczej oraz zainteresowania w działaniach bojowych. Między innymi należy określić wielkość strefy i zakres wykorzystania spektrum elektromagnetycznego, które mają decydujący wpływ na skuteczność zakłóceń.

Wielkość SOR określona przez przełożonego i zakres częstotliwości pracy środków elektronicznych przeciwnika wiąże się po pierwsze z normami prowadzenia działań bojowych przez siły i środki oceniającego, po drugie z rodzajem działań bojowych (obronne, zaczepne). Przełożony znając możliwości bojowo-rozpoznwcze podwładnego nie powinien wyznaczać zbyt rozległego obszaru odpowiedzialności rozpoznawczej. Inną miarą zakresu zadań mogą być siły i środki przeciwnika działające w SOR na oceniającego, zależne od rodzaju prowadzonych działań bojowych, warunków terenowych oraz jakości środków walki.

[24] Podczas gwałtownych zmian na polu walki może zaistnieć taka sytuacja, że proces decyzyjny do zakłócania informacyjnego rozpocznie się zanim zostanie przekazane zadanie bojowe. Wówczas proces ten rozpocznie się tylko częściowo i dotyczyć będzie przede wszystkim oceny sił i środków elektronicznych. Zdarzenie takie może mieć miejsce gdy jednostka będzie już w walce i strefa odpowiedzialności rozpoznawczej jest jej częściowo znana, a szczegóły zadania otrzyma później.

Można więc stwierdzić, że uzyskiwane właściwych wyników podczas oceny przeciwnika wiąże się z prowadzeniem tego procesu w takim obszarze i zakresie częstotliwości aby obejmowała co najmniej pas działań bojowych szczebla oceniającego oraz obszary na prawo i lewo o jeden szczebel niżej (w zależności od rodzaju działań ta szerokość będzie inna) a natomiast zakres częstotliwości powinien obejmować pasmo częstotliwości wykorzystywane przez dany rodzaj wojsk[25].

W praktyce wyróżnia się następujące formy oceny sił i środków elektronicznych i informatycznych przeciwnika:

1) Indywidualna; dokonywana przez dowódcę, szefa sztabu lub szefa komórki G2;
2) Kolektywna; prowadzona przez dowódcę oraz zespół oficerów z G2 i G3 w składzie których powinien znajdować się oficer walki elektronicznej;
3) Prowadzona z wykorzystaniem środków automatyzacji procesu dowodzenia.

W zależności od stylu pracy dowódcy oraz sztabu, a także od posiadanych umiejętności, wiedzy i środków technicznych wspomagających proces decyzyjny oraz organizacyjny dowódca narzuca odpowiednią formę pracy. Forma ta będzie obowiązywała w całym sztabie. Nie zawsze jest ona optymalna dla wszystkich oficerów, ale dowódca ponosi odpowiedzialność za podjęte decyzje.

Umiejętne stosowanie ogólnie przyjętych metod badawczych przyczynia się do osiągnięcia poprawnych wyników oceny, zapewniających pełne wykorzystanie danych i sporządzenie prognozy zagrożenia elektronicznego w wymaganym czasie.

Polega to na realizacji kolejnych etapów postępowania w czasie oceny przeciwnika (wstępna ocena dotychczasowych danych o siłach elektronicznych przeciwnika, wnioskowanie przygotowawcze, wnioskowanie zasadnicze, zestawienie wyników wnioskowania). Jest to kolejność postępowania oceniającego.

Metody szczegółowe to: analiza, synteza, porównanie, analogia, wnioskowanie redukcyjne, wnioskowanie dedukcyjne. Metody te są przywiązane do poszczególnych etapów oceny i prognozy. We wstępnej ocenie stosuje się analizę i syntezę, w okresie przygotowawczym stosuje się przede wszystkim wnioskowanie redukcyjne (od szczegółu do ogółu) i analogię, w okresie zasadniczym stosuje się wnioskowanie dedukcyjne (od ogółu do szczegółu), analogię i porównanie. „Ogół" w powyższym przypadku oznacza model i cel działania przeciwnika, „szczegół" – elementy zamiaru przyszłych działań bojowych.

[25] Przykładowo zakres UKF wojsk lądowych obejmuje częstotliwości od 20 do 88 MHz.

Znajomość metod badawczych nie należy interpretować jako „przenaukowienie" procesu oceny przeciwnika, gdyż wielokrotnie w sposób nieświadomy oficerowie komórki walki elektronicznej stosują je w praktyce. Racjonalnego postępowania przy rozwiązywaniu problemów złożonych, a takimi są działania zbrojne, oficerowie uczą się przed wszystkim w czasie ćwiczeń.

Wybór metody postępowania będzie miał wpływ na wnioski jakie sekcja WE musi wypracować w procesie wypracowania decyzji. Stosowanie powyższych wnioskowań przyczynia się do usprawnienia tego procesu i podjęcia właściwej decyzji.

Graficzna ocena sytuacji odzwierciedla prawdopodobne elektroniczne działanie przeciwnika, co pozwala dowódcy wpływać na przebieg bitwy, a nie biernie reagować na działanie przeciwnika. W trakcie działań wojennych graficzna ocena sił elektronicznych i informatycznych przeciwnika oraz zadania bojowe mogą ulegać zmianie wraz z dynamicznie rozwijającą się sytuacją na polu walki. Wskazanie najsłabszych punktów w ugrupowaniu przeciwnika oraz czasu i kierunku przemieszczenia się jego wojsk pozwala na przejęcie inicjatywy przez wojska własne nad przeciwnikiem.

Powyższy proces z dużym prawdopodobieństwem umożliwia dowódcom określić cele wysoko opłacalne (HPT)[26], między innymi cele elektroniczne, w obszarze walki. Będą to najważniejsze cele, na podstawie których zbudowana jest koncepcja walki dowódcy. Cele te należy atakować tak, aby zmniejszyć efektywność oddziaływania sił przeciwnika, opóźniać jego działanie lub wymusić na przeciwniku użycie kolejnych sił (odwodów), które mogą stać się przedmiotem kolejnego ataku ogniowego, oddziaływania elektronicznego, dywersyjnego lub propagandowego.

Proces ten powinien uwzględniać ocenę oddziaływania środków elektronicznych przeciwnika na tyły wojsk własnych.. Dowódcy jednostek powinni być świadomi skutków oddziaływania przeciwnika również na elementy logistyczne i to zarówno w działaniach zaczepnych jak i obronnych. Dlatego oficerowie komórki WE powinni rozpatrywać wszystkie możliwe warianty wykorzystania środków elektronicznych przeciwnika.

Innym aspektem wypracowania decyzji, patrząc na wymiar powietrzno lądowy są działania w przestrzeni powietrznej. Oprócz szerokości i głębokości pola walki w nowoczesnej i dynamicznej wojnie od dowódcy wymaga się zdolności

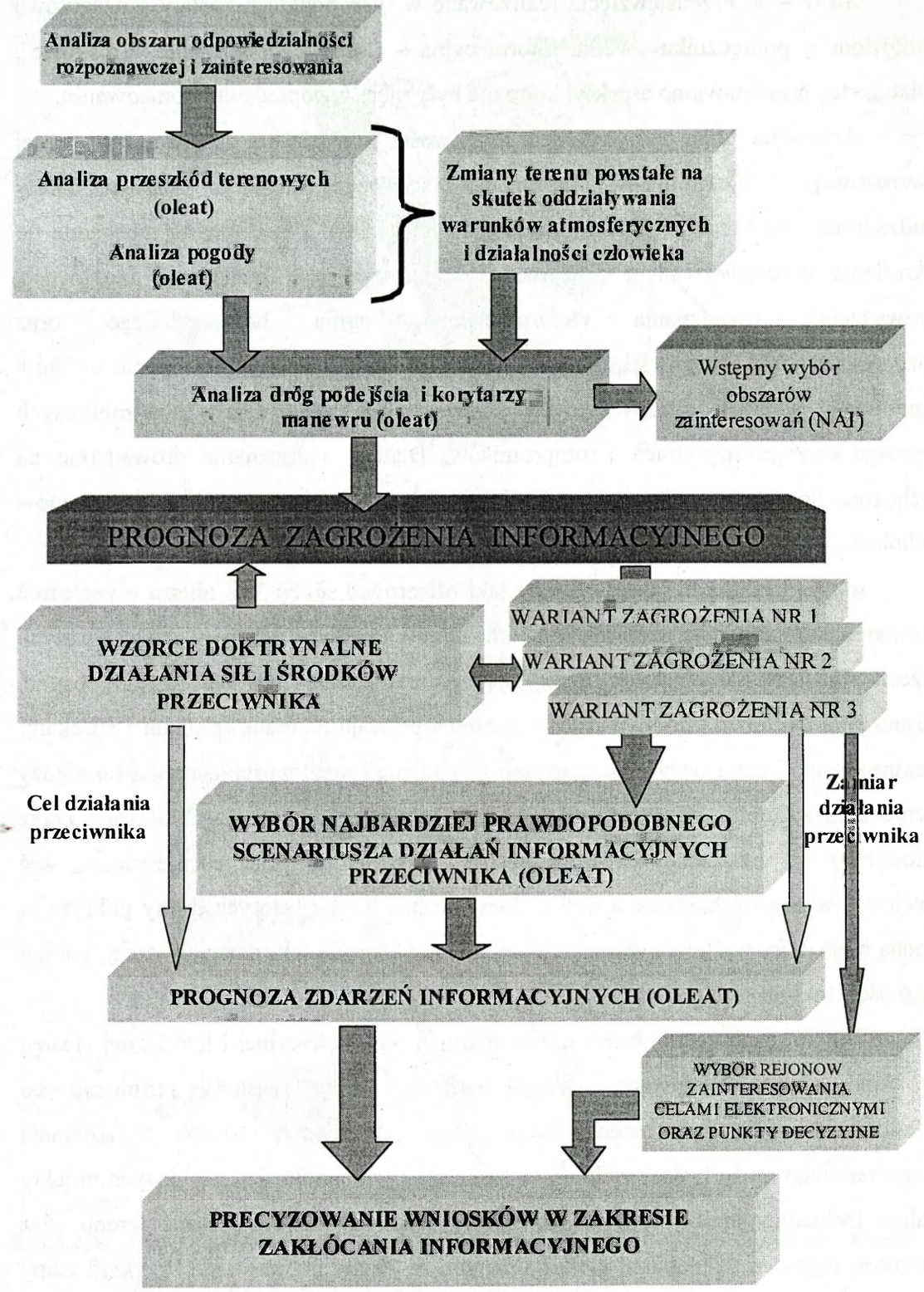
[26] HPT (High payoff targets) Cele wysoko opłacalne. Są to najbardziej istotne cele wynikające z sytuacji bojowej (elektronicznej).

uzmysłowienia sobie trzeciego wymiaru i zagrożenia nie tylko z lądu ale i z powietrza. Poznanie sposobów użycia sił powietrznych (ich systemów rozpoznania i zakłócania), w tym lotnictwa wojsk lądowych i obrony powietrznej, pozwala na uzyskanie sukcesu w starciu zbrojnym. Konflikt zbrojny w Zatoce Perskiej dobitnie wskazał, iż działania elektroniczne w przestrzeni powietrznej są integralną i pierwszoplanową częścią działań bojowych, o czym nie mogą zapominać analitycy prognozujący działania w strefie taktycznej (operacyjnej i strategicznej).

W procesie przygotowania zakłócania informacyjnego przedstawia się elektroniczne warianty zagrożenia, które wykonywane są aby odzwierciedlić (graficznie i opisowo) siły i środki walki elektronicznej przeciwnika, węzły elektroniczne i łączności oraz zakres ich oddziaływania. Analizie podlegają możliwości bojowo-rozpoznawcze sprzętu walki elektronicznej przeciwnika lądowego i powietrznego (urządzenia naziemne, samoloty wsparcia, śmigłowce i BŚR), sposoby jego działania oraz słabe punkty w ugrupowaniu.

Przebieg procesu przygotowania zakłócania informacyjnego (schemat 3.2.1) jest następujący:

1. Analiza obszaru odpowiedzialności rozpoznawczej i zainteresowania (na podstawie informacji otrzymanych od przełożonego, sąsiadów a w działaniach w styczności od własnych elementów);
2. Analiza terenu pod względem przeszkód terenowych utrudniających rozprzestrzenianie się fal EM, obszarów zakrytych dla fal EM;
3. Analiza pogody pod kątem rozprzestrzeniania fal elektromagnetycznych;
4. Ocena dróg podejścia i wykonywania manewrów pododdziałami elektronicznymi przeciwnika (węzłami łączności, węzłami elektronicznymi), szczególnie pododdziałami WE;
5. Prognoza zagrożenia informacyjnego a w niej;
   - ocena bieżącej sytuacji elektronicznej i informatycznej;
   - porównanie wzorców doktrynalnych działania przeciwnika z bieżącą sytuacją elektroniczną i informatyczną;
   - prognoza działania sił i środków przeciwnika;
6. Prognozowanie zdarzeń informacyjnych;
7. Precyzowanie wniosków w zakresie potrzeb zakłócania informacyjnego (ocena posiadanych sił i środków, ich możliwości w aspekcie wykonywanego zadania).



Rysunek 3.2.1. Przebieg procesu planowania zakłócania informacyjnego

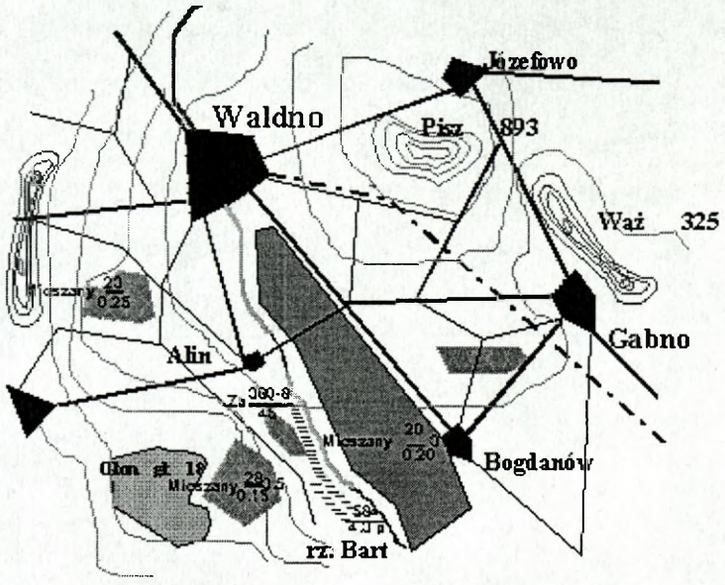
Ad. 1 – 4. Przedsięwzięcia realizowane w tych punktach zostały szczegółowo omówione w podręczniku „Walka informacyjna – Część I Rozpoznanie Wojskowe". Dlatego też przedstawiono aspekty, które nie były ujęte w poprzednim opracowaniu.

