



**AKADEMIA OBRONY NARODOWEJ**

**WYDZIAŁ STRATEGICZNO – OBRONNY**

**POJĘCIE, ISTOTA  
ORAZ TENDENCJE ROZWOJOWE  
ZAGROŻEŃ ASYMETRYCZNYCH**

**Studium teoretyczne**

**65230**

~~Biblioteka Główna  
Akademii Obrony Narodowej  
6/5308~~



~~05-005308-001-0~~

PMB

**WARSZAWA**

**2002**



**AKADEMIA OBRONY NARODOWEJ**

---

**WYDZIAŁ STRATEGICZNO - OBRONNY**

**POJĘCIE, ISTOTA ORAZ TENDENCJE ROZWOJOWE  
ZAGROŻEŃ ASYMETRYCZNYCH**

**STUDIUM TEORETYCZNE**



**PRACA ZBIOROWA  
POD KIEROWNICTWEM NAUKOWYM  
płk. dr. hab. Jacka PAWŁOWSKIEGO**

## **ZESPÓŁ AUTORSKI**

płk dr hab. Jacek PAWŁOWSKI – kierownik zespołu

płk dr hab. Mariusz WIATR

kmdr mgr inż. Piotr GAWLICZEK

płk mgr inż. Jerzy SZUBERT

kmdr ppor. dr Krzysztof KUBIAK

## **Korekta autorska**

## **Redakcja techniczna:**

Kmdr mgr inż. Piotr GAWLICZEK



## SPIS TREŚCI

WSTĘP .....	5
1. OGÓLNE INTERPRETACJE POJĘCIA ASYMETRIA .....	11
2. ROZUMIENIE POJĘCIA ASYMETRIA W KONTEKŚCIE ZADAŃ SIŁ ZBROJNYCH .....	15
2.1. Istota podejścia NATO .....	17
2.2. Istota podejścia amerykańskiego .....	19
2.3. Istota podejścia francuskiego.....	22
2.4. Istota podejścia niemieckiego.....	23
2.5. Istota podejścia brytyjskiego .....	32
2.6. Wnioski i propozycje w zakresie definicji zagrożeń asymetrycznych .....	33
3. CHARAKTERYSTYKA ZAGROZEŃ (DZIAŁAŃ) ASYMETRYCZNYCH .....	36
3.1 Działania asymetryczne według klasyfikacji NATO .....	36
3.1.1 Walka informacyjna .....	37
3.1.2 Broń masowego rażenia .....	39
3.1.3. Broń radiologiczna .....	40
3.1.4 Technika antysatelitarna .....	41
3.1.5 Tanie uzbrojenie i amunicja .....	41
3.1.6 Broń obezwładniająca .....	42
3.1.7 Środki antymateriałowe.....	43
3.1.8 Broń psychotroniczna.....	44
3.1.9 Broń etniczna.....	44
3.1.10 Środki walki wpływające na środowisko naturalne .....	45
3.1.11 Broń geofizyczna.....	46
3.1.12 Cybernetyczny wymiar pola walki.....	46
3.2. Kategorie zagrożeń asymetrycznych według literatury amerykańskiej .....	59
3.3. Kategorie asymetryczne według literatury brytyjskiej .....	61
3.4. Zagrożenia asymetryczne według literatury niemieckiej .....	64
4. DZIAŁANIA ASYMETRYCZNE W PRZESTRZENI REALNEJ I CYBERPRZESTRZENI.....	71
4.1. Sposoby działań asymetrycznych w wybranych środowiskach .....	71
4.1.1. Działania asymetryczne w przestrzeni realnej .....	71
4.1.2. Działania asymetryczne w przestrzeni wirtualnej .....	77

4.2. Prognoza zagrożeń asymetrycznych w odniesieniu do środowiska morskiego .....	78
4.2.1. Piraci, a terroryści morscy .....	79
4.2.2. Potencjalne sposoby prowadzenia działań terrorystycznych wymierzonych w handel morski i żeglugę handlową .....	81
4.2.3. Przyczyny atrakcyjności akwenów morskich jako obszaru działań terrorystycznych .....	95
4.2.4. Próba prognozy .....	100
5. WYBRANE PROBLEMY BEZPIECZEŃSTWA NATO I POLSKI W KONTEKŚCIE ZAGROŻEŃ ASYMETRYCZNYCH .....	102
ZAKOŃCZENIE .....	116
BIBLIOGRAFIA .....	118
ZAŁĄCZNIKI .....	122

## WSTĘP

Rozwojowi złożonych procesów cywilizacyjnych towarzyszy zazwyczaj dynamiczny postęp w zakresie zdolności tworzenia i wytwarzania<sup>1</sup>. Powoduje to określone zmiany odniesień pomiędzy czynnikami (parametrami<sup>2</sup>) wielowymiarowego układu, opisującego całokształt zjawisk społecznych i cywilizacyjnych oraz ich wzajemnych związków i relacji. Parametry określające występowanie takich czynników, a także wielkość ich udziału w tworzeniu ilościowej bądź jakościowej asymetrii są dynamicznie zmienne.

W minionych okresach, pomimo przejawów i krótkotrwałego wpływu uwarunkowań jakościowych, przeważał zdecydowanie czynnik ilościowy. Ekspansja i podboje strony dominującej były najczęściej konsekwencją występowania asymetrii powodowanej narastaniem zróżnicowania ilościowego, w mniejszym stopniu – jakościowego. Wiek XX, a zwłaszcza jego druga połowa, stał się okresem przewartościowań jakościowych na niespotykaną dotychczas skalę<sup>3</sup>, zmieniających udział tej grupy czynników w powstawaniu asymetryczności i generowaniu zagrożeń.

Natomiast w ostatniej dekadzie XX wieku byliśmy świadkami ogromnych zmian cywilizacyjnych: technologicznych, politycznych, społecznych i kulturowych. Postęp w technice, procesach wytwarzania, przetwarzania i przekazywania informacji dokonał się na oczach niemal jednego pokolenia i umożliwił budowanie zupełnie nowej jakości życia i pracy. Zmiany te, poza już obecnie oczywistymi, cechuje także:

<sup>1</sup> Tworzenie – odnoszone jest zazwyczaj do sfery wrażliwości twórczej (duchowej i intelektualnej).

<sup>2</sup> Czynniki, które można sparametryzować i zmierzyć, a następnie zobrazować i zinterpretować (np. w oparciu o techniki ekonometryczne). Wielowymiarowy model układu może zawierać kilkadziesiąt (i więcej) parametrów, dla których idealnym i jedynie teoretycznym odwzorowaniem stanu symetrii jest powierzchnia kuli. W rzeczywistości jest to tylko powierzchnia nieregularnej bryły, utworzona z połączenia wierzchołków wektorów reprezentujących wszystkie parametry opisywanego modelu. „Bezpiecznym” przedziałem ufności odwzorowania asymetrii, która w procesie naturalnych zmian (rozwoju, stagnacji i regresu) nie generuje znaczących zagrożeń jest, wyznaczana (szacowana) oddzielnie dla każdego modelu porównywanych stron, przestrzeń utworzona z różnicy promieniami ( $r_{\max} - r_{\min}$ ) wyznaczających dwie hipotetyczne kule o granicznej asymetrii  $A_{\max}$  i  $A_{\min}$ , przekroczenie których sygnalizuje przejście w obszary ryzyka.

<sup>3</sup> Dynamizacja postępu w nauce i technice, w tym rewolucja w dziedzinie wojskowości – RMA (Revolution in Military Affairs).

- wzrost społecznej otwartości na osiągnięcia i wartości innych narodów, kultur, grup, i pojedynczych ludzi;
- popularyzacja idei wolności, solidarności, tolerancji;
- ograniczanie suwerenności państwa na rzecz instytucji samorządowych i grup lokalnych jak również instytucji i przepisów międzynarodowych;
- humanizacja stosunków międzyludzkich głównie poprzez zastępowanie przymusu wolnym i świadomym wyborem;
- zanikanie tradycyjnych podziałów społecznych i równoczesny wzrost znaczenia ludzi wykształconych - merytokracji.<sup>4</sup>

Nie bez znaczenia jest tutaj fakt, iż z postępu technicznego i technologicznego oraz wymiany informacji o zasięgu światowym zaczęły czerpać korzyści kraje, które dotychczas nie dysponowały dostępem do najnowszych osiągnięć w dziedzinie zaawansowanej techniki, w tym techniki bojowej. Powoduje to określone następstwa i zmiany, a ponadto wymaga właściwego ich rozpoznawania i rozumienia powstających zwłaszcza na tym tle zagrożeń, by można było podejmować szybkie decyzje oraz reakcje, a także przeciwdziałać adekwatnie do skali tych zagrożeń.

Szczególnie ważną rolę zaczęła odgrywać w tym procesie szeroko pojęta problematyka proliferacji, odnosząca się zwłaszcza do BMR i spraw związanych z upowszechnianiem (udostępnianiem) najnowszej techniki bojowej oraz sposobów i metod jej wytwarzania.

Ostatnie dekady minionego wieku umożliwiły wykreowanie nowych form i sposobów działań proliferacyjnych, określanych specyficznymi terminami – „technologie nieuchwytny” (Intangible technology)<sup>5</sup> oraz „nieuchwytny

<sup>4</sup> Zob. A. Piskozub, *Przemiany kulturowe i cywilizacyjne w perspektywie społeczeństwa postindustrialnego i aspekty globalizacji kulturowej – uwarunkowania i wnioski*, [w:] *Polska na drodze do nowoczesnej cywilizacji*, t. II, Warszawa 1990, s. 33.

<sup>5</sup> Termin ten jest stosowany m.in. w dokumentach porozumienia z Wassenaar oraz reżimu kontrolnego technologii raketowych (Missile Technology Control Regime - MTCR).

transfer” (Intangible transfer). Pierwszy z nich odnosi się do technik i technologii z grupy tzw. środków podwójnego zastosowania (Dual using), a więc takich, które w całości lub w formie komponentów mogą znaleźć zastosowanie wojskowe, bądź też pozamilitarne, na przykład w chemii, farmacji, bio- i nanotechnologiach, elektronice i innych. Drugi, ma natomiast związek z coraz łatwiejszym i powszechniejszym dostępem do najnowszych systemów komunikacyjnych i wymiany informacji (np. Internetu, sieci lokalnych - LAN i szerokich - WAN) oraz środków umożliwiających skryte porozumiewanie się, w tym z użyciem najnowocześniejszych systemów szyfrowania. Pozwala to na skryty i niekontrolowany przekaz informacji, w tym dokumentów objętych reżimami międzynarodowej kontroli<sup>6</sup>.

Tak rozumiana problematyka proliferacji ma odniesienie, zarówno do pojedynczych państw, jak i ich grup powiązanych np. porozumieniami politycznymi, gospodarczymi i militarnymi, a ostatnio również do tzw. organizacji pozapaństwowych (Non-state actors<sup>7</sup>).

Zagrożenia o charakterze militarnym mają coraz bardziej charakter poza państwowy i asymetryczny. Współcześnie coraz częściej już nie państwa – jako takie – zagrażają innym państwom lecz procesy i zjawiska, jakie występują w zmieniających się społeczeństwach. Właśnie biedne społeczeństwa występują przeciwko bogatym, a systemy totalitarne przeciwko demokracji. Asymetryczność wyraża się swego rodzaju niepodzielnością celów, metod lub środków działania, przyjmowanych przez obie strony potencjalnego lub realnego konfliktu. Być może do klasycznych działań asymetrycznych zaliczone zostaną uderzenia terrorystyczne z 11 września 2001 roku w Nowym Jorku i Waszyngtonie, które niespełna pół roku później nazwano pierwszą bitwą wojny asymetrycznej. Większość ekspertów zgadza się, że wydarzenia te należą do przełomowych w

---

<sup>6</sup> Na przykład: Konwencja o Zakazie Broni Biologicznych i Toksyn (Biological and Toxin Weapons Convention - BTWC), Konwencja o Zakazie Broni Chemicznej (Chemical Weapons Convention - CWC).

<sup>7</sup> Termin przyjęty w NATO do określania międzynarodowych i pozarządowych organizacji terrorystycznych, organizacji przestępczych (mafijnych), religijnych (w tym sekt), nacjonalistycznych i innych.

historii. Jest to wyraz coraz wyraźniej rysującego się i powszechnie zauważalnego elementu rozwoju społecznego, który w sensie globalnym jawi się w ogromnych dysproporcjach międzypaństwowych, międzyregionalnych czy wręcz coraz bardziej powszechnej asymetrii rozwojowej świata. Na początku lat 90-tych ubiegłego stulecia zaczęto dostrzegać coraz wyraźniej towarzyszący tym zjawiskom powiększający się potencjał militarnych zagrożeń asymetrycznych.

Mając na uwadze powiększający się obszar zagrożeń asymetrycznych należy mieć na uwadze możliwość wystąpienia nagłego ryzyka związanego z użyciem i dalszym rozprzestrzenianiem się broni masowego rażenia i środków jej przenoszenia. Należy podkreślić, że coraz liczniejsza jest grupa państw (w tym prowadzących politykę konfrontacyjną), bliskich wejścia w jej posiadanie. Jeżeli dodać do tego, że do dysponowania tą bronią dążą również skrajne ugrupowania polityczne, religijne, a nawet przestępcze, to możliwość ewentualnego jej użycia wykracza niekiedy już poza sferę wyobraźni.

Uwzględniając przedstawione uwarunkowania, a zwłaszcza odpowiednio do wagi narastającego od kilku lat problemu, przedmiotem badań prowadzonych w latach 2001 i 2002 były zagrożenia asymetryczne. Chodzi tu zwłaszcza o badania podstawowe, dotyczące pojęcia i istoty zagrożeń asymetrycznych, a także odpowiednio – tendencji rozwojowych. Natomiast celem badawczym, którego wyniki zawiera niniejsze opracowanie, było przedstawienie wniosków z badań, dotyczących ogólnej interpretacji pojęcia asymetria, a zwłaszcza definicji zagrożeń asymetrycznych. Ponadto dokonano charakterystyki zagrożeń asymetrycznych także w odniesieniu do przestrzeni realnej i cyberprzestrzeni.

Główny problem badawczy zawierał się w pytaniu: czym są i co charakteryzuje zagrożenia (działania) asymetryczne i jakie mogą być sposoby działań asymetrycznych w wybranych środowiskach?

W końcowej części niniejszego studium skoncentrowano uwagę na odniesieniu się do niektórych problemów bezpieczeństwa NATO i Polski w kontekście zagrożeń asymetrycznych. Studium składa się z wstępu, pięciu rozdziałów, zakończenia, bibliografii oraz załączników.

W rozdziale pierwszym przedstawiono ogólne interpretacje pojęcia asymetria w odniesieniu do sfery materialnej i duchowej. Ponadto zwrócono uwagę na wpływ czynników ilościowych i jakościowych.

W rozdziale drugim rozumienie pojęcia asymetria przedstawiono w kontekście zadań sił zbrojnych. Omówiona została istota podejścia w NATO, USA, Francji, Niemczech i Wielkiej Brytanii. W końcowej części rozdziału zawarto wnioski i propozycje w zakresie definicji zagrożeń asymetrycznych.

Rozdział trzeci zawiera charakterystykę zagrożeń (działań) asymetrycznych. Działania te przedstawiono według klasyfikacji stosowanej w NATO. Ponadto rozdział ten obejmuje kategorie zagrożeń asymetrycznych według literatury amerykańskiej, brytyjskiej i niemieckiej.

Rozdział czwarty jest poświęcony wynikom badań w zakresie działań asymetrycznych w wybranych środowiskach. Najwięcej miejsca poświęcono środowisku morskemu.

Rozdział piąty dotyczy wybranych problemów bezpieczeństwa NATO i Polski w kontekście zagrożeń asymetrycznych. Na uwagę zasługują zwłaszcza możliwości działań ukierunkowane na sprostanie zagrożeniom asymetrycznym.

Dla osiągnięcia celu badań, a zwłaszcza udzielenia odpowiedzi na sformułowany problem badawczy, a także wykonania zadań badawczych, dokonano wielu analiz, syntez i ocen zagrożeń oraz działań asymetrycznych na podstawie istniejącej bibliografii oraz wniosków z badań zagranicznych instytutów i organizacji naukowych, w tym zwłaszcza państw wchodzących w skład NATO. Cennym i ważnym źródłem wiedzy był osobisty udział Autorów studium w pra-

cach grup roboczych NATO, podejmujących problematykę zagrożeń, a także w konferencjach naukowych i seminariach. Przykład stanowią między innymi:

- konferencja na temat „Terroryzm jako zagrożenie dla żeglugi morskiej”, zorganizowana przez Stowarzyszenia Armatorów Polskich 21 lutego 2002 roku w Gdańsku;
- konferencja na temat „Terroryzm międzynarodowy. Źródła i przejawy we współczesnym świecie”, zorganizowana przez Uniwersytet Warszawski w terminie 28-29.05. 2002 roku;
- konferencja na temat „Bezpieczne niebo”, zorganizowana 10 września 2002 roku w Akademii Obrony Narodowej, pod patronatem Biura Bezpieczeństwa Narodowego oraz Ministerstwa Obrony Narodowej;
- konferencja na temat „Zmniejszając lukę w wojskowych technologiach między USA, a europejskimi krajami NATO”, zorganizowana w terminie 15-17.10.2002 roku w Warszawie, w ramach programu CDE (Concept, Development and Experimentation) przez Naczelne Dowództwo PSZ NATO na Atlantyku, Urząd ds. Transformacji Sił Zbrojnych USA oraz Sztab Generalny Wojska Polskiego;
- konferencja na temat „Przed Szczytem NATO w Pradze”, zorganizowana 18 października 2002 roku w Krakowie przez Ministerstwo Spraw Zagranicznych, Instytut Stosunków Międzynarodowych oraz The German Marshall Fund of the United States;
- trzynaste niemiecko - polskie seminarium oficerów starszych na temat „Zagrożenia terrorystyczne oraz sytuacja bezpieczeństwa w Azji”, zorganizowane w terminie 21-25.10.2002 roku w Akademii Europejskiej Meklemburgii i Pomorza Przedniego w Waren-Mueritz, w ramach współpracy z Bundeswehrą i Akademią Obrony Narodowej;

## 1. OGÓLNE INTERPRETACJE POJĘCIA ASYMETRIA

„Asymetria” i „asymetryczność” są pojęciami określającymi różnorodne formy dysproporcji, zróżnicowania i dysharmonii, które w sposób naturalny lub zamierzony występują w otoczeniu przeciwstawianych sobie rzeczywistości. Dotyczą one zarówno ich sfery materialnej, głównie gospodarczej, ekonomicznej, naukowej, technicznej, informacyjnej i militarnej, jak i sfery duchowej – obejmującej aspekty kulturowe, religijne, etyczne i inne<sup>8</sup>. Wzajemna symetria czynników opisujących wielowymiarowy układ porównywanych ze sobą zależności minimalizuje, w określonym przedziale ufności<sup>9</sup>, możliwość generowania zagrożeń oraz stabilizuje względnie trwałą równowagę ich zmian.

Oznacza to, że „asymetryczność” jest antonimem hipotetycznego stanu „symetrycznej” równowagi, odnoszącego się do całokształtu zjawisk społecznych i cywilizacyjnych oraz do ich wzajemnych związków, relacji i oddziaływań. Symetria (zarówno w mikro- jak i makroskali) jest bowiem determinantą trwałości i stabilności zmian zachodzących w całym systemie procesów ewolucyjnych.

Czynniki warunkujące powstawanie asymetryczności pomiędzy zantagonizowanymi stronami, stają się, po przekroczeniu określonego poziomu ryzyka<sup>10</sup>, stymulatorami realnych zagrożeń, które w dalszym etapie ich narastania prowadzą do konfliktów i konfrontacji. Polem konfrontacji staje się nieuchronnie obszar występowania czynnika asymetryczności, na wykorzystanie którego

<sup>8</sup> Także aspekty psychiczne dotyczące sfery uczuć, emocji i zwyczajów (w tym np. rozpowszechnionych obrzędów i rytuałów), czy dominujących poglądów w kwestiach rasowych, narodowościowych i etnicznych.

<sup>9</sup> Swoista strefa bezpieczeństwa, wyznaczana (szacowana) w oparciu o wybrane funkcje rachunku prawdopodobieństwa. Jej przekroczenie determinuje powstawanie zagrożeń.

<sup>10</sup> Próby oszacowania „progu ryzyka”, po przekroczeniu którego następuje stymulacja procesów generowania zagrożeń, a także wielowymiarowych sposobów zobrazowania towarzyszących im zjawisk, są obecnie prowadzone (np. z wykorzystaniem technik ekonometrycznych) w wielu amerykańskich ośrodkach naukowych, w tym m.in. w wyspecjalizowanych instytutach Uniwersytetu Obrony USA (NDU – National Defense University) oraz Uniwersytetu w Pittsburgu (Pittsburgh University).

decyduje się zwykle strona agresywna, zdesperowana, bądź nieodpowiedzialna<sup>11</sup>. W **sferze materialnej** może się to przejawiać w formie:

- **walki zbrojnej** – w której zamiarem strony dominującej jest dążenie do inwazji terytorialnej, okupacji i całkowitego podporządkowania sobie przeciwnika;
- **wojny gospodarczej** – niszczącej i bezwzględnie uzależniającej gospodarkę słabszego od dominującej i ekspansywnej gospodarki silniejszego;
- **wojny ekonomicznej** – niszczącej bazę ekonomiczną słabszego, bądź jako element wojny gospodarczej, podporządkowującej ją bazie ekonomicznej silniejszego;
- **walki informacyjnej** – obejmującej wszelkie działania informacyjne<sup>12</sup> w odniesieniu do przeciwnika, prowadzone z zamiarem promowania określonego celu politycznego, gospodarczego lub wojskowego, przy równoczesnym zapewnieniu odpowiedniej ochrony własnym systemom informacyjnym;
- **konfrontacji naukowej** – obejmującej działania zmierzające do zniszczenia samodzielności naukowej przeciwnika, do degradacji jego bazy naukowej, w tym zwłaszcza ośrodków akademickich i placówek naukowo-badawczych (zarówno wojskowych jak i cywilnych)<sup>13</sup>;
- **konfrontacji technicznej** – zmierzającej do uzyskania nad przeciwnikiem bezwzględnej (asymetrycznej) przewagi technicznej i technologicznej, która poprzez dokonania rewolucjonizujące zdolność bo-

---

<sup>11</sup> Również nieobliczalna lub niezdolna do realnej oceny skutków swoich działań.

<sup>12</sup> Także jako element zakrojonych na szeroką skalę przedsięwzięć prowadzonych w ramach wojny psychologicznej (PSYWAR – uwzględniającej także oddziaływanie w zakresie sfery duchowej).

<sup>13</sup> Jednym z kierunków konfrontacji naukowej jest np. dążenie do pełnego podporządkowania i uzależnienia bazy naukowej przeciwnika od bazy własnej.

jową sił zbrojnych jednej ze stron, odbiera drugiej możliwość skutecznego przeciwstawienia się, czy nawet zabezpieczenia przed skutkami oddziaływania stosowanych środków rażenia.

Z kolei w **sferze duchowej** może się to przejawiać w formie:

- **wojny kulturowej** – zmierzającej do narzucenia przeciwnikowi własnych wzorców kulturowych i zwyczajów, zdecydowanie wypierających dotychczasowe oraz zacierających tożsamość narodową i więzi społeczne<sup>14</sup> wśród ludności strony przeciwnej;
- **wojny religijnej** – polegającej na narzucaniu społeczeństwu strony przeciwnej, dogmatów religijnych głoszonych przez stronę ekspansywną, w tym norm, zwyczajów i obrzędów; prowadzona jest z zastosowaniem wszelkich dostępnych środków, przy jednoczesnym, bezwzględny zwalczaniu innych form i przejawów kultu religijnego;
- **konfrontacji etycznej**<sup>15</sup> – zmierzającej do narzucenia grupom społecznym i środowiskowym przeciwnika, a docelowo całości jego społeczeństwa, obcych mu zasad i wzorców, degradujących obowiązujące wartości moralno-etyczne, wprowadzających zamęt, niestabilność nastrojów i nieprzewidywalność zachowań; konfrontacji tej towarzyszy zwykle rozwój patologii społecznych w postaci upowszechniania narkomanii, alkoholizmu, pornografii, epatowania przemocy oraz innych tego typu zjawisk.

Względna asymetryczność zantagonizowanych stron, zarówno w sferze materialnej, jak i duchowej oraz wynikające z niej zagrożenia, są z zasady wa-

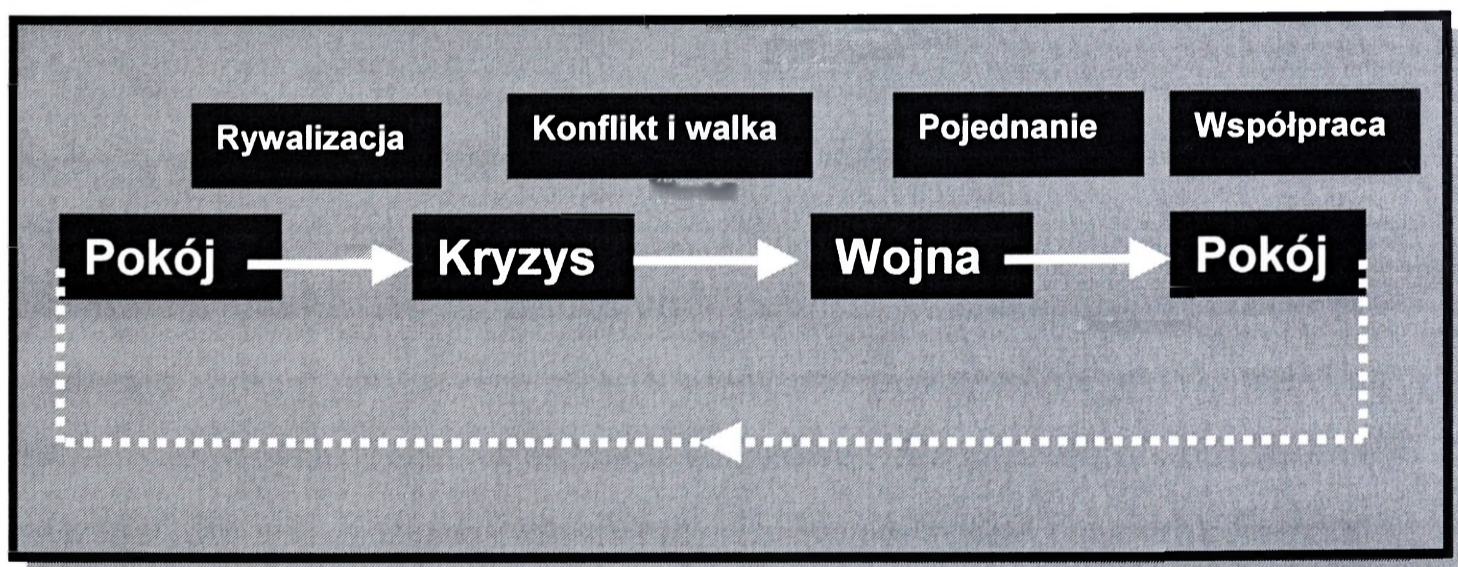
<sup>14</sup> Zarówno etniczne, grupowe (klanowe), rodzinne, jak i jednostkowe.

<sup>15</sup> Podobnie jak walka informacyjna oraz wojna kulturowa jest elementem szerszego planu działań w ramach przedsięwzięć PSYWAR.

runkowane łącznym wpływem czynników ilościowych i jakościowych, tworzących wypadkową udziału i jednych i drugich.