Analizując teren pod względem możliwości prowadzenia obserwacji optycznej (wzrokowej) i elektronicznej (horyzontu radiowego), analityk rozważa strefy widzialności wzrokowej i horyzontów radiowych (LOS)[27]. Strefy te są niezbędne do określenia w rozpatrywanym obszarze charakterystycznych punktów i możliwości prowadzenia rozpoznania elektronicznego, ognia bezpośredniego oraz rozprzestrzeniania energii elektromagnetycznej. Bardzo często rozmieszczenie środków ogniowych, punktów obserwacyjnych i miejsc dyslokacji środków elektronicznych wymaga szeregu uzgodnień i kompromisów. Dlatego rozpoznanie prowadzone na głębokość horyzontu radiowego realizuje się między innymi przy użyciu systemów radiolokacyjnych i rozpoznania elektronicznego.

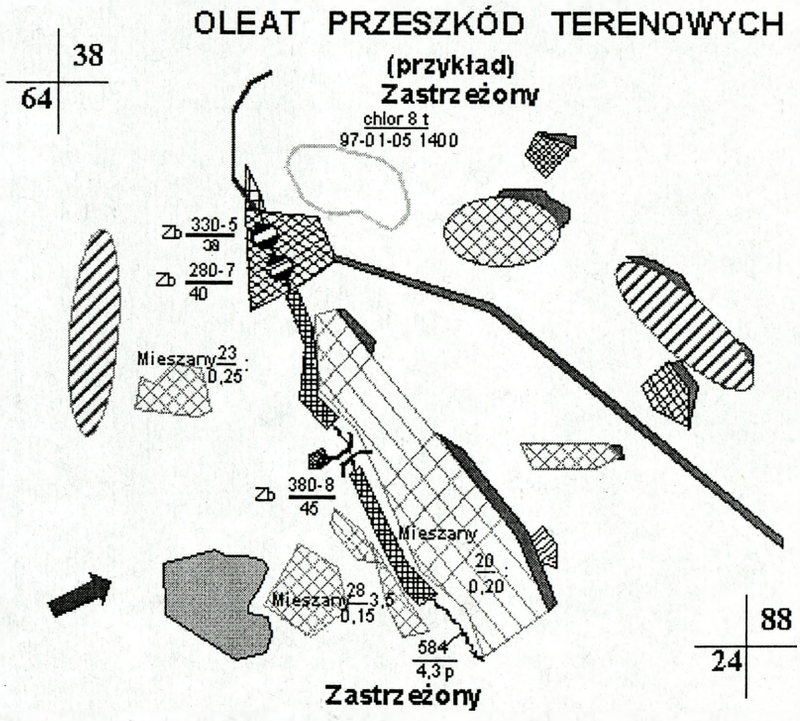
Innym czynnikiem oceny terenu jaki oficerowie sekcji WE muszą uwzględnić jest określenie zdolności manewrowych elementów i całych systemów elektronicznych przeciwnika i wojsk własnych. Przeszkody naturalne, takie jak lasy, jeziora, bagna, wzniesienia terenowe i góry, w istotny sposób wpływają na manewr siłami i środkami elektronicznymi mają wpływ na czas jego wykonania i możliwości łączności pomiędzy elementami systemu. Infrastruktura terenu (przeszkody terenowe wybudowane przez człowieka) tj. urządzenia hydrotechniczne, elektrownie, linie energetyczne, sieć kolejowa, wysoka zabudowa, a nawet domy wolno stojące, których dachy pokryte są blachą mają duży wpływ na rozprzestrzenianie się energii elektromagnetycznej, zaniku łączności, zakłóceń na ekranach SRL.

W celu utrudnienia obserwacji wzrokowej, radiolokacyjnej i termicznej stosuje się kolorowe, metalizowane, dymy, aerozole, mgły, zasłony termiczne co w konsekwencji utrudnia ocenę terenu. Ten podstawowy sposób maskowania bezpośredniego może być uzupełniany przez całą gamę środków pozorujących obiekty realne. Dokładna analiza tych czynników wpływa na właściwą ocenę terenu oraz prognozę zagrożeń działaniami elektronicznymi ze strony przeciwnika. Przykład mapy terenu otrzymanej z sekcji topograficznej i wykonanej na jej podstawie oleaty przeszkód terenowych ilustrują rysunki 3.2.2 i 3.2.3.

[27] LOS (Line of sight) - Linia obserwacji (widzialności).



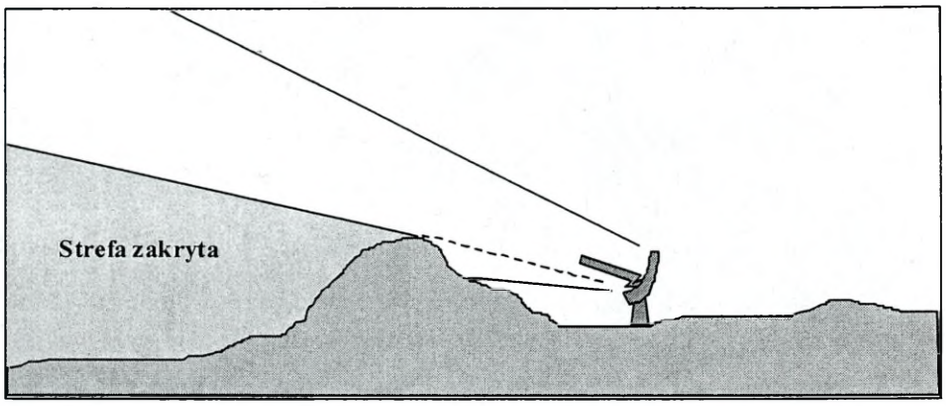
Rys.3.2.2. Przykładowa mapa terenu z wyszczególnionymi przeszkodami terenowymi otrzymana z sekcji topograficznej



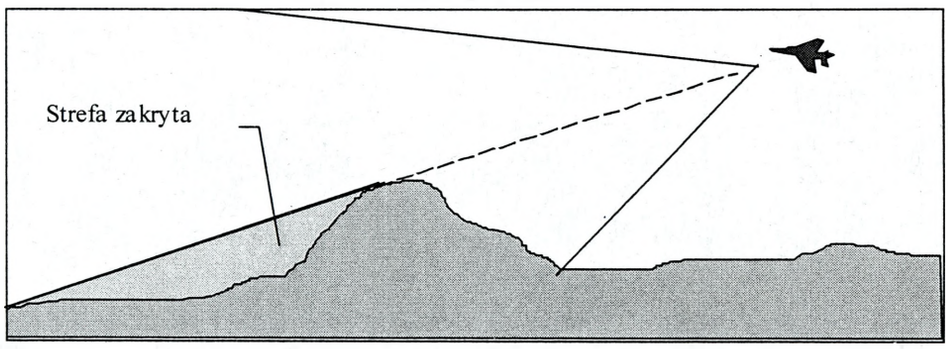
Rys.3.2.3. Oleat przeszkód terenowych z przeszkodami utrudniającymi manewr pododdziałom elektronicznym wykonywany przez sekcję WE

Obok lądowych dróg podejścia analizie poddaje się drogi podejścia w przestrzeni powietrznej. Oleat z taką drogą podejścia również nie jest wykonywany przez analityków sekcji WE. Analitycy korzystają z przygotowanych powietrznych dróg podejścia samolotów i śmigłowców wykonanych przez oficerów z zespołu

planowania powietrznego wchodzących w skład sekcji planowania i kierowania rozpoznaniem G2. Podczas gdy w działaniach naziemnych rozpatrywane są głównie strefy widzialności optycznej i horyzontu radiowego, to w działaniach powietrznych rozpatruje się skośną i pionową linię horyzontu radiowego. Rysunki 3.2.4 i 3.2.5 przedstawiają skośną linię horyzontu radiowego (wzrokowego) z ziemi i z powietrza, natomiast rysunek 3.2.6 przedstawia pionową linię widoczności (LOS) z powietrza.

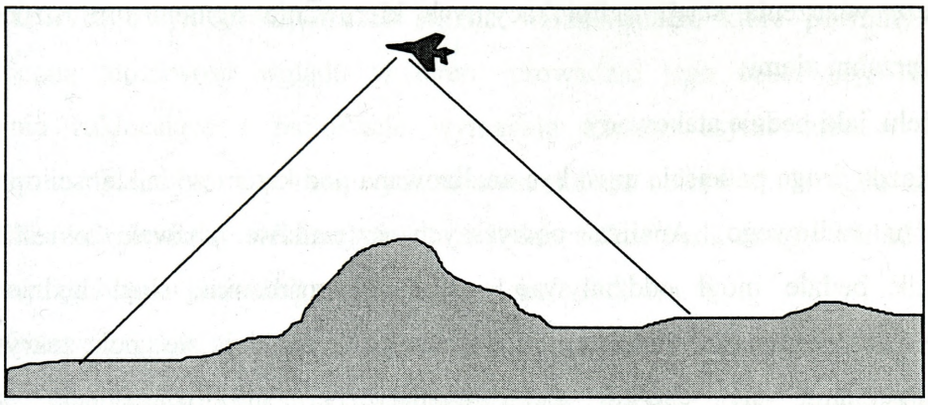


Rys. 3.2.4. Ukośna linia widoczności z ziemi



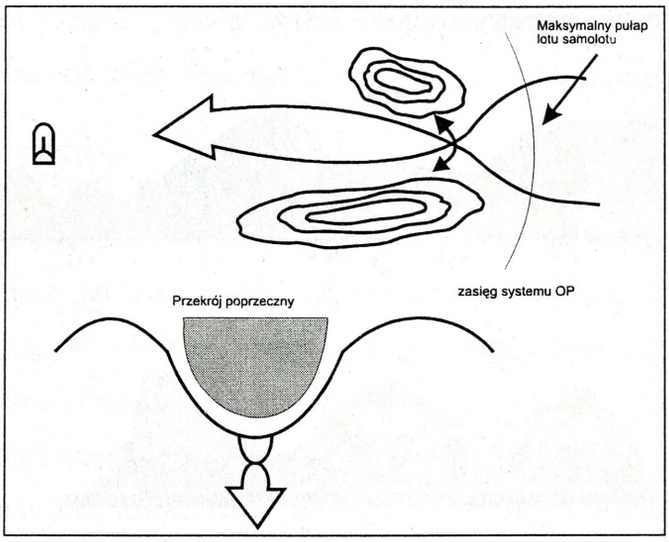
Rys .3.2.5. Ukośna linia widoczna z powietrza

Analizę przestrzeni powietrznej prowadzi się dla określenia tras, które gwarantują najlepszą ochronę lotnictwu wchodzącemu w obszar pola walki, oraz tych, które stwarzają samolotom najlepsze warunki przeprowadzenia ataku na cel w warunkach zakłócania elektronicznego. W toku analizy rozważa się: po stronie własnej miejsca dyslokacji środków obrony powietrznej, radiolokacyjnych i walki elektronicznej oraz określa gdzie lotnictwo może uzyskać najlepsze warunki do prowadzenia ognia oraz zakłócania elektronicznego, a po stronie przeciwnika rejony dyżurowania samolotów w powietrzu, z których można spodziewać się zakłóceń elektronicznych.



Rys. 3.2.6. Pionowa linia widoczności

Powietrzna droga podejścia powinna pozwalać na manewr i jednocześnie umożliwiać maskowanie przede wszystkim przed systemami obrony przeciwlotniczej ZT przeciwnika. Rysunek 3.2.7 przedstawia przykład powietrznej drogi podejścia.



Rysunek 3.2.7. Przykład powietrznej drogi podejścia[28]

Dodatkowo analiza powietrznych dróg podejścia musi uwzględnić niestałe czynniki, - takie jak:

— typy aparatów latających w danym nalocie;

— maksymalny pułap praktyczny tych aparatów;

— profil ataku, jaki może zostać wykorzystany w danym nalocie;

— systemy broni i uzbrojenia użyte w danym nalocie;

— strefy dyżurowania w obrębie strefy odpowiedzialności rozpoznawczej ZT, z których należy spodziewać się zakłóceń elektronicznych lub możliwe jest prowadzenie rozpoznania elektronicznego;

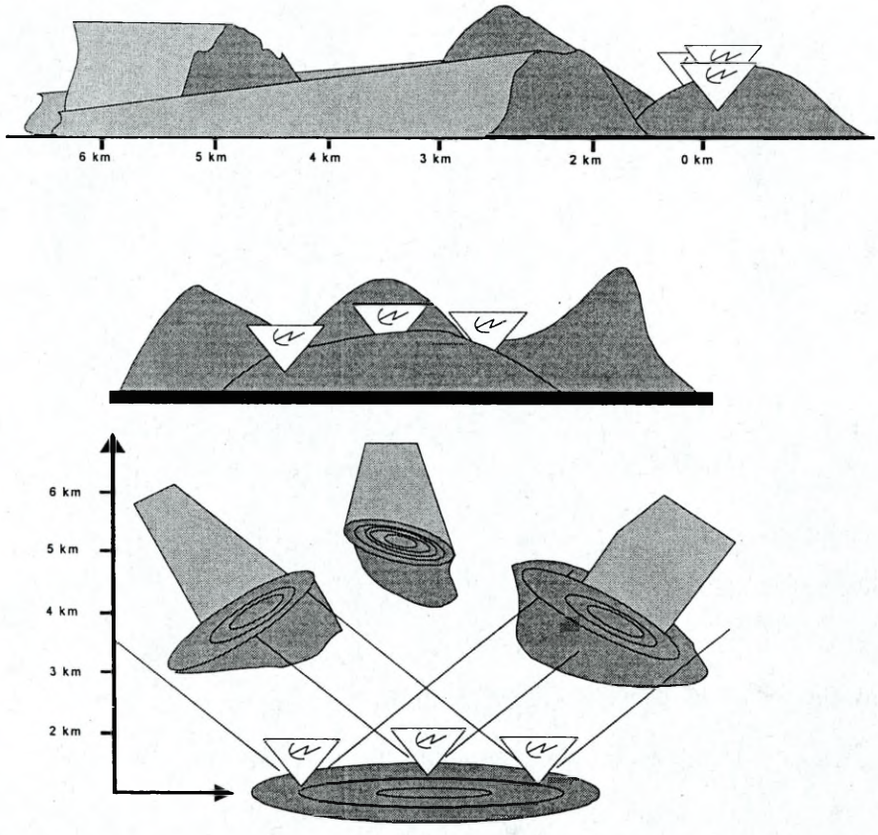
[28] FM -34-130, Inteligence Preparation of the Battlefield, Headquarters, Department of the Army, May 1989

— rubieże włączenia stacji radiolokacyjnych kierowania ogniem lub rozpoznania powierzchni ziemi;

— typ celu, jaki będzie atakowany.

Każda droga podejścia musi być analizowana pod kątem widzialności optycznej i horyzontu radiowego. Analiza powyższych czynników pozwala określić czy przeciwnik będzie mógł oddziaływać ogniem bezpośrednim, skąd będzie mógł prowadzić zakłócenia elektroniczne, jak również gdzie znajdują się „pola zakryte" dla rozprzestrzeniania się energii elektromagnetycznej lub rozwinięcia sprzętu elektronicznego.

Rozpatrując wykorzystanie przez przeciwnika środków łączności UHF i VHF na drogach podejścia połączony zespół oficerów WE i sił powietrznych dokonuje analizy przeszkód terenowych. Brak łączności może być spowodowany złą pogodą lub wysokimi przeszkodami terenowymi (rys. 3.2.8).



Rys. 3.2.8. Przeszkody terenowe i ich wpływ na obserwację

Taki teren ogranicza emisję fal elektromagnetycznych wysyłanych przez stacje radiolokacyjne nadzorujące pole walki lub wykrywające cele powietrzne. Pododdziały

radiotechniczne zwykle rozmieszcza się na wzniesieniach, które powinny (mając niezakłóconą możliwość wglądu w teren) prowadzić jego obserwację. Również urządzenia zakłócające i radiostacje wymagają takiego usytuowania w terenie, w którym strefy horyzontów radiowych w stosunku do obiektów nie będą utrudniać pracy własnych środków elektronicznych, a jednocześnie będą mogły zakłócać pracę środków przeciwnika prowadzących korespondencję radiową.

Oleat przeszkód terenowych z liniami widoczności optycznej i radiowej, stanowi podstawę do określania rejonów „zakrytych" oraz miejsc, gdzie przeciwnik może rozmieścić swoje środki elektroniczne.

Ad. 5. Prognoza zagrożenia informacyjnego stanowi część składową prognozy zagrożenia ogólnego, a w procesie wypracowania decyzji, jest to jeden z jej filarów służący poprawnemu jej opracowaniu. Rozpatrując zagadnienia związane z położeniem, stanem i możliwościami oddziaływania elektronicznego oraz przewidywanym charakterem działań sił elektronicznych przeciwnika jest elementem, który trudno przecenić.

Drugim aspektem prognozy jest element praktycznej wiedzy z zakresu przygotowania i prowadzenia działań taktycznych przez pododdziały elektroniczne przeciwnika. Poziom jej znajomości lub niewiedzy decydują często o skutkach prowadzonej walki. W okresie pokoju przygotowanie odpowiednich materiałów służących poszerzeniu wiedzy o siłach i środkach elektronicznych przeciwnika powinien zajmować się zespół rozpoznania studyjnego w sekcji WE G2. Dane do tych materiałów powinny być uzupełniane na bieżąco z własnych źródeł rozpoznawczych i od przełożonego.

Do zasadniczych wymagań stawianych zespołowi prognozy zagrożenia elektronicznego zdaniem autorów należy:

— znajomość i świadomość celu działania;
— szczegółowa i wnikliwa znajomość sił i środków elektronicznych przeciwnika;
— ciągłość i systematyczność pracy;
— umiejętność prognozowania zagrożenia;
— bazowanie na informacjach wiarygodnych;
— uwzględnienie wszystkich zależności i czynników mogących mieć wpływ na przyszłe działania elektroniczne przeciwnika;
— w wynikach prognozy zachowanie proporcji w szczegółowości i ogólności;

— przestrzeganie terminowości podczas dokonywania prognozy;

— formułowanie wniosków z przeprowadzonej prognozy w sposób syntetyczny.

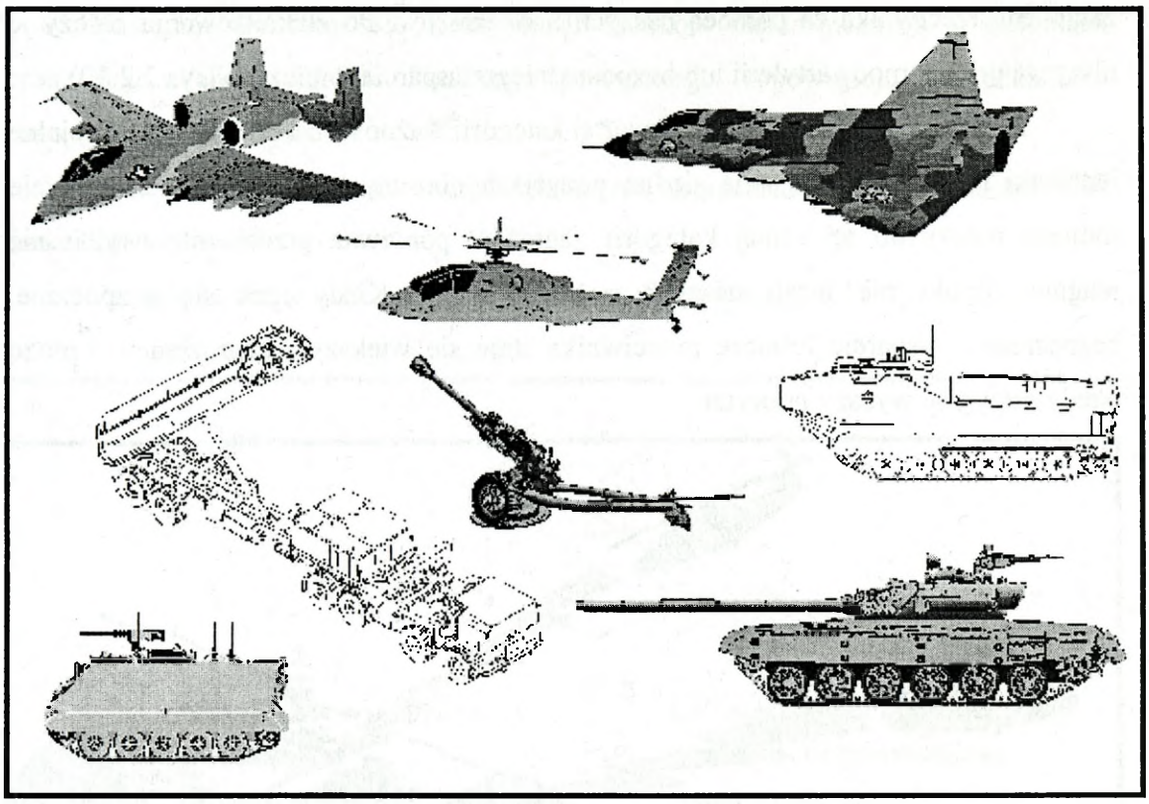
Prognoza zagrożeń informacyjnych polega na określeniu podstawowych danych dotyczących zagrożenia i możliwości bojowych (oddziaływania elektronicznego) przeciwnika. Dokumenty oceny zagrożeń elektronicznych wykonuje się w postaci tabel, schematów, wykresów oraz graficznie na oleatach (np. węzłów elektronicznych, łączności, ugrupowania sił i środków walki elektronicznej, działania lotnictwa i innych). Z punktu widzenia walki elektronicznej prognoza zagrożenia pociąga za sobą opracowanie danych w aneksie walki elektronicznej do rozkazu operacyjnego dotyczącego działań systemów i środków elektronicznych oraz oceny zagrożeń jednostek elektronicznych. Szczegółowo ocenia się możliwości przeciwnika w zakresie zapewnienia łączności, prowadzenia walki elektronicznej i innych środków wykorzystujących energię elektromagnetyczną (np. stacje radiolokacyjne). Komputerowe bazy danych powinny zawierać informacje na temat stanu etatowego i rodzajów środków łączności, stanowisk dowodzenia poszczególnych szczebli, innych środków emitujących energię, ugrupowania środków rozpoznania i zakłóceń radiowych, a także środków elektronicznych, jakie mogą wystąpić na każdym szczeblu dowodzenia i w każdej jednostce organizacyjnej przeciwnika.

W etapie tym G2 i G3 identyfikują różnego rodzaju systemy broni i możliwe zagrożenie z ich strony (rys. 3.2.9).

Te systemy broni i funkcje zagrożeń są wyszczególnione według kategorii ważności na podstawie ich największej mocy bojowej i stopnia zagrożenia dla naszych jednostek.

Jednostki przeciwnika określa się w kategoriach ważności (od 1 do 4) na podstawie analizy potencjalnych zagrożeń z ich strony. Należy wyszczególnić każdą jednostkę ogniową oraz systemy broni w kategorii ważności i funkcjach zagrożeń.

Największe zagrożenie, pierwszej kategorii ważności, przyjmuje się dla elementów rozpoznawczych przeciwnika. Oczekuje się, że od elementów rozpoznawczych zależne są (przez przekazywanie poufnych danych) działania innych jednostek i systemów broni. Jeśli sukcesywnie zakłócimy te elementy, opóźnimy przekaz danych, a tym samym atak systemów broni. Zakłócanie opóźni czas reakcji ogniowej przeciwnika co jest równoznaczne z opóźnieniem czasu ataku na nasze siły.



Rys. 3.2.9. Identyfikacja systemów broni przeciwnika

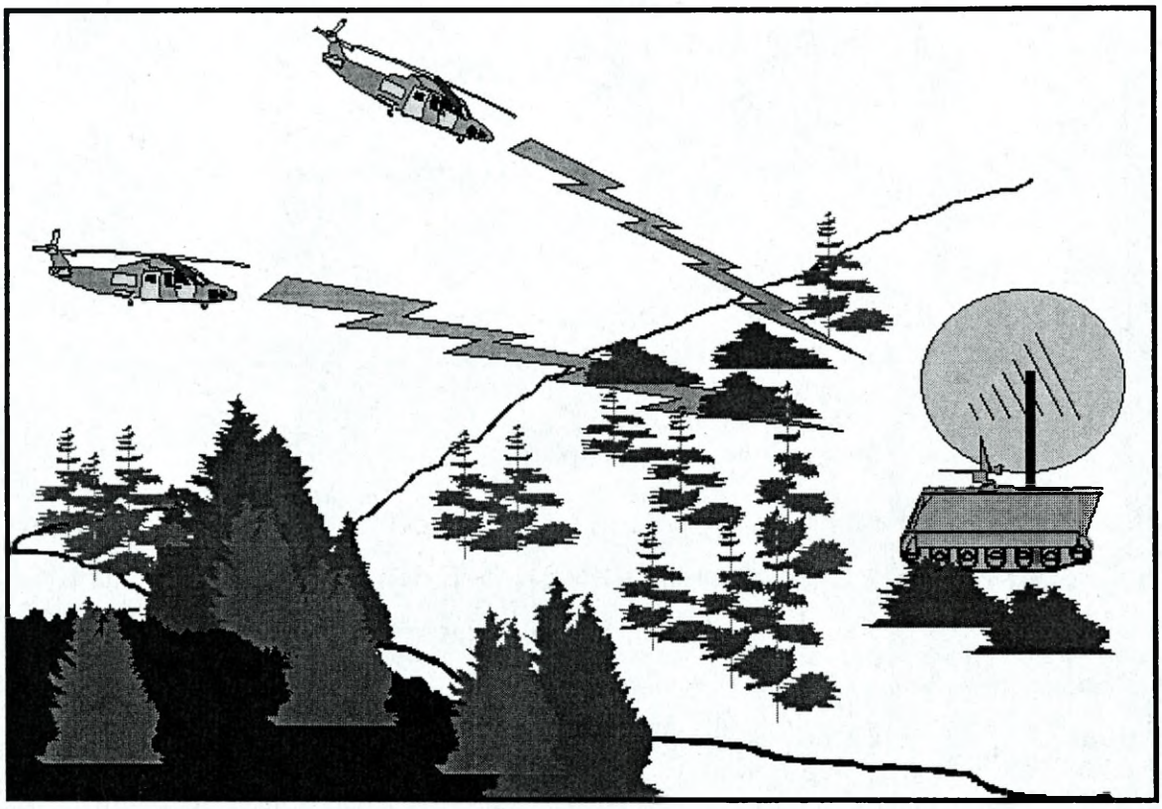
System kierowania przeciwpancernymi pociskami kierowanymi przeciwnika jest obiektem drugiej kategorii ważności. Przeciwnik może wykryć nasze siły szykujące się do ataku i rozpocząć ostrzeliwanie naszych kluczowych elementów. Kluczowe elementy obejmują: stan osobowy, systemy broni, czołgi, BWP itp. Zakłócenie łączności systemu ppk obniża koordynację i efektywne wykorzystanie tych systemów broni.