Klasyczne już uwarunkowania ilościowe powodują, że bazą dla asymetrycznej przewagi jednej ze stron jest jej dominująca przewaga ilościowa. Może to mieć odniesienie do liczebności wojsk, ilości posiadanych środków rażenia (broni), wielkości wytwarzanych dóbr czy też innych, wpływających bezpośrednio na przebieg konfrontacji i decydujących o jej powodzeniu.

Uwarunkowania jakościowe charakteryzują się natomiast znacznie większym udziałem czynników wpływających na postęp i rozwój cywilizacyjny<sup>16</sup>. Ich obecność powoduje, że nawet przy zbliżonych i porównywalnych potencjałach ilościowych występuje asymetria jakościowa dająca przewagę jednej ze stron. Oznacza to najczęściej większą skuteczność i efektywność wykorzystania będących w jej posiadaniu środków, decydujących o szybkim<sup>17</sup> uzyskaniu przewagi na polu konfrontacji. Wariant cyklu zdarzeń towarzyszącemu asymetryczności przedstawiono na rysunku 1.



**Rys. 1 Cykl zdarzeń towarzyszący asymetryczności rozwoju stron (wariant)**

**(opracowanie własne)**

<sup>16</sup> Określanych także mianem „skoku cywilizacyjnego”.

<sup>17</sup> Np. niemiecki Blitzkrieg z okresu II Wojny Światowej oraz użycie broni jądrowej w 1945 r., a obecnie – możliwość zastosowania nowych rodzajów broni, w tym BMR lub opartych na wykorzystaniu nowych zjawisk w dziedzinie fizyki.

## 2. ROZUMIENIE POJĘCIA ASYMETRIA W KONTEKŚCIE ZADAŃ SIŁ ZBROJNYCH

Terminy „asymetria”, „asymetryczność”, „przeciwsymetria”, „działania asymetryczne”, „podejście asymetryczne”, „opcje asymetryczne” stanowią określenia pojawiające się często na łamach wydawnictw wojskowych, przede wszystkim w kontekście rozważań nad nowymi zagrożeniami. Sądząc po różnych zastosowaniach tego określenia, między innymi jako:

- nieuczciwa walka;
- uderzenie w słaby punkt;
- walka informacyjna
- walka w sferze opinii publicznej<sup>18</sup>;
- groźba lub wykorzystanie broni masowego rażenia

istnieją duże rozbieżności interpretacyjne definicji asymetrii w odniesieniu do środowiska bezpieczeństwa.

Asymetryczna koncepcja prowadzenia działań nie jest w historii szeroko pojmowanej rywalizacji państw, w tym również na płaszczyźnie wojskowej, ani zjawiskiem nowym, ani też rzadko występującym. Takie sposoby i formy prowadzenia walki pojawiały się na styku cywilizacji, względnie jako konsekwencja rewolucyjnych zmian w technice wojskowej. Sięgając do historii możemy doszukać się takich sugestywnych przykładów jak walka Dawida z Goliatem, podboje Hetytów, czy też użycie przez Hannibala „słoni bojowych”.

David L. Grange podaje trzy sztandarowe przykłady stanowiące przełom w możliwościach wykorzystania sił:

---

<sup>18</sup> Jako zespół przedsięwzięć realizowanych w ramach wojny psychologicznej.

- w I Wojnie Światowej - taktyka działań szturmowych (niem. Sturmtrupp) przełamujących linie okopów i umocnień, a także walka w trzech wymiarach, będąca skutkiem wprowadzenia do działań lotnictwa;
- w II Wojnie Światowej – działania niemieckich związków pancernych w okresie kampanii we Francji;
- w przedostatniej dekadzie minionego wieku – Strategiczna Inicjatywa Obronna (Strategic Defence Initiative – SDI), która przyczyniła się do zakończenia wyścigu zbrojeń między USA i Związkiem Radzieckim.

Zagrożenie asymetryczne jest stwarzane najczęściej przez stronę, która dążąc do konfrontacji nie jest zdolna przeciwstawić się przeciwnikowi w sposób symetryczny, z użyciem tych samych lub podobnych środków walki. W takiej sytuacji, strona opierająca się na strategii działań asymetrycznych stara się tak wybrać pole konfrontacji, aby maksymalnie ograniczyć możliwość wykorzystania przez stronę przeciwną jej przeważającego potencjału bojowego. Z działaniami asymetrycznymi możemy mieć do czynienia także w przypadku, kiedy jedna ze stron dokona przełomu technicznego lub technologicznego, rewolucjonizującego możliwości i zdolność bojową sił zbrojnych. Przełom taki wystąpił np. w wyniku wyprodukowania i użycia broni jądrowej.

Należy mieć także świadomość, że nowe środki oddziaływania, bazujące zarówno na zjawiskach znanych, ale dotychczas nie wykorzystywanych jako narzędzie walki, jak i na zjawiskach nowo poznanych, umożliwiły wyprodukowanie broni porównywalnej do klasycznych środków walki oraz stworzenie zupełnie nowych środków, będących produktem wykorzystywania szczególnie zawansowanych technik i technologii.

## 2.1. Istota podejścia NATO

Należy odnotować, że 6 grudnia 2001 roku, w czasie konferencji prasowej zorganizowanej po spotkaniu Rady Północnoatlantyckiej, sekretarz generalny NATO, lord Robertson, zapytany o sposób przygotowań Sojuszu do globalnej walki z terroryzmem stwierdził, że *„należy najpierw zdefiniować te zdolności, które zapewniają ochronę naszych sił zbrojnych oraz ludności cywilnej w sytuacjach, które określamy jako ataki asymetryczne (asymmetric attacks), zwłaszcza przy użyciu takich nowych środków jak broń chemiczna oraz biologiczna”*.

Z kolei w oświadczeniu wydanym 7 grudnia 2001 roku przez Grupę Kierowniczą ds. Współpracy w Dziedzinie Bezpieczeństwa w Południowo-Wschodniej Europie (South East Europe Security Cooperation Steering Group – SEEGROUP) stwierdzono, że w ramach wdrażania nowych instrumentów oraz środków wzmacniania bezpieczeństwa regionalnego należy *“określić i promować pakiet przedsięwzięć do zwalczania zagrożeń asymetrycznych w Południowo-Wschodniej Europie, włącznie z terroryzmem i zorganizowaną przestępczością”*.

Również 7 grudnia 2001 roku, w ramach spotkania ministrów spraw zagranicznych Rady Współpracy Euroatlantyckiej (Euro-Atlantic Partnership Council – EAPC) wydane zostało oświadczenie krajów członkowskich Grupy Wileńskiej (Albania, Bułgaria, Chorwacja, Estonia, Łotwa, Litwa, Macedonia, Rumunia, Słowacja i Słowenia) o tym, że w pełni identyfikują się one z treścią oświadczenia EAPC noszącego tytuł „Odpowiedź NATO na terroryzm”, dodając, że *„plaga terroryzmu, nowe wyzwania i wylaniające się zagrożenia asymetryczne wymagają przyjęcia dynamicznego programu, który jest obecnie opracowywany w ramach różnych forów międzynarodowych, w tym Rady Współpra-*

cy Euroatlantyckiej”.

W wystąpieniu sekretarza generalnego lorda Robertsona z 18 lutego 2002 roku w Chatham House (Londyn), na temat „NATO: proces poszerzenia i redefinicji”, znalazły się słowa o tym, że „ponieważ NATO jest najefektywniejszą na świecie organizacją wojskową, z tego tytułu ma do odegrania kluczową rolę w sferze reagowania kryzysowego, włącznie ze sprostaniem zagrożeniom asymetrycznym. Szczyt w Pradze skonsoliduje pozycję Sojuszu jako organizacji dysponującej siłami zbrojnymi zdolnymi do pokonania terroryzmu i sprostania innym wyzwaniom terrorystycznym”.

Nowa rola i wzrastające znaczenie problematyki zagrożeń asymetrycznych zostały dostrzeżone już we wczesnych latach 90., głównie w kontekście przyczyn ich powstawania, potencjalnego ryzyka generowania konfliktów, krótko- i długoterminowych prognoz ich występowania, a także oceny ewentualnych skutków (lokalnych, regionalnych i globalnych). W ramach struktur wykonawczych NATO (komitetów, grup i sekcji roboczych), a także powoływanych „ad hoc” ciał doradczych i eksperckich, podjęto w tym zakresie szereg przedsięwzięć, których efektem stały się systematycznie uaktualniane analizy, opracowania i dokumenty normatywne, z których najważniejsze są zatwierdzane przez zwierzchnie organy sojuszu<sup>19</sup>.

Państwa NATO, zgodnie z obowiązującą strategią, muszą być przygotowane do prowadzenia wielu, często równoległych operacji wojskowych o zróżnicowanym stopniu intensywności, w różnych miejscach świata, jak również być zdolne do realizowania zadań we wszystkich warunkach, w tym wobec stosowania przez przeciwnika asymetrycznych sposobów walki m.in. z użyciem środków masowego rażenia<sup>20</sup> oraz terroryzmu. Zakłada się przy tym, że w warunkach zdecydowanej przewagi wojskowej państw NATO, głównie Stanów

<sup>19</sup> M.in. SEEGROUP ACTION PLAN 2002 – plan działania dla państw SEEGROUP (South East Europe Security Cooperation Steering Group) oraz dokumenty komitetów Politycznego i Wojskowego NATO.

<sup>20</sup> Jądrowych (radiologicznych), chemicznych lub biologicznych.

Zjednoczonych, potencjalni przeciwnicy w celu uzyskanie pożądaných rezultatów polityczno-wojskowych będą coraz częściej stosowali asymetryczne sposoby walki obejmujące niekonwencjonalną strategię i taktykę działania oraz (a być może zwłaszcza) technikę.

## 2.2. Istota podejścia amerykańskiego

W Stanach Zjednoczonych pojęcie asymetria, w kontekście zaangażowania sił zbrojnych USA, pojawiło się oficjalnie w 1995 roku, w publikacji doktrynalnej *Połączona Walka Sił zbrojnych USA* (Joint Warfare of the Armed Forces of the United States - JP 1). Było definiowane jako starcia między sobą różnych RSZ, na przykład sił powietrznych z siłami lądowymi czy też siłami morskimi. Mieliśmy do czynienia z wąskim pojęciem koncepcji asymetrii.

Zjawisko to w szerszym wymiarze zostało opisane w tym samym roku w Narodowej Strategii Wojskowej (National Military Strategy), wskazując na takie **zagrożenia asymetryczne** jak na przykład terroryzm, wykorzystanie (lub sama groźba użycia) broni masowego rażenia, walka informacyjna.

W miarę upływu czasu zagrożenia asymetryczne zaczęły skupiać coraz większą uwagę. W 1997 roku, w Raporcie Czteroletniego Przeglądu Obronnego (Quadrennial Defence Review) stwierdzono, że (...) *dominacja Stanów Zjednoczonych w dziedzinie uzbrojenia konwencjonalnego może zachęcić przeciwnika do wykorzystania środków asymetrycznych w celu zaatakowania sił amerykańskich stacjonujących za granicą lub Amerykanów w ich kraju.*

W raporcie przedłożonym w tym samym roku przez Narodowy Panel Obronny (National Defence Panel), w którego skład wchodziłi eksperci powołani przez Kongres stwierdzono, że (...) *można założyć, że nasi przyszli przeciwnicy wyciągnęli wnioski z wojny w Zatoce Perskiej. Nie jest prawdopodobne, aby stawili nam czoła wykorzystując formacje pancerne, siły powietrzne czy też zespoły okrętów, to znaczy na płaszczyznach, na których USA posiadają miazdzą-*

ca przewagę. Zamiast tego mogą przyjąć nowe sposoby do zaatakowania naszych interesów, sił i obywateli.

W raporcie zwrócono szczególną uwagę na możliwość:

- dużych strat jakie mogą być zadane przez BMR, jednocześnie skutkującymi trudnościami lub opóźnieniem dostępu sił USA do rejonu działań;
- uderzeń na amerykańskie systemy informacyjne;
- wykorzystania min i pocisków raketowych w rejonach cieśnin oraz podejść do wybrzeża;
- działań terrorystycznych.

Reakcją amerykańskich kręgów polityczno – wojskowych na powyższy dokument było szczegółowe zajęcie się asymetrią oraz jej potencjalnymi skutkami. Problemowi temu poświęcona została doroczna konferencja strategiczna, zorganizowana w 1998 roku w Akademii Wojennej Sił Lądowych USA. Tematem konferencji były: „Zagrożenia symetryczne i asymetryczne Stanów Zjednoczonych: czy Ameryka może zostać pokonana?”. Natomiast w wymiarze merytorycznym skupiono uwagę na ocenie możliwości i odpowiedzi na pytanie: czy USA mogą zostać zwyciężone uderzeniem środkami asymetrycznymi w przyszłości pięcie Achillesa sił zbrojnych względnie, w znaczącym stopniu niechronione, kluczowe ośrodki infrastruktury cywilnej. W toku prowadzonej dyskusji odpowiedź na postawione w tytule konferencji była następująca: „*USA nie mogą zostać pokonane w wyniku ataku symetrycznego, natomiast mogą być pokonane w wyniku ataku asymetrycznego*”.

Należy zauważyć, że w trakcie dyskusji zostały podważone treści opracowania „Wspólna Wizja’2010” („Joint Vision’2010”), opublikowanego w 1997 roku przez Przewodniczącego Kolegium Połączonych Sztabów i przedstawiającego zadania, strukturę i sposoby działania sił zbrojnych USA w perspektywie

roku 2010. Konkluzją dyskusji było również to, że administracja amerykańska nie jest właściwie przygotowana, wyposażona i zorganizowana do sprostania wszystkim typom zagrożeń, a z tego tytułu dla administracji federalnej rodzi się konieczność opracowania koncepcji, doktryn oraz zasad organizacyjnych dotyczących współpracy wykraczającej poza granice kulturowe, prawne i budżetowe.

Jak wynikało z podsumowania konferencji, jej uczestnicy byli zgodni co to tego, że (...) *dotarcie do umysłów nieprzyjaciela jest ważniejsze od dotarcia do jego bitów*. Podkreślono także, że dysponowanie nowoczesnymi technologiami może stanowić w sytuacjach walki asymetrycznej poważną słabość. Sposobem odniesienia sukcesu jest zrozumienie istoty zagrożeń, a przez to uzyskanie zdolności zapobiegania im w takim czasie, aby było możliwe zapobieżenie konfliktowi.

Można przypuszczać, że druzgocąca krytyka, jakiej zostało poddane opracowanie „Wspólna Wizja’2010” stanowiło przyczynę opublikowania już w 2000 roku przez Przewodniczącego Kolegium Połączonych Sztabów kolejnego dokumentu o podobnym tytule „Wspólna Wizja’2020” (Joint Vision’2020), z tą jednak różnicą, że konieczność sprostania zagrożeniom asymetrycznym została przedstawiona jako jedno z wiodących wyzwań przyszłości SZ USA. Koncepcja operacyjna, jaka stanowi podstawę opracowania „Wspólna Wizja’2020” dotyczy dominacji w pełnym spektrum (full spectrum dominance), będącej pochodną następujących zdolności sił zbrojnych USA, jakie powinny zostać osiągnięte do około 2020 roku:

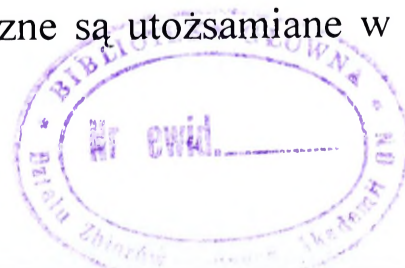
- dominującego manewru (dominant maneuver);
- precyzyjnych działań bojowych (precision engagement);
- zogniskowanej logistyki (focused logistics);
- ochrony w pełnym spektrum (full-dimensional protection).

Również w dorocznych raportach Sekretarza Obrony dla Kongresu z 1998 roku, a potem z 1999 roku podkreślono, że dominacja SZ USA w dziedzinie uzbrojenia klasycznego zachęca przeciwników do poszukiwania środków asymetrycznych dla zaatakowania amerykańskich SZ, interesów USA oraz obywateli Stanów Zjednoczonych. W opracowaniach jakie dotyczyły przedmiotowego zagadnienia szczególne znaczenie posiadało studium „Przegląd połączonej strategii 1999 roku – Podejście asymetryczne do walki” (1999 Joint Strategy Review, *Asymmetric Approaches to Warfare*), stanowiące podstawę koncepcyjną oraz zawierające liczne rekomendacje.

Od kiedy w dokumentach Departamentu Obrony pojawiło się wiele definicji działań i zagrożeń asymetrycznych, większość z nich wprost identyfikuje specyficzne problemy bezpieczeństwa. Ponadto definicje te, w sposób ograniczony analitycznie, odzwierciedlają „amerykański centryzm”. Na przykład „Połączony Przegląd Strategiczny 1999” wprowadził szerokie uogólnienie asymetrii. Stanowi ono, że (...) *asymetryczne podejścia to próby oszukania lub podkopania siły Stanów Zjednoczonych poprzez uwypuklanie słabości USA przy użyciu metod, które w sposób wyszukany różnią się od metod operacyjnych stosowanych przez Stany Zjednoczone. Podejścia te szczególnie poszukują głównych obszarów psychologicznego oddziaływania, jak szok lub zmieszanie, które w efekcie dają przeciwnikowi możliwości przejęcia inicjatywy, swobodę działania, lub spełnienie swej woli. Metody asymetryczne wymagają doceniania podatności na czułe miejsca – własne i przeciwnika. Podejścia asymetryczne często angażują metody innowacyjne, nie tradycyjne taktyki, uzbrojenie, lub technologie. Mogą być używane na wszystkich szczeblach w walce zbrojnej – w strategii, sztuce operacyjnej i taktyce – oraz w całym spektrum operacji wojskowych”.*

### 2.3. Istota podejścia francuskiego

Według ocen **francuskich** zagrożenia asymetryczne są utożsamiane w



pierwszym rządzie z terroryzmem, nazywanym „bronią biednych”. Stają się one zagrożeniem coraz groźniejszym, potężniejszym, lepiej zorganizowanym i wymierzonym przede wszystkim w najsłabsze punkty świata zachodniego jakim są jego ludność oraz terytorium. W ramach prowadzonej debaty są zadawane pytania o to, co należy zrobić, aby położyć kres działalności organizacji potrafiących wykorzystać do swych celów newralgiczne elementy systemu światowych powiązań (media, przepływ kapitału, kryptografia, piractwo komputerowe, gadżety elektroniczne, wyniki badań chemicznych i bakteriologicznych itp.)?

Ciekawa definicja zagrożenia asymetrycznego została sprecyzowana przez generała Christian Quesnot, prezydenta Komitetu Studiów Obrony Narodowej, który określił nim *„każdą formę zagrożenia ze strony ukonstytuowanej grupy, lub nie, zależnej od państwa, lub nie, na które to zagrożenie państwo, lub grupa państw, sojusz względnie instytucja nie są przygotowane kulturowo, strukturalnie, intelektualnie, ani też z punktu widzenia legislacyjnego, administracyjnego lub regulaminowego tak, aby móc zareagować natychmiastowo, skutecznie i ostro”*.

#### 2.4. Istota podejścia niemieckiego

Zagrożenia asymetryczne do 11 września 2001 roku uznawane były w Niemczech za dość abstrakcyjną teorię<sup>21</sup>. W specjalistycznych opracowaniach zwracano wprawdzie uwagę na nowe zagrożenia, ale nie stanowiły one dominującego obszaru rozważań. Wynikało to prawdopodobnie z faktu, iż wcześniej społeczeństwa zachodnie miały do czynienia przede wszystkim z wojnami między państwami lub konfliktami zbrojnymi wewnątrz państwa. Obecnie pojawiają się pozapaństwowi, międzynarodowi aktorzy dysponujący nieprzewidywal-

<sup>21</sup> V. Rühle, *Sicherheitspolitik nach dem 11. September: Herausforderungen für die Außenpolitik*, Deutsch-französisches Seminar der Konrad Adenauer-Stiftung, Roquebrune, 22. November 2001.

nym potencjałem zniszczenia. Wysoce technicyzowane społeczeństwa okazują się szczególnie wrażliwe.

Eurocentryczna perspektywa postrzegania wojny ograniczona do starcia między regularnymi siłami zbrojnymi przeciwstawnych państw określa dominujący obraz wojny nie tylko w polityce, siłach zbrojnych i opinii społecznej, lecz także w nauce. Tymczasem wojna między państwami tylko w stosunkowo krótkim okresie historycznym i na ograniczonym obszarze geograficznym była dominującą formą wojny. Postrzeganie wojny jako stanu prawnego między państwami jest rezultatem wojny trzydziestoletniej i nierozłącznie związane z powstawaniem państw terytorialnych. Podejście takie oznaczało także pewne unormowanie wojny, gdyż miała ona być prowadzona według skodyfikowanych reguł ciągle doskonalonego prawa wojennego. Jednym z najważniejszych rezultatów nowego podejścia do wojny – przynajmniej w odniesieniu do jej politycznych i militarnych założeń – był fakt, iż obiektem działań militarnych miały być siły zbrojne, a nie ludność cywilna przeciwnika. Znamienne jest jednak, że te unormowania wojny były w zasadzie ograniczone do stosunków między państwami europejskimi. Ograniczenia prawne nie obowiązywały w równoległe prowadzonych wojnach tych państw w ich koloniach lub przeciwko innym, pozaeuropejskim państwom<sup>22</sup>.

Zwraca się przy tym uwagę, że równoległe do wojen między państwami występowała także inna forma wojny. Charakteryzowała się ona – nie tak jak wojny między państwami – wzajemnie uznanymi regułami, lecz właśnie ich brakiem. Są to tzw. „małe wojny” (*kleinen Kriege*)<sup>23</sup>. Dla opisanego zjawiska we współczesnej literaturze niemieckiej przedmiotu używa się zamiennie określeń: konflikt o obniżonej intensywności, wojna partyzancka, wojna asymetryczna czy wojna postnarodowa. Chodzi przy tym o te wszelkie wojny, które

<sup>22</sup> M. Hoch, *Krieg und Politik im 21. Jahrhundert* [w:] *Workshop Krieg im 21. Jahrhundert*, Clausewitz-Protokolle 2001, nr 1, s. 2.

<sup>23</sup> Pojęcie małej wojny w niemieckim obszarze językowym rozpowszechnił Carl von Clausewitz dla odróżnienia tego zjawiska od „dużych” wojen między państwami.

nie są prowadzone między regularnymi armiami nowoczesnych państw. Obecnie w wojnach takich ścierają się z zasady regularne siły zbrojne państw i tzw. niepaństwowi aktorzy.

Żadne z przytoczonych wyżej określeń nie oddaje w pełni fenomenu wojny asymetrycznej. W tych „małych” wojnach najpełniej uzewnętrznia się pierwotna, niczym nieograniczona natura wojny. Przyznaje się przy tym, iż taki właśnie charakter miała większość wojen w historii ludzkości, a duże wojny, czyli wojny między państwami, toczone przez regularne siły zbrojne, względnie ich poprzedników, prowadzone według wzajemnie uznanych reguł, były raczej wyjątkiem. Podkreśla się ponadto, że tzw. duże i małe wojny postrzegać należy jako teoretycznie idealne typy wojny, które niekoniecznie, jeśli w ogóle, występują w czystej formie. Tylko na podstawie możliwości wyraźnego zdefiniowania przeciwstawnych stron – państwo przeciwko państwu lub państwo przeciwko niepaństwowym aktorom – możliwe jest w miarę precyzyjne różnicowanie<sup>24</sup>.

W niemieckiej literaturze przedmiotu **wojna asymetryczna** określana jest jako **mała wojna lub konflikt o obniżonej intensywności, w którym państwa lub społeczeństwa wystawione są na zagrożenia ze strony aktorów państwowych lub niepaństwowych, np. grup terrorystycznych, bojowników o wolność, hakerów komputerowych, stosujących najczęściej niekonwencjonalne środki**<sup>25</sup>. O ile jednak wcześniejsze „małe” wojny z punktu widzenia teorii prowadzenia działań wojennych rozpatrywane były przez stronę słabszą i jako takie nie stanowią istotnego novum, to obecne rozważania dotyczące konfliktów asymetrycznych odnoszą się przede wszystkim do sposobów działania państwa wystawionego na uderzenia nie zawsze zidentyfikowanego przeciwnika. Wysoce rozwinięte państwa dysponujące zróżnicowanym uzbrojeniem trudno jest pokonać w bezpośredniej konfrontacji. Działania asymetryczne ukierun-

<sup>24</sup> M. Hoch, *Krieg und Politik ...*, s. 3.

<sup>25</sup> *Bundesnachrichtendienst-Lexikon*, <http://www.bundesnachrichtendienst.de/faq/lexikon.htm>.

kowane są w takiej sytuacji na wrażliwe miejsca społeczeństw połączonych skomplikowanymi układami powiązań gospodarczych i informacyjnych.

Podczas gdy zachodnia sztuka prowadzenia wojen opiera się na myśleniu systemowym i ukierunkowana jest na środki ciężkości przeciwnika, to takie myślenie nie występuje raczej po stronie terrorystów czy innych uczestników konfliktu asymetrycznego. Nowoczesne organizacje terrorystyczne czy też kryminalne wykorzystują wrażliwość zachodnich struktur społecznych do prowadzenia własnych działań. Uderzenia skierowane są na najbardziej wrażliwe systemy wielokrotnie przeważającego przeciwnika, aby poprzez wywołany strach i emocje ludności, sprowokować go do podjęcia błędnych decyzji, a tym samym do niewłaściwego działania<sup>26</sup>. Przewaga w uzbrojeniu może mieć decydujące znaczenie w symetrycznej wojnie między przeciwnikami, którzy operują w podobny sposób. Istotne znaczenie mają również takie aspekty, jak strategia, taktyka czy morale walczących wojsk. Wydarzenia z początku 21 wieku unaoczniają ograniczoną zdolność technologii do sprostania wszelkim wyzwaniom. Tak zwana rewolucja w sprawach wojskowych oznacza zdolność najbardziej zaawansowanych technologicznie mocarstw do uzyskiwania rozstrzygnięcia na odległość przy możliwie najmniejszych stratach. Przekonanie, iż przewaga technologiczna upraszcza drogę do zwycięstwa, wydaje się jednak poważnym nieporozumieniem. W wojnie asymetrycznej korzyści z przewagi uzbrojenia mogą być niewielkie. Specjaliści niemieccy przywołują tu dla przykładu porażkę wojsk amerykańskich w Wietnamie i izraelski sukces w wojnie sześciodniowej.

O ile działania symetryczne w podejściu Akademii Dowodzenia Bundeswehry<sup>27</sup> uznawane są za konfrontacje między siłami podobnego rodzaju, a więc posiadającymi zbliżone struktury, środki i poziom technologiczny, to działania asymetryczne określane są jako konfrontacje między nierównymi siłami charak-

---

<sup>26</sup> A. Stahel, *Null-Verluste Strategie und virtueller Krieg*, Österreichische Militärische Zeitschrift 2002, nr 3, s. 376.

<sup>27</sup> *Reader Zentrum Führung Gemeinsamer Operationen*, Führungsakademie der Bundeswehr, Hamburg 2000, s. 3-8 – 3-10.

teryzującymi się dysproporcją możliwości, odmiennymi strukturami i standardami technologicznymi, metodami i formami działania. Charakterystyczne dla podejścia niemieckiego jest bardzo szerokie postrzeganie asymetrii, niekoniecznie obserwowane u pozostałych sojuszników. Zgodnie z tym stanowiskiem pojęcia symetrii i asymetrii odnosić się mogą także do konfrontacji między rodzajami sił zbrojnych przeciwnych państw. Tak więc jako symetryczne określane są starcia między takimi samymi rodzajami sił zbrojnych, a jako asymetryczne starcia między różnymi rodzajami sił zbrojnych, np. między siłami morskimi i siłami powietrznymi, między siłami morskimi i siłami lądowymi. Działania symetryczne i asymetryczne mogą także wynikać z różnic strukturalnych, organizacyjnych, uzbrojenia i wyszkolenia stron konfliktu.

Innym wyróżnikiem niemieckiego podejścia jest rozpatrywanie wojny asymetrycznej nie tylko z pozycji strony zaatakowanej, mającej przeciwstawić się niekonwencjonalnym zagrożeniom, lecz także z punktu widzenia strony stosującej takie podejście w konfrontacji z przeważającym przeciwnikiem. Zdaje się to mieć źródła w wieloletniej pruskiej i niemieckiej tradycji wojskowej. Położenie Niemiec w centrum Europy, subiektywne poczucie okrążenia oraz zagrożenia wojną spowodowały, iż wojna na dwa fronty znalazła się w centrum niemieckich rozważań strategicznych już na przełomie dziewiętnastego i dwudziestego wieku. Strategiczny stosunek sił i konstelacje sojusznicze jednoznacznie wskazywały, iż Rzesza Niemiecka nie jest w stanie jednocześnie skutecznie prowadzić ofensywy na dwóch frontach. Dlatego też gen. Alfred von Schlieffen, biorąc pod uwagę uwarunkowania geopolityczne, zdecydował się na działania ofensywne, zakładając, iż po szybkim sukcesie na zachodzie, zwolnione siły będą mogły przejść do skutecznego rozstrzygającego uderzenia przeciwko Rosji<sup>28</sup>.

---

<sup>28</sup> G. Roth, *Der Vernichtungsgedanke im militärischen Denken bei Carl von Clausewitz und Graf Alfred von Schlieffen* [w:] *Operatives Denken bei Clausewitz, Moltke, Schlieffen und Manstein*, Freiburg im Breisgau 1988, s. 9.

Również w okresie międzywojennym centralne położenie Niemiec w Europie rodziło subiektywne poczucie zagrożenia, przekonanie o konieczności przeciwstawienia się przeważającym, połączonym siłom sąsiadów. Niemcy nie miały wystarczających surowców i zasobów ani wyszkolonych rezerw umożliwiających prowadzenie długotrwałej wojny na wyczerpanie. Obawiano się również wojny na dwa fronty. Dlatego też myślenie operacyjne w Niemczech skoncentrowano na wypracowaniu koncepcji umożliwiającej słabszym liczebnie wojskom niemieckim szybkie uzyskanie rozstrzygnięć operacyjnych poprzez pokonywanie kolejnych przeciwników i postawienie ich sojuszników przed faktami dokonanymi. Z tej właśnie tradycji zdaje się wynikać zalecenie, iż również obecnie działania asymetryczne mogą być szczególnie skuteczne, gdy przeciwnik nie jest na nie przygotowany i nie jest w stanie na takie działania skutecznie reagować. Zwraca się jednak uwagę, że prowadzenie działań asymetrycznych wymaga większej koordynacji niż ma to miejsce podczas operacji symetrycznych. Ponieważ jednak działania asymetryczne są z reguły skuteczniejsze i ograniczają własne straty, zaleca się stosowanie tego sposobu podejścia w operacjach połączonych. Połączone działania własnych rodzajów sił zbrojnych mają z kolei, dzięki szerokiemu spektrum różnorodnych możliwości, skutecznie przeciwdziałać skutkom operacji asymetrycznych prowadzonych przez przeciwnika<sup>29</sup>.

Główny nurt rozważań niemieckich w odniesieniu do wojny asymetrycznej dotyczy jednak sytuacji, w której to silniejsza strona wystawiona jest na niekonwencjonalne ataki słabszego z definicji przeciwnika. Podkreśla się przy tym, iż te „małe” asymetryczne wojny wcale nie muszą być mniejsze od „dużych” wojen – ani w odniesieniu do ich intensywności czy czasu trwania, ani też siły niszczenia. Charakterystyczny natomiast dla tych wojen jest brak lub też łamanie obowiązujących reguł prowadzenia działań wojennych. W sposób szczególny uzewnętrznia się to w braku rozróżnienia między kombatantami i ludnością

---

<sup>29</sup> *Reader Zentrum Führung Gemeinsamer Operationen ...*, s. 3-9.

cywilną – stanowiącym przecież sedno nowoczesnego prawa humanitarnego. Z tego też powodu dla określenia takich wojen używa się także pojęcia „wojny nietrynitarnie”, w których nie funkcjonuje – charakterystyczne dla nowoczesnego państwa – rozróżnienie między rządem, siłami zbrojnymi a ludnością cywilną<sup>30</sup>.

Wojna asymetryczna już z definicji jest wojną nieograniczoną, tak więc zastosowanie w niej znajdują wszelkie możliwe środki i w swej charakterystycznej brutalności, zwłaszcza wobec ludności cywilnej, a przede wszystkim kobiet i dzieci, przyjmuje kierunki rozwoju zbliżające ją do fenomenu wojny totalnej. **Symetria**, a więc ograniczenie walki tylko do żołnierzy przeciwnej strony, charakteryzuje dużą wojnę, małe asymetryczne wojny charakteryzują się natomiast świadomym dążeniem do **asymetrii** w walce przeciwko najbardziej wrażliwemu miejscu przeciwnika, a więc oddziaływaniem na ludność cywilną<sup>31</sup>.

W rozważaniach niemieckich obecny jest także kolejny istotny aspekt wojny asymetrycznej, a mianowicie błyskawiczny wzrost liczebny niepaństwowych aktorów w polityce międzynarodowej. Zyskują oni ciągle na znaczeniu i zwiększają swe wpływy. Obok klasycznych ruchów niepodległościowych i struktur ruchu oporu, zalicza się do nich zorganizowaną przestępczość, prywatne siły zbrojne oraz prywatne organizacje bezpieczeństwa i wywiadowcze. Pojawiają się także inni niepaństwowi aktorzy, tacy jak np. działające globalnie koncerny czy też organizacje pozarządowe, które jednak (jeszcze) nie występują jako strony bezpośrednio zaangażowane w konflikty, nawet jeśli mogłyby one w nich uczestniczyć lub wywierać na nie wpływ. Uważa się przy tym, że uczestnicy tacy mogą działać zarówno we własnym interesie, jak również na zlecenie państwa lub innego niepaństwowego aktora<sup>32</sup>.

<sup>30</sup> M. Hoch, *Krieg und Politik ...*, s. 3.

<sup>31</sup> Tamże.

<sup>32</sup> Tamże, s. 7.

Uwarunkowania te znacznie komplikują międzynarodowe i wewnętrzne stosunki polityczne. Państwa przestały już być jedynymi dysponentami przemocy w polityce międzynarodowej, co w rezultacie powoduje zanik państwowego monopolu oraz współistnienie lub konkurencję państwowego i niepaństwowego użycia siły. Większość wojen od 1945 roku była i prawdopodobnie będzie prowadzona nie między państwami, lecz między państwami i niepaństwowymi aktorami, były to więc i będą wojny asymetryczne. Niejako przy okazji zauważa się, że w nowoczesnym systemie państw istniały do tej pory, wprawdzie nie wyłącznie, ale przede wszystkim, państwa, które dla realizacji interesów panujących elit, prowadziły wojny. Obecnie zarysowują się tendencje do „odpaństwowienia” wojny w dwóch kierunkach<sup>33</sup>. Z jednej strony wzrasta liczba wojen wewnętrznych, między społecznościami, prowadzonych przez różnorodne grupy dla osiągnięcia często trudnych do zdefiniowania celów politycznych. Z drugiej strony natomiast obserwuje się multinacjonalizację jej prowadzenia. Wszystkie interwencje militarne w imieniu wspólnoty międzynarodowej, a więc legitymizowane przez Narody Zjednoczone lub jedną z organizacji regionalnych, są w zasadzie wielonarodowe. W takiej wojnie poszczególne państwa spełniać mają funkcje dostarczycieli zasobów niezbędnych do jej prowadzenia. Z całą pewnością dotyczy to państw, które zamierzają aktywnie uczestniczyć w takiej międzynarodowej polityce bezpieczeństwa, w czym mogą mieć całkowicie różne interesy.

W tym kontekście specjaliści niemieccy postrzegają zasadniczą transformację ogólnego fenomenu wojny. Otóż zjawisko wojny wydaje się coraz bardziej wychodzić z celowej racjonalnej sfery działalności politycznej. Podstawę decyzji o wojnie mogą stanowić nie tylko racjonalne rozważania na gruncie interesów, rzeczowego rachunku korzyści i strat, lecz także o wiele trudniejsze do dostrzeżenia dla postronnych powody ideologiczne lub emocjonalne. Wojna

---

<sup>33</sup> W. Bredow, *Militär, Krieg und Nation – Zukunftsorientierte Überlegungen im Anschluß an Clausewitz* [w:] *Clausewitz und die Zukunft von Krieg und Militär*, Clausewitz-Information 2002, nr 1, s. 3.

może ponadto być celem samym w sobie, na przykład wówczas, gdy staje się sposobem na życie. Tak więc clausewitzowska definicja wojny jako formy polityki między suwerennymi państwami staje się nieaktualna. Ponadto w wojnie asymetrycznej bardzo nieostre są granice między wojną a pokojem, będące przecież podstawą współczesnego zachodniego rozumienia wojny. Obowiązujące do tej pory zróżnicowanie między wojną a pokojem, bezpieczeństwem zewnętrznym a wewnętrznym, sferą prywatną a społeczną w tej nowej formie konfliktu bardzo się rozmyło. Wraz z przenikaniem zanikają różnice między polityką, wojskiem, wywiadem, policją i dystrybutorami informacji. Dla wojen asymetrycznych charakterystyczne jest ponadto także ściśle powiązanie z mniej lub bardziej zorganizowaną przestępczością, na przykład handlem narkotyków, aby pozostać tylko przy tym jednym przykładzie. Wyrazem bezradności państw wobec nowych wyzwań związanych z konfliktami asymetrycznymi jest niepewność terminologiczna, która z jednej strony dotyczy zwalczania terroryzmu i przestępczości, z drugiej zaś mówi o wojnie, zwycięstwie i klęsce, charakteryzując dość powszechną jeszcze niepewność państwa w stosunku do roli, jaką ma ono odgrywać w tej walce<sup>34</sup>.

Z przedstawionych w tym podrozdziale uwarunkowań nie wynika, że według specjalistów niemieckich wojny asymetryczne po prostu zastąpią w spektrum konfliktów 21 wieku klasyczne duże wojny. Uznaje się, iż raczej dojdzie do rozszerzenia możliwych scenariuszy, niż zastąpienia dotychczasowych nowymi. W dalszym ciągu możliwy będzie zarówno klasyczny konflikt między regularnymi siłami zbrojnymi, jak i konflikt z zastosowaniem broni masowego rażenia. Wydaje się jednak, że w ogólnym spektrum możliwych konfliktów wojna między państwami nie będzie stanowić dominującej formy. Zwraca się przy tym uwagę na fakt, iż chodzi tu o tę formę wojny, do której państwa zachodnie – chociażby z powodu świadomości i potencjału militarnego – są najlepiej przygotowane. Mogą więc w przyszłości wykazywać tendencję do rozgrywania

<sup>34</sup> G. Palm, *Kapituliert der Staat?* <http://www.heise.de.tp/deutsch/inhalt/co/11013/1.html>

wania konfliktów militarnych na poziomie dużej wojny. Czy im to się uda i czy będzie skuteczne wobec niepaństwowych aktorów – pozostaje pytaniem otwartym<sup>35</sup>.

## 2.5. Istota podejścia brytyjskiego

Również koncepcja rozwoju sił zbrojnych **Wielkiej Brytanii** ma ogniskować się na problematyce zdolności do skutecznej obrony (lub działań uprzedzających) przed środkami asymetrycznymi. Jak stwierdził minister obrony Geoff Hoon (...) *ataki terrorystyczne ukazały w pełnej jaskrawości, że istnieje uzasadniona potrzeba przeorientowania SZ Wielkiej Brytanii pod kątem zagrożeń terrorystycznych oraz rosnącego prawdopodobieństwa działań asymetrycznych.*

W opublikowanym w 1997 roku Strategicznym Przeglądzie Obronnym (Strategic Defence Review – SDR) rozdział 2 nosił tytuł „Priorytety bezpieczeństwa w zmieniającym się świecie”. Stwierdzono w nim, że (...) *tam gdzie my (lub nasi Sojusznicy) wykorzystują technologię dla wzmocnienia naszej przewagi w dziedzinie uzbrojenia klasycznego, nasi potencjalni przeciwnicy mogą zastosować alternatywne uzbrojenie lub niekonwencjonalne (lub asymetryczne) strategie, prawdopodobnie atakując nasze czułe miejsca w otwartych społeczeństwach cywilnych.*

W wydanej w 1999 roku Białej Księdze Obronności (Defence White Paper 1999), w rozdziale nr 1, poświęconym kontekstowi strategicznemu, określone zostały nowe zagrożenia i wyzwania. Zaliczono do nich (...) *konsekwencje rozpadu państw, konflikty etniczne i religijne, napięcia na tle ludnościowym i środowiskowym, walka o dostęp do surowców, przemyt narkotyków, terroryzm i przestępczość ....., a wydarzenia w Kosowie i na Wschodnim Timorze oraz działania jakie podejmujemy w dziedzinie proliferacji i zagrożeń asymetrycznych*

<sup>35</sup> M. Hoch, *Krieg und Politik ...*, s. 10.

wzmocniły niektóre z naszych obaw i podkreśliły wagę realizowanego przez nas procesu modernizacji sił zbrojnych.

W opracowaniu stwierdzono ponadto, że (...) postęp w technologiach wykorzystywanych w naszych siłach zbrojnych oraz SZ sojuszników jest znaczący, natomiast jest paradoksem to, że rosące, konwencjonalne zdolności bojowe sprawiają, że rosą jednocześnie zagrożenia niekonwencjonalne. Potencjalni przeciwnicy mogą dojść do przekonania, że nie są w stanie rywalizować w ramach walki konwencjonalnej i poszukiwać płaszczyzn lub metod konfliktu, w których mogą uzyskać przewagę. Taki rodzaj zagrożeń jest potocznie nazywany zagrożeniami asymetrycznymi.

Z kolei w brytyjskiej strategii nauk wojskowych i innowacji (Defence Science and Innovation Strategy) stwierdza się, że rosące tempo cywilnego postępu technologicznego powoduje, iż osiągnięcie celów wojskowych staje się coraz bardziej możliwe w różny sposób. Z drugiej strony dostęp potencjalnych przeciwników do nowoczesnych technologii komercyjnych powoduje, że jeśli zostałyby one efektywnie wykorzystane, wtedy przeciwnicy mogliby, choć jedynie w pewnych obszarach, dysponować zdolnościami porównywalnymi z NATO. Z pewnością potencjalni przeciwnicy (...) zwiększą zdolności walki asymetrycznej, szczególnie w obszarach informacji, technologii, elektroniki, łączności oraz biotechnologii.

## **2.6. Wnioski i propozycje w zakresie definicji zagrożeń asymetrycznych**

Podstawowe różnice pomiędzy definicjami zagrożeń asymetrycznych proponowanymi przez głównych animatorów sojuszu (Stany Zjednoczone, Wielką Brytanię, Niemcy i Francję) polegają na różnicach w ocenianiu udziału nowych technologii i sposobów walki w osiąganiu celów strategicznych oraz znaczenia występowania w nich czynnika psychologicznego. Są one istotne,

zwłaszcza dla rozważań o tym jak „asymetryczni aktorzy” zamierzają osiągać swoje cele, które (czy to zrealizowane czy nie) są przez jednych uznawane za przedsięwzięcia o charakterze strategicznym, a przez innych (jak Stany Zjednoczone) za taktyczne lub co najwyżej operacyjne. Nie zmienia to jednak faktu, iż zagrożenia asymetryczne istniały i wciąż istnieją na wszystkich możliwych poziomach konfrontacji, w odniesieniu do wszystkich sfer życia i działalności, szczebli dowodzenia i rodzajów sił zbrojnych, a związani z nimi „aktorzy” (state- oraz non-state actors) będą je wykorzystywali, zarówno do działań dyplomatycznych, jak i do walki. Jedną z maksym głosi, że „słabym – jest ten kto robi jedynie to co może, silnym – ten kto decyduje się na wykonanie tego co konieczne”. Oznacza to, że nie w pełni angażująca się w konflikt strona (nawet mocarstwo), motywująca swoje działania obiektywnymi trudnościami i słabszy teoretycznie przeciwnik, mogą stworzyć asymetryczność, która w wyniku konfrontacji da zwycięstwo słabszemu, ale zdesperowanemu i zdecydowanemu na najbardziej ryzykowne działania przeciwnikowi.

W licznie formułowanych definicjach między innymi znajdujemy, że: przez asymetrię należy rozumieć umiejętność wykorzystania wszelkiego rodzaju różnic w szeroko pojmowanych potencjałach stron – od strony materialnej po psychologiczną – zarówno przed, jak i w toku prowadzenia działań, w celu osiągnięcia przewagi nad przeciwnikiem.

Można też definicje bardziej precyzyjne. Określa się w nich, że przez asymetrię w sferze bezpieczeństwa i strategii należy rozumieć myślenie i działanie odmienne od przeciwnika, w celu maksymalizowania własnej przewagi, wykorzystania słabości przeciwnika, a także zdobycia inicjatywy lub uzyskania większej swobody operacyjnej. Poziom rozważań, ocen i działań dotyczy sfery polityczno-strategicznej, strategicznej i operacyjnej. Może stanowić też ich kombinację.

Dotychczas nie istnieje jednolita i uznana przez wszystkich definicja za-

grożeń asymetrycznych, a większość terminów została sformułowana głównie przez amerykańskich teoretyków wojskowych. Trwają również uzgodnienia oraz próby wypracowania jednoznacznej definicji zagrożeń asymetrycznych w ramach Sojuszu Północnoatlantyckiego.

Na obecnym etapie uzgodnień i prób wypracowania **definicji zagrożeń asymetrycznych** przyjmuje się w NATO, że „**powstają one w wyniku obniżenia siły przeciwnika poprzez wykorzystanie jego słabych stron i przy użyciu metod różniących się w sposób istotny od standardowych procedur działania oraz zastosowanych środków**”.

### 3. CHARAKTERYSTYKA ZAGROŻEŃ (DZIAŁAŃ) ASYMETRYCZNYCH

#### 3.1 Działania asymetryczne według klasyfikacji NATO

Typowe działania asymetryczne, które mogą być podejmowane w okresach zwiększonego napięcia, organizowania ataków terrorystycznych, w wojnach partyzanckich i w otwartych konfliktach, polegają na:

- wprowadzaniu zamieszania lub obezwładnianiu w wybranym czasie, kluczowych elementów infrastruktury cywilnej lub wojskowej przeciwnika;
- uniemożliwianiu przeciwnikowi (opóźnianiu) rozwinięcia jego wojsk w okresie otwartego konfliktu;
- zrywaniu interoperacyjności w celu utrudnienia prowadzenia działań koalicyjnych;
- osłabianiu skuteczności wojskowej przeciwnika, w tym zwłaszcza poprzez ograniczanie możliwości użycia techniki przed i w trakcie prowadzenia działań bojowych;
- zwiększaniu kosztów operacji w wymiarze politycznym oraz zaangażowania zasobów ludzkich i materiałowych;
- ograniczaniu tempa prowadzenia operacji;
- uniemożliwianiu przeciwnikowi osiągnięcia przewagi informacyjnej i prawidłowej oceny sytuacji bojowej;
- osłabianiu poparcia politycznego udzielanego przeciwnikowi przez jego sojuszników.

Różnorodność środków asymetrycznych będących w dyspozycji potencjalnego przeciwnika jest obecnie bardzo duża, a w przyszłości prawdopodobnie jeszcze się zwiększy. Mogą one obejmować następujące elementy:

- walkę informacyjną<sup>36</sup> (Information Warfare - IW);
- broń masowego rażenia BMR;
- broń radiologiczną (Radiological Weapons - RW);
- technikę antysatelitarną (Anti-Satellite Technology - ASAT);
- tanie uzbrojenie i amunicję;
- broń obezwładniającą<sup>37</sup> (Non-Lethal Weapons - NLW);
- środki antymateriałowe;
- broń psychotroniczną;
- broń etniczną;
- środki walki wpływające na środowisko naturalne (Environmental Warfare - EW);
- broń geofizyczną.

### 3.1.1 Walka informacyjna

Stały wzrost wykorzystania nowoczesnej techniki informacyjnej przez rozwinięte państwa powoduje, że wiodące elementy ich infrastruktury wojskowej i cywilnej stają się podatne (wrażliwe) na różnego typu oddziaływania destrukcyjne, zakłócające ich prawidłowe funkcjonowanie. W siłach zbrojnych tych państw wykonanie precyzyjnych uderzeń ogniowych oparto np. na całkowicie skomputeryzowanym uzbrojeniu, poczta elektroniczna weszła na trwałe

---

<sup>36</sup> Pojęcie „walka informacyjna” pojawiło się na początku lat 90., a zdefiniowane zostało przez amerykańskich specjalistów wojskowych w 1996 r.

<sup>37</sup> NLW – broń o zmniejszonej (ograniczonej) śmiertelności.

do systemów łączności wojskowej i nawet funkcjonowanie logistyki stało się całkowicie zależne od techniki informatycznej. Podobnie przedstawia się sprawa z cywilnym sektorem państwowym i w gospodarką.

Zgodnie z przyjętą w NATO definicją – „*walka informacyjna to działania informacyjne prowadzone w okresie kryzysu lub konfliktu zbrojnego z zamiarem promowania określonego celu politycznego lub wojskowego w odniesieniu do wskazanego przeciwnika lub przeciwników*”.

Jej elementami wykonawczymi są **operacje informacyjne** dotyczące – „*działań wspierających wyselekcjonowane cele polityczne i wojskowe, podejmowane z zamiarem wpłynięcia na decydentów i polegające na oddziaływaniu na procesy informacyjne atakowanej strony, procesy oparte na informacji oraz systemy dowodzenia łączności i rozpoznania, przy równoczesnym zapewnieniu odpowiedniej ochrony własnemu systemowi informacyjnemu.*”

Możliwe są następujące formy ataku informacyjnego:

- zrywanie procedur wymiany informacji;
- manipulowanie informacją (dezinformacja, zatajanie, zniekształcanie);
- nieautoryzowane korzystanie z zasobów informacyjnych (baz danych) oraz kopiowanie i niszczenie zgromadzonych danych;
- masowe niszczenie oprogramowania systemowego.

Kompleksowe zastosowanie takich form ataku może doprowadzić do zablokowania skutecznego użycia broni, zarówno BMR, jak i konwencjonalnej. Narzędzia i metody walki informacyjnej, jakie mogą być stosowane to:

- wirusy komputerowe;
- bomby logiczne (specyficzne aplikacje programowe);
- blokowanie wymiany informacji w systemach łączności;

- fałszowanie informacji znajdujących się i przekazywanych w systemach łączności przeciwnika;
- wprowadzanie w obieg spreparowanych (tendencyjnych) informacji, za pośrednictwem środków masowego przekazu i kanałów łączności rządowej (wojskowej).

Ofensywne formy operacji informacyjnych stanowią wyraźne zagrożenie asymetryczne, głównie ze względu na uzależnienie od systemów informacyjnych stanowiących podstawę funkcjonowania systemów wypracowania decyzji. Taka sytuacja umożliwia przeciwnikowi skuteczne blokowanie lub opóźnianie procesów decyzyjnych, co może mieć szczególnie niebezpieczne konsekwencje w przypadku synergistycznego wpływu kilku form działań asymetrycznych równocześnie.

### **3.1.2 Broń masowego rażenia**

Proliferacja techniki i technologii produkcji broni jądrowej, biologicznej i chemicznej oraz środków ich przenoszenia stanowi obecnie jedno z najpoważniejszych wyzwań. Biorąc pod uwagę zarówno efekt psychologiczny, jak i fizyczny, BMR musi być traktowana jako potencjalna broń asymetryczna. Względna łatwość produkcji środków chemicznych i biologicznych oraz ich potencjał bojowy wpływają na wzrost możliwości ich wytwarzania przez państwa o ograniczonej infrastrukturze, a także organizacje i ugrupowania pozapaństwowe (non-state actors). Dlatego bardzo ważna jest dalsza nieprolifracja chemicznych i biologicznych środków walki oraz przestrzeganie obowiązujących w tym zakresie reżimów. Tymczasem wiele państw posiada infrastrukturę potrzebną do realizacji programów wytwarzania tej broni, a ich liczba stale rośnie.

Z trzech rodzajów broni masowego rażenia, technologia broni jądrowej

będzie w dalszym ciągu najtrudniejsza i najdroższa do uzyskania. Środki podjęte przeciwko jej proliferacji okazały się częściowo skuteczne. Niemniej jednak liczba państw dysponujących technologią produkcji broni jądrowej będzie rosła<sup>38</sup>. Państwa sponsorujące terroryzm nie posunęły się jednak dotychczas do uzbrojenia grup terrorystycznych w broń jądrową, prawdopodobnie z obawy przed działaniami odwetowymi oraz potrzebą dysponowania taką bronią dla realizacji własnych celów strategicznych. Jednocześnie bariery dla samodzielnego uzyskiwania środków chemicznych i biologicznych przez organizacje i ugrupowania pozapaństwowe mogą w perspektywie średnio- i długoterminowej zanikać. Uwzględniając większą dostępność BMR i jej proliferację, niektóre państwa mogą zdecydować się na wykorzystanie sponsorowanych przez siebie grup terrorystycznych do incydentalnego użycia takiej broni.

### 3.1.3. Broń radiologiczna

Broń radiologiczna jest środkiem, który może spowodować radioaktywne skażenie środowiska, żywności lub osób. Obecnie nadaje się do tego celu około 200 izotopów, posiadających wystarczająco długi czas (okres) połowicznego rozpadu, które mogą zostać rozprzestrzenione przy użyciu konwencjonalnych ładunków wybuchowych (bomb lotniczych, pocisków raketowych i artyleryjskich oraz granatów)<sup>39</sup>.

Taki sam efekt można uzyskać przez wykonanie ataku na instalacje jądrowe (elektrownie i urządzenia przetwarzania paliwa jądrowego), magazyny pośrednie i końcowe oraz transporty z materiałami rozszczepialnymi.

Wiele państw dysponuje możliwościami wyprodukowania broni radiologicznej na bazie posiadanych materiałów promieniotwórczych, np. zużytego

<sup>38</sup> Przykład Indii i Pakistanu z lipca 1998 roku.

<sup>39</sup> M.in. podczas konfliktów w Zatoce Perskiej, byłej Jugosławii i Afganistanie.

paliwa jądrowego. Może ona również zostać udostępniona organizacjom i ugrupowaniom pozapaństwowym, w tym o charakterze terrorystom.

### 3.1.4 Technika antysatelitarna

Zdolność do zwalczania sztucznych satelitów Ziemi, w tym zwłaszcza ze składu konstelacji operujących na niskich orbitach, może stać się w niedługim czasie bronią asymetryczną, ponieważ coraz większa liczba państw opanowuje technikę wynoszenia na orbitę satelitów<sup>40</sup> do prowadzenia rozpoznania, łączności, nawigacji oraz jako nosicieli broni.