Zagrożenie ogniem artylerii należy do trzeciej kategorii ważności. Zakłóca się sieć kierowania ogniem artylerii pomiędzy dowództwem, posterunkiem obserwacyjnym, a bateriami ogniowymi. Dowódca dywizji może także dążyć do zniszczenia artylerii przeciwnika. W tym wypadku elementy rozpoznania elektronicznego mogą być wykorzystane do lokalizacji tych obiektów (celów) dla bezpośredniego wsparcia lotniczego.

Zagrożenie WE przeciwnika należy do czwartej kategorii ważności. Podczas atakowania przeciwnika możliwość użycia własnych radiostacji staje się bardzo ważna. Aby zapewnić wykorzystanie tych środków radiowych, należy zlokalizować stacje

zakłóceń przeciwnika za pomocą naszych namierników. Po zlokalizowaniu należy je niszczyć przy pomocy artylerii lub bezpośredniego wsparcia lotniczego (rys 3.2.10).

Siły manewrowe należą do czwartej kategorii ważności od czasu kiedy specjalne jednostki przeciwnika pojawią się na pozycjach obronnych. Bezpośrednie wsparcie lotnicze należy do tej samej kategorii zagrożeń, ponieważ przeciwnik zwykle nie reaguje dopóki nie ustali naszych punktów ataku. Kiedy atak się rozpocznie, bezpośrednie wsparcie lotnicze przeciwnika staje się większym zagrożeniem i może wtedy otrzymać wyższy priorytet.



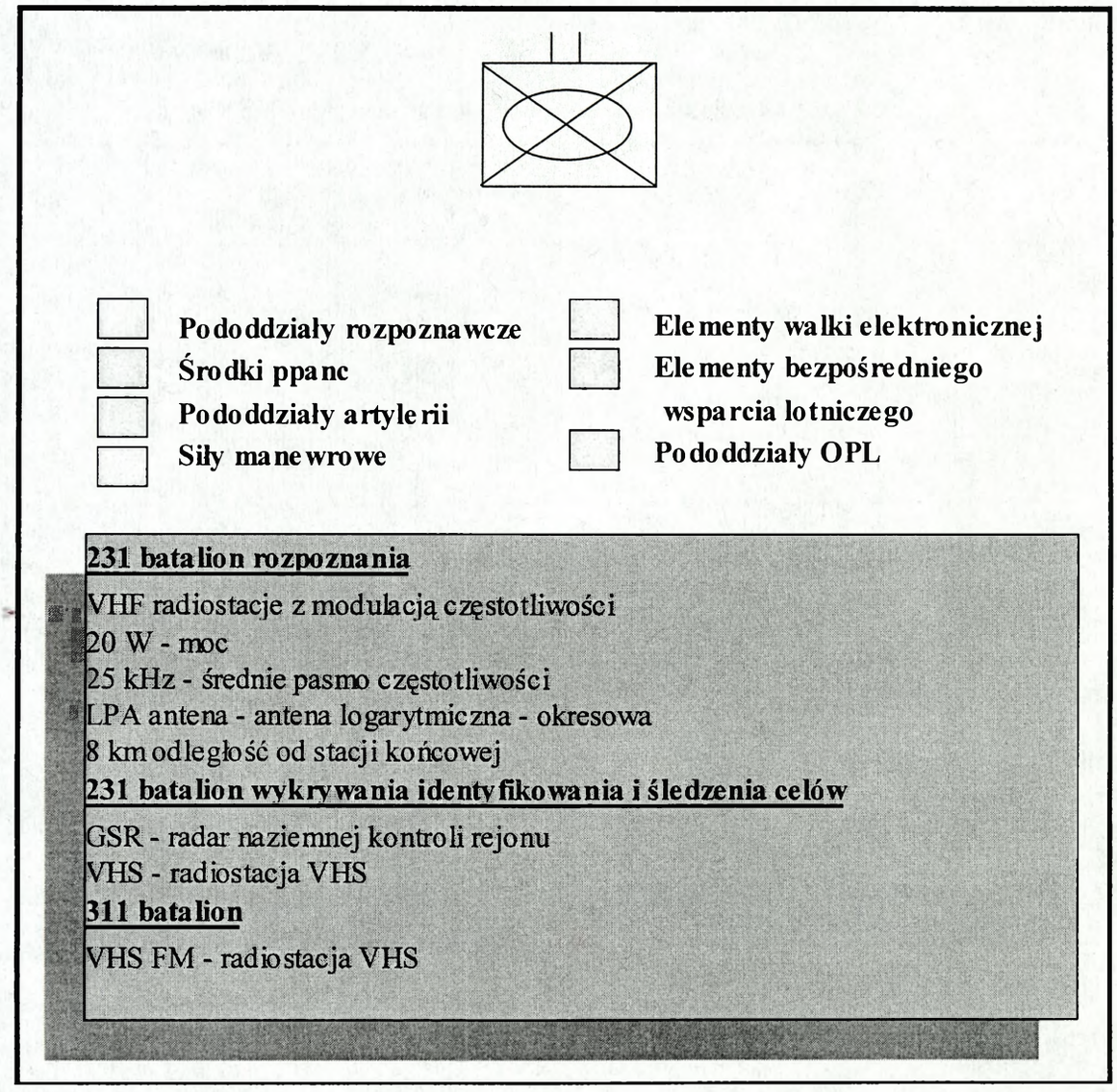
Rys. 3.2.10. Rażenie stacji zakłóceń przeciwnika

Artyleria przeciwlotnicza jest umiejscowiona na ostatnim miejscu w kolejności zagrożeń, ponieważ nasz atak może nie wymagać wsparcia powietrznego. Konieczne jest jednak utrzymanie w gotowości elementów rozpoznania elektronicznego do wykrywania i lokalizacji SRL przeciwnika w strefie działań bojowych. Jeśli nasz atak przeciąga się, możemy wykorzystać bezpośrednie wsparcie lotnicze dla osiągnięcia przewagi. Bezpośrednie wsparcie lotnicze prowadzi się w celu obezwładnienia stacji radiolokacyjnych przeciwnika (zlokalizowanych przez elementy rozpoznania elektronicznego), podczas gdy nasze stacje zakłóceń zakłócają jego radiostacje.

Następnie dokonuje się identyfikacji środków elektronicznych w systemach broni przeciwnika (3.2.11). Realizacja powyższego zobowiązuje do udzielenia odpowiedzi na dwa pytania:

1. Jakie systemy łączności współdziałają (są współzależne) z tymi środkami i ich funkcjami zagrożeń?

2. Jakie są znane dane taktyczno-techniczne tych systemów?



Rys. 3.2.11. Identyfikacja sił i środków elektronicznych przeciwnika

Zwykle znane są ogólne dane nt. systemów elektronicznych przeciwnika. Jest wiadomym, że niektóre systemy wykorzystują te same środki radiowe. Zakłócanie może być bardziej skuteczne w stosunku do jednych środków, a mniejsze w stosunku do innych. Ponadto pojedyncze zakłócenie nie spowoduje totalnej destrukcji systemów przeciwnika.

W tym etapie następuje wyraźny postęp w planowaniu, ponieważ tworzony jest plan obezwładnienia celów.

W etapie tym określa się dane taktyczno-techniczne środków elektronicznych przeciwnika (tabela 3.2.1). Powyższe przedsięwzięcie wymaga szczegółowej współpracy TCAE z EWS. TCAE planuje zakłócanie dla S3 (batalion informacji wojskowej) na podstawie wstępnego planowania rozpoczętego przez G2, G3 i EWS. TCAE określa listę celów z aneksu WE w kolejności kategorii ważności i następnie dane taktyczno-techniczne dla każdego celu.

Tabela 3.2.1

Dane taktyczno-techniczne środków elektronicznych przeciwnika

Jedn. przeci-nika	Częst.	Sygnał rozp.	Moc	Typ anteny	Wys. ant.	Odl do stacji kontroln	Pozycja nadajnika	Wys nad. n.p.m..	Pozycja odb.	Wys. Odb n.p.m..
81 br	44.25	AK17	20	WHIP	10	8 km	AT 245976	321 m	AT 435968	348 m
231 bat wykryw. Identyf. i śledzenia	40.50	TK12	20	WHIP	10	12 km	AT 765213	250 m	AT 976217	295 m
311 bat	26.25		25	0	26	16 km	AT 211283	225 m	AT 470531	325 m.
.										
.										
.										
.										
.										
.										
4 BZ	43.50	SK01	50	WHIP	30	10	AT648294	389 m	AT743219	409 m

Podaje się następujące dane:

— jednostka,

— częstotliwość,

— sygnał rozpoznawczy,

— typ anteny,

— wysokość anteny,

— odległość do stacji kontrolnej (sieci łączności),

— pozycja,

— lokalizacja nadajnika przeciwnika,

— wysokość n.p.m. nadajnika przeciwnika.,

— pozycja odbiornika przeciwnika,

— wysokość n.p.m. odbiornika przeciwnika.

Doktrynalne wzorce działań przeciwnika powinny zawierać wszystkie informacje o sposobach działań taktycznych i sprzęcie przeciwnika zawarte w regulaminach i instrukcjach taktyczno-technicznych przekształcone w obraz graficzny. Powinny być tworzone w czasie pokoju, a ich aktualizacji dokonuje się na bieżąco na podstawie obserwacji z ćwiczeń dowódczo-sztabowych, ćwiczeń z wojskami, treningów, a także zmian w metodach szkolenia jednostek potencjalnego przeciwnika. Każda baza danych o siłach i środkach przeciwnika powinna podlegać modyfikacji, szczególnie gdy stwierdzimy wprowadzenie do jednostek elektronicznych nowego sprzętu.

Oprócz danych dotyczących systemów i sprzętu elektronicznego w bankach informacji powinny być gromadzone charakterystyki osobowo-zawodowe dowódców poszczególnych szczebli dowodzenia (jednostek elektronicznych). Są to informacje potrzebne do prognozowania zamiaru działania strony przeciwnej, którego należy spodziewać się po określonym dowódcy. Przygotowanie doktrynalnych wzorców działań przeciwnika spoczywa na przełożonym. Technika ich tworzenia jest różna w czasie pokoju i wojny. W czasie pokoju informacje o przeciwniku powinny być dostarczane przez przełożonego, a w czasie wojny nowe dane oraz informacje potwierdzające działanie przeciwnika jako pierwsze uzyskają pododdziały prowadzące walkę. Jest to więc obieg informacji odwrotny od pokojowego.

W obydwu przypadkach sekcja WE jest zobowiązana do posiadania aktualnej bazy danych o przeciwniku. Obowiązek aktualizacji baz danych spoczywa na sekcji WE w G2 zajmującej się wnikliwą analizą wszelkich konfliktów zbrojnych. Taktyka i sposoby wykorzystania sprzętu stosowanego w różnych konfliktach zbrojnych powinny być analizowane i przesyłane do zainteresowanych jednostek jako załączniki do obowiązujących instrukcji i regulaminów. Wzorce doktrynalne powinny być przechowywane w specjalnych bankach informacji. Po rozpoczęciu działań wojennych wzorce opisujące węzły elektroniczne wykorzystywane są do wskazywania ważnych obiektów, które należy obezwładnić oraz obiekty podlegające rozpoznaniu

elektronicznemu. Służą one także do wskazania celów, które powinny być niszczone środkami ogniowymi.

Informacje zawarte we wzorcach działań elektronicznych potwierdza sekcja walki elektronicznej, do której napływają dane od jednostek pełniących dyżury bojowe lub od przełożonego. Zweryfikowane dane służą do opracowania modeli doktrynalnych w czasie oceny zagrożenia przed rozpoczęciem działań wojennych, a w czasie jej trwania do ich korekty w zależności od zmian w ugrupowaniu przeciwnika.

Osobno tworzy się wzorzec zawierający informacje o węzłach łączności, kolejny o pozostałych urządzeniach emitujących energię elektromagnetyczną, a jeszcze inny o zasadach użycia sił i środków elektronicznych. Pomimo tego, że powstaje kilka wzorców dla jednego związku taktycznego, to pomagają one uniknąć dwuznaczności obrazu sytuacji elektronicznej. Wzorce powinny też uwzględniać liczbę i typ urządzeń związanych z każdym węzłem elektronicznym przeciwnika. Poziom szczegółowości oraz klasyfikacja tych wzorców zależy od obowiązujących wymagań.

Do pełnego zobrazowania sytuacji elektronicznej niezbędna jest również analiza działań przeciwnika powietrznego i systemów przeciwlotniczych. Dlatego ze szczególną uwagą powinno się analizować wzorce doktrynalne działań samolotów (śmigłowców) i elementów OPL. Wykonując wzorce doktrynalne węzłów łączności i węzłów elektronicznych na potrzeby oceny i prognozy zagrożenia ze strony przeciwnika (np. zakłócania radiowego), dokonujemy oceny tego zagrożenia o jeden szczebel w dół, gdy wojska własne są w obronie, a o dwa szczeble w dół, gdy prowadzimy natarcie.

Na szczeblu związku taktycznego sekcja walki elektronicznej zbiera dane z rozpoznania elektronicznego i zakłócania elektronicznego, które wykorzystuje do opracowania sytuacji elektronicznej oraz sprecyzowania kierunku działania przeciwnika oraz celu, jaki chce osiągnąć. Podległe pododdziały (np. batalion rozpoznawczy) analizują warianty zagrożenia elektronicznego i zdarzeń elektronicznych opracowane przez sekcję WE i przekształcają je do takiego poziomu szczegółowości, jaki wymagany jest dla wsparcia jednostek wykonujących zadanie bojowe.