Potencjalny przeciwnik może wykorzystać do bezpośredniego ataku pociski rakietowe, własne satelity umieszczane na tzw. orbitach kolizyjnych lub broń wiązkową DEW<sup>41</sup>, mające na celu zniszczenie lub obezwładnienie (zmniejszenie efektywności działania) satelitów przeciwnika.

### 3.1.5 Tanie uzbrojenie i amunicja

Standardem w zakresie taniego uzbrojenia i amunicji jest obecnie używanie prostych materiałów wybuchowych. Są one z reguły bardzo łatwe do wyprodukowania z ogólnie dostępnych komponentów. W połączeniu z odpowiednią techniką detonacji (zapalniki elektryczne i radiowe oraz czujniki) powodują szkody, których nie można lekceważyć.

Miny przeciwpancerne lub przeciwpiechotne są technicznie mało skomplikowane. Dotyczy to także raketowych przeciwpancernych pocisków kierowanych (rppk). W połączeniu z nowoczesnymi czujnikami i elektroniką mogą stać się systemami precyzyjnego i bardzo skutecznego rażenia. Czujniki, powiązane z urządzeniami celowniczymi, pozwalają na całkowicie automatyczne od-

<sup>40</sup> Chiny, Indie, Japonia, Korea Płn. i wiele innych.

<sup>41</sup> DEW (Directed Energy Weapons) – obejmuje m.in. broń częstotliwości radiowych RFW (Radio Frequency Weapons), broń mikrofalową HPM (High Power Microwave), broń laserową oraz broń cząstek elementarnych PBW (Particle Beam Weapons).

palanie rppk, a przez to na efektywne zamknięcie odcinka ostrzeliwanego terenu.

Innymi niebezpiecznymi systemami są przenośne przeciwlotnicze zestawy raketowe (PZR). Obecnie wykorzystują je SZ wielu państw świata. Stanowią one poważne zagrożenie, zwłaszcza w warunkach potencjalnych konfliktów asymetrycznych. Ugrupowania terrorystyczne dysponujące PZR i operujące np. w pobliżu lotnisk skutecznie mogą powodować katastrofy startujących i lądujących samolotów.

Programy budowy bezzałogowych aparatów latających, w tym małych i mikro UAV (Unmanned Aerial Vehicle), są realizowane w wielu krajach. Dzięki odbiornikowi GPS i automatycznemu pilotowi mogą odbywać długie loty i osiągać cel z niezwykłą precyzją. Technologicznie jest możliwe wyposażenie tych aparatów w odpowiednie uzbrojenie, m.in. pociski raketowe, bomby i działka. Obrona przeciwko takiemu zagrożeniu mogłaby okazać się w przyszłości krańcowo trudna, ponieważ przy użyciu technologii o obniżonej wykrywalności (stealth), niewielkie echo radarowe tych aparatów powoduje, że ich wykrycie jest bardzo trudne.

Bezpośrednie zagrożenie dla państw NATO wynikające z użycia takich systemów broni (zwłaszcza UAV) jest możliwe dopiero w perspektywie średnio- i długoterminowej. Może się to jednak zmienić w sytuacjach użycia wojsk w regionach kryzysowych. Natomiast wykorzystanie przez ugrupowania terrorystyczne lub podczas wojny partyzanckiej prostych ładunków wybuchowych, min, rppk i PZR jest w pełni realne, co ma (miało) miejsce w wielu obecnych konfliktach m.in. w Afganistanie, Angoli, Irlandii Płn., Somalii, Tajlandii oraz w wojnie palestyńsko-izraelskiej.

### **3.1.6 Broń obezwładniająca**

Broń „nieletalna”, określana mianem broni o zmniejszonej śmiertelności lub obojętnej, służy z założenia do wyłączenia przeciwnika z walki bez potrzeby jego uśmiercania. Działanie tej broni opiera się na zasadach wykorzystywanych m.in. w niskoenergetycznych odmianach broni wiązkowej DEW<sup>42</sup>, środkach materiałowych (substancje chemiczne, farmakologiczne i mikroorganizmy) oraz środkach makroskopowych (kleje, aerozole itp.). Wiele z nich znajduje się w powszechnym obrocie handlowym.

Możliwości broni „nieletalnej” są różnorodne, ale ograniczone w działaniu, ze względu na selektywne wykorzystanie specyficznego sposobu oddziaływania. Jej typowo obronny charakter sprawia, że jest mniej interesująca dla państw przejawiających agresywne zamiary<sup>43</sup>. Zagrożenie dla NATO ze strony takiej broni jest jednak możliwe, zwłaszcza w przypadku jej wykorzystania przez pozapaństwowe ugrupowania terrorystyczne i organizacje przestępcze oraz przeciwko żołnierzom pełniącym służbę w kontyngentach wojskowych różnych misji pokojowych.

### 3.1.7 Środki antymateriałowe

Zadaniem środków antymateriałowych jest doprowadzenie, poprzez wpływanie na struktury wewnętrzne kluczowych składników urządzeń technicznych<sup>44</sup>, do trwałego zakłócenia ich funkcji. Szczególne znaczenie ma to w przypadku powodowania uszkodzeń materiałów sztucznych i metali, poprzez oddziaływanie na substancje nieorganiczne występujące m.in. w metalowych i ceramicznych pancierzach, w paliwie, czy w oponach samolotów i pojazdów lądowych. Substancja płynna typu LME (Liquid Metal Embitterment) powoduje np. zmianę budowy molekularnej metali oraz stopów, a specjalne mikroby wy-

<sup>42</sup> Takich jak impulsowe emitory światła powodujące okresowe lub trwałe oślepienie (poprzez wywołanie efektu stroboskopowego na siatkówce oka), lasery oraz nadajniki mikrofalowe i akustyczne.

<sup>43</sup> Państw zaliczanych do grupy tzw. terroryzmu państwowego.

<sup>44</sup> Np. silników, agregatów i akumulatorów, podzespołów elektronicznych (procesorów) i innych.

tworzą enzymy powodujące rozkład wyrobów gumowych, albo nieprzydatność materiałów pędnych czy zmianę parametrów olejów silnikowych (np. lepkość).

Znane jest również oddziaływanie na człowieka światła stroboskopowego i generatorów akustycznych oraz innych środków psychotronicznych.

Materiały i składniki umożliwiające uzyskanie takich efektów są ogólnie dostępne. Ataki tego typu mogą stanowić zagrożenie dla NATO w perspektywie średnio- i długoterminowej, a incydentalnie – już obecnie podczas ataków terrorystycznych.

### **3.1.8 Broń psychotroniczna**

Mianem broni psychotronicznej określa się niskoenergetyczne urządzenia emitujące specjalnie uformowane (spreparowane) sygnały elektromagnetyczne bardzo niskich częstotliwości ELF<sup>45</sup> i mikrofal oraz inne, np. akustyczne, oddziałujące na psychikę i fizjologię ludzi. Za ich pomocą można wpływać na ludzki organizm, w tym zwłaszcza na centralny układ nerwowy, powodując odwracalne (lub trwałe) negatywne zmiany psychiczne oraz psychofizjologiczne. Skutkiem takiego oddziaływania mogą być zaburzenia (omamy) słuchowe i wzrokowe, dezorientacja, brak koncentracji, zaniki pamięci, nadpobudliwość, zmiany osobowościowe, bóle, dysfunkcje fizjologiczne, a w krańcowych przypadkach nawet śmierć. Z możliwym zagrożeniem ze strony takiej broni należy się liczyć dopiero wtedy, gdy wspomniany wyżej sposób oddziaływania zostanie jednoznacznie (praktycznie) potwierdzony. Niektóre źródła wskazują, że prace nad tego typu bronią były prowadzone m.in. w Australii, Chinach, Francji, Japonii, Niemczech, USA, Wielkiej Brytanii oraz byłym ZSRR (obecnie w Rosji).

### **3.1.9 Broń etniczna**

---

<sup>45</sup> ELF (Extremely Low Frequency) sygnały o częstotliwościach z zakresu poniżej 300 Hz.

Broń etniczna ma w swoim założeniu wywierać destrukcyjny i destabilizujący wpływ na selektywnie określone grupy ludzi (rasy, narodowości, społeczności itp.), oddziałując na nie poprzez wykorzystanie różnic biologicznych, w tym genetycznych. Jako podstawę skuteczności jej działania zakłada się istnienie struktur genetycznych, na które można celowo wpływać za pomocą specjalnych substancji chemicznych lub biologicznych.

Uzyskanie założonych efektów jest teoretycznie możliwe. Dotychczas nie zostały jednoznacznie określone różnice genetyczne, które stanowiłyby bazę do zbudowania broni etnicznej. W perspektywie krótko- i średnioterminowej nie należy oczekiwać zagrożenia ze strony takiej broni.

Jednak z chwilą pojawienia się jej powstanie nowa kategoria broni masowego rażenia o szczególnych własnościach i zastosowaniu.

### **3.1.10 Środki walki wpływające na środowisko naturalne**

Walka w obrębie środowiska naturalnego może być prowadzona z wykorzystaniem konwencjonalnych i niekonwencjonalnych środków walki. Działania te można podzielić na trzy główne kategorie:

- wyzwalenie, manipulacja i nadużywanie zjawisk naturalnych (poprzez wykorzystywanie ich energii, składu, masy lub potencjałów biologicznych);
- długotrwała zmiana środowiska naturalnego w celu uzyskania określonych efektów negatywnych w kategoriach wojskowych (np. zmiana krajobrazu, biegu rzek oraz cieków wodnych, wycinanie lasów itp.);
- działania bojowe, terrorystyczne czy typu partyzanckiego mające na celu uzyskanie krótkotrwałego efektu ważnego dla celów wojskowych, powodujące bezpośrednie szkody w środowisku naturalnym

(np. wysadzanie rurociągów, zapór rzecznych, skażenia gleby i wody).

Niektóre ze wskazanych możliwości będą wymagały wykorzystania energii jądrowej, z uwagi na wielkość energii potrzebnej do zainicjowania i przeprowadzenia określonych procesów lub zakłócenia naturalnej równowagi środowiska.

Działania w zakresie zmian środowiskowych, które nie wymagają tak znacznego zaangażowania energetycznego, mogą być prowadzone z mniejszą intensywnością i jako szczególnie trudne do rozpoznania, pozostać niewykryte nawet przez długi czas. Co więcej, efekty tego rodzaju zagrożeń mogą być przypisywane czynnikom „niewojskowym” (obiektywnym), zmniejszając w oczywisty sposób ryzyko działań odwetowych.

### **3.1.11 Broń geofizyczna**

Broń geofizyczna ma służyć przede wszystkim zakłócaniu warunków geofizycznych środowiska. Zalicza się do niej środki do wywierania długoterminowego wpływu na klimat, powodowania zaburzeń warstwy ozonowej oraz sztucznego wywoływania trzęsień ziemi i fal wodnych zwanych Tsunami.

Zastosowanie takich działań w skali lokalnej jest wątpliwe. Niebezpieczeństwo sztucznego wywoływania trzęsień ziemi i Tsunami jest (na obecnym etapie) uzależnione od posiadania broni jądrowej, co w warunkach konieczności ukierunkowanego jej działania jest bardzo trudne do wykonania.

### **3.1.12 Cybernetyczny wymiar pola walki**

Wszystkie formy działań asymetrycznych łączy wspólna „przestrzeń cybernetyczna”, która może być traktowana jako piąty wymiar pola walki (c), istniejący obok trójwymiarowej przestrzeni kartezjańskiej (x,y,z) i wymiaru cza-

sowego (t). Wewnątrz tej przestrzeni rozgrywają się losy walki informacyjnej i operacji informacyjnych, które są główną składową działań asymetrycznych. Dynamika kształtowania przestrzeni cybernetycznej, specyficzne środki oddziaływania na tą przestrzeń i powszechna dostępność do jej podstawowych składowych stwarza warunki do wprowadzenia zaburzeń w jej funkcjonowaniu, niewspółmiernych w skutkach z zastosowanymi środkami i prowadzących do poważnych konsekwencji w wymiarze bezpieczeństwa wojskowego, ekonomicznego i politycznego zaatakowanego państwa. **Zrozumienie wpływu wymiaru cybernetycznego na efektywność wszystkich form działań asymetrycznych ma znaczenie kluczowe dla oceny istoty rzeczywistych zagrożeń asymetrycznych.**

Według raportu Transforming Defense<sup>46</sup> – „światowa infrastruktura informacyjna (czyli realna infrastruktura wymiaru cybernetycznego), to aspekt strefy konfliktu obejmujący pełny zakres zjawisk elektromagnetycznych i pozaludzki wymiar rozpoznania (wykrywania celów), w którym siły zamaskowane technicznie (stealth) – trudne do wykrycia środkami technicznymi – prowadzą operacje zaczepne lub ukrywają się przed takimi operacjami.” Oznacza to, że światowa infrastruktura informacyjna to faktycznie realna infrastruktura wymiaru cybernetycznego.

Zaakceptowanie piątego – cybernetycznego wymiaru pola walki – jest więc odejściem od jego liniowej koncepcji, w której każdy uczestnik ma określone miejsce w trójwymiarowej przestrzeni (x,y,z) i czasie (t). Pozwala też przewyciężyć obecne ograniczenia, wynikające bezpośrednio z natury jego czterowymiarowości, takie jak:

- fizyczna odległość i położenie w przestrzeni;

<sup>46</sup> Opracowanie amerykańskiego forum doradczego - National Defense Panel, powołanego w ramach opracowywania Czteroletniego Przeglądu Obrony 1997 roku.

- czas ( $t$ ) konieczny do przebycia odległości między dwoma wojskowymi obiektami;
- fizyczna struktura i wymiary ( $x,y,z$ ) obiektów wojskowych.

### ***Zmiana odległości i położenia obiektów w przestrzeni***

Obecnie na polu walki obiekt o współrzędnych  $(x_1, y_1, z_1)$  znajduje się w mierzalnej odległości od innego obiektu o współrzędnych  $(x_2, y_2, z_2)$ . Odległość między tymi obiektami i ich wzajemne położenie w przestrzeni ma kluczowe znaczenie wojskowe. Relacje tego typu określają w terminologii wojskowej takie pojęcia jak front, skrzydło, tyły, linia styczności, itp. Wymiar cybernetyczny zniekształca te relacje poprzez ***powiększanie*** i ***zmniejszanie*** istniejącej przestrzeni.

**Proces powiększania przestrzeni** oznacza, że dwa obiekty wojskowe leżące blisko siebie stają się bardzo odległe. Trudno wykrywalne samoloty (stealth) mogły np. swobodnie latać w nocy nad Bagdadem ponieważ dla nieświadomych tego osób samoloty te nie istniały. Gdyby były widzialne z pewnością zostałyby wówczas ostrzelane. Podobne procesy można zaobserwować w odniesieniu do terrorystów. Policjanci czy żołnierze nie mogą wiedzieć, że w niewielkiej odległości od nich (np. kilku metrów) stoi terrorysta ponieważ działa on skrycie (stealth) i niczym nie wyróżnia się z otoczenia. Dla nich obu terrorysta taki nie istnieje lub jest bardzo odległy.

**Proces zmniejszania przestrzeni** powoduje z kolei sprowadzenie do bezpośredniej bliskości odległych od siebie fizycznie obiektów. Zastosowanie do celów wojskowych Internetu, telemedycyny oraz audycji medialnych prowadzonych w czasie rzeczywistym, to powszechnie znane przykłady procesu zmniejszania przestrzeni. Osoby odległe o tysiące kilometrów mogą spotkać się wirtualnie na polu walki w celu wsparcia funkcjonowania struktur wojskowych

(analiza celów, sposobów ich niszczenia, konsultacje eksperckie, itp.), albo jako obiekt ataku psychologicznego realizowanego za pośrednictwem mediów.

### *Wpływanie na czas konieczny do przebycia odległości między obiektami*

Jeśli jeden obiekt znajduje się w miejscu  $M_1 (x_1, y_1, z_1)$ , a drugi w miejscu  $M_2 (x_2, y_2, z_2)$  to możemy powiedzieć, że istnieje między nimi przestrzeń czasowa (czasoprzestrzeń). W przypadku wystrzelonego pocisku będzie to ściśle związane z czasem lotu pocisku do celu. Wymiar cybernetyczny pola walki może spowodować **kompresję przestrzeni czasowej** albo nawet **eliminację czasu**. Broń DEW wykorzystująca ukierunkowaną energię (np. działło laserowe) eliminuje takie pojęcie jak „czas lotu do celu” we wszystkich jej zastosowaniach praktycznych. „Wystrzał” i „trafienie” są w tym przypadku prawie jednoczesne. Znika również możliwość stosowania zabezpieczeń polegających na ostrzeganiu przed atakiem ponieważ, żaden ze znanych systemów obronnych i ochronnych nie działa z porównywalną prędkością<sup>47</sup>.

### *Fizyczna struktura i wymiary obiektów wojskowych*

We współczesnym świecie mechanicznym obronne konstrukcje wojskowe<sup>48</sup> chronią żołnierzy bezpośrednio (fizycznie) i dopiero zniszczenie tych konstrukcji pozwala wyeliminować z walki siłę żywą. Postmechaniczna istota wymiaru cybernetycznego pozwala przewyciężyć ograniczenia wnoszone przez taką właśnie – fizyczną strukturę celu. Ograniczenia te można przewyciężyć stosując podczas ataku np. energię elektromagnetyczną, zamiast energii kinetycznej lub chemicznej. Wiadomo, że fale milimetrowe dużej mocy HPM przenikają przez struktury fizyczne celów i mogą obezwładnić lub porazić załogę

<sup>47</sup> Z prędkością światła  $c$  – ok. 300 000 km/s.

<sup>48</sup> Np. ściany umocnień polowych chronią żołnierzy obsług karabinów maszynowych, a pancerze czołgów ich załogi przed uderzeniami pocisków przeciwpancernych.

czołgu czy transportera opancerzonego. Podobnie broń neutronowa – pozwala wyeliminować z walki załogi czołgów i transporterów bez fizycznego niszczenia samych wozów bojowych.

Omówione możliwości pokonywania ograniczeń czterowymiarowego pola walki w przypadku uwzględnienia wymiaru cybernetycznego wskazują wyraźnie, iż przestrzeń cybernetyczna wnosi nowe możliwości bojowe zarówno w przypadku prowadzenia walki konwencjonalnej jak i walki asymetrycznej.

Asymetryczność jakościowa realizowana w technice wojskowej i koncepcji „niewidzialności” (stealth) za pomocą procedur i technik przewyżających środki rozpoznania i wykrywania, pozwoliła wojsku realnie wkroczyć do przestrzeni cybernetycznej. Określa się to terminami – „manewr w przestrzeni cybernetycznej” lub „manewr cybernetyczny”. Manewr taki pozwala wyjść poza czterowymiarową przestrzeń, doświadczaną powszechnie przez człowieka i bezpiecznie skryć się w piątym wymiarze (cybernetycznym).

**Dostęp do cybernetycznych narzędzi manipulowania czasem i przestrzenią** w omówionym uprzednio znaczeniu **jest z natury rzeczy dostępem do asymetrycznych środków walki**. Dostęp ten jest oczywiście zróżnicowany z uwagi na nierównomierność dokonań w zakresie rozwoju techniki. Technika maskowania samolotów (stealth) uniemożliwiająca ich wykrycie środkami technicznymi, czyli pozwalająca na ich ukrycie w wymiarze cybernetycznym, dysponują obecnie tylko nieliczne państwa. Trwają także prace nad maskowaniem technicznym (stealth) pocisków raketowych, okrętów oraz czołgów i innych opancerzonych wozów bojowych.

Jedną z najprostszych, a obecnie szczególnie ważnych, form maskowania technicznego (stealth) jest podszywanie się terrorystów pod spokojnych obywateli i ich umiejętność „wtapiania” się w otoczenie. Taka forma maskowania jest dostępna dla wszystkich stron, zarówno dla terrorystów i kryminalistów, jak i dla żołnierzy działań specjalnych.

Nowym źródłem zagrożeń w sferze działań asymetrycznych z wykorzystaniem narzędzi walki informacyjnej może być przemysł działający w warunkach globalizacji. Przekazanie przez amerykańskie siły lądowe ochrony systemów komputerowych w 400 instalacjach wojskowych cywilnej firmie Internet Security Systems, Inc. świadczy o tym, że sektor prywatny może być lepiej przygotowany niż tradycyjne struktury wojskowe do prowadzenia wojny w nowym wymiarze pola walki. Jest to złowieszczy trend ponieważ działania w przestrzeni cybernetycznej mogą wpłynąć na podważenie monopolu państwa na dysponowanie potencjałem wojennym, podobnie jak już obecnie czynią to duże monopole międzynarodowe, które czasami podważają suwerenność państwową w wymiarze gospodarczym i politycznym.

Skryty atak informacyjny w niesprzyjających warunkach jest zdolny spowodować masowe zakłócenia w funkcjonowaniu społeczności cywilnej. Przeciwnik może mieć „prywatnych sojuszników” rozlokowanych w państwach NATO, w tym w Polsce, jak również poza granicami państw sojuszu, którzy przy bezpośredniej pomocy „sponsora” (lub bez) są zdolni do prowadzenia operacji w przestrzeni cybernetycznej. Atak informacyjny o skutkach zwracających uwagę opinii publicznej i mediów spowoduje prawdopodobnie odwrócenie uwagi czynników rządzących i spowolnienie procesów decyzyjnych, co w przypadku równoczesnego wystąpienia np. zamachów terrorystycznych może doprowadzić do mnożenia się niepotrzebnych ofiar.

Internet stworzył nowe możliwości kompresji czasu i szybkiej transmisji dużych zbiorów informacji, co jest powszechnie wykorzystywane zarówno przez struktury siłowe państw rozwiniętych jak i przez organizacje terrorystyczne czy kryminalne.

Z wymiarem cybernetycznym pola walki wiążą się także inne formy działań ofensywnych i defensywnych, z których najważniejsze dotyczą koncepcji **atakowania powiązań** oraz **tarczy cybernetycznej**.

### *Atakowanie powiązań*

Koncepcja atakowania powiązań pozwala w swojej istocie na uniknięcie masowych zniszczeń fizycznych towarzyszących prowadzonym dotychczas operacjom wojskowym. Zgodnie z nią atakuje się nie same obiekty (formacje), ale istniejące pomiędzy tymi obiektami powiązania. Taki sposób ataku odnosi się do wszystkich formacji od poziomu mikro do makro – od cząsteczek atomowych do państw i ich koalicji, łącznie z otoczeniem w jakim one występują. Efektem końcowym ma być zmiana charakteru powiązań wewnątrz obiektu ataku, pomiędzy obiektami lub między obiektem i jego środowiskiem. Naruszenie tych powiązań powstaje w wyniku degradacji, odcięcia lub pomieszania (splątania) powiązań i więziami, które określają istnienie obiektu ataku.

Atak na powiązania na poziomie mikro może oddziaływać na substancje nieorganiczne występujące np. w metalowych i ceramicznych pancerzach, czy w oponach samolotów i pojazdów lądowych. W odniesieniu do opancerzonych wozów bojowych atak na powiązania może nie tylko osłabić pancerz, ale również uniemożliwić pracę silnika w wyniku wprowadzenia do komory spalania (wraz z powietrzem) odpowiednich środków blokujących zapłon mieszanki paliwowo-powietrznej. Inną formą takiego ataku jest pokrycie szybko twardniejącą substancją wszystkich otworów obserwacyjnych i celowniczych pojazdu opancerzonego, co zrywa wizualny kontakt załogi pojazdu z otoczeniem. Impuls elektromagnetyczny EMP (Electromagnetic Pulse) może spowodować uszkodzenie elektronicznego wyposażenia pojazdu bojowego, w tym pokładowego komputera kierowania ogniem i radiostacji, co jest również postrzegane jako atak na powiązania.

Atak na powiązania wewnątrz struktur wojskowych i państwowych wymaga manipulowania polem elektromagnetycznym w pełnym jego zakresie oraz informacjami w Internecie, a także odcięcia lub przeładowania informa-

cjami kluczowych węzłów i sieci, co może doprowadzić do kaskadowego załamania systemowego. Grupy społeczne i polityczne funkcjonujące w formie struktur państwowych lub zabiegające o uznanie ich państwowości, mogą istnieć tylko dzięki więziom utrzymującym je w spójności. W tradycyjnych państwach podstawą takiej spójności są m.in. wielostronne powiązania i więzi między rządem, ludnością i strukturami wojskowymi (siłowymi). Atak na te powiązania osłabia państwo i wcześniej lub później prowadzi do klęski całej grupy społecznej.

Pod pojęciem ataku na powiązania mieści się również atak na środowisko, modyfikacja pogody i użycie środków biologicznych powodujących katastrofalną redukcję zbiorów rolnych czy produkcji mleczarskiej. Odmianą takiego ataku jest np. zakłócenie pracy systemów wspomagających funkcjonowanie tego typu struktur w wyniku wygenerowania silnego impulsu EMP.

Obecnie wielu teoretyków wojskowych wskazuje, że w związku z niską efektywnością bojową wojsk operacyjnych użytych do prowadzenia walk w terenie zurbanizowanym (miejskim) należy rozwinąć koncepcję ataku na powiązania do takiego poziomu, by można było pogrążyć miasto w całkowitym chaosie bez konieczności wprowadzania tam wojsk. **Ekstrapolacja tej metody na wyższy poziom oznacza podjęcie takich działań, by prowadząc atak na wroga państwo, miasto czy społeczność wyłącznie w przestrzeni cybernetycznej doprowadzić je do stanu rzeczywistego chaosu wewnętrznego.**

Operacje informacyjne oraz specyfika piątego wymiaru pola walki umożliwiają organizacjom i ugrupowaniom pozapaństwowym (terrorystom, kryminalistom, partyzantom, zbuntowanym ugrupowaniom o celach religijnych, etnicznych i politycznych) oraz wojowniczym państwom o niskim potencjale wojskowym i politycznym prowadzenie zmasowanych działań asymetrycznych o charakterze terrorystycznym. W tym kontekście operacje informacyjne mogą być traktowane jako **broń masowego zrywania powiązań.**

Zgodnie z analizami przeprowadzonymi w National Defence University implikacje walki informacyjnej są wielowymiarowe. Po pierwsze terytoria poszczególnych państw stały się informacyjnie przezroczyste tzn. przestały być sanktuariami i zamkniętymi enklawami. Mogą być one atakowane bezpośrednio, często anonimowo, przez obce państwo lub organizacje pozapaństwowe jak również przez zbuntowane korporacje, czy indywidualnych fanatyków. Tradycyjne środki walki nie stanowią już bariery ilościowej w generowaniu zagrożeń asymetrycznych, ponieważ decydującym kryterium stał się czynnik jakościowy, z dominującym i przenikającym wszystkie inne formy walki, udziałem walki informacyjnej.

Po drugie, nawet w przypadku zaistnienia tradycyjnych form walki (gdzie wrogi siły wojskowe prowadzą walkę w określonym terenie, w przestrzeni powietrznej lub akwenie wodnym) broń o działaniu kinetycznym może stanowić tylko część arsenału dostępnego dla oponentów. Elektroniczne rozpoznanie i sabotaż, ataki psychologiczne wykonywane przy użyciu środków masowego przekazu, cyfrowe metody mylenia przeciwnika i ataki hakerów na systemy dowodzenia, będą również stosowane dla zneutralizowania działań tradycyjnych sił zbrojnych przeciwnika. Działania w wymiarze cybernetycznym (tylko w odniesieniu do państw najbardziej zaawansowanych technologicznie) umożliwią przy tym efektywniejszą koncentrację ognia i sił w odpowiednim momencie i miejscu na polu walki.

Formami i narzędziami nowego stylu prowadzenia walki mogą być:

- „zapadnie” ukryte w kodzie kontrolującym protokoły komunikacyjne łącznic sieci telefonicznych, powodujące ich blokadę na zdalnie wydaną komendę;
- przeciążenia, przekraczające wydolność lokalnego systemu telekomunikacyjnego w wyniku zmasowanej realizacji połączeń abonentów i ich komputerów osobistych;

- „bomby logiczne”, wprowadzane do systemów sterowania, sygnalizacji i kontroli (np. w przypadku komputerowych systemów sterowania zwrotnicami i sygnalizatorami kolejowymi, może prowadzić do katastrof i utraty zaufania maszynistów do kolejowych systemów sygnalizacji);
- zdalne wprowadzenie przez hakerów zmian do formuł i procesów technologicznych dotyczących produkcji lekarstw u producenta farmaceutyków lub informacji dotyczących pacjentów (np. grupy krwi) w medycznej bazie danych;
- skoncentrowane ataki „wirusami komputerowymi” za pośrednictwem poczty elektronicznej<sup>49</sup>, mogące powodować przeciążenie (przekroczenie wydolności) kluczowych sieci informatycznych lub ich całkowity paraliż;
- „blokady informacyjne” powodujące, że z danego państwa nie wypłynie oraz nie wpłynie do niego żadna informacja w formie elektronicznej.

Z ogólnego punktu widzenia, takie formy walki można uznać za wymierzone w powiązania między obiektami. Nie są więc one precyzyjnymi uderzeniami fizycznymi wymierzonymi w konkretne obiekty, często powodującymi ogromne zniszczenia i liczne ofiary w ludziach. Pożądanym przez stronę atakującą efektem końcowym tych działań będzie ściśle ograniczone naruszenie więzi wewnątrz obiektów, między obiektami lub między obiektami i środowiskiem ich funkcjonowania, które warunkują istnienie omawianych obiektów.

Atak na powiązania może być prowadzony na wszystkich poziomach od taktycznego do strategicznego. Może on mieć charakter bezpośredni lub refleksyjny, a Polska była w przeszłości wielokrotnie obiektem strategicznych ataków

---

<sup>49</sup> Np. w maju 2000 r. wprowadzenie za pośrednictwem poczty elektronicznej wirusa „I LOVE YOU” a następnie wirusa „MELISA”, który spowodował uszkodzenie ponad miliona komputerów (kosztem ok. 80 mln USD).

tego typu. Istnieje też bardzo wiele linii manipulacji i możliwych punktów oparcia dla ataku na powiązania w wymiarze strategicznym. Różnica między obecnymi i historycznymi przykładami polega przede wszystkim na technicznych możliwościach skrócenia cyklu od pomysłu do realizacji, na zwiększeniu zasięgu ataków do skali globalnej oraz wzroście natężenia oddziaływania kampanii psychologiczno-propagandowej, w tym z użyciem środków audio-wizualnych dostarczających na bieżąco selektywnie dobranych lub odpowiednio zniekształconych danych uwiarygodniających tezę, na której oparto linię ataku. Strona atakowana dowiaduje się o ataku najczęściej wtedy, kiedy został on już wykonany. Dzieje się tak zazwyczaj dlatego, że środowiska odpowiedzialne za wczesne ostrzeżenie o tego rodzaju atakach unikają niestety, ze względu na poprawność polityczną, wskazywania źródeł i prawdopodobnych celów takiego ataku asymetrycznego.

Zarówno obecnie, jak i kiedyś w historii, realizacja strategicznych ataków na powiązania wymaga (wymagała) znaczących nakładów finansowych. Dotyczy to również nakładów na złożone systemy wczesnego ostrzeżenia o możliwości ich wystąpienia oraz przewidywanych kierunkach.

### *Tarcza cybernetyczna*

Pojęcie tarczy cybernetycznej (cybershielding) zostało wprowadzone do słownictwa wojskowego w połowie lat 90. Oznacza ono zdolność do przezwyciężenia uderzenia broni precyzyjnego rażenia w wyniku utworzenia niewidzialnej tarczy wokół wojsk, które utraciły możliwość maskowania technicznego (*stealth*). Tarcza taka może spowodować przedwczesną detonację środka ogniowego precyzyjnego rażenia przy użyciu np. impulsu elektromagnetycznego lub stworzenie „półstałej” bariery fizycznej, bazującej np. na „nieletalnych” środkach obezwładniających NLW.

Tracza cybernetyczna musi w pierwszej kolejności chronić przed atakiem w wymiarze międzynarodowym oraz wewnątrzpaństwowym. Natomiast na najniższym poziomie powinna również chronić pojedynczych żołnierzy oraz wozy bojowe i samoloty przed bronią opartą m.in. na technice fal radiowych RFW i mikrofal HPM.

W zakres pojęcia tarczy cybernetycznej wchodzi na szczeblu taktycznym:

- kryptograficzne metody ochrony informacji, regulacji zewnętrznego dostępu do systemu oraz oznaczania wewnętrznych zmian danych w systemie;
- filtry pozwalające na przekazywanie między urządzeniami tylko limitowanej liczby informacji;
- media archiwizujące informacje, w taki sposób, by nie można ich było wymazać oraz chroniące informacje przed wirusami;
- izolacja galwaniczna części systemów (tzw. luka powietrzna);
- „ściany ogniowe” (firewall);
- wykrywacze anomalii;
- programy antywirusowe.

Tarcza cybernetyczna może również przyjąć formę niematerialnej bariery skierowanej przeciwko broni precyzyjnego rażenia. Ten rodzaj tarczy przykrywa całość sił operujących w określonym rejonie. Tarczę taką tworzy m.in. aparatura *Shortstop*, generująca barierę elektromagnetyczną, powodującą np. przedwczesny wybuch pocisku w wyniku przesłania fałszywego sygnału do zapalnika. Generatory (emitery) fal radiowych RFW i mikrofal dużej mocy HPM mogą tworzyć podobne bariery, powodujące przepalenie układów elektronicznych atakujących pocisków lub przedwczesną detonację. Bariery takie mogą być

również stosowane przeciwko atakującym samolotom i śmigłowcom.

Istnieją również inne, specjalne rodzaje tarczy cybernetycznej. Specyficzną jej formą jest m.in. *walka radioelektroniczna*, która z jednej strony chroni własne środki uderzeniowe (np. grupę samolotów bojowych lub okrętów) przed wykryciem i zniszczeniem, z drugiej – pozwala paraliżować działalność systemów dowodzenia, łączności i rozpoznania przeciwnika, w wyniku stosowania grupowych aktywnych i pasywnych środków zakłócających. Szczególnie użyteczne jest zakłócanie radiowych urządzeń nawigacyjnych, w tym satelitarnych systemów nawigacji. Efektywne działanie na tym polu gwałtownie zmniejsza skuteczność bojową samolotów i całych rodzin nowoczesnej amunicji klasy powietrze-ziemia. Zakłócanie systemów nawigacyjnych przynosi korzyści we wszystkich rodzajach działań bojowych.

*Indywidualne środki ochrony radio- i optoelektronicznej* samolotów, okrętów i wozów bojowych sił lądowych to inna znana forma tarczy cybernetycznej.

Kolejną jest *kurtyna akustyczna*, która może być stawiana pomiędzy formacjami chroniącymi obiekty rządowe i atakującym tłumem. Efekt oddziaływania biofizycznego takiej kurtyny jest różnicowany od lekkich objawów, polegających na zaburzeniach słuchowych i wzrokowych, dezorientacji, braku koncentracji i dysfunkcjach fizjologicznych, po ostrzejsze symptomy związane z nadpobudliwością, zanikami pamięci, zmianami osobowości, ostrymi bólami i utratą świadomości.

*Hologramy* mogą również tworzyć tarcze cybernetyczną, która wywołuje iluzję murów, blokad drogowych i przeszkód terenowych lub maskuje np. rozrzucone gwoździe czy inne środki do przebijania opon. Kurtyny akustyczne i wykonane z hologramów znajdują się jeszcze w fazie badań.

Już obecnie, możliwe jest natomiast tworzenie *bariery optycznej* o głębokości do 500 m przy użyciu ręcznego laserowego urządzenia oślepiającego<sup>50</sup>. Bariera taka może wywoływać dezorientację znajdujących się w jej zasięgu osób i częściowo je zatrzymywać.

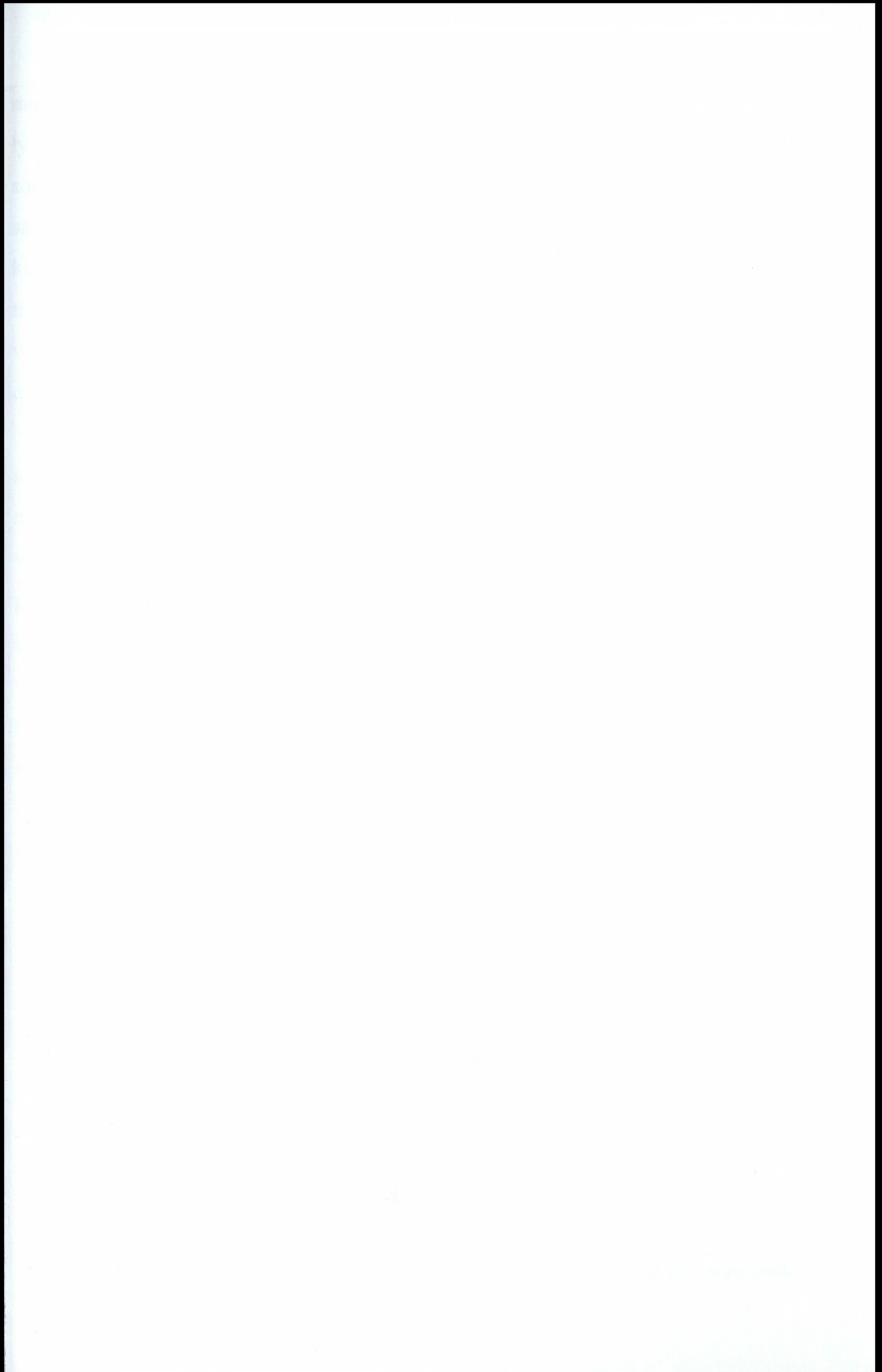
Wstępna ocena możliwości technicznych i organizacyjnych wskazuje, że tarcza cybernetyczna szczebla taktycznego i operacyjnego będzie z większym powodzeniem wykorzystywana przez państwa rozwinięte. Dzięki niej państwa tej grupy mogą okresowo zyskiwać przewagę nad potencjalnym przeciwnikiem wywodzącym się z grupy państw słabiej rozwiniętych. Nie musi to być regułą i państwa te (w tym z NATO) powinny się liczyć z możliwością czasowej utraty przewagi w tej dziedzinie, czasem wręcz nieproporcjonalną do środków znajdujących się w dyspozycji przeciwnika. Nie zawsze będą również skuteczne strategiczne ataki na ich infrastrukturę, szczególnie w odniesieniu do konfrontacji pomiędzy państwami należącymi do różnych cywilizacji lub subkultur, ponieważ ich charakter może sam w sobie stanowić tarczę cybernetyczną przeciwko atakowi obliczonemu na rozpad danej struktury organizacyjnej czy państwowej.

### 3.2. Kategorie zagrożeń asymetrycznych według literatury amerykańskiej

W Stanach Zjednoczonych Niektórzy analitycy amerykańscy określając asymetrię ujmują ją przede wszystkim w kategoriach wizji. Na przykład Lloyd J. Matthews<sup>51</sup> przedstawia wizję strategiczną, definiując asymetrię jako każdą, znacząco wojskowo różnicę obu rywalizujących stron. Stanowi to bezpośrednie nawiązanie do definicji zamieszczonej w słowniku Webstera, jako że w leksykonie amerykańskim określenie jest wyjaśniane przy zastosowaniu pojęcia „niewspółmierność”, czyli związek między rzeczami, nie mającymi wspólnej

---

<sup>50</sup> W urządzenie, pracujące na bezpiecznej dla wzroku fali o długości 532 nm, jest wbudowany układ inicjujący efekt stroboskopowy oraz programowany regulator mocy do wzmocnienia wywoływanego efektu dezorientacji.



miary<sup>52</sup>. Analityk amerykański twierdzi, że „proces kalkulacji wyniku oddziaływania różnych wektorów sił pochodzących ze strony dwóch, powiązanych ze sobą asymetrycznie przeciwników – w celu zmierzenia wymiaru zagrożeń jakie są wzajemnie powodowane – może być problematyczny. Jest to jednak proces, który należy podjąć, jeśli mamy nadać właściwą rangę wszystkim istotnym elementom siły<sup>53</sup>”. L. Matthews dodaje, że w analizowanym kontekście ważne jest występowanie zdolności do powodowania zagrożeń, niezawodność systemów oraz oddziaływania na słabe strony.

Kolejną wizjonerską definicję przedstawiają **Steven Metz i Doulas Johnson** z Szkoły Wojennej Sił lądowych USA, twierdząc, że asymetria „jest działaniem, organizacją i myśleniem *innym* niż przeciwnika w celu maksymalizacji własnych korzyści odniesienia zwycięstwa, uwypuklenia słabości przeciwnika, przejęcia inicjatywy, lub osiągnięcia większej swobody działania. Może być polityczno – strategiczna, wojskowo – strategiczna, operacyjna, lub kombinacją ww. Może angażować różne metody, technologie, wartości, organizację, perspektywę czasową, lub wiele kombinacji ww. Może być krótko terminowa lub długo terminowa. Może być stosowana poprzez *rozważanie* lub *brak*. Może być dyskretna lub występować w połączeniu z podejściem symetrycznym. Może obejmować rozmiar psychologiczny i psychiczny”<sup>54</sup>

Kolejny Amerykanin, emerytowany gen. brygady David L. Grange twierdzi, że jest najlepiej rozumiana jako strategia, taktyka lub metoda prowadzenia walki lub konfliktu, podkreślając, że stratedzy definiują walkę asymetryczną jako konflikt będący pośrednią konsekwencją nierównowagi sił<sup>55</sup>. Najciekawsze spojrzenie na kategorie zagrożeń asymetrycznych zostało zawarte w opracowaniu Kennetha F. McKenzie Jr. „Zagrożenia asymetryczne, a przyszły

<sup>51</sup> Matthews L.J. Wstęp do „Wyzywając USA symetrycznie i asymetrycznie: Czy USA można pokonać?”, Strategic Studies Institute, July 1998, s. 20

<sup>52</sup> Webster's Third New International Dictionary of English Language, Springfield 1981, s. 136

<sup>53</sup> Tamże, s. 20

<sup>54</sup> Metz S. i Johnson D.V. „Asymetria a strategia wojskowa USA”, USAWC, SSI, January 2001, s.5-6

<sup>55</sup> Grange D.L. „Walka asymetryczna. Stara metoda, nowe troski”, ROA National Security Report, March 2001,

Czteroletni Przegląd Obrony”. W rozdziale 2, dotyczącym typologii asymetrii, znalazły się rozważania na takie tematy jak:

- skala potencjalnych zagrożeń asymetrycznych;
- broń jądrowa (wykorzystanie taktyczne, operacyjne i strategiczne) oraz wnioski jej dotyczące;
- broń chemiczna (wykorzystanie taktyczne, operacyjne i strategiczne) oraz wnioski jej dotyczące;
- broń biologiczna (wykorzystanie taktyczne, operacyjne i strategiczne) oraz wnioski jej dotyczące;
- operacje informacyjne (wykorzystanie taktyczne, operacyjne i strategiczne) oraz wykorzystanie impulsu elektromagnetycznego dużej wysokości (High- altitude electromagnetic pulse - HEMP);
- inne koncepcje operacyjne (wykorzystanie taktyczne, operacyjne i strategiczne);
- terroryzm.

Spis treści (w języku polskim) stanowi załącznik 1 niniejszego opracowania. W załączniku 2 przedstawiono natomiast wykładnię asymetrii oraz ataków asymetrycznych zamieszczone w regulaminie polowym armii amerykańskiej FM -03 Operations. Załącznik 3 stanowi robocze tłumaczenie raportu specjalnego Instytutu Studiów Strategicznych SL USA (ISS), z września 2001 roku, na temat: „Wojny wewnętrzne – ponowne przemyślenie problemu oraz reakcje” - autor Max G. Manwaring.

### **3.3. Kategorie asymetryczne według literatury brytyjskiej**

Według specjalistów Wielkiej Brytanii globalizacja, liberalizacja życia w byłych państwach autorytarnych, rosnąca prywatyzacja, a przede wszystkim rewolucja w technice komputerowej, telekomunikacji i sposobach przekazywa-

nia danych (nazywane też jako rewolucja informacyjna; Information Revolution – IR) wywarły duży wpływ na środowisko bezpieczeństwa międzynarodowego oraz na naturę zagrożeń współczesnego świata<sup>56</sup>. Te czynniki zrewolucjonizowały proces przekazywania danych - społeczeństwa stały się bardziej otwarte, natomiast wiedza oraz informacja są przekazywane na drugi koniec świata jedynie za przysłowiowym „kliknięciem myszki”. Jedną z konsekwencji takiej sytuacji było pojawienie się terminu zagrożeń asymetrycznych. Specjaliści brytyjscy oceniają, że te zagrożenia zaczynają dominować od 1990 roku, przyjmując postać nie - tradycyjną, czyli odbiegającą od modelu silnie uzbrojonych stron, znajdujących się naprzeciwko siebie. Rysujące się nowe sytuacje, choć nie stanowią dla świata zachodniego zagrożenia wojną konwencjonalną, to jednak przedstawiają sobą porównywalne, a nieraz nawet większe zagrożenie dla ludności i rządów tych państw.

Specjaliści brytyjscy oceniają, że w nowym środowisku bezpieczeństwa, świat oczekuje rosnąca liczba konfliktów o małej intensywności (Low Intensity Conflicts - LIC). Obejmuje to zwłaszcza aktorów zdolnych do dysponowania BMR, nie wyłączając grup ekstremistycznych. Konsekwencją tego stanu może być znaczący wzrost liczby ataków terrorystycznych, choć przede wszystkim o wymiarze lokalnym. W podejściach, jakie może być przyjęte przez aktora asymetrycznego, wyróżnia się trzy kategorie. **Pierwsza** wiąże się z dostępem do BMR, względnie balistycznych raketowych pocisków kierowanych lub pocisków manewrujących. Potencjalni przeciwnicy regionalni mogą stworzyć dla sił NATO poważne zagrożenie, na przykład w ramach eskalacji napięcia. Nawet bez fizycznego użycia tej broni, samo nią dysponowanie może wpływać na poziom bezpieczeństwa, warunkując ewentualnie działania wojskowe. Broń masowego rażenia może być również wykorzystana jako skuteczny środek do obezwładniania systemów dowodzenia i łączności – poprzez wykorzystywanie

---

<sup>56</sup> K. O'Brien, J. Nusbaum, *Intelligence gathering asymmetric threats*, Jane's Intelligence Review 2000.

impulsu elektromagnetycznego<sup>57</sup>. **Druga kategoria** wynika z dostępu do środków walki cybernetycznej oraz możliwości zakupu na wolnym rynku najnowocześniejszych technologii informacyjnych, telekomunikacyjnych oraz niektórych typów uzbrojenia i sprzętu wojskowego. Sytuacja ta może być określana jako „strategia wykorzystywania niszy rynkowej” (strategy of the niche player), w ramach której narzędzia walki cybernetycznej mogą być wykorzystane na przykład do zrywania wojskowych i cywilnych systemów telekomunikacyjnych, a nawet paraliżować gospodarkę i infrastrukturę państw NATO. W ramach **trzeciej kategorii** wyróżnia się środowisko walki, na przykład tereny zurbanizowane lub dżungle, niewygodne dla sił konwencjonalnych, znacznie obniżające zdolności sił zbrojnych Sojuszu do lokalizacji oraz niszczenia i obezwładniania celów ważnych z wojskowego punktu widzenia. Wymienione kategorie, skróto nazywane jako BMR, operacje informacyjne (Information Operations – IO) oraz operacje niekonwencjonalne (Non-Conventional Operations – NCO), choć występowały już w tej czy też innej formie w przeszłości, to dopiero w latach 90-tych ubiegłego stulecia nabrały znaczenia. Mniej skomplikowane technicznie uzbrojenie, w warunkach walki asymetrycznej może okazać się bardzo skuteczne, na przykład na szczeblu taktycznym. Mogą to być również tak proste sposoby działania jak stosowanie „żywych tarcz”, generatorów ciepła do mylenia czujników pracujących w paśmie podczerwieni, ograniczenie pracy środków łączności, stosowanie makiet sprzętu itp.

Jak oceniają specjaliści brytyjscy, jest ironią losu, że państwa rozwinięte gospodarczo, w tym wchodzące w skład NATO, „ułatwiają pracę” aktorom walki niesymetrycznej ze względu na coraz większe uzależnianie się od informacji przekazywanych Internetem. W większości przypadków, państwa NATO polegają w bardzo dużym stopniu na tzw. krytycznej narodowej infrastrukturze informacyjnej (National Critical Information Infrastructure – NCII), tworzonej

---

<sup>57</sup> W literaturze brytyjskiej stosowane jest określenie broń masowego przerywania połączeń (Weapon of Mass Disruption)

przez serwery organizacji rządowych i korporacji, sieć telekomunikacyjną i usługodawców (providers) internetowych. Wszystkie te elementy stanowią gotowe obiekty ataku asymetrycznego. Dlatego najpilniejszego rozpatrzenia wymaga kwestia podjęcia skoordynowanych działań prewencyjnych i opracowanie procedur postępowania w sytuacjach ataków cybernetycznych.

### 3.4. Zagrożenia asymetryczne według literatury niemieckiej

Zakończenie zimnej wojny nie oznaczało, wbrew dość powszechnym oczekiwaniom, zaniku zagrożeń. Zmienił się jedynie ich charakter. Obok scenariuszy wymagających „klasycznych” działań sił zbrojnych, pojawiają się subkonwencjonalne „asymetryczne” formy konfliktów. Dynamiczne procesy transformacyjne powodują z jednej strony rozwój struktur kooperacyjno-integracyjnych w kluczowych regionach świata, z drugiej zaś struktur konfrontacyjnych. Procesy te przyczyniają się nie tylko do rozwoju i powstawania nowych regionów rozwiniętej gospodarki i demokratycznych struktur, lecz także do powstawania potencjalnych konstelacji kryzysogennych. To właśnie ta dynamiczna zmiana struktur, z powodu asymetrycznego przebiegu procesów rozwoju – między różnicowaniem a integracją – obejmuje cały katalog niepewności. Spektrum poglądów obejmuje przy tym optymistyczne prognozy, przepowiadające światową falę demokratyzacji połączoną z nowymi formami globalizacji gospodarczej i politycznej, oraz poważne ostrzeżenia przed nowym konfliktem światowym między kręgami kulturowymi i cywilizacjami<sup>58</sup>.

Podstawowy punkt wyjścia analizy konstelacji kryzysowych i konfliktowych w 21 wieku stanowi dla specjalistów niemieckich dość powszechnie zim-

---

<sup>58</sup> H.F. Seller, *Konfliktkonstellationen im internationalen System*, Österreichische Militärische Zeitschrift 1999, nr 5. s. 547.

na wojna<sup>59</sup>. Miała ona według nich swe źródła w upadku eurocentrycznego „koncertu mocarstw” w rezultacie dwóch wojen światowych i na ponad czterdzieści lat zdominowała procesy polityczne, które z kolei określają ogólne ramy obecnym strukturom. Istotną właściwością struktur bezpieczeństwa w okresie konfrontacji Wschód-Zachód była relatywna przewidywalność politycznych działań jednej i reakcji drugiej strony, która pomimo, a może właśnie dzięki ogromnym potencjałom zniszczenia obu stron – zawsze była przewidywalna. Dwubiegunowa struktura bezpieczeństwa przez kilkadziesiąt lat wytworzyła wzajemnie respektowany obszar bezpieczeństwa obejmujący unikanie, a co najmniej kontrolowanie konfliktów w ramach własnego systemu sojuszy. Ponieważ każdy kryzys prowadzić mógł do niekontrolowanej eskalacji militarnej, wymuszał więc niejako dyscyplinowanie własnej hemisfery geostrategicznej. Potwierdzać to mają powtarzające się w latach 1948-1961 kryzysy berlińskie, wojna koreańska 1950-1953, ale także kryzys węgierski w 1956 r., kryzys kubański 1962, kryzys w Czechosłowacji w 1968 oraz kryzys w Afganistanie w 1979 roku<sup>60</sup>. Niemniej jednak, zwłaszcza w miejscach styku bloków, istniały konstelacje i zarzewia konfliktów, które wprawdzie, dzięki obustronnemu samoograniczeniu i wspólnej woli stabilizacji, były regulowane, nie zostały jednak rozwiązane. Te ogniska konfliktów istnieją także obecnie i według poglądów niemieckich, stanowią punkty wyjścia dla nowych kryzysów i konfliktów<sup>61</sup>.