Oleat sytuacji elektronicznej sekcja WE wykonuje na podstawie sytuacji bieżącej, wiadomości od przełożonego, jednostek ze styczności własnych pododdziałów oraz sąsiadów i innych źródeł (np. uchodźców, dezerterów, wojsk OT). Treścią tego dokumentu jest graficzny obraz odzwierciedlający sytuację elektroniczną połączoną z koncepcją doktrynalną, zgodną z obowiązującymi zasadami rozmieszczenia techniki

elektronicznej i prawdopodobnym zamiarem przeciwnika, bez dowiązania do terenu i warunków meteorologicznych. Celem sporządzenia tego oleatu jest stworzenie podstawy do dalszych rozważań nad prawdopodobnym działaniem przeciwnika. Dokument ten sporządzany jest na co najmniej dwóch oleatach, w takiej skali jak wykorzystywane mapy[29]. Na jednej oleacie rysowana jest aktualna liczba węzłów łączności a na drugiej inne emitery energii EM. Mogą być wytworzone kolejne wzorce, np. z rozmieszczeniem środków walki elektronicznej - będzie to tylko zależało od potrzeb i szczegółowości oceny.

Oleaty służą podobnie jak mapa sytuacyjna z elementami niepotwierdzonymi przez systemy rozpoznawcze, mogą też być traktowane jako jeden z wariantów działania. Dla przejrzystego zobrazowania sytuacji wszystkie potwierdzone wiadomości o przeciwniku uzyskane od przełożonego i podwładnych traktowane są jako pewne i nanoszone są linią ciągłą, natomiast położenie jednostek elektronicznych wynikające z zasad doktrynalnego działania przedstawia się liniami przerywanymi. W ten sposób powstaje przejrzysty prawdopodobny obraz aktualnego położenia elementów elektronicznycho wojsk przeciwnika (fotografia sytuacji).

Oleaty sytuacji elektronicznej stanowią pomocnicze narzędzie w ręku oficerów walki elektronicznej, niezbędne do określenia potrzeb w zakresie uzupełnienia danych o elementach elektronicznych.

Podczas oceny sytuacji elektronicznej analizuje się i ustala:

— ogólną ilość obiektów w pasie rozpoznania (w strefie odpowiedzialności rozpoznawczej dywizji);
— ilość źródeł rozpoznania obsługujących obiekty w pasie rozpoznania dywizji z podziałem na pasma częstotliwości;
— ilość i rodzaj obiektów oraz źródeł rozpoznania, które mogą się znaleźć w zasięgu rozpoznania elektronicznego w trakcie realizacji zadania;
— najbardziej prawdopodobne rodzaje emisji, ich ewentualną informatywność i cechy rozpoznawcze możliwe do identyfikacji w procesie rozpoznania;
— gęstość zajętości pasma częstotliwości.

W zakończeniu oceny sytuacji radioelektronicznej precyzuje się wnioski wynikające z potrzeb rozpoznawczych, to znaczy określa się liczbę obiektów i źródeł,

[29] L. Ciborowski, Planowanie i organizowanie walki zbrojnej wg poglądów NATO cz. II. Informacyjna preparacja pola walki, AON 1996, s.36.

których rozpoznanie jest konieczne (lub pożądane) z uwagi na zadania bojowe realizowane przez dywizję. Ponadto ustala się priorytety rozpoznawcze co do poszczególnych obiektów i źródeł.

Kolejnym etapem pracy oficerów walki elektronicznej będzie wypracowanie prawdopodobnych wariantów działania elektronicznego przeciwnika w walce. Wypracowane warianty potrzebne są między innymi oficerom komórki G3 i wsparcia ogniowego, do skoordynowania działań jednostek wykonujących zadanie bojowe.

Ad. 6. Warianty zdarzeń elektronicznych powinny być opracowywane z uwzględnieniem oceny realizowanej przez oficerów z sekcji planowania i kierowania rozpoznaniem. Na tej podstawie oficerowie sekcji walki elektronicznej określają prawdopodobny wariant działania przeciwnika oraz potrzeby w zakresie uzupełniania brakujących danych.

Wariant ten powinien uwzględnić wpływ pogody i terenu na działania bojowe przeciwnika oraz w określonym czasie opisowo lub w sposób graficzny prognozować jak jego siły i środki będą wykonywać manewr (np. wzdłuż dróg podejścia i korytarzy manewru z wykorzystaniem jakich środków łączności). Ponadto powinien podpowiadać w jakim zakresie działanie przeciwnika może odbiegać od wzorców doktrynalnych lub w jaki sposób przeciwnik może zmieniać szerokość i głębokość ugrupowania, czy rozmieszczenie elementów ugrupowania bojowego, aby sprostać wymaganiom pogody i terenu.

Rozważając wpływ pogody i terenu warunki rozprzestrzeniania się energii elektromagnetycznej oraz działań przeciwnika odbiegających od wzorców doktrynalnych, należy dokonać analizy jego możliwości w zakresie zapewnienia łączności, wykrywania celów, kierowania ogniem, rozpoznania i zakłócania elektronicznego. Analiza taka jest niezbędna w celu zapewnienia maksymalnej ochrony przed oddziaływaniem elektronicznym przeciwnika na systemy wojsk własnych. Opracowywany wariant zagrożenia elektronicznego powinien uwzględniać, które pozwolą na ustalenie urządzeń, za pomocą których przeciwnik może prowadzić rozpoznanie i zakłócanie elektroniczne oraz obszarów gdzie może prowadzić obserwację optyczną i radiolokacyjną.

Analitycy sekcji WE zwykle stosują technikę w której wzorce doktrynalne nakładane są na oleaty przeszkód terenowych i dróg podejścia - w celu określenia najlepszych linii horyzontu optycznego i radiowego (dla urządzeń emitujących energię elektromagnetyczną), którą przeciwnik może wykorzystać do zakłócania potencjalnych

celów (obiektów). Należy rozważyć także działania przeciwnika mające na celu maskowanie stanowisk dowodzenia (punktów obserwacyjnych) przed rozpoznaniem i zakłóceniami stosowanymi przez stronę przeciwną. W obrębie danego segmentu korytarza manewru analizuje się przewidywane rozmieszczenie jednostek przeciwnika (węzłów łączności) oraz innych emiterów energii. W trakcie wariantowania zdarzeń elektronicznych (sytuacji) muszą zostać rozważone normy taktyczne, sposoby i możliwości działania przeciwnika, szczególnie aby odzwierciedlić jego wysiłki zmierzające do uzyskania korzystnego stosunku sił oraz korzystnego tempa działań, zaskoczenia i gwałtownych uderzeń. Chociaż analiza informacji z rozpoznania elektronicznego z wariantami zdarzeń elektronicznych koncentruje się na liniach widzialności optycznej i radiowej, analizie muszą zostać poddane również i inne czynniki. Na przykład należy ustalić najlepsze obszary nadające się do ukrycia i maskowania, bądź ugrupowania wojsk, które zmniejszają możliwości rozpoznania przez przeciwnika i odwrotnie, obszary, które wojska własne wykorzystają do tych samych celów. Analiza musi uwzględniać rejony, z których przeciwnik może uzyskać jak najlepszą linię horyzontu radiowego.

W wariantach zdarzeń elektronicznych powinno się ujmować zarówno charakterystyki emisji elektromagnetycznych poszczególnych elementów, jak i ich umiejscowienie. Pogoda i teren mają wpływ na wykorzystanie systemów łączności i innych urządzeń emitujących energię oraz ograniczają rozmieszczenie poszczególnych elementów tych systemów. Charakterystyka wariantów użycia źródeł energii elektromagnetycznej zmienia się w zależności od czasu i miejsca na polu walki, coraz bardziej odbiegając od tego co zostało opisane. Oficerowie grupy rozpoznania i zakłóceń elektronicznych, dokonując analiz systemów elektronicznych i węzłów doktrynalnych, muszą się z tym liczyć i reagować na zmiany z odpowiednim wyprzedzeniem.

Po rozpoczęciu zbierania danych przez własne systemy, do sekcji WE przekazywane są aktualne dane o ugrupowaniu przeciwnika, jego ruchach oraz działaniach elektronicznych. Analitycy WE wstępnie opracowują napływające dane i porównują je z danymi zawartymi (opisanymi) w wariantach sytuacji, we wzorcu zagrożeń i węzłów elektronicznych, pozwala to:

- ◊ zebrać i przeanalizować dane oraz przekazać je przełożonemu i podległym jednostkom w celu wzbogacenia danych o przeciwniku;

- ◊ dokonać korekty wariantów zagrożenia elektronicznego i zdarzeń elektronicznych;
- ◊ dokonać identyfikacji emiterów energii elektromagnetycznej przez sekcję walki elektronicznej, wraz ze współpracującymi oficerami z innych rodzajów służb;
- ◊ skorygować lokalizację obiektów elektronicznych przeciwnika na podstawie ich cech identyfikacyjnych, ustalić linie rozgraniczenia wojsk oraz wyselekcjonować ważne cele[30] (obiekty) elektroniczne;

Efektem pracy oficerów WE z G2 jest opracowanie prawdopodobnego wariantu działania przeciwnika, co podczas odprawy decyzyjnej jest weryfikowane przez pozostałe komórki sztabowe. Finałem odprawy decyzyjnej jest akceptacja wybranego wariantu zagrożeń elektronicznych (wariant kompatybilny z wariantem zagrożenia wykonanym przez sekcję planowania G2), na podstawie którego następuje szczegółowe planowanie użycia pododdziałów elektronicznych. W przypadku gdy wariant wybrany przez G2 nie zostaje zaakceptowany, wraca się do pozostałych wariantów, wcześniej odrzuconych.

Przy wariantowaniu zdarzeń powinien również powstać plan alternatywny (zapasowy), który znacząco odbiega od wzorców doktrynalnych. Taki wariant działania przeciwnika, zazwyczaj przeczy logice działania i czasami jest sprzeczny z zasadami walki znanymi dotychczas stronie przeciwnej. Planem alternatywnym może być także odrzucony wariant zagrożenia z niektórymi elementami działania przeciwnika sprzecznymi z obowiązującymi normami.

Na podstawie wariantu zagrożenia elektronicznego (wspólnie z G2) sporządzany jest *wariant zdarzeń elektronicznych*. Swoją formą nie odbiega od oleatu zdarzeń wykonywanego prze oficerów z sekcji planowania i kierowania rozpoznaniem G2, różni się jednak położeniem rejonów zainteresowania (NAI) i ich znaczeniem (chociaż w niektórych przypadkach mogą się one pokrywać). Jeżeli czas pozwala, opracowuje się kolejne oleaty zdarzeń elektronicznych do pozostałych wariantów oceny zagrożenia. Połączenie danych z rozpoznania elektronicznego przełożonego i własnych elementów rozpoznawczych pozwala na określenie ważnych zdarzeń na polu walki oraz wytypowanie urządzeń promieniujących fale elektromagnetyczne, które dostarczają danych na temat kierunków prowadzonych działań przez przeciwnika i celów jakie

[30] Każdy cel jest obiektem, ale nie każdy obiekt jest celem.

pragnie osiągnąć. Oficer WE dokonujący analizy musi dostrzec różnicę pomiędzy zdarzeniami, które już zostały zaobserwowane, a tymi, które są tylko przewidywane. Ponadto kontroluje działania przeciwnika zmierzające do wprowadzania nas w błąd, aby nie dopuścić do skupienia wysiłku własnych jednostek rozpoznania na obiektach (obszarach) pozornych.

Po rozpoczęciu działań bojowych wiedza o tym, gdzie i kiedy może nastąpić istotne zdarzenie na polu walki, może zostać wzbogacona[31]. Wariant zagrożenia elektronicznego opisuje potencjalne cele (obiekty) elektroniczne, co może zostać wykorzystane przez siły własne. Gdy przeciwnik porusza się po drogach podejścia, wówczas rozpoznanie elektroniczne może ujawnić węzły łączności (elektroniczne) stanowisk dowodzenia i stacji kontroli w szczególnie ważnych (kluczowych) obszarach. Obszary te zostają oznaczone jako NAI.

Rejony zainteresowania celami nie zawsze będą się znajdować w drogach podejścia. Często występować będą poza nimi, ze względu na specyfikę pracy oraz możliwości bojowe sprzętu elektronicznego. Rejony te dlatego są ważne, że znajdują się w najbardziej prawdopodobnych miejscach ważnych zdarzeń czy też działań na polu walki oraz dlatego, że mogą w nich występować cele wysoko opłacalne[32].

Rejony zainteresowania stanowią podstawę do wariantowania zdarzeń, ponieważ wskazują kierunki działania przeciwnika, ogniskują zbieranie danych oraz są uwzględniane w opracowaniu wymagań wobec informacji pozyskiwanych przez rozpoznanie. Rejony zainteresowania celami są dla rozpoznania i zakłócania elektronicznego obszarami wzdłuż dróg podejścia, oraz poza nimi, gdzie występowanie źródeł emisji elektromagnetycznych przeciwnika może potwierdzić lub zaprzeczyć przebieg działań. Aktywność urządzeń promieniujących energię elektromagnetyczną w obrębie drogi podejścia lub obszaru określonego jako NAI, może być porównana ze wskaźnikami aktywności występującymi w obszarze innego NAI, w obrębie innej drogi podejścia w tym celu, aby określić trafnie zamiary przeciwnika. Poziom aktywności urządzeń promieniujących energię może również stanowić dla rozpoznania i zakłócania elektronicznego wskazówkę o istnieniu jakiegoś urządzenia w obrębie obszaru nie kontrolowanego. Numeracja NAI ustalana jest w czasie spotkań koordynacyjnych wewnątrz G2, pomiędzy oficerami sekcji planowania i WE. Ustalenia te są niezbędne

[31] Przeciwnik dążyć będzie do ograniczenia informacji o swoim działaniu i stan naszej wiedzy może nie ulec zmianie mimo rozpoczęcia działań.
[32] Cel o znaczeniu decydującym dla działania wojsk przeciwnika.

dla wyeliminowania błędów i dwuznaczności w oznaczeniach lub oznaczeń dublujących, ponieważ niektóre obszary NAI mogą występować w tym samym miejscu.

Wariant zdarzeń opracowany przez analityków grupy rozpoznania elektronicznego z sekcji WE w procesie EPB dostarcza danych do ustalenia kolejności oddziaływania na przeciwnika oraz w oparciu o rozpoznane emisje EM, sposobu i rodzaju zakłócania. Wariant zdarzeń elektronicznych konkretyzowany jest w toku „gry wojennej" (pomiędzy G2 i G3) - dla każdego wariantu działań przeciwnika, od momentu ich rozpoczęcia do momentu osiągnięcia celów (obiektów) tych działań. Jeśli będą miały miejsce zdarzenia lub działania wojsk sygnalizowane pracą urządzeń promieniujących energię elektromagnetyczną, wówczas do ich synchronizacji w obrębie każdej drogi podejścia wykorzystywane będą czasowe linie wyrównania (TPL)[33].

Elektroniczny wzorzec wsparcia decyzji[34] jest dokumentem wykonywanym na potrzeby śledzenia prognozowanej sytuacji elektronicznej przeciwnika i pomocny dowódcy w procesie podejmowania decyzji.

Z elektronicznego wzorca wsparcia decyzji na wzorzec wsparcia decyzji wykonywany przez G3 nanoszone są tylko informacje niezbędne w procesie podejmowania decyzji przez dowódcę ZT, które będą wspierać jego zamiar rozegrania walki i podpowiedzą mu jak tę walkę „wygrać". Pozostałe informacje z elektronicznego wzorca wsparcia decyzji służą G2 i sekcji walki elektronicznej do kontroli działania przeciwnika.

W wyniku analizy zdarzeń elektronicznych wskazywane są i opisywane kluczowe elektroniczne obiekty (cele) przeciwnika wraz z obszarami oddziaływania elektronicznego (TAI)[35]. Oficerowie sekcji WE prowadzący analizę danych otrzymanych z pododdziału WE określają obszary oddziaływania elektronicznego (ogniowego). Podstawą wyboru TAI jest analiza obszarów NAI w czasie odprawy koordynacyjnej wewnątrz G2 oraz wiadomości z rozpoznania elektronicznego napływające w czasie przebiegu procesu EPB. Podczas odprawy koordynacyjnej ustala się rejony TAI które są najistotniejsze do rozpoznania i zakłócania oraz te, które się tylko kontroluje, nie zapominając iż przeciwnik może rozwinąć swoje środki

---

[33] TPL (Timephase line)- Czasowa linia wyrównania

[34](EDST - Electronic decision support template) Elektroniczny wzorzec wsparcia decyzji może kojarzyć się w swoim znaczeniu z dokumentem wykonywanym przez komputer. Wynika to z przetłumaczenia oryginalnego dokumentu z języka angielskiego. Dokument ten może być wykonywany przy pomocy techniki komputerowej, ale nie jest dokumentem elektronicznym.

[35] TAI (Target Areas of Interest) - Obszar oddziaływania ogniowego. W rozumieniu walki elektronicznej jest to obszar oddziaływanie energią elektromagnetyczną.

elektroniczne poza prognozowanymi rejonami zainteresowania. Obszary NAI i TAI służą do kontroli przemieszczania elementów elektronicznych przeciwnika, dając w ten sposób obraz jego działań. Jednak kontrolować należy cały obszar odpowiedzialności rozpoznawczej.

Gdy wariant przebiegu walki elektronicznej i niszczenia obiektów przeciwnika jest już ustalony, sekcja WE G2 opracowuje EDST aby zapewnić dowódcy dywizji pełny obraz proponowanych rozwiązań. Dowódca, posiadając takie informacje o przeciwniku, jest w stanie określić, jak najefektywniej wykorzystać środki walki znajdujące się pod jego kontrolą.

Wzorzec wsparcia decyzji w zakresie elektroniki opisuje obszary oddziaływania elektronicznego (określone przez rozpoznanie elektroniczne), punkty decyzyjne (określone przez G3) oraz czasowe linie wyrównania - wzdłuż każdej dróg podejścia (korytarza ruchu) i rejonów poza nimi, gdzie dowódca może zatrzymać siły przeciwnika lub ograniczyć jego możliwości: ogniowe, manewrowe, elektroniczne oraz uniemożliwić mu działania. Obszar oddziaływania elektronicznego jest rejonem, gdzie siły i środki przeciwnika można ograniczyć albo pozbawić zdolności bojowej bądź też spowodować przyjęcie narzuconego mu sposobu albo zaniechanie planowanego wariantu działania.

Obszary oddziaływania ogniowego (elektronicznego), pierwotnie mogą być identyfikowane jako NAI. Ponieważ NAI wykorzystuje się w celu zbierania danych potwierdzających słuszność prognozowanego wariantu działania przeciwnika mogą być usytuowane w głębi ugrupowania przeciwnika. Z kolei TAI wyznacza się na głębokości oddziaływania środków ogniowych lub elektronicznych. Jeżeli NAI i TAI pokrywają się wówczas obszary zainteresowania nie muszą być uwzględniane na wzorcu wsparcia decyzji. Decyzje co do sposobu wykorzystania środków walki elektronicznej mogą być wypracowywane dla każdego punktu decyzyjnego i linii czasowej. Decyzje te mogą dotyczyć wspomagania działań obronnych, zaczepnych, opóźniających i pościgowych. Mogą mieć na celu wprowadzenie w błąd przeciwnika albo spowodowanie zmiany priorytetów w zbieraniu danych. Podobnie jak w przypadku wykorzystania innych środków, punkty decyzyjne dotyczące wykorzystania środków WE wskazują dowódcy te momenty walki, które wymagają podjęcia decyzji. Gdy EDST jest już przygotowany, dowódca zapoznaje się z jego treścią i opiniami innych specjalistów, aby upewnić się, że działania wojsk własnych będą efektywne.

Elektroniczny wzorzec wsparcia decyzji wraz z oleatem przeszkód terenowych (MCOO)[36] przesyła się do batalionu rozpoznawczego, w celu weryfikacji postawionego zadania. Zbieranie danych wymaga bowiem skoordynowanego wysiłku wszystkich zbierających i potwierdzających dane z rejonów zainteresowań celami elektronicznymi (NAI). Sztab batalionu rozpoznawczego na podstawie prognozy zdarzeń musi sprecyzować potrzeby informacyjne z wybranych obszarów zainteresowania.

Proces planowania walki elektronicznej kończy się z chwilą podjęcia decyzji przez dowódcę. Dla sekcji WE jest to sygnał do rozpoczęcia szczegółowego opracowania dokumentów w stosunku do przyjętego wariantu działania wojsk własnych i przeciwnika.

Ad. 7. W tym etapie (tabela 3.2.2) TCAE wykorzystuje dane taktyczne ustalone w etapie 5 aby obliczyć minimalną moc wyjściową stacji zakłóceń wymaganą do skutecznego zakłócenia.

Tabela 3.2.2

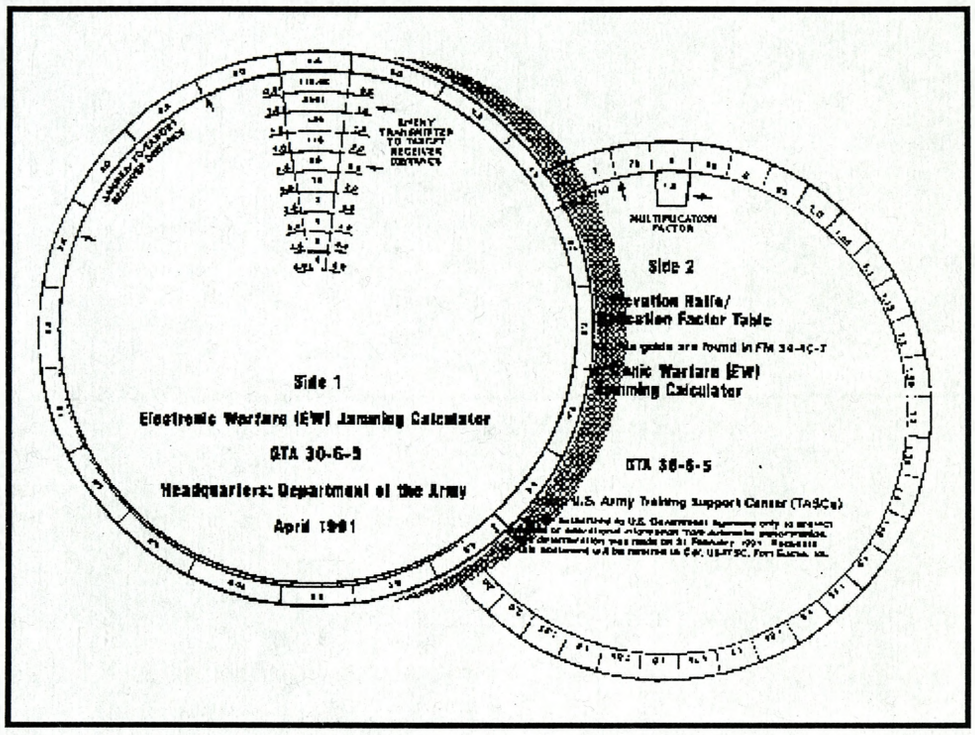
Harmonogram zakłóceń elektronicznych

Obiekt Kolejność	Częst.	Sygnał Rozp.	Azymut Magnet.	ZAKŁÓCANIE			Czas Włączenia	Czas Wyłączenia	Uwagi
				Moc	Pozycja	Typ anteny			
1 1A	44.25	AK17	42^0	20	AT 245976	WHIP	H-30	H-15	32.25
2 1B	40.50	TK12	53^0	20	AT 765213	WHIP	H-40	H-35	55.25
50 18G	16.90	WS45	78^0	5	Ek1 26546	WHIP	H+180	H+190	23.45

Stacja zakłóceń musi być zdolna do wytworzenia tej mocy aby wykonać zadanie w zakresie skutecznego zakłócania. Te same dane mogą być także wykorzystane do obliczenia maksymalnej odległości lokalizacji stacji zakłóceń od celu zakłócanego, przy maksymalnej mocy wyjściowej. Te same informacje wraz z kategorią ważności celów i czasem zakłóceń, są częścią wieloaspektowego planu zakłóceń dla urządzeń prowadzących zakłócenia.

[36] MCOO (Modified combined obstacie overlay) - Zmodyfikowana oleata przeszkód terenowych

Dane do zakłócania są opracowywane przez efektywne planowanie i kierowanie przez personel sekcji TCAE. Wysiłki TCAE dostosowywane są do potrzeb określanych przez G3. W etapie 5 i 6 określane są niektóre dane dostępne z zarządzenia WE. Do obliczeń wykorzystuje się kalkulator zakłócania elektronicznego GTA-30-6-5 (rys. 3.2.12).

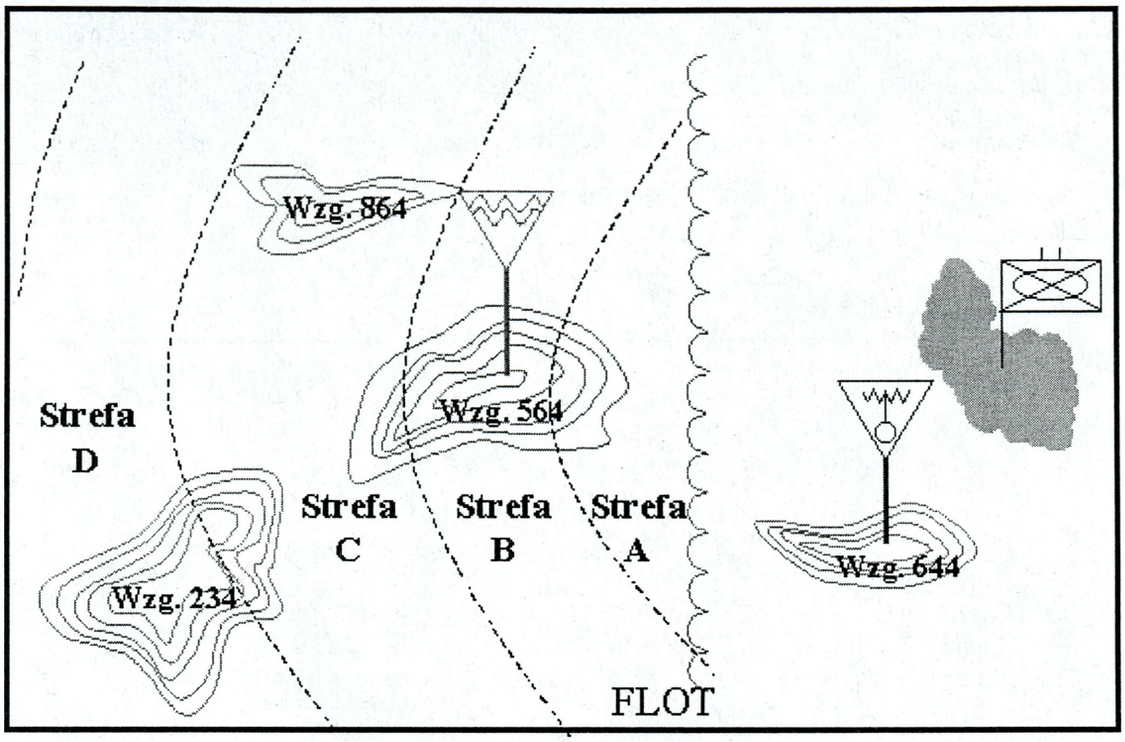


Rys. 3.2.12. Kalkulator GTA – 30 – 6 – 5

Kalkulator zakłócania elektronicznego umożliwia szybkie i łatwe obliczanie minimalnej mocy stacji zakłóceń w celu skutecznego zakłócania. Ten kalkulator może zostać wykorzystany do map w różnych skalach.

W etapie 6 prowadzone są takie obliczenia, aby stacja zakłóceń mogła być rozwinięta na określonej pozycji (np. wzgórze 564 w strefie B – rys. 3.2.13) i prowadzić skuteczne zakłócenia.

Planujący zakłócanie określa minimalną moc wyjściową potrzebną do skutecznego zakłócania urządzeń odbiorczych przeciwnika. W wypadku gdy moc ta jest zbyt wysoka, przeciwnik łatwo może wykryć i zlokalizować naszą stację zakłóceń. Aby pododdział zakłócania mógł wykonać swoje zadanie, planujący oprócz podania mocy musi określić odległość pomiędzy stacjami zakłóceń, a odbiornikami radiostacji. Należy także uwzględnić odległość pomiędzy nadajnikiem i odbiornikiem radiostacji przeciwnika.