Koniec uwarunkowanego ideologicznie dwubiegunowego antagonizmu zmienił wprawdzie charakter konfliktów regionalnych, ale ich nie usunął. Do istniejących zagrożeń dołączyły nowe wyzwania, które poprzez swą nieprzewidywalność przyczyniają się do destabilizacji, zwłaszcza peryferii regionów geostrategicznych. Konstelacje kryzysogenne przyszłości wydają się nieporównywalne z dotychczasowymi. Niestabilność polityczna w połączeniu z fanatyzmem

<sup>59</sup> Por. m.in.: M. Hoch, *Krieg und Politik im 21. Jahrhundert* [w:] *Workshop Krieg im 21. Jahrhundert*, Clausewitz-Protokolle 2001, nr 1 oraz H.F. Seller, *Konfliktkonstellationen ...*

<sup>60</sup> H.F. Seller, *Konfliktkonstellationen...*, s. 547.

<sup>61</sup> Tamże, s. 548.

i fundamentalizmem, działalnością terrorystyczną, napięciami społecznymi i etnicznymi, prowadzącymi często do rozpadu struktur władzy państwowej i regionalnej w powiązaniu z czystkami etnicznymi, niesie z sobą ogromne ryzyko dla bezpieczeństwa regionalnego i globalnego.

W niemieckiej literaturze przedmiotu zwraca się uwagę na szereg problemów, jakie musi rozwiązać państwo i siły zbrojne wobec wyzwań związanych z zagrożeniami asymetrycznymi. Nowy terroryzm łączy bowiem wojnę partyzancką z gotowością do ofiary z własnego życia oraz wirtualnymi sieciami, aby pogrążyć struktury państwowe<sup>62</sup>. Terrorysty chcą zadawać ciosy, którym nie można zapobiec klasycznymi, wojskowymi, zgodnymi z prawem środkami i sposobami. Dla podkreślenia jak bardzo cel niepaństwowego aktora w wojnie asymetrycznej może odbiegać od schematu myślenia w kategoriach racjonalności celów, przytacza się obserwację Henry Kissingera poczynioną podczas wojny w Wietnamie: „*Guerilla wygrywa, jeśli nie przegrywa. Regularna armia przegrywa, jeśli nie wygrywa*”<sup>63</sup>. Tak więc przeciwnik w konflikcie asymetrycznym już tylko dzięki samej długotrwałości konfliktu może zyskać potwierdzenie głoszonych celów, legitymizację i uznanie na arenie międzynarodowej, i to w zasadzie niezależnie od własnych sukcesów militarnych. Można to zobrazować chociażby na przykładzie konfliktu izraelsko-palestyńskiego i wzrostu znaczenia Organizacji Wyzwolenia Palestyny. Intensyfikacja konfliktu w celu pokonania niepaństwowego przeciwnika – co w wojnie między państwami byłoby preferowanym sposobem działania – w warunkach konfliktu asymetrycznego okazać się może wręcz zabójcza. Może to mieć miejsce zwłaszcza wówczas, gdy straty ponoszone przez aktora państwowego stanowią większy problem niż dla niepaństwowego przeciwnika.

W tym kontekście zwraca uwagę fakt, iż ze współczesnym konfliktem asymetrycznym związana jest konieczność redefinicji samego pojęcia państwa.

---

<sup>62</sup> G. Palm, *Kapituliert der Staat?*, <http://www.heise.de/tp/deutsch/inhalt/co/11013/1.html>

Jeżeli wcześniej możliwe było oddziaływanie bronią dalekiego zasięgu głęboko poza klasyczną linię frontu, to obecnie – wraz ze swobodnie przemieszczającymi się po całym świecie wojownikami i ruchliwością w cyberprzestrzeni, bezsensowne stają się granice państw. Te „straty” terytorialne oznaczają jednocześnie uszczerbek definicji państwa. Takie straty obserwuje się obecnie we wszystkich miejscach tej wojny bez frontów. Zarówno w Afganistanie, jak i w samych Stanach Zjednoczonych. Przywódca Ameryki permanentnie mówi o długotrwałej lub nawet ciągłej kampanii przeciwko złym siłom tego świata, w tym o celu wojny, którego w rzeczywistości nie można ograniczyć ani czasowo, ani przestrzennie. Według poglądów specjalistów niemieckich jest to bardzo niebezpieczna opcja. Jeżeli bowiem państwu nie uda się w realnej perspektywie czasowej zapewnić bezpieczeństwa swoim obywatelom, zwłaszcza wewnątrz kraju, to społeczeństwo utracić może zdolność oporu. W konflikcie asymetrycznym państwo bezwzględnie powinno osiągnąć szybkie zwycięstwo nad niepaństwowymi aktorami, jeżeli nie chce być narażone na ciągle nowe uderzenia, utracić swej wiarygodności, a tym samym narazić swej egzystencji<sup>64</sup>.

W opracowaniach niemieckich podkreśla się, że państwo – mimo przewagi środków militarnych – musi pokonać zasadniczo większe trudności, aby odnosić sukcesy w asymetrycznych konfliktach z niepaństwowymi aktorami. Podstawowy dylemat małej wojny stanowi w tym kontekście fakt, iż w konflikcie asymetrycznym to właśnie państwo znajduje się w niedogodnej sytuacji. Brak reguł i wyraźnego rozgraniczenia wojny od pokoju rodzi sprzeczności z politycznymi i etycznymi podstawami funkcjonowania państwa, a tym samym zagraża porządkowi społecznemu. Natomiast przeciwnik niepaństwowy z faktu niestosowania reguł osiąga wyłącznie korzyści, przede wszystkim dużą swobodę działania. Świadomość społeczeństw zachodnich narzuca siłom zbrojnym ograniczenia, które nie dotyczą przeciwnika w konflikcie asymetrycznym, odnoszą

---

<sup>63</sup> Cyt. za: M. Hoch, *Krieg und Politik ...*, s. 8.

<sup>64</sup> G. Palm, *Kapituliert der Staat ...*

się one zwłaszcza do rozróżniania kombatantów i ludności cywilnej. Jeżeli podczas wojny asymetrycznej aktor państwowy naruszy własne reguły, to fakt ten może być łatwo wykorzystany zarówno przez przeciwnika, jak i wewnętrzną opozycję polityczną<sup>65</sup>.

W tym kontekście zwraca się uwagę na kolejne zagrożenie dla aktora państwowego. Otóż także regularne siły zbrojne, działając w konflikcie asymetrycznym przeciwko siłom nieregularnym, wykazują tendencję do przejmowania sposobów walki przeciwnika. Kto zbyt długo walczy z terrorystami, być może w końcu sam stanie się terrorystą. Dla potwierdzenia tej tezy przywołuje się chociażby działania sił specjalnych, takich jak Navy Seals, których wyszkolenie niewiele odbiega od wyszkolenia terrorystów, i które prawdopodobnie tak walczą<sup>66</sup>. Dowodzi to jak trudne jest wspomniane wcześniej zróżnicowanie między tak odmiennymi przecież uczestnikami konfliktu. Przyznaje się, że z wojskowego punktu widzenia stosowanie takich metod może być niezbędne, jeżeli w ogóle ma być mowa o jakichkolwiek sukcesach, znacznie jednak podważa państwową legitymizację w odniesieniu do kontrolowanego sprawowania władzy i użycia siły.

Konflikty asymetryczne prowadzone są często w trudnym terenie, w obszarach zurbanizowanych, leśnych czy trudno dostępnych regionach górskich, w których stosunkowo ciężkie i zaawansowane technologicznie środki rozpoznania i walki regularnych sił zbrojnych tylko w ograniczonym stopniu mogą skutecznie działać. Postęp technologiczny i praktycznie nieograniczone możliwości wykorzystania technologii komunikacyjnych i informatycznych działają na korzyść niepaństwowych aktorów. Coraz mniejsze grupy dysponują coraz większymi możliwościami oddziaływania. Właśnie na korzyść takich przeciwników działa fakt, iż mogą oni przy pomocy prostych i tanich środków uzyskać spektakularne rezultaty, pozostają przy tym trudni do wykrycia i nie mają łatwej

---

<sup>65</sup> M. Hoch, *Krieg und Politik ...*, s. 10.

do zidentyfikowania bazy, w której można by było ich zaatakować<sup>67</sup>. Nie można ich w łatwy sposób wyodrębnić z otaczającej ich ludności cywilnej. Inteligentne uzbrojenie czy chirurgiczne ciosy nie sprawdzają się w wojnie asymetrycznej. Ich zastosowanie uzależnione jest od „rozsądnych przeciwników” gotowych określić się jako żołnierze i w rezultacie pozwalających się zniszczyć<sup>68</sup>.

Inny aspekt tego problemu to tzw. straty uboczne. Pojawia się tu sprzeczność między dążeniem do ograniczenia strat własnych i unikania szkód ubocznych. Im mniej własnych strat dzięki zastosowaniu np. bombowców strategicznych, tym więcej szkód ubocznych po stronie przeciwnika. Było to bardzo widoczne podczas wojny z Talibami<sup>69</sup>. Wirtualny świat mediów podsyca ponadto spór o rzeczywiste straty i skutki uboczne, a tym samym i o wojnę. W ten sposób wojna asymetryczna przekształca się w wojnę wirtualną, która dla postronnego obserwatora może już nie mieć nic wspólnego z rzeczywistością.

Z zasadniczo politycznej natury wojny wynika, że jest ona zjawiskiem społecznym i w społeczeństwie medialnym taką też pozostanie. Równoległe do działań wojennych toczyć się więc będą, zarówno wewnątrz społeczeństw prowadzących wojnę, jak i na arenie międzynarodowej, ostre spory o praworządność, celowość i adekwatność środków i działań podejmowanych w akcjach militarnych. Tak więc polityka w dalszym ciągu wywierać będzie bezpośredni wpływ na przebieg działań militarnych, czy to przez nakaz minimalizowania szkód ubocznych oraz strat własnych, czy też przez długotrwałość politycznych procesów decyzyjnych, lub też przez konieczność tworzenia koalicji w ramach NATO bądź UE i na arenie międzynarodowej oraz uczestnictwo w operacjach militarnych z przyczyn sojuszniczych lub gestów politycznych, mimo że nie zostały naruszone żywotne interesy narodowe. Inne polityczne czynniki, które przyczyniać się mogą do ograniczenia efektywności działań militarnych, to żą-

<sup>66</sup> G. Palm, *Kapituliert der Staat ...*

<sup>67</sup> M. Hoch, *Krieg und Politik ...*, s. 4.

<sup>68</sup> G. Palm, *Kapituliert der Staat ...*

<sup>69</sup> A. Stahel, *Null-Verluste Strategie und virtueller Krieg*, Österreichische Militärische Zeitschrift 2002, nr 3.

danie szybkiego uzyskania znaczących rezultatów czy też ograniczona liczba lub specyficzny skład zaangażowanych sił.

Ograniczenie się wyłącznie do środków militarnych tylko w nielicznych sytuacjach powoduje bezpośrednie rozwiązanie problemu. Nasuwa się zatem pytanie czy działania militarne mogą być uzasadnione z powodów etycznych lub pragmatycznych, jeżeli ich skutki nie prowadzą do istotnej i trwałej zmiany sytuacji politycznej. Z tym właśnie punktem odniesienia będą się musiały mierzyć decyzje o ewentualnym użyciu środków wojskowych jako instrumentu polityki<sup>70</sup>. Prymat polityki zawarty w clausewitzowskim postrzeganiu wojny jako kontynuacji polityki nie oznacza bowiem tylko podporządkowania działań militarnych celom politycznym, lecz także szczególną odpowiedzialność za użycie sił zbrojnych i ich polityczne wykorzystanie. Bez dyplomatycznego wykorzystania sukcesów militarnych oraz wynikającej stąd zasadniczej i akceptowanej przez drugą stronę zmiany politycznej – działania militarne jako środek polityki 21 wieku nie będą ani sensowne, ani też odpowiedzialne<sup>71</sup>.

Wyzwania związane z konfliktami asymetrycznymi wymagają od sił zbrojnych 21 wieku zasadniczego rozszerzenia możliwości. Odpowiedzią na asymetryczne zagrożenia jest pozyskanie określonych zdolności. Przeciwnik w konflikcie asymetrycznym to nie tylko desperat wyposażony w karabinek automatyczny, lecz także intelektualista wykorzystujący najnowsze zdobycze technologiczne i najskuteczniejsze metody. Również dlatego, że ma wystarczająco dużo środków, aby sobie na to pozwolić. Tak więc przy pomocy sił zbrojnych i koncepcji działania wywodzących się z dwudziestego wieku, nie będzie można rozwiązywać przyszłych konfliktów<sup>72</sup>.

---

<sup>70</sup> M. Hoch, *Krieg und Politik ...*, s. 13.

<sup>71</sup> Tamże, s. 14.

<sup>72</sup> H.F. Sellar, *Konfliktkonstellationen ...*, s. 552.

## 4. DZIAŁANIA ASYMETRYCZNE W PRZESTRZENI REALNEJ I CYBERPRZESTRZENI

### 4.1. Sposoby działań asymetrycznych w wybranych środowiskach

Obecnie działania asymetryczne mogą wystąpić we wszystkich wymiarach *przestrzeni realnej* (obszary lądowe, morskie i przestrzeń powietrzna nad nimi) oraz w cyberprzestrzeni, tworzonej przez wszystkie działające w czasie rzeczywistym (i współdziałające ze sobą) systemy rozpoznania i łączności z obszaru *przestrzeni realnej* oraz ich holograficzne odwzorowania, na bazie których można tworzyć modele symulacyjne wspomagające procesy decyzyjne m.in. w dowodzeniu i kierowaniu (w sytuacjach kryzysowych, podczas klęsk żywiołowych itp.).<sup>73</sup> Założyć można, że obecnie i w przewidywalnej przyszłości jednym z podstawowych instrumentów działań asymetrycznych będzie terroryzm.

#### 4.1.1. Działania asymetryczne w przestrzeni realnej

Rozwinięte państwo demokratyczne jest szczególnie atrakcyjnym środowiskiem działania terrorystów. Składa się na to szereg przyczyn o zróżnicowanym charakterze. Jedną z istotniejszych jest demokratyczny porządek wewnętrzny znacznej części z nich. Przedstawicielski system rządów stwarza bowiem przesłanki umożliwiające wymuszenie określonych zachowań rządów poprzez oddziaływanie terrorystyczne na przypadkowych obywateli (zastraszanie, wywołanie poczucia powszechnego zagrożenia). Zagrożone (rzeczywiście lub jedynie potencjalnie) zbiorowości mogą, w określonych przypadkach, domagać się za pośrednictwem swoich reprezentantów w organach ustawodawczych, podjęcia kroków ukierunkowanych na eliminację stwarzanej przez terrorystów groźby.

---

<sup>73</sup> Por. Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 25.

W warunkach niepowodzenia akcji siłowych zmierzających do fizycznej eliminacji sprawców lub pozbawienia ich warunków do działania naciski te mogą wymusić spełnienie (bezpośrednie lub co bardziej prawdopodobne pośrednie) żądań strony prowadzącej działania metodami terrorystycznymi. Podkreślić przy tym należy, że to właśnie osoby przypadkowe (*cywile, tłum*) stanowią ponad połowę ofiar wszystkich aktów terrorystycznych przeprowadzonych w ostatnich latach. Polaryzacja nastrojów społecznych spowodowana aktami przemocy może wymusić spełnienie żądań sprawców zwłaszcza wtedy, gdy cele organizatorów kampanii przemocy nie kolidują w sposób oczywisty z celami zaatakowanego społeczeństwa, lub kiedy społeczeństwo nie rozumie i nie identyfikuje się z działaniami rządu, będącymi bezpośrednią przyczyną zainicjowania kampanii terrorystycznej. Organizowanie akcji wymierzonych w osoby przypadkowe, w *tłum*, jest z punktu widzenia sprawców znacznie łatwiejsze i obarczone mniejszym ryzykiem niż atakowanie chronionych obiektów państwowych lub eliminowanie funkcjonariuszy państwowych dysponujących ochroną policyjną.

Demokratyczne państwo, gwarantujące jednostce pewne niezbywalne prawa (prawo do swobodnego przemieszczania się, prawo do wolności osobistej, zakaz pozbawiania wolności bez wyroku sądowego, nakaz udowodnienia winy w przypadku pociągania do odpowiedzialności, itp.) jest bardziej atrakcyjnym *środowiskiem* prowadzenia działalności terrorystycznej niż autorytarne (totalitarne) systemy polityczne. Potencjalni sprawcy mogą praktycznie bez ograniczeń podróżować po kraju, wynajmować lokale, samochody, korzystać z usług bankowych i telekomunikacyjnych, czyli w swoich działaniach wykorzystywać wszystkie zdobycze cywilizacyjne i ustrojowe. Można nawet stwierdzić, parafrazując Ho Chi Minha, który mówił: partyzant by działać skutecznie, musi mieć gdzie *pływać* czyli dysponować poparciem miejscowej ludności, a współczesne rozwinięte państwa demokratyczne są właśnie takim obszarem, gdzie terrorysta może *pływać* ze znacznym stopniem swobody.

Z tych samych względów znacznie trudniej jest w państwach demokratycznych organizować skuteczne działania przeciwterrorystyczne. Wynika stąd, że zdobycze demokracji i demokratyczne procedury obok uczciwych obywateli z pełną bezwzględnością wykorzystują przestępcy. Jest ceną jaką płaci większość za gwarancje swych praw.

Na marginesie zauważyć można, że strategia działania lewackich ugrupowań terrorystycznych w latach siedemdziesiątych, przede wszystkim zachodniemieckiej Frakcji Czerwonej Armii (Rote Arme Fraktion), opierała się o założenie, że państwo podejmując działania obronne zmuszone będzie ograniczyć prawa jednostki. Zaostrzenie obowiązującego porządku prawnego doprowadzić miało do wystąpienia powszechnych objawów niezadowolenia uwięzionych rewolucją i likwidacją *starego porządku*. Pokrewne konstrukcje myślowe prezentują niektórzy skrajni autorzy i działacze, zarówno na prawym jak i na lewym skrzydle sceny politycznej. Twierdzą oni mianowicie, że zagrożenie terrorystyczne jest mitem sztucznie powołanym do życia przez pewne służby państwowe zainteresowane zwiększeniem stopnia kontroli obywateli. Opinie takie świadczą jednak o tym, że znalezienie *złotego środka* między poszanowaniem praw jednostki, a występującą w pewnych sytuacjach koniecznością ich ograniczenia, w imię różnie definiowanego *interesu zbiorowości*, jest problemem bardzo trudnym do rozwiązania w sposób budzący powszechną akceptację. Nadmierna restrykcyjność może bowiem wywołać opór, zaś nadmierna liberalizacja otworzyć drogę do władzy ugrupowaniom niedemokratycznym głoszącym konieczność przywrócenia *prawa i porządku*.

Terrorystom sprzyja też, ściśle związana z demokratycznym systemem prawnym, rola odgrywana w krajach rozwiniętych przez środki masowej komunikacji. Czynniki te należy rozpatrywać w dwóch aspektach. Po pierwsze media relacjonując skutki działań terrorystycznych umożliwiają sprawcom osiągnięcie tak zwanego *efektu teatru*, czyli wciągnięcie w bezpośrednią orbitę oddziaływa-

nia aktu przemocy grupy wielokrotnie liczniejszej niż ta, którą dotknęły jego skutki bezpośrednie. Poprzez przekaz prasowy, radiowy, a przede wszystkim telewizyjny, jednostkowy akt przemocy staje się sprawą publiczną, bez medialnych relacji oddziaływanie aktu przemocy ograniczałoby się jedynie do bezpośrednich ofiar, nie docierałoby do szerszego audytorium - społeczności będącej rzeczywistym obiektem działań terrorystów. Obiektywnie rzecz ujmując, to właśnie media są największym (choć w większości przypadków mimowolnym) sojusznikiem terrorystów, dzięki któremu mogą oni liczyć na wywołanie poczucia psychozy zagrożenia o powszechnym zasięgu.

Po drugie, media nie bez przyczyny określane jako *czwarta władza* wywierać mogą poprzez określony dobór prezentowanego materiału wpływ na działania władzy wykonawczej i przyczyniać się do zaogniania lub wygaszania sytuacji kryzysowej wywołanej działaniami terrorystycznymi (zjawisko, w którym polityk obraca się w sferze faktów medialnych a nie rzeczywistych Amerykanie z dużą dozą złośliwości nazywają *CNN - nizacją świata*). Warty podkreślenia jest fakt, że już obecnie wzajemne interakcje między mediami a społeczeństwem uważane są przez część badaczy za czynnik zachęcający do podejmowania działań metodami terrorystycznymi. Wydaje się więc, że w najbliższych latach znalezienie kompromisu między prawem do informacji a wynikającą z racjonalnych przesłanek koniecznością nakładania w pewnych przypadkach różnych form swoistego *embarga informacyjnego* na określone wydarzenia, stać się może jednym z najpoważniejszych dylematów demokracji. Jest to zatem druga już sprzeczność, przed którą staje demokratyczne państwo zaatakowane *sposobem terrorystycznym*.

Działania terrorystyczne uderzają więc pośrednio w fundament ustrojowy otwartych społeczeństw demokratycznych. Mogą one doprowadzić do bardzo silnej polaryzacji postaw obywateli (wręcz zantagonizowania wielkich grup społecznych) wokół dwóch skrajnych stanowisk, z których jedno zakładać bę-

dzie konieczność utrzymania, nawet w sytuacji kryzysowej, wszystkich praw i wolności obywatelskich, zaś drugie zakładać będzie konieczność ich daleko idącego ograniczenia w imię zwiększenia możliwości obrony przed terroryzmem. Niewykluczone jest wówczas wystąpienie w zaatakowanym państwie głębokiego kryzysu ustrojowego prowadzącego do sparaliżowania jego struktur wykonawczych. Obezwładniony w ten sposób podmiot stosunków międzynarodowych będzie wówczas znacznie bardziej podatny na inne rodzaje presji takie jak nacisk ekonomiczny czy groźba użycia siły zbrojnej.

Prócz czynników ustrojowych działaniom terrorystycznym w rozwiniętych krajach demokratycznych sprzyjają zachodzące w nich procesy społeczne i demograficzne przede wszystkim zaś rozrost miast. Wielkie skupiska ludzkie są przy tym jednocześnie potencjalnym obiektem oddziaływania terrorystów jak i środowiskiem ich działania. W pierwszym wymiarze sprawcom aktów przemocy sprzyja skupienie znacznego procentu populacji w ośrodkach miejskich i uzależnienie poprawnego funkcjonowania aglomeracji (nazywanych niekiedy nie bez przyczyny *megapolis*) od jednostkowych instalacji zasilających infrastrukturę socjalno - bytową (zasilanie w gaz, energię elektryczną, wodę pitną, utylizacja odpadów, itp.). Umożliwia to spowodowanie powszechnego zagrożenia dla wielkich zbiorowości poprzez oddziaływanie na wybrane elementy infrastruktury nie będące obiektami wojskowymi i nie podlegające szczególnej ochronie ze strony służb państwowych. Podobnie jak w przypadku działań wymierzonych w tłum ich organizatorzy i bezpośredni wykonawcy ponoszą stosunkowo niewielkie ryzyko zaś osiągnąć mogą efekty niewspółmiernie duże do poniesionych nakładów. Na podkreślenie zasługuje wielość możliwych do zastosowania czynników oddziaływania, od zamachów bombowych ukierunkowanych na spowodowanie rozległych zniszczeń poczynając a na użyciu środków chemicznych, biologicznych czy nawet broni jądrowej kończąc.

Miasta są przy tym nie tylko obszarami koncentracji ludności ale punk-

tami centralnymi współczesnej, rozwiniętej, cywilizacji przemysłowej. W ich obrębie nastąpiło skupienie produkcji, zasobów finansowych i władzy politycznej. Terrorystyczne uderzenie w wielkie aglomeracje może zatem spowodować skutki niewspółmierne do ilości ludzi bezpośrednio zagrożonych i doprowadzić do paraliżu całych państw. Z punktu widzenia sprawców wielka aglomeracja jest obszarem ułatwiającym planowanie, przygotowywanie i prowadzenie działań terrorystycznych. Nie bez przyczyny członkowie wielu organizacji ekstremistycznych nazywali się *partyzantami miejskimi*.<sup>74</sup> W miastach powszechnym zjawiskiem jest tak zwana *anonimowość tłumu*. Sprawcy aktów przemocy mogą *wtapiać się w tłum* podczas przygotowywania do akcji oraz w trakcie ucieczki z miejsca przestępstwa, wynajmowane mieszkania pełnić mogą rolę lokali konspiracyjnych zaś istniejąca komunalna infrastruktura komunikacyjna ułatwia skryte przemieszczanie się w obrębie aglomeracji.

Podatność rozwiniętych społeczeństw na zagrożenie terrorystyczne wzmagana jest dodatkowo przez wysoki i cały czas wzrastający pułap potrzeb i aspiracji konsumpcyjnych ich obywateli. Wspomniane wcześniej uderzenia w węzłowe punkty infrastruktury bytowej z pewnością utrudni zaspokajanie owych potrzeb, co w krótkim czasie może znaleźć bezpośrednie odzwierciedlenie w naciskach wybieralnych przedstawicieli organów ustawodawczych na władze wykonawcze. Truizmem jest stwierdzenie, że wysoki poziom konsumpcji nie sprzyja godzeniu się na wyrzeczenia, lecz ten element psychologii mas również musi być uwzględniany przy dokonywaniu oceny podatności określonego państwa na presję terrorystyczną.

---

<sup>74</sup> Partyzanci miejscy - terminem tym posłużył się po raz pierwszy Carlos Marighella (1911 – 1969), aktywista brazylijskiej partii komunistycznej, członek jej Komitetu Centralnego i Biura Politycznego, a od 1966 przywódca rozłamowej Acao Libertadora Nacional. W opublikowanym w 1969 roku, tuż przed zastrzeleniem przez policję opublikował on *Mini podręcznik partyzanta miejskiego* będący zbiorem ogólnych zaleceń dla bojówek zbrojnych okraszonych obficie *rewolucyjną* frazeologią. Jako pierwsza aktywne działania terrorystyczne miejsce, zgodnie z wytycznymi zawartymi w *Mini podręczniku*, rozpoczęła w 1969 roku urugwajska lewacka organizacja ekstremistyczna Tupamaros. Jej przywódca Raul Sendic stwierdził wówczas: [...] *dysponujemy teraz trzystoma kilometrami ulic i alei do zorganizowania walk partyzanckich*.

#### 4.1.2. Działania asymetryczne w przestrzeni wirtualnej

Terroryzm *fizyczny* nie wyczerpuje zagrożeń, przed którymi stają państwa najwyżej rozwinięte. Zupełnie nową płaszczyznę działań terrorystycznych otworzyło ich postępujące uzależnienie od elektronicznego przekazu informacji. Trudno obecnie w warunkach polskich ocenić na ile realne jest zagrożenie tak zwanym *infoterroryzmem* (*terroryzmem informatycznym, terroryzmem sieciowym, cyber terroryzmem*) ale w wielu państwach zjawisko to jest dostrzegane. Za symptomatyczną należy uznać opinię Winn Schwartau, konsultanta do spraw komunikacji firmy Inter - Pactu. Stwierdził on, że: „[...] ponad 100 milionów komputerów łączy nas wzajemnie poprzez niesłychanie złożony system układów komunikacyjnych, zarówno naziemnych jak i satelitarnych. [...] rządowe i komercyjne systemy komputerowe są tak słabo dziś chronione, że można je praktycznie uznać za bezbronne. Czeka nas zatem elektroniczne Pearl Harbour”<sup>75</sup>.