Rys. 3.2.13. Pozycje stacji zakłóceń

Każde użycie stacji zakłóceń w konkretnej sytuacji taktycznej jest inne. Dlatego też, należy przeprowadzić w tym zakresie niezbędne obliczenia. Ważne znaczenie w tym zakresie odgrywa również teren, co związane jest z zasięgiem horyzontu radiowego i optycznego. Ponadto należy rozważyć typ stacji zakłóceń gdyż mają one różną moc wyjściową.

Planowanie zakłócania wymaga zdobycia dużej ilości danych o przeciwniku np. struktura jednostki, jej pozycje bojowe, czas wykonywania zadań itp. Zakłócanie musi być zsynchronizowane z rażeniem ogniowym, siłami manewrowymi i innymi, aby możliwe było uzyskanie maksymalnych efektów działań. Dlatego też w tym celu wykonuje się między innymi listę obiektów do rażenia elektronicznego lub artyleryjskiego (tabela 3.2.3).

Planowanie zakłócania może być realizowane jako zadanie: bezpośrednio ofensywne, pośrednio ofensywne lub wprowadzające w błąd:

- *zadanie bezpośrednio ofensywne* - zakłócanie będzie prowadzone przeciwko atakowanej jednostce przeciwnika;
- *zadanie pośrednio ofensywne* będzie polegać na zakłócaniu tych pododdziałów przeciwnika, które mogłyby wzmocnić jednostkę atakowaną;
- *zadanie wprowadzające w błąd* obejmuje prowadzenie zakłóceń pozornych przeciwko wybranej jednostce i atakowaniem innej jednostki przeciwnika.

Tabela 3.2.3

Lista celów elektronicznych (do niszczenia artyleryjskiego)

Arkusz ... z....

Lp	Numer Obiektu (celu)	Opis	Pozycja	Wysokość n.p.m.	Wysokość w powietrzu	Długość	Szerokość	Źródło	Uwagi				
1													
2													
3													
4													

Typ zadania zależy od sytuacji taktycznej, stopnia znajomości sytuacji przeciwnika, możliwości użycia sił i środków oraz celu realizowanego zadania.

Planowanie zadań będzie obejmować: planowe zakłócanie i zakłócanie na sygnał.

Planowe zakłócanie. W tym wypadku na planie zakłóceń określa się jednostkę przeciwnika, pozycję obiektu, czas prowadzenia zakłóceń. Czas zakłócania jest zsynchronizowany z czasem rażenia ogniowego, tak aby jednostki manewrowe miały jak najwyższy stopień wsparcia.

Zakłócanie na sygnał zależy od rodzaju jednostki, zajmowanych pozycji oraz sytuacji taktycznej. Prowadzi się je przeciwko jednostkom wzmocnienia oraz drugim rzutom. Musi ono być zsynchronizowane z planem rażenia ogniowego. Określone środki łączności powinny być również utrzymywane w gotowości do natychmiastowego przekazania sygnału do prowadzenia zakłóceń.

Tabela 3.2.4

Harmonogram obezwładniania celów

KOLEJNOŚĆ		Czas	Cel pododdział	Pozycja celu	Działalność celu	Mechanizm kontroli	Sprzężenie zwrotne
Rozpozn. Elektron.	Rażenie elektron.						

Planowanie zakłócania zależy od rodzaju działań i obejmuje takie czynności jak:

- ✓ ustalenie obiektów pracujących na częstotliwościach zastrzeżonych;
- ✓ wybór środków;
- ✓ ocena skuteczności zakłóceń;

Ustalenie obiektów pracujących na częstotliwościach zastrzeżonych. Planujący zakłócanie uzyskuje dane o obiektach (celach) przeciwnika. Jeśli informacja o potencjalnym obiekcie (celu) jest potwierdzona, dokonuje się analizy jego częstotliwości pracy, czy nie pokrywają się one z częstotliwościami zastrzeżonymi. W wypadku takiego problemu należy złożyć meldunek do odpowiedniego dowództwa w celu rozwiązania powyższego problemu. Nierozwiązane problemy są odnotowywane w dokumentacji jako częstotliwości zastrzeżone do czasu, aż problem ten zostanie rozwiązany.

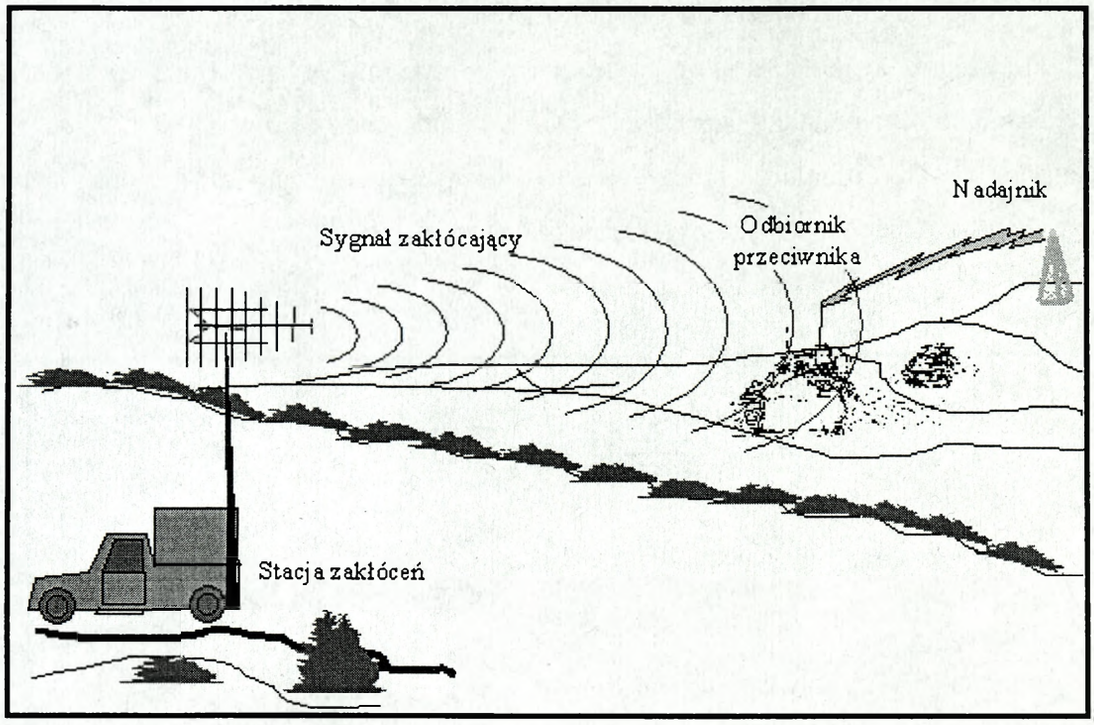
Wybór środków. Następnym krokiem jest porównanie realizowanego zadania zakłócania z odpowiednimi środkami (stacjami zakłóceń). Dane taktyczno – techniczne, typ, ilość oraz pozycje własnych stacji zakłóceń są niezbędne do planowania i prowadzenia zakłócania. Potrzeby w zakresie wykonania zadania powinny uwzględniać wykorzystanie nie tylko własnych środków etatowych ale także zapotrzebowanych z wyższego szczebla.

Ocena skuteczności zakłóceń. Jeśli moc sygnału stacji zakłóceń jest większa od sygnału radiostacji przeciwnika, wtedy zakłócanie będzie skuteczne (rys. 3.2.14).

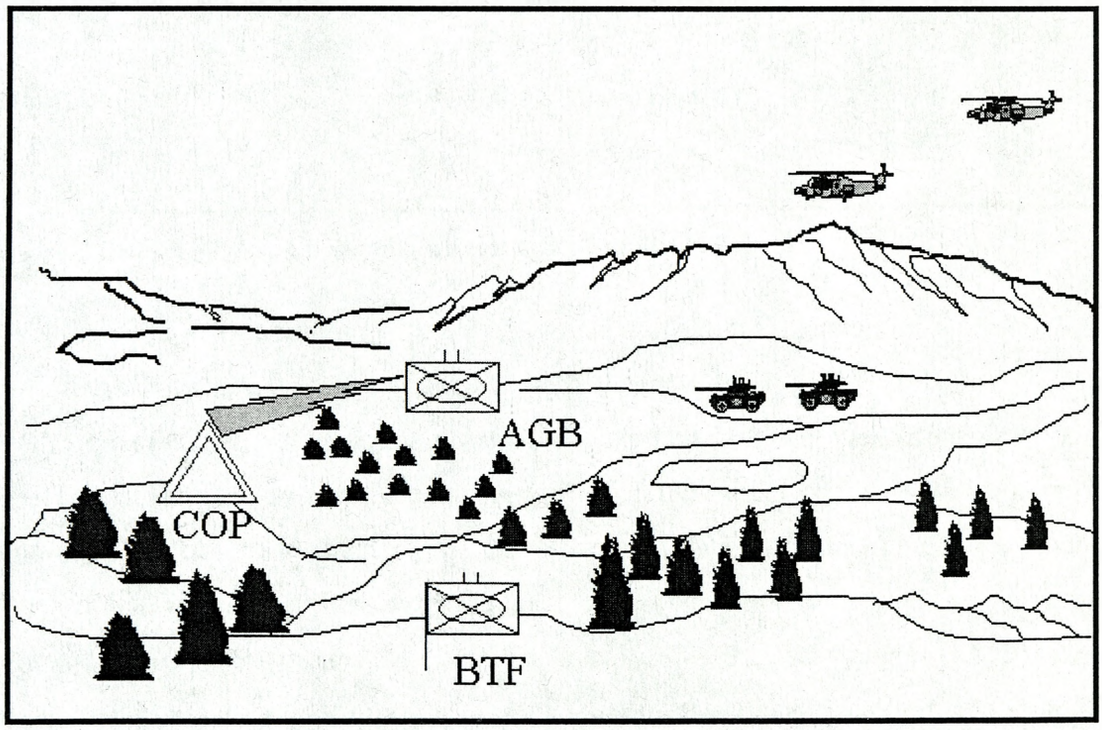
Skuteczne zakłócanie dezorganizuje lub pozbawia przeciwnika łączności. Moc wyjściowa sygnału zakłócającego nie powinna być zbyt wysoka (wymagana jest jak najmniejsza), gdyż wtedy może przyczynić się do lokalizacji własnej stacji zakłóceń przez przeciwnika. Moc wyjściowa stacji zakłóceń powinna zapewnić obezwładnienie elektroniczne odbiornika radiostacji przeciwnika.

Skuteczne zakłócanie dezorganizuje lub pozbawia przeciwnika łączności. Moc wyjściowa sygnału zakłócającego nie powinna być zbyt wysoka (wymagana jest jak najmniejsza), gdyż wtedy może przyczynić się do lokalizacji własnej stacji zakłóceń przez przeciwnika. Moc wyjściowa stacji zakłóceń powinna zapewnić obezwładnienie elektroniczne odbiornika radiostacji przeciwnika.

Aby zrozumieć sens zakłócania można rozważyć następującą sytuację. Posterunek obserwacyjny przeciwnika (COP) zlokalizował nasz batalion wykonujący zadanie (BTF) – rys. 3.2.15.



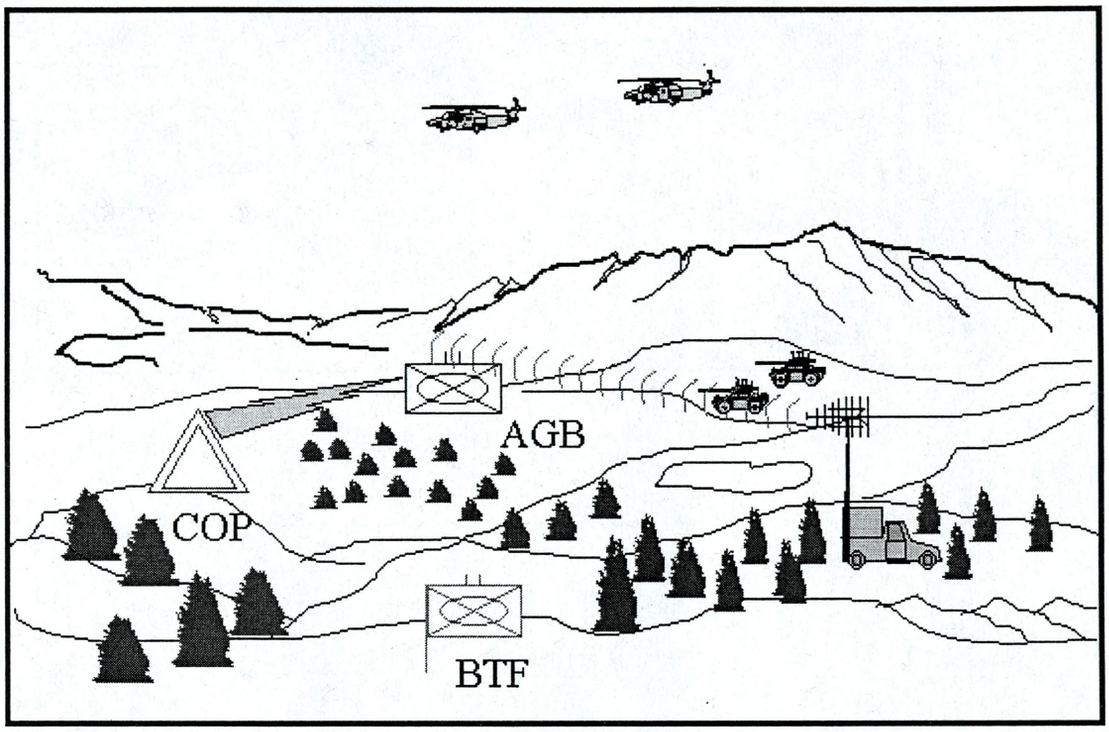
Rys. 3.2.14. Zakłócanie systemu odbioru przeciwnika



Rys. 3.2.15. Sytuacja taktyczna

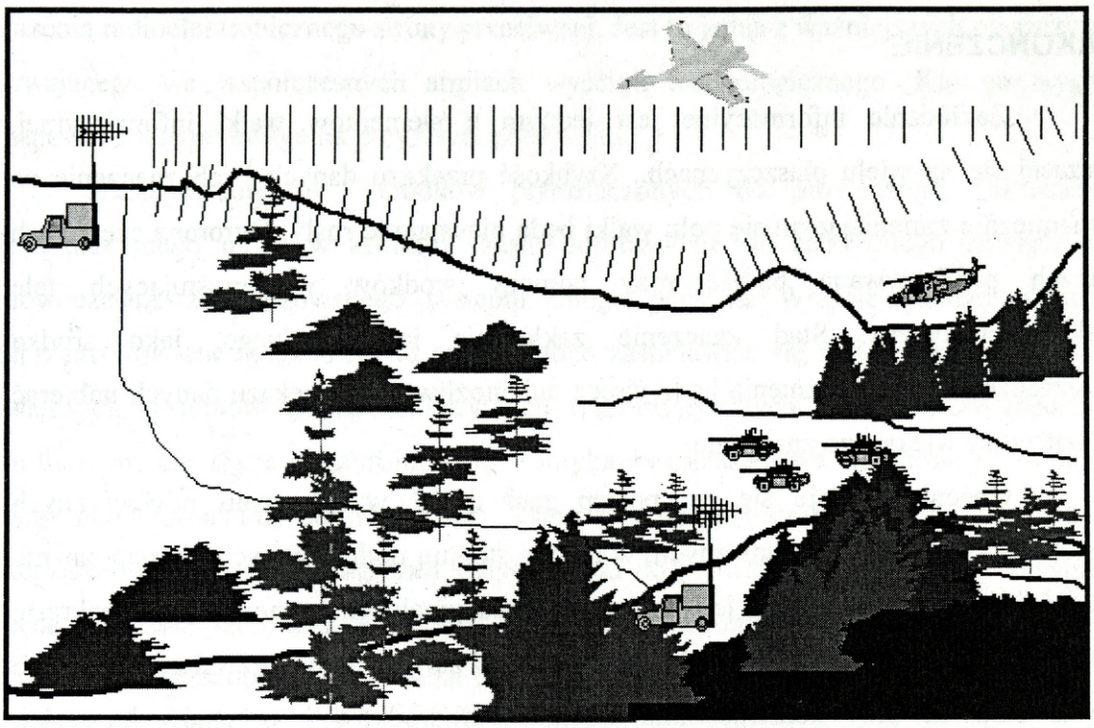
W tej sytuacji przesyła dane do swojego batalionu osłony (AGB). Ze względu na brak stosowania zakłóceń operator łączności w batalionie osłony otrzymuje dokładną wiadomość od COP.

Nasze rozpoznanie ustaliło częstotliwość pracy środków łączności przeciwnika oraz określiło pozycje punktu obserwacyjnego i batalionu osłony. Dane te zostały przekazane do sekcji analizy technicznej (TCAE), która planuje prowadzenie zakłóceń. Planiści określili minimalną moc wyjściową oraz pozycję stacji zakłóceń w celu skutecznego zakłócenia powyższego kierunku radiowego (rys. 3.2.16).



Rys. 3.2.16. Stanowisko stacji zakłóceń

Podczas planowania zakłócania należy uwzględnić minimalną wartość mocy wyjściowej stacji zakłóceń, która pozwoli na skuteczne obezwładnienie pracy środków łączności przeciwnika. Jest to zadanie bardzo trudne, czasami wręcz niemożliwe do wykonania. Kryteria jego realizacji nie są uniwersalne. Przede wszystkim należy się zapoznać z sytuacją taktyczną, otrzymanym zadaniem i terenem w którym prowadzone będą działania. Przede wszystkim należy brać pod uwagę warunki wpływające na propagację fal, między innymi takie, jak: ukształtowanie terenu, przewodność ziemi, roślinność oraz pogoda (rys. 3.2.17).



Rys. 3.2.17. Wpływ warunków terenowych na zakłócanie

ZAKOŃCZENIE

Zakłócanie informacyjne jest jednym z elementów walki informacyjnej, toczącej się na wielu płaszczyznach,. Szybkość przekazu danych i ich znaczenie na dynamicznie zmieniającym się polu walki będą nieustannie rosły. Ogromna część tych danych przekazywana będzie przy pomocy środków wykorzystujących fale elektromagnetyczne. Stąd znaczenie zakłócania informacyjnego, jako środka przeznaczonego do opóźnienia bądź wręcz uniemożliwienia przekazu danych nabierać będzie coraz większego znaczenia.

Obecnie wydaje się, że postęp zachodzący w tworzeniu nowoczesnych systemów i środków elektronicznych, w dużym stopniu uodpornionych na rozpoznanie i zakłócanie przesyłanych za ich pomocą danych przebiega szybciej niż w zakresie tworzenia systemów i środków walki informacyjnej zdolnych do ich zwalczania. Bierze się to stąd, że przy konstruowaniu wojskowych środków i systemów łączności, radiolokacji, radionawigacji itp. korzysta się z bogatych doświadczeń dynamicznie rozwijających się systemów łączności cywilnej. Przykładem mogą być systemy łączności satelitarnej, GPS czy telefonii komórkowej.

Z powyższego wynika, że jedną z cech przyszłego pola walki będzie wysoce skomplikowana sytuacja informacyjna. Wyrażać się to będzie z jednej strony ogromnym zapotrzebowaniem na informacje przez dowództwa, sztaby, zespoły ludzkie i pojedyncze osoby, z drugiej zaś istnieniem wielu barier w procesie przepływu informacji między komórkami i zespołami w pionie i poziomie. Działanie ludzi sprawujących funkcje kierownicze można stosunkowo łatwo zakłócić, z jednej strony – poprzez oddziaływanie dezinformujące prowadzone w sieciach dowodzenia i kierowania wojskami, z drugiej – przez imitację rzekomych ruchów wojsk i wykorzystanie niektórych akustycznych elementów na polu walki. Działania dezinformujące będą często prowadzone w ścisłym współdziałaniu ze specjalistycznymi służbami i rodzajami wojsk.

Oddziałując bezpośrednio na systemy informacyjne przeciwnika, każda z walczących stron stara się zmniejszyć zdolność bojową strony przeciwnej, efektywność wykorzystania przez nią uzbrojenia, a tym samym obniżyć skuteczność działania. Ma to bezpośredni wpływ na jednoczesne poszukiwanie jak najlepszych rozwiązań organizacyjnych i technicznych mających na celu zabezpieczenie własnych środków radioelektronicznych przed oddziaływaniem coraz doskonalszych środków

rażenia radioelektronicznego strony przeciwnej. Jest to jedna z ważniejszych płaszczyzn trwającego we współczesnych armiach wyścigu technologicznego. Kto go wygra zapewni sobie przewagę na przyszłym polu walki.

Zastosowanie sił i środków przeznaczonych do prowadzenia zakłócania informacyjnego może w krótkim czasie doprowadzić do całkowitego zniszczenia nowocześnie zorganizowanego systemu całego państwa. Właśnie dlatego wysoko uprzemysłowione społeczeństwa są zmuszone zastanawiać się nad środkami ochrony własnych systemów telekomunikacyjnych i informatycznych, nie tylko w aspekcie militarnym ale także pozamilitarnym. Polityka bezpieczeństwa narodowego zyskuje więc pewien zupełnie nowy wymiar. Formy organizacji i strategii będą musiały być dopasowane do nowych zagrożeń. Siły i środki do prowadzenia walki informacyjnej będą narażone na oddziaływanie w tym zakresie strony przeciwnej. Ponadto siły polityczne z rzekomo mało znaczących regionów, mają dzisiaj dostęp do tego rynku technologicznego. Niezbędne środki (komputery osobiste, oprogramowanie, itp.) są dostępne na całym świecie. Dlatego też siły te nie muszą już dzisiaj wydawać ogromnych sum pieniędzy na zakup systemów uzbrojenia i broni, które zresztą objęte są zakazem eksportu do tych regionów. Rozwój w tej dziedzinie trwać będzie w tych regionach z pewnością jeszcze dłuższy czas, dlatego już teraz muszą być poczynione wysiłki, które uodpornią własne systemy na oddziaływanie środków walki informacyjnej przeciwnika.

Formacje do prowadzenia operacji informacyjnych organizuje się we wszystkich rodzajach sił zbrojnych USA. Środki i technologie informacyjne stosowane w walce zbrojnej, mogą w znaczny sposób wprowadzić w błąd przeciwnika co do posiadanych sił i prowadzonych działań, co zwiększy zdolność bojową własnych sił i zrekompensuje braki w posiadanych systemach broni. Dzięki cyfrowemu zobrazowaniu (zwiększeniu „świadomości sytuacyjnej") nastąpi wyeliminowanie niepewności i podjęcie niezbędnych środków bezpieczeństwa.

LITERATURA:

1. Burhans W. A.: *Iraqi Air Defences — Initial Soviet Post — Mortem.* W: *„Journal of Electronic Defense"*, October 1991.
2. Campen A. D: *„The first Information War"*. Virginia 1992.
3. Ciborowski L.: *„Przestrzenie walki informacyjnej"*. AON, Warszawa 1997.
4. Donald R., White J.: *„A Handbook Series on Elektromagnetic Interference and Copmpatibility"*. Wyd. Germantown, Maryland 1973.
5. Falicber O.: *Shilka`versus the B-52* . W: *„Krasnaja Zwiezda"* (Red Star), 4/1991.
6. Fitzgerald M. C.: *Russian views on information warfare.* W: *„Army"*, 5/1994.
7. FM 34-40-7 Communications jamming handbook, Headquarters, Department of the Army, Washington DC, 23 November 1992
8. FM 34-130, Intelligence preparation of the battlefield, Headquarters, Department of the Army, May 1989.
9. FM-101-5, Staff organisation and operations, Washington 1984.
10. Giboney T. B.: *Chaos informacyjny.* W: *„Military Review"*, 11/91.
11. Grabau. R.: *Sechs Dimensionen des Kriegers.* W: *„Soldat und Technik"*, nr 6/1986.
12. Grier P.: *Information Warfare.* W: *„Air Force"*, 4/1994.
13. Intelligence preparation of the battlefield, United States Marine Corps, Marine Corps Combat Development Command, Quantico, Virginia, 9 May 94.
14. Kręcikij J., Przygotowanie działań taktycznych w NATO (Na przykładzie procedur Wojsk Łądowych SIŁ Zbrojnych USA), AON 1996.
15. Nowacki G.. *„Operacje informacyjne"*. AON, Warszawa 2001.
16. Nowacki G.. *„Walka informacyjna – próba kategoryzacji"*. Rozprawa doktorska pod kier. naukowym L. Ciborowskiego. AON, Warszawa 1999.
17. Nowacki G.. *„Współczesne poglądy na prowadzenie walki informacyjnej"*. AON, Warszawa 2001.
18. Nowacki G., Scheffs W., *„Elektroniczne przygotowanie pola walki"*. AON. Warszawa 1998.
19. Nowacki G., Scheffs W., Błażejczyk W.: *„Zakłócanie elektroniczne na szczeblu taktycznym według poglądów amerykańskich"*. AON, Warszawa 1999. S/4244.
20. Keramas J. G.: *„Workforce Training for Global Copmpetitivenes"*. AFCEA — Stockholm Symposium and Exposition, 1995.

21. Keuren E. V., Knighten J.: *„Implications of the High — Power Microwave Weapon Threat in Electronic System Design"*. IEEE Intern. Symp. on EMC, Cherry Hill, 1991.
22. Riccardelli R. F.: The Information and Intelligence. W: „Military Review", 5/95.
23. Ross J. D.: *Wojna o informację*. W: *„Army"*, 2/1994.
24. Schwartau Winn.: „Information Warfare — Cyberterrorism: Protecting Your Personal Security in the Electronic Age". 1993.
25. Starry M. D., Arneson C. W.: Operacje informacyjne. W: „Military Review", 6/96.
26. Staff College Organization Handbook, Foundation Studies Team, Camberley, Spt 1993
27. Student text 101-5, Command and staff decision processes, U.S. Army Command and General Staff College, Fort Leavenworth, Kansas, Feb 1995.
28. Sullivan G. R., Dubik J. M.: War in the Information Age. W: „Military Review", 4/1994.
29. Toffler Alvin i Heidi: „Wojna i antywojna" (War and Antiwar). 1993.

SPIS TREŚCI

ERRATA

do numeru 2(43) 2001 „Zeszytów Naukowych AON"

Strona	Wiersz (od góry)	Jest	Powinno być
3	13	Deficyt budżetowy	**Deficyt ekonomiczny**
5	14	Budget Deficit	**Economic Deficit**
83	2	DEFICYT BUDŻETOWY	**DEFICYT EKONOMICZNY**
88	streszczenie w języku angielskim	Col. Zbigniew DYLEWSKI, M.A. BUDGET DEFICIT – NEW MACROECONOMIC NOTION *The author discusses the notion of "budget deficit" and its influence on monetary balance in the country. He lists operations aiming at deficit reduction. Then he analyses the notion of "economic deficit" and presents the economic deficit of public finances in 1998 – 2003.* *The author concludes that if disintegration, centralisation, commercialisation and inappropriate structure of public sectors incomes contribute largely to its significant weakness then it means that Poland needs deep and comprehensive restructuring of public finances.*	Col. Zbigniew DYLEWSKI, M.A. ECONOMIC DEFICIT – NEW MACROECONOMIC NOTION *The author discusses the new notion of economic deficit and its influence on monetary balance in the country. He mentions possible actions to limit or eradicate the budget deficit. Then he analyses the notion of "economic deficit" and presents the economic deficit construction of public finances in 1998 – 2003.* *The author concludes that if disintegration, centralisation, commercialisation and inappropriate structure of public sectors incomes contribute largely to its significant weakness then it means that Poland needs deep and comprehensive restructuring of public finances.*