Systemy komputerowe mogą być przedmiotem działań terrorystycznych dwojakiego rodzaju. Możliwe jest stosowanie wobec nich *soft kill* - czyli destrukcyjnego oddziaływania na oprogramowanie poprzez specjalne programy niszczyielskie nazywane popularnie wirusami. Nie można też wykluczyć zastosowania *hard kill* ukierunkowanego na fizyczne zniszczenie centrów informacyjnych takich kluczowych punktów jak giełda, bank centralny, itp. Szczególnie skutecznym instrumentem drugiego rodzaju działań może okazać się niejądrowa broń, działająca na zasadzie inicjowania silnego impulsu elektromagnetycznego, uszkadzającego sprzęt i niszczącego systemy informacyjne (w tym duże sieci informatyczne). Wspomniane już *elektroniczne Pearl Harbour* należy więc w tym kontekście rozumieć jako próbę sparaliżowania państwa poprzez fizyczne lub *programowe* oddziaływanie na systemy przekazu danych.

---

<sup>75</sup> Tofler H i A., *Wojna i antywojna*, Warszawa 1997, s. 218.

#### 4.2. Prognoza zagrożeń asymetrycznych w odniesieniu do środowiska morskiego

Wydaje się, że obecnie najgroźniejszą formą działań asymetrycznych na morzu jest terroryzm. Atak na amerykański niszczyciel *Cole*<sup>76</sup> pobierający paliwo w Adenie przeprowadzony 12 września 2000 roku oraz wydarzenia 11 września 2001 roku wymusiły przeprowadzenie ponownego stanu oceny bezpieczeństwa na morzach. Ośrodki analityczne bagatelizujące dotąd obszary morskie szybko doszły do wysoce niepokojących wniosków. Powiązano atak na *Cole'a* z działaniami prowadzonymi na morzu przez separatystów tamilskich oraz akcjami rozmaitych frakcji palestyńskich, ponownie zwrócono uwagę na fakty posługiwania się przez południowoamerykańskie kartele narkotykowe sterowanymi przewodowo pojazdami podwodnymi, powtórnej analizie poddano doniesienia o próbach budowy przez ruchy ekstremistyczne i organizacje kryminalne miniaturowych okrętów podwodnych. Wszystkie te działania doprowadziły do sformułowania nowych, wysoce niepokojących ocen oraz prognoz dotyczących stanu bezpieczeństwa na wodach Oceanu Światowego. Uznano mianowicie, że wobec postępującego zwiększania wysiłków ukierunkowanych na poprawę bezpieczeństwa kluczowych instalacji i obiektów lądowych oraz lotnictwa cywilnego

---

<sup>76</sup> USS „Cole” (DDG 67), niszczyciel typu Arleigh Burke, zbudowany w Ingalls Shipbuilding, położenie stępki 28 lutego 1994, wodowanie 10 lutego 1995, wejście do służby czerwiec 1996; wyporność pełna 8422 tony, długość 153,8 metra, szerokość 20,4 metra zanurzenie kadłuba 6,3 metra, zanurzenie z opuszczonym przetwornikiem stacji hydroakustycznej 9,9 metra; 4 turbiny gazowe GE LM 2500 o mocy 78 330 kW pracujące na dwie śruby, prędkość maksymalna 32 węzły, zasięg przy prędkości 20 węzłów 4400 mil morskich. Uzbrojenie: wertykalna wyrzutnia Mk 41 mod. 0 na dziobie (29 cel) i Mk 41 mod. 2 na rufie (61 cel) dla rakiet przeciwlotniczych Standard SM - 2MR Block 4, raketotorped ASROC i pocisków manewrujących Tomahawk (do odpalania Tomahawków przystosowane jest łącznie 56 cel), 8 rakiet przeciwokrętowych Harpoon, 127 mm armata Mk 45 mod. 2, 2 artyleryjskie zestawy obrony bezpośredniej Vulcan – Phalanx, 2 x III wyrzutnie torped, 2 śmigłowce SH 60 B/F LAMPS III. Wyposażenie elektroniczne obejmuje m. in: okrętowy system walki AEGIS Mk 99 mod 3 ze stacją radiolokacyjną SPY – 1D, stację radiolokacyjną dozoru nawodnego SPS 64, systemy transmisji danych Link 4A, 11, 14, 16, SATCOM SRR – 1, kompleks hydroakustyczny SQQ 89 - (V)6, kompleks walki radioelektronicznej SLQ 32 (V)2 zintegrowany z wyrzutniami termicznych i radiolokacyjnych celów pozornych SRBOC, hydroakustycznym holowanym celem pozornym NIXIE i wyrzutniami celów pozornych Sea Gnat. Załoga 303 (29 oficerów) + 38 dodatkowych koji dla grupy abordażowej, komandosów, itp. Ponieważ *Cole* utracił możliwość ruchu a transoceaniczne holowanie uznano za zbyt niebezpieczne, postanowiono przewieźć go do USA na pokładzie wycarterowanej jednostki do transportu ładunków wielkogabarytowych – tak zwanego ciężarowca. Ostatecznie okręt wprowadzono metodą dokową (ciężarowiec zanurzył pokład ładunkowy) na *Blue Marlin*. Ciężarowiec ze swym nietypowym ładunkiem osiągnął Norfolk w pierwszych dniach grudnia 2000 roku. Remont zakończono w drugim kwartale 2002 roku. Zamknął się kwotą około 100 mln USD.

współczesny i przyszłościowy terroryzm może skupić się na atakowaniu *miękkiego podbrzusza* najbogatszych krajów świata czyli handlu morskiego oraz żeglugi handlowej.

#### 4.2.1. Piraci, a terroryści morsecy

Przez wiele lat wszystkie bezprawne akty przemocy na morzu obejmowano wspólnym terminem *piractwo*. Jednak już w 1961 roku, kiedy to sprawców uprowadzenia portugalskiego statku pasażerskiego nie uznano za piratów i udzielono im azylu politycznego w Brazylii okazało się, że klasyczna definicja *piractwa* nie obejmuje wszystkich bezprawnych aktów przemocy, które mogą być podejmowane na morzu.

Dla potrzeb niniejszego artykułu, upraszczając nieco problem, za czynnik różnicujący *piratów* od *terrorystów morskich* uznać można motyw kierujący sprawcami i ściśle tym związane zagadnienie ich stosunku do problemu zachowania anonimowości (skrytości). Współcześni piraci kierują się żądzą zysku, a w związku z tym starają się unikać rozgłosu medialnego, pozostawiania śladów i świadków. Ich zasadniczym celem jest zdobycie *łupu* (niezależnie czy jest to wyposażenie kabin, odzież i pieniądze marynarzy w przypadku tak zwanego *piractwa łodziowego*, czy też zagarnięcie całego oceanicznego frachtowca wraz z ładunkiem co często czynią azjatyckie *pirackie syndykaty*).<sup>77</sup>

Terroryści przeciwnie, jednym z ich zasadniczych celów było zdobycie zainteresowania mediów (co stwarza możliwość wygłaszania oświadczeń, wydawania odezw i apeli) i wykorzystanie do maksimum tak zwanego *efektu teatru*. Obecnie w kontekście wydarzeń, które rozegrały się 11 września 2001 roku w USA prognozować można, że wspomniany *efekt teatru* osiągną w inny sposób - nie poprzez przetrzymywanie zakładników i długotrwałe negocja-

<sup>77</sup> Na marginesie rozważań o terroryzmie morskim zauważyć należy, że obecnie notuje się istotne zwiększenie ilości aktów *piractwa*. O ile w roku 1991 zgłoszono niewiele ponad 100 pirackich napadów na statki to w roku 2000 miało miejsce 469 takich aktów przemocy. 57 % ataków miało miejsce na wodach przybrzeżnych i archi-

cje lecz drogą wywoływania zdarzeń o następstwach katastrofalnych, związanych z olbrzymią ilością ofiar i trudnymi do oszacowania stratami materialnymi. Tym samym terroryzm, pojmowany zgodnie z XIX wiecznym anarchistycznym paradygmatem jako rodzaj *propagandy przez czyn* przeistoczył się w instrument nowej globalnej wojny domowej posiadającej wszelki cechy *konfliktu asymetrycznego*. Owa przeistoczenie się terroryzmu z instrumentu wywierania presji i przyciągania uwagi w narzędzie totalnej destrukcji odnosi się w całej rozciągłości do potencjalnych działań terrorystycznych prowadzonych na morzu. Oznacza to również zasadnicze rozejście się dróg piractwa i terroryzmu morskiego.

W oparciu o powyższe założenie można ponadto prognozować zaistnienie jednej jeszcze poważnej różnicy między piractwem a terroryzmem morskim. Pierwsze z wymienionych zjawisk zachowa prawdopodobnie nadal charakter procederu ograniczonego terytorialne. Ścisłe powiązanie tego rodzaju przestępczej aktywności z sytuacją w państwach nadbrzeżnych czyni mało prawdopodobnym rozszerzenie granic geograficznych intensywnej działalności piratów. Piractwo jest zatem i prawdopodobnie pozostanie nadal zjawiskiem w znacznym stopniu prognozowalnym zaś ryzyko z nim związane odnosić się będzie do żeglugi po określonych akwenach.

Sprawcy aktów terrorystycznym na morzu w znacznie mniejszym stopniu związani są z realiami państw nadbrzeżnych. Postawić można nawet tezę, iż dysponują oni pełną swobodą wyboru miejsca, czasu, obiektu oddziaływania i sposobu przeprowadzenia akcji. Wszelkie ograniczenia w wymienionych kwestiach wynikają jedynie z możliwości organizacyjnych, zaplecza kadrowego i zasobności finansowej planującej działania terrorystyczne ugrupowań ekstremistycznych. W związku z tym praktycznie niemożliwe jest przeprowadzenie jakichkolwiek prognoz szczegółowych dotyczących rejonów szczególnie narażonych na wystąpienie aktów terroryzmu morskiego. Zagrożenie to ma i w prze-

widywalnej przyszłości będzie miało zasięg globalny a odnosić się będzie w równym samym stopniu do jednostek pływających co do szeroko pojmowanej infrastruktury żeglugi (kanały, oznakowanie nawigacyjne, infrastruktura portowo – przeładunkowa, itp.).

#### **4.2.2 Potencjalne sposoby prowadzenia działań terrorystycznych wymierzonych w handel morski i żeglugę handlową**

Analiza aktów terrorystycznych wymierzonych w żeglugę w ciągu ostatniego półwiecza umożliwia przeprowadzenia typizacji potencjalnych sposobów działania sprawców podobnych aktów przemocy w przyszłości. Za prawdopodobne uznać więc należy:

- zamachy bombowe przeprowadzane w portach lub na morzu przy użyciu materiału wybuchowego dostarczanego na statek wraz z ładunkiem,
- zamachy bombowe przeprowadzane w portach lub na morzu przy użyciu materiału wybuchowego wnoszonego na statek przez członka (członków) organizacji terrorystycznej,
- uprowadzenia statków handlowych przez osoby znajdujące się na ich pokładzie,
- uprowadzenia statków handlowych dokonywane z innych jednostek pływających,
- ostrzał z brzegu statków handlowych manewrujących w rejonach przybrzeżnych lub na śródlądowych torach wodnych,
- ostrzał statków z innych jednostek pływających, głównie szybkich łodzi motorowych,
- działania przy użyciu jednostek wybuchowych, sterowanych zdalnie lub obsadzonych przez samobójców,

- działania pływających jednostek bojowych,
- działania prowadzone przy użyciu broni minowej,
- niszczenie oznakowania nawigacyjnego i systemów technicznych wspomagania nawigacji morskiej.

Działania przy użyciu materiałów wybuchowych dostarczanych na pokład jednostki pływającej wraz z towarami przeznaczonymi do załadunku (frachtem) uznać należy za najprostsze do zorganizowania i przeprowadzenia. Materiał wybuchowy może być umieszczony w dowolnym ładunku (masowym, drobnicy, kontenerze) podczas jego przewozu transportem kolejowym lub samochodowym i wyposażony w zapalnik czasowy powodujący eksplozję po umieszczeniu na statku (w porcie lub już po wyjściu jednostki na morze). Podstawową wadą tego sposobu działania są ograniczone możliwości określenia dokładnego miejsca eksplozji związane z ewentualnością wystąpienia rozmaitych przestojów w czasie transportu oraz trudności związane z oszacowaniem niszczącego wpływu eksplozji na jednostkę pływającą (infrastrukturę portową). Efekt wybuchu może być bowiem spotęgowany lub ograniczony, w zależności od tego, gdzie ostatecznie na statku ulokowano fracht, w którym ukryty został ładunek wybuchowy. Z powyższych względów celem działań prowadzonych powyższym sposobem jest raczej stworzenie poczucia zagrożenia, psychozy strachu, a nie zniszczenie lub uszkodzenia konkretnych, wyselekcjonowanych obiektów.

Zalety omawianego sposobu działania to, z punktu widzenia organizatorów: trudność w identyfikacji sprawcy (sprawców), względna łatwość umieszczenia ładunku we frachcie, niski poziom ponoszonego przez sprawcę (sprawców) ryzyka, bardzo ograniczone możliwości zorganizowania skutecznego przeciwdziałania,<sup>78</sup> możliwość prowadzenia działań bez szczegółowych informacji o

<sup>78</sup> Problem kontroli ładunków w portach morskich często postrzegany jest przez pryzmat kontroli bagażu prowadzonych na lotniskach. Tymczasem chodzi o zupełnie inną skalę zjawiska. Tylko w polskich terminalach promowych (a więc dane te nie odnoszą się do całości obrotów w polskich portach) przeładowano w roku 2000 2 157 914 ton różnorodnych ładunków, 18 671 wagonów kolejowych, 125 095 samochodów ciężarowych, 162

pracy portów, terminach wyjść i wejść statków, przeznaczeniu frachtu itp. Ponadto podkreślić należy, że takim sposobem (idea jego podobna jest do często stosowanego rozsyłania eksplodujących listów) posługiwać się mogą grupy nie-liczne, dysponujące stosunkowo prymitywnym, łatwym do pozyskania, wyposażeniem działające poza obszarem wybrzeża, zarówno w kraju jak i za granicą.

Akcje terrorystyczne (zamachy bombowe) prowadzone przy użyciu materiału wybuchowego wnoszonego na statek przez członka (członków) organizacji terrorystycznej umożliwiają przeprowadzenie ataków na wybrane, starannie wyselekcjonowane cele, a w związku z tym na spotęgowanie efektu eksplozji ładunku wybuchowego poprzez jego właściwe umieszczenie na pokładzie statku oraz, co wydaje się być bardzo ważnym aspektem omawianego zagadnienia, zwiększenie skali zagrożenia wywołanego przez atak, drogą zniszczenia lub uszkodzenia jednostki przewożącej ładunek niebezpieczny. Organizacja tego rodzaju akcji wymaga pozyskania szczegółowych informacji o ruchu statków w wybranym porcie (portach), rodzaju transportowanych przez nie ładunków, systemie ochrony portu, systemie pełnienia wacht portowych na jednostce będącej obiektem ataku, danych o konstrukcji (przede wszystkim rozkładzie pomieszczeń i ciągów komunikacyjnych). Założyć można, że wymagałoby to prowadzenia długotrwałej obserwacji statku i portu, w którym zaplanowano atak lub, co bardziej prawdopodobne, pozyskania osobowych źródeł informacji rekrutujących się z załogi, personelu zatrudnionego na terenie poru oraz w stoczni, która zbudowała wybrany statek. Prócz tego w planowaniu ataku dużą rolę odegrać mogą informacje pozyskane z ogólnie dostępnych źródeł (publikacje prasowe, strony internetowe, materiały reklamowe przedsiębiorstw armatorskich i stoczni, itp.). W odróżnieniu od działań omówionych wcześniej sprawcy tego rodzaju akcji muszą posiadać określoną wiedzę z zakresu budownictwa okrętowego, a

---

716 samochodów osobowych. Granicę morską na pokładach promów przekroczyło 919 389 osób. Por. Bauer P., Żegluga promowa na fali, Gazeta Wyborcza z 26 marca 2002, s. 6. O ile szczegółowe monitorowanie strumienia podróźnych jest wykonalne i już obecnie realizowane, o tyle dokładna – w aspekcie omawianych zagrożeń – kontrola masy towarowej nie jest możliwa bez skokowego wzrostu kosztów transportu morskiego oraz spowodowania daleko idącego paraliżu terminali promowych.

ponadto ponoszą duże ryzyko osobiste, związane z ewentualnością wykrycia na terenie portu, a zwłaszcza na pokładzie statku osób trzecich. Część wymienionych niedogodności wyeliminować można wprowadzając członków organizacji terrorystycznej w skład załogi statku będącego obiektem ataku.

Jednostki pływające są również prawdopodobnymi obiektami uprowadzenia. Za najbardziej prawdopodobne uznać należy tego rodzaju akcje wymierzone w:

- statki pasażerskie (promy pasażerskie i pasażersko - towarowe, wycieczkowce); ich atrakcyjność z punktu widzenia sprawców wynika z możliwości pojmania i efektywnego nadzorowania dużej liczby osób,<sup>79</sup> z zamiarem użycia ich w charakterze zakładników lub zgładzenia, ponadto statek morski (zwłaszcza wycieczkowiec) dysponuje znaczną autonomicznością uniezależniającą sprawców, od ułatwiającego przeprowadzenia odbicia jednostki, zaopatrywania z zewnątrz i wyposażony jest w środki łączności o zasięgu globalnym;
- statki transportujące ładunki niebezpieczne (zbiornikowce, gazowce, chemikaliowce), ich atrakcyjność jako obiektów uprowadzenia wynika z możliwości przejęcia niebezpiecznego ładunku w celu uzyskanie silnej pozycji negocjacyjnej lub zniszczenia jednostki i wywołania w ten sposób katastrofalnych następstw.

Analiza dotychczasowych akcji terrorystycznych ukierunkowanych na zawładnięcie statkami pasażerskimi oraz wymierzonych we frachtowce i jednostki rybackie umożliwia sformułowanie tezy, że sprawcy mogą się przedostać na jednostkę pływającą:

---

<sup>79</sup> W przypadku uprowadzenia włoskiego statku pasażerskiego *Achille Lauro* czterech terrorystów sprawowało pełną kontrolę nad ponad tysiącem pasażerów i członków załogi.

- w porcie, w sposób skryty, z zamiarem rozpoczęcia akcji po wyjściu jednostki w morze,
- w porcie, jawnie i legalnie (z wykupionym biletem), wraz z pasażerami, z zamiarem przeprowadzenia akcji po opuszczeniu portu,<sup>80</sup>
- w porcie, z użyciem przemocy, z zamiarem opanowania jednostki podczas postoju i późniejszego zmuszenia załogi do jej wyprowadzenia na morze,<sup>81</sup>
- podczas postoju na redzie lub kotwiczowisku,<sup>82</sup>
- podczas przejścia morzem, można wyróżnić przy tym dwa sposoby :
  - ◇ skryte przeniknięcie na pokład manewrującej jednostki i rozpoczęcie działań ukierunkowanych na jej opanowanie dopiero po przedostaniu się grupy szturmowej na pokład, umożliwia on uzyskanie pełnego zaskoczenia i uniemożliwia załodze powiadomienie o wydarzeniach zachodzących na pokładzie,<sup>83</sup>
  - ◇ wymuszenie zatrzymania statku ogniem broni maszynowej (artylerii małokalibrowej) prowadzonej z szybkich łodzi motorowej, a następnie obsadzenie jednostki przez grupę abordażową, sposób

<sup>80</sup> W taki sposób terroryści działali podczas – wspomnianego już - uprowadzenia portugalskiego statku pasażerskiego *Santa Maiai* 22 stycznia 1961 roku; włoskiego statku *Achille Lauro* 7 października 1986 roku; próby uprowadzenia greckiej jednostki *City of Poros* 11 czerwca 1988 roku; uprowadzenia tureckiego promu *Avrasya* 13 stycznia 1996 roku. Por. Kubiak K., Terroryzm morski - zagrożenie dla żeglugi, *Morze* 1990 nr 5; Groźba wysadzenia promu, *Rzeczpospolita* z 18 stycznia 1996 roku.

<sup>81</sup> Akcja taka może mieć charakter zaplanowany, w takim przypadku należy się jej spodziewać po zaokrętowaniu / załadowaniu (lub przed wyokrętowaniem / wyładowaniem) większości pasażerów / ładunku lub wymuszony okolicznościami (przykładem akcji wymuszonej jest uprowadzenie promu *Laju* w Singapurze 3 stycznia 1974 roku, kiedy to czterech sprawców rekrutujących się z Ludowego Frontu Wyzwolenia Palestyny i Japońskiej Armii Czerwonej opanowało jednostkę i wzięło pięciu zakładników po przeprowadzeniu zamachu na instalacje Shell Oil Co).

<sup>82</sup> Przykładem takiej akcji terrorystycznej jest wymordowanie w roku 1994 na redzie algierskiego portu Iijel pogrążonej we śnie załogi włoskiego statku handlowego *Lucina* przez fundamentalistów muzułmańskich);

<sup>83</sup> Jest to sposób stosowany przede wszystkim przez współczesnych piratów. Dokumenty IMO (International Maritime Organisation – Międzynarodowa Organizacja Morska) opisują, że w celu skrytego przedostania się nocą na pokład statku znajdującego się w drodze stosowane są przykładowo dwa gumowe pontony (pozbawione odbijaczy kątowych, a przez to praktycznie niewidoczne dla radaru) połączone pływającą na wodzie liną. Umieszcza się je na prawdopodobnym kursie statku. Jednostka zaczepiając o linę ściąga oba pontony do burt. Por. Kubiak K., Piraci czy terroryści, *Komandos* 1996 nr 3.

ten nie daje gwarancji uzyskania pełnego zaskoczenia, zaatakowana jednostka ma możliwość wezwania pomocy.<sup>84</sup>

Rozpatrując zagrożenie statków pasażerskich wprowadzeniem zauważyć należy, że zasadniczym czynnikiem uwzględnianym przez sprawców w czasie wyboru obiektu akcji i jej planowania jest narodowość (obywatelstwo) pasażerów, których zatrzymać można w wyniku opanowania jednostki. Bandera podnoszona przez jednostkę nie ma praktycznie żadnego znaczenia. Zagrożenie promów pasażerskich obsługujących stałe trasy i przewożących w większości pasażerów z kilku (tych samych przez cały czas) krajów zaistnieć może w przypadku wejścia przez taki kraj w konflikt (bezpośredni lub pośredni) z grupami terrorystycznymi lub sponsorującym je państwem. Zagrożenie jednostek wycieczkowych ma charakter zmienny i w głównej mierze zależy od ilości pasażerów określonej narodowości zaokrętowanych w danym rejsie. Zwiększa się ono wraz ze wzrostem liczby obywateli państw znajdujących się aktualnie w stanie konfliktu z organizacją terrorystyczną lub w stanie kryzysu międzynarodowego.

Statek może stać się obiektem akcji terrorystycznej prowadzonej poprzez oddziaływanie ogniowe z brzegu, podczas gdy jednostka manewruje po przybrzeżnym lub śródlądowym torze wodnym, oczekuje na redzie na wejście do portu lub stoi w porcie. Dotychczas w tego rodzaju działaniach (zarówno akcjach terrorystycznych jak i działaniach prowadzonych w czasie konfliktów lokalnych) używane były moździerze, wyrzutnie niekierowanych pocisków rakietowych (zarówno typowe jak i konstruowane doraźnie przez sprawców) oraz granatniki przeciwpancerne i granatniki ręczne różnych typów. Obecnie nie można wykluczyć również użycia przeciwpancernych pocisków kierowanych, granatników automatycznych i wielkokalibrowych karabinów wyborowych.

<sup>84</sup> Opisany sposób działania stosowany jest przez piratów przede wszystkim w rejonach, gdzie intensywność działań jednostek w służbie państwowej (policyjnych i wojskowych) jest niewielka lub tam, gdzie państwa nadbrzeżne nie sprawują efektywnej kontroli nad swoimi obszarami morskimi. Stosowany był on między innymi przez ugrupowania erytrejskie w rejonie cieśniny Bab el - Mandeb.

Konieczność pozyskania wymienionych rodzajów uzbrojenia wraz z amunicją, ich transportu w rejon akcji oraz rozmieszczenia ich na stanowiskach ogniowych poważnie ogranicza możliwość prowadzenia omawianych działań przez organizacje słabe, nie dysponujące poparciem państw lub powiązanych z nimi ugrupowań terrorystycznych.

Przy użyciu moździerzy i wyrzutni niekierowanych pocisków rakietowych atakowane mogą być przede wszystkim jednostki manewrujące ze stosunkowo niewielką prędkością lub nieruchome. Zwłaszcza oddziaływanie na jednostki nieruchome jest stosunkowo atrakcyjnym – z punktu widzenia sprawców – sposobem działania, gdyż w zakładanej sytuacji możliwe jest posłużenie się uzbrojeniem uruchamianym zdalnie, spoza obrębu pozycji ogniowej co wydatnie zmniejsza ryzyko ponoszone przez sprawców, a jednocześnie poważnie utrudnia organizację skutecznego przeciwdziałania.<sup>85</sup> Wadą akcji prowadzonych w omawiany sposób jest względnie mała celność prowadzonego ognia.

Inną specyfikę posiadają akcje terrorystyczne prowadzone przeciwko jednostkom pływającym przy użyciu granatników przeciwpancernych i wielkokalibrowych karabinów wyborowych). Z uwagi na możliwość przewożenia tego rodzaju uzbrojenia możliwe jest jego stosowanie przez lub dwu - trzy osobowe zespoły), wykorzystujące samochody osobowe, a nawet motocykle. O ile więc akcje przeciwko statkom znajdującym się w rejonach przybrzeżnych (na śródlądowych torach wodnych) prowadzone z użyciem moździerzy miałyby prawdopodobnie charakter statyczny i planowy (założyć można, że podobnie prowadzone byłyby działania z użyciem przeciwpancernych pocisków kierowanych) o tyle sprawcy posługujący się granatnikami i wielkokalibrowymi karabinami wyborowymi mogą działać w sposób dynamiczny dysponując równocześnie znacznie większą swobodą wyboru obiektów ataków.

---

<sup>85</sup> Był to typowy sposób działania partyzantów północnowietnamskich podczas ataków na statki handlowe poruszające się śródlądowym torem wodnym łączącym Sajgon z morzem. Por. Schreadley R. L., SEA LORDS, USNI Proceedings 1970 nr 8; Schreadley R. L., The Naval War in Vietnam 1950 - 1970, USNI Proceedings 1971 nr 5.

W okresie powojennym zanotowano kilkadziesiąt przypadków oddziaływania ogniowego na statki z pokładów jednostek pływających, w szczególności szybkich, uzbrojonych łodzi motorowych.<sup>86</sup> Doświadczenia wskazują, że były one używane zarówno jako platformy dla uzbrojenia oraz jako tak zwane łodzie wybuchowe (wypełniane materiałem wybuchowym i kierowane w kierunku celu, w tym również kierowane przez samobójców).

W działaniach bojowych używane były łodzie już od wyporności 1,3 tony uzbrajane w broń maszynową, granatniki, wyrzutnie przeciwpancernych pocisków kierowanych, wyrzutnie niekierowanych pocisków raketowych, a nawet przenośne raketowe zestawy przeciwlotnicze, osiągające prędkość (przy niskim stanie morza) do 40 węzłów. Przyjąć można, że wyporność szybkich łodzi motorowych, które potencjalnie mogą zostać użyte do działań przeciwko polskiej komunikacji morskiej nie będzie przekraczać 20 - 25 ton, napędzane będą one prawdopodobnie silnikami gaźnikowymi o dużej mocy nadającymi im prędkość 35 - 45 węzłów, ich zasięg (bez dodatkowych zbiorników paliwa) nie będzie przekraczał 400 - 500 mil morskich. W większości przypadków pozyskiwanie jednostek przewidzianych do działań przeciwko komunikacji odbywać się będzie poprzez ich zakup na rynku cywilnym, co dodatkowo ułatwi ich maskowanie jako jednostek turystyczno - sportowych).

Parametry instalowanego na szybkich łodziach motorowych uzbrojenia (przede wszystkim skuteczny zasięg przy strzelaniu z mało stabilnej platformy jaką jest łódź) determinować będą w zasadniczy sposób ich taktykę. Skuteczne użycie broni maszynowej, granatników, wyrzutni niekierowanych pocisków raketowych wymaga zbliżenia się do obiektu ataku na odległość nie przekraczającą 300 - 400 metrów, przy czym zmniejszenie tej odległości podnosi celność prowadzonego ognia.

---

<sup>86</sup> <sup>86</sup> W okresie powojennym uzbrojone łodzie motorowe stosowali m.in: antycastrowskie ugrupowania kubańskie, terroryści arabscy prowadzący działania przeciwko żegludze i wybrzeżom Izraela, nikaraguańscy contras zwalczający sandinistów irański morskie formacje nieregularne w czasie wojny iracko - irańskiej, siły chorwackie w czasie jugosłowiańskiej wojny domowej, Tamilowie podczas konfliktu wewnętrznego na Sri Lance.

Przyjąć zatem można, że w przypadku działań przeciwko statkom handlowym prowadzonych z wykorzystaniem szybkich, uzbrojonych łodzi motorowych akcja terrorystyczna sprowadzałaby się do:

- szybkiego, w miarę możliwości skrytego, zbliżenia jednej lub kilku łodzi do obiektu ataku,
- zmasowanego użycia uzbrojenia trwającego kilka do kilkunastu minut (bardziej prawdopodobny jest przy tym ogień do powierzchni tj. nadbudówek i burt z ześrodkowaniem w rejonie górnych kondygnacji nadbudówki niż precyzyjny ogień celowany do konkretnych elementów konstrukcji zaatakowanej jednostki),
- odwrotu.

Uzbrojenie w jakie wyposażane mogą być szybkie łodzie motorowe nie stwarza poważniejszego, bezpośredniego zagrożenia dla pływalności statku handlowego średniej wielkości. Prawdopodobne jest jednak spowodowanie strat w załodze, uszkodzeń poszycia powyżej linii wodnej i ładunku, uszkodzeń nadbudówek, wywołanie pożarów. Podkreślić należy, że zwłaszcza spowodowanie pożaru może w konsekwencji doprowadzić do utraty jednostki.

Szybkie, uzbrojone łodzie motorowe działać mogą w oparciu o:

- bazy (bazę) brzegowe,
- z jednostki bazowe,
- sposobem kombinowanym (działanie z brzegu przy wsparciu jednostki bazowej).

Działanie z bazy brzegowej wymaga najmniej nakładów i jest najprostsze do zorganizowania. Wobec małego zakresu prac jakie przeprowadzić trzeba w związku z przygotowywaniem jednostki do działań (ograniczającego się do demontażu odbijacza kąтового i ewentualnie do zmiany malowania) nie wymaga ono nawet posiadania dyskretnej przystani umożliwiającej ich przeprowa-

dzenie. Zauważyć należy, że łodzie wykorzystywane do działań przeciwko komunikacji z bazy brzegowej będą zazwyczaj zakupione w sposób całkowicie legalny (są one przedmiotem normalnego obrotu handlowego i do ich nabycia nie są wymagane specjalne zezwolenia) i najprawdopodobniej zarejestrowane. Będą one upozorowane na jednostki turystyczno - sportowe, a ich właściciele korzystając prawdopodobnie będą, dla dodatkowego kamuflażu, z istniejącej bazy klubów żeglarskich lub motorowodniackich (przystanie klubowe, mariny, itp.). Wykorzystywanie jednostki uprzednio skradzionej jest mało prawdopodobne gdyż zwiększa ryzyko ujawnienia planowanej akcji w fazie przygotowawczej.

Za wadę omawianego wariantu działania, realizowanego bez wsparcia lub dyskretnego przyzwolenia służb policyjnych państwa, z terytorium którego jest ono prowadzone, uznać należy trudności mogące wstąpić ze skrytym uzbraniem jednostek w miejscu stałego bazowania. Za mało prawdopodobne uznać należy montaż, czy nawet przyjmowanie uzbrojenia na pokład, w ogólnie dostępnej marinie. Prócz ryzyka przypadkowego ujawnienia przygotowań wzmógłoby to zagrożenie ze strony służb policyjnych i granicznych. Można, więc przyjąć, że okrętowanie uzbrojenia na pokład nastąpiłoby po opuszczeniu przez jednostkę przystani i załatwieniu wszystkich wymaganych w danym państwie formalności. Po wyjściu z przystani (mariny) jednostka prawdopodobnie pobierałaby by je z ustalonego wcześniej, ustronnego miejsca na brzegu. Prócz działań z bazy brzegowej szybkie, uzbrojone łodzie motorowe operować mogą z jednostki bazowej. Za prawdopodobne uznać należy zaadaptowanie do roli jednostki bazowej statku handlowego (zwłaszcza drobnicowca samorozładowującego wyposażonego w bomby ładunkowe o dużym unosie i pokrywy ładowni o znacznych wymiarach).<sup>87</sup>

---

<sup>87</sup> W ostatnich dekadach z jednostki bazowej (prawdopodobnie zaadaptowanego frachtowca pod banderą panamską) operowały łodzie motorowe Contras u wybrzeży Nikaragui. Podczas wojny iracko - irańskiej część szybkich łodzi motorowych irańskiej Dywizji Morskiej Korpusu Strażników Rewolucji Islamskiej działała z pokładów okrętów desantowych. Siły morskie Koreańskiej Republiki Ludowo Demokratycznej posiadają prawdopodobnie osiem jednostek upozorowanych na statki handlowe, a przeznaczonych do wypełniania zadań baz pływających miniaturowych okrętów podwodnych i nawodnych środków dywersji (szturmowych).

Zauważyć przy tym należy, że w krajach prowadzących liberalną politykę żegludową zarejestrowanie działalności armatorskiej oraz pozyskanie statku ograniczone jest jedynie możliwościami finansowymi grupy planującej działania terrorystyczne.<sup>88</sup> Przyjąć zatem można, że legalne zdobycie statku z przeznaczeniem na jednostkę bazową szybkich łodzi motorowych znajduje się w zasięgu możliwości grup terrorystycznych. Przy właściwym wyborze statku, który zamierza się wykorzystać jako jednostkę bazową szybkich łodzi motorowych prace adaptacyjne ograniczone mogą być do minimum, możliwego do zrealizowania siłami załogi.

Trzecim wariantem działań szybkich łodzi motorowych jest tak zwany sposób kombinowany. Polega on na połączeniu wysiłku szybkich łodzi motorowych operujących z baz brzegowych i jednostek operujących na morzu pełnym. Prawdopodobny scenariusz akcji przeprowadzonej w tym wariantcie zakłada, że sprawcy działań przeciwko komunikacji dysponują łodzią (łodziami) w państwie nadbrzeżnym. Są one upozorowane na jednostki turystyczno - sportowe i wykorzystywane w zgodzie z miejscowymi przepisami (są one zalegalizowane). Po otrzymaniu sygnału o rozpoczęciu działań przeciwko żegludze jednostki takie wychodziłyby na morze (przestrzegając wszystkich obowiązujących przepisów), a następnie kierowały się w określony punkt, wyznaczony na morzu pełnym, poza zasięgiem brzegowych środków obserwacji i w oddaleniu od uczęszczanych torów wodnych. Tam następowałoby przekazanie uzbrojenia na szybkie łodzie motorowe. Następnie działałyby one w sposób opisany wcześniej. Po przeprowadzeniu akcji uzbrojenie i wszelkie ślady mogące zdemaskować sprawców byłyby usuwane z łodzi.

Szczególnym przypadkiem łodzi uzbrojonej są tak zwane jednostki wybuchowe (wypełnione dużą ilością materiału wybuchowego, eksplodujące po doprowadzeniu w bezpośrednią bliskość celu). Dotychczas (w okresie powojen-

---

<sup>88</sup> Opinię tę potwierdza łatwość z jaką pozyskują statki zorganizowane grupy przestępcze zajmujące się organizowaniem nielegalnej imigracji. Por. Kusovac Z., Stemming the flow of people – smuggling at sea, Jane's Navy

nym) stosowane były jednostki wybuchowe naprowadzane na cel przez sternika, który opuszczał łódź po skierowaniu jej w stronę celu<sup>89</sup> oraz jednostki sterowane przez samobójców.<sup>90</sup> Rozwój i proliferacja zaawansowanej technologii prawdopodobnymi czynią obecnie również ataki łodzi wybuchowych sterowanych zdalnie. Najbardziej prawdopodobnymi obiektami oddziaływanie jednostek samobójczych są obecnie, prócz okrętów wojennych, te same jednostki, które uznano wcześniej za szczególnie narażone na uprowadzenie, czyli statki pasażerskie (promy, wycieczkowce) oraz statki przewożące ładunki niebezpieczne (zbiornikowce, gazowce, chemikaliowce). W pierwszym przypadku akcja samobójczych łodzi wybuchowych spowodowałaby zapewne znaczne ofiary w ludziach, w drugim mogłaby ona zakończyć się spowodowaniem rozległej katastrofy o trudnych do przewidzenia następstwach.<sup>91</sup>

W kilku przypadkach w okresie powojennym miały miejsce działania przeciwko żegludze prowadzone przez płetwonurków bojowych wyszkolonych i wyekwipowanych przez podmioty pozapaństwowe. Organizację akcji tym sposobem ułatwia fakt, że szkolenie płetwonurków, przynajmniej w zakresie podstawowym, jest w większości krajów rozwiniętych elementem szeroko rozumianego segmentu usług rekreacyjnych zaś podstawowy sprzęt znajduje się w normalnym obrocie handlowym. Oczywiście sprawca przeszkolony na kilkudniowym kursie i wyposażony w ekwipunek nabyty w sklepie sportowym prezentuje możliwości bojowe nieporównywalnie niższe od żołnierza formacji specjalnego przeznaczenia sił morskich, ale nadal – szczególnie gdy działa z zaskoczenia – pozostaje niebezpiecznym przeciwnikiem.

---

International vol. 107, no 4, May 2002, p. 18 -20.

<sup>89</sup> Posługując się jednostką tego rodzaju Izraelczycy zatopili 21 października 1948 roku egipski transportowiec *Emir Farouk* i uszkodzili towarzyszący mu trałowiec.

<sup>90</sup> Jednostki obsadzone przez samobójców wykorzystywali rebelianci tamilscy na Sri Lance. Przy ich użyciu zatopiono: okręt patrolowy *Sogarawardene* we wrześniu 1994 roku, okręty patrolowe *Suraya* i *Ranasuru* w kwietniu 1995 roku, okręt dowodzenia, pełniący również rolę jednostki bazowej kutrów patrolowych, *Edithara* w lipcu 1995 roku, kuter patrolowy izraelskiego typu *Dvora* w sierpniu 1995 roku, kuter patrolowy i okręt desantowy w roku 1999, szybki transportowiec w roku 2001. Nadmienić też należy, że ewentualne zmasowane ataki irańskich łodzi wybuchowych obsadzonych przez samobójców budziły poważne obawy dowództwa amerykańskiego w czasie prowadzonych na Zatoce Perskiej działań systematycznych w ochronie zbiornikowców realizowanych w latach 1987 – 1988.

„Płetwonurków – amatorów” mogą zatem wystawić już organizacje stosunkowo słabe i nie dysponujące poważnymi środkami finansowymi. Zaznaczyć jednak należy, że jest to jedyne zagrożenie. Ugrupowania silne i zamożne mogą sobie bowiem pozwolić na organizowania i szkolenia w pełni profesjonalnych zespołów dywersji podwodnej, nawet gdy nie dysponują wsparciem państw (na marginesie zauważyć można, że jako pierwsze grupy płetwonurków bojowych zorganizowali Palestyńczycy przy wsparciu Jugosławii). Przykładem tego są płetwonurkowie bojowi Tamilskich Tygrysów wyposażeni na między innymi w aparaty oddechowe o obiegu zamkniętym (nabyte w Holandii), których nie powstydzilyby się morskie spec formacje wielu państw.

Środkiem walki szczególnie przydatnym do prowadzenia działań terrorystycznych przeciwko żegludze jest broń minowa. Decyduje o tym:

- stosunkowo niskie ryzyko ponoszone przez sprawców w czasie stawiania min,
- względna łatwość pozyskania uzbrojenia minowego wynikająca z jego proliferacji,<sup>92</sup>
- możliwość uaktywnienia uzbrojenia po dłuższym czasie od postawienia co dodatkowo utrudnić może identyfikację stawiacza,
- niemożność udowodnienia powiązań między jednostką manewrującą w określonym rejonie, a faktem postawienia tam min w sposób inny niż przechwycenia stawiacza w czasie stawiania min,
- możliwość stworzenia długotrwałego zagrożenia (długotrwałych perturbacji w ruchu statków) przy użyciu stosunkowo niewielkiej ilości min,

<sup>91</sup> Skalę potencjalnej katastrofy ilustrują następstwa zatonięć lub uszkodzeń zbiornikowców przewożących ropę.

<sup>92</sup> Według Jane's Underwater Weapon System miny morskie produkują: Brazylia, Chile, ChRL, Dania, Hiszpania, Irak, Jugosławia, Korea Północna, Niemcy, Polska, Rosja, Stany Zjednoczone, Szwecja, Republika Chin (Tajwan), Włochy, Wielka Brytania. Tylko w arsenałach byłej marynarki radzieckiej znajdowało (według szacunków amerykańskich) się od 250 000 do 450 000 min morskich rozmaitych typów i przeznaczenia. Por. Kelso F.B II, Building Blocks of Naval Power, USNI Proceedings 1992 nr 11, s. 40. Proliferację uzbrojenia minowego potwierdzają ponadto prawdopodobne posługiwanie się nim przez rebeliantów Tamilskich. Wskazuje na to m. in

- konieczność rozwinięcia przez zaatakowane państwo znacznych sił trałowych w celu likwidacji zagrożenia.

W oparciu o doświadczenia okresu powojennego<sup>93</sup> stosowania broni minowej w działaniach terrorystycznych przeciwko statkom handlowym spodziewać należy się: na redach, kotwicowiskach, torach podejściowych do portów, odcinkach torów wodnych wiodących do (z) portów zaatakowanego państwa. Jej użycie w sposób zagrażający interesom państw trzecich uznać należy za znacznie mniej prawdopodobne.

Za realne uznać należy użycie w charakterze stawiaczy min doraźnie zaadaptowanych jednostek upozorowanych na statki handlowe, turystyczno - sportowe i jednostki rybackie. Podczas użycia broni minowej w działaniach terrorystycznych należy się spodziewać stosowania przede wszystkim min dennych. Wynika to z ich mniejszych - w porównaniu z minami kotwicznymi rozmiarów - ułatwiających ich maskowanie na pokładzie, a nawet upozorowanie na część ładunku; prostszego, w zdecydowanej większości przypadków, końcowego przygotowaniu do postawienia, większej tolerancji na takie czynniki jak prędkość stawiacza i wysokość zrzutu do wody. Użycie niekontaktowych min kotwicznych prawdopodobne jest jedynie wówczas, gdy głębokości w danym rejonie uniemożliwiają stosowanie min dennych zaś zagrożenie komunikacji poprzez postawienie min dennych w innych rejonach jest niemożliwe lub niecelowe. Posłużenie się przez sprawców kotwicznymi minami kontaktowymi jest mało prawdopodobne choć nie można go definitywnie wykluczyć. Liczyć należy się ponadto z wprowadzaniem dużych nastaw na licznikach krotności min lub

---

fakt uszkodzenia przez eksplozję podwodną greckiego statku o nośności 29 423 t na podejściach do Trinkomali. Miało to miejsce 29 maja 1987 roku. Por. Shipping News, BIMCO Weekly News no.26, 4425 June 1997, s. 3.

<sup>93</sup> W okresie powojennym broń minowa wykorzystywana była kilkakrotnie „sposobem terrorystycznym”: w działaniach *contras* przeciwko sandinowskiej Nikaragui, przez organizację UNITA podczas wojny domowej w Angoli (głównie na podejściach do Luandy), przez irańskie formacje nieregularne podczas działań przeciwko żegludze na Zatoce Perskiej podczas wojny iracko – irańskiej, przez libijski siły morskie i służby specjalne na Zatoce Sueskiej w 1984 roku, przez separatystów tamilskich.

ich wyposażania w urządzenia czasowe powodujące uzbrojenie min kilka - kilkanaście dni po opuszczeniu rejonu (portu) przez stawiacz.

Powyższa analiza sposobów działań, które potencjalnie mogą być zastosowane w trakcie ataków terrorystycznych wymierzonych w żeglugę wykazuje, że sprawcy tego rodzaju akcji dysponują szerokim wachlarzem możliwości zbrojnego oddziaływania. Zagrożenie dla statku handlowego mogą stworzyć zatem nie tylko ugrupowania silne, dysponujące poważnymi środkami materialnymi i setkami członków oraz sympatyków (niekiedy wspierane również przez państwa) ale również organizacje słabe, pozbawione szerszego zaplecza kadrowego, finansowego i sprzętowego.

Stosunkowo atrakcyjnym – z punktu widzenia sprawców – sposobem działań wymierzonych w żeglugę może być niszczenie oznakowania nawigacyjnego i innych technicznych środków wspomagających nawigację. Oczywiście zniszczenie bądź uszkodzenie konkretnych urządzeń nie jest w tym przypadku celem samym w sobie lecz środkiem do spowodowania katastrofy morskiej. Z działaniami tego rodzaju liczyć się należy przede wszystkim w rejonach o dużej intensywności ruchu jednostek pływających. Mogą one przybrać form fizycznego ataku na wybrane elementy systemu oznakowania nawigacyjnego bądź ataku przeprowadzonego w urządzenia komputerowe nadzorujące owe systemy.

#### **4.2.3. Przyczyny atrakcyjności akwenów morskich jako obszaru działań terrorystycznych**

O atrakcyjności obszarów morskich z punktu widzenia organizacji i ugrupowań posługujących się terroryzmem decyduje kilka czynników. Pierwszym z nich jest niewątpliwie fakt, że żegluga handlowa i światowy handel morski odgrywają kluczową rolę dla funkcjonowania globalnej gospodarki, a jednocześnie są niesłychanie wrażliwe na rozmaite działania terrorystyczne. Zagrożenie terroryzmem morskim nigdy – o czym już wspomniano – nie było traktowane jako czynnik istotny. W związku z tym o ile państwa względnie dużą uwagę

przywiązywały do ochrony instalacji lądowych oraz lotnictwa cywilnego, o tyle żegluga handlowa traktowana była w tej kwestii prawdziwie po macoszemu. Praktycznie żadne z państw morskich nie dysponuje w tej chwili gotowymi planami i procedurami objęcia swej żeglugi ochroną przed atakami terrorystycznymi. O ile zamierzenia takie mogą być stosunkowo szybko zrealizowane w rejonach przybrzeżnych, o tyle ich wdrożenie na morzu otwartym jest mało prawdopodobne. Podkreślić należy, że poza wojennymi doświadczeniami konwojowymi oraz wnioskami wynikającymi z amerykańskiej ochrony zbiornikowców na Zatoce Perskiej, w latach 1986 – 1988, nie ma żadnych historycznych wzorców, na których oprzeć by można organizację ochrony żeglugi.

Sprawcom potencjalnych działań terrorystycznych przeciwko żegludze handlowej sprzyja również status obszarów morskich. W odniesieniu do akwenów leżących poza wodami terytorialnymi państw nadbrzeżnych obowiązuje zasada „wolności mórz” i „wolności żeglugi”. Żadne państwo nie może rozciągać swojej kontroli na morze otwarte (z wyjątkiem ściśle określonych uprawnień wynikających z istnienia wyłącznych stref ekonomicznych) i ograniczać możliwości uprawiania żeglugi. W odróżnieniu od obszarów lądowych morze otwarte pozostaje zatem poza jurysdykcją jakiegokolwiek państwa zaś uprawnienia władcze w stosunku do jednostek pływających są wyłączną domeną państwa, którego banderę statek podnosi.

Prawo morza (Konwencja o prawie morza z 1982 roku) określa jedynie kilka odstępstw od przedstawionej wyżej generalnej reguły. Pierwszym jest tak zwane *prawo pościgu* upoważniające jednostki (samoloty i inne statki powietrzne) w służbie państwowej do ścigania statku innej bandery, który dopuścił się naruszenia przepisów prawnych obowiązujących na wodach wewnętrznych i morzu terytorialnym.. Pościg musi być jednak rozpoczęty, kiedy obcy statek lub jedna z jego łodzi znajduje się na wodach wewnętrznych lub morzu terytorialnym państwa ścigającego. Prawo pościgu ustaje, gdy ścigany statek wpłynie na

morze terytorialne własnego kraju lub państwa trzeciego. Poza omówionym wyżej przypadkiem, ograniczenie wyłącznej suwerenności państwa bandery (realizacja przez jednostkę w służbie państwowej tak zwanego *prawa wizyty*) może mieć miejsce w przypadku: zwalczania piractwa, zwalczania handlu niewolnikami, zwalczania niedozwolonego handlu narkotykami i substancjami psychotropowymi, zwalczania nielegalnego nadawania audycji z morza otwartego, w przypadku zaistnienia podejrzenia, że statek podnosi tę samą banderę co jednostka w służbie państwowej lecz odmawia ujawnienia tego faktu.

Zauważyć jednak należy, że praktyczne użycie wymienionych wyżej regulacji obwarowane jest zasadami w poważny sposób ograniczającymi ich skuteczność. Praktycznie we wszystkich przypadkach do wizyty na pokładzie statku obcej bandery dojść może jedynie w przypadku *zaistnienia rozsądnych podstaw do podejrzenia*, że jednostka ta trudni się jednym z wymienionych wyżej procedurów. W przypadku nieuzasadnionego przeprowadzenia wizyty kontrolowanej jednostce przysługuje prawo do rekompensaty. Zapis ten dość skutecznie *stępi* ostrze zapisów o *prawie wizyty* i możliwość posłużenia się nimi do zwalczania terroryzmu morskiego.

W przypadku zwalczania aktów bezprawnych skierowanych przeciwko bezpieczeństwu żeglugi oraz handlu narkotykami państwo (jednostka w służbie państwowej) nadbrzeżne posiada prawo zajęcia statku pirackiego (opanowanego przez piratów) lub używanego do transportu narkotyków, aresztowania znajdujących się na nim osób i zajęcia mienia, zaś sąd państwa, które dokonało zatrzymania może zadecydować o wymiarze kary i działaniach w stosunku do osób i mienia.

Nowych instrumentów zwalczania aktów przemocy wykraczających poza klasyczną definicję piractwa dostarcza Konwencja rzymska o zwalczaniu bezprawnych aktów przemocy w obrębie szelfu kontynentalnego 1988 roku wraz z protokołem dodatkowym traktującym o stałych platformach posadowio-

nych w obrębie szelfu. Konwencja precyzuje, iż państwo winno rozciągnąć swoją jurysdykcję na sprawców szeregu dokładnie wyspecyfikowanych czynów stanowiących zagrożenie żeglugi handlowej lub platform. Konwencja rzymska niewątpliwie wytycza więc właściwy kierunek postępowania ale jej regulacje nadal w istotny sposób ograniczają możliwość skutecznego użycia jednostek w służbie państwowej, zwłaszcza zaś w zakresie prewencji i tak zwanej *obrony wyprzedzającej*. Z przykrością należy zatem skonstatować fakt, że *wolność mórz* będąca przez wieki jednym z filarów zachodniej cywilizacji może być obecnie z całą bezwzględnością wykorzystana przez różnej maści politycznych ekstremistów.

Na jeszcze większe trudności może napotkać skuteczne zwalczanie terroryzmu morskiego na wodach przybrzeżnych, zwłaszcza w sytuacji, gdy sprawcy działań bezprawnych operują z wód terytorialnych państwa, które nie sprawuje nad nimi efektywnej kontroli, a jednocześnie odmawia nawiązania współpracy międzynarodowej w kwestii wyplenienia morskiej przestępczości. Obecnie wymienić można co najmniej kilka państw nadbrzeżnych i archipelagowych, których jurysdykcja nad wodami terytorialnymi ma charakter czysto formalny, ale które zdecydowanie odmawiają przyjęcia obcej pomocy na przykład w zwalczaniu piractwa. Swoista *nadwrażliwość* wielu państw w kwestii własnej suwerenności, połączona z rozgałęzionymi powiązaniem korupcyjnymi wśród lokalnej administracji i służb policyjnych czyni obecnie zwalczanie piractwa na wielu akwenach po prostu niemożliwym. Podobnie wyglądać może kwestia operacji przeciwko terroryzmowi morskiemu.

Mimo, że istniejące regulacje prawne utrudniają skuteczne przeciwdziałanie terroryzmowi morskiemu ich zmiana w przewidywalnej przyszłości jest bardzo mało prawdopodobna. Państwa podejmujące działania antyterrorystyczne na morzu będą więc zmuszone do działań jak *bokser, którego prawa ręka przywiązana jest do narożnika* bądź też działań na granicy lub nawet poza grani-

cą obowiązujących obecnie uregulowań prawnych. Sytuacja powyższa w znaczący sposób sprzyja sprawcom działań terrorystycznych, a ponadto może ona wybitnie negatywnie odbić się na sposobie postrzegania morskich operacji antyterrorystycznych przez opinię światową.

Kolejnym czynnikiem sprzyjającym sprawcom działań terrorystycznych na morzu jest fakt, że znaczna ilość sprzętu niezbędnego do prowadzenia tego typu akcji może zostać nabyta w normalnym obrocie handlowym i jego zakup nie podlega żadnym ograniczeniom. Szybkie łodzie i jachty motorowe, skutery wodne, sprzęt do nurkowania oraz podobne wyposażenie traktowane są w krajach rozwiniętych jako artykuły sportowo – rekreacyjne. Tymczasem praktycznie każdy element wyposażenia motorowodniackiego oraz nurkowego jest klasycznym sprzętem *podwójnego zastosowania* – bez poważniejszych prac adaptacyjnych może on zostać zastosowany przez terrorystów planujących działania na morzu. Podobnie ma się kwestia szkolenia. Zarówno w odniesieniu do sterników łodzi motorowych jak i płetwonurków – o czym wspomniano wyżej – może być ono przeprowadzone przez podmioty specjalizujące się w usługach sportowo rekreacyjnych.

Istotnym czynnikiem ułatwiającym prowadzenia działań terrorystycznych na morzu jest również względna łatwość pozyskania dużej jednostki pływającej (z zamiarem wykorzystania jej jako jednostki bazowej nawodnych środków dywersji, jako platformy uzbrojenia podczas krótkotrwałego oddziaływania na wybrane cele, w charakterze stawiacza min) wynikająca z liberalnych przepisów rządzących rynkiem żeglugowym (zwłaszcza w państwach tzw. taniej bandery) oraz rynkiem używanego tonażu. W związku z powyższym nabycie jednostki i jej zarejestrowanie (czyli faktyczna legalizacja) wiąże się w praktyce jedynie z kwestiami finansowymi. Ceny używanych drobnicowców o pojemności około 7 500 DWT, budowanych w latach 1980 - 85, wahają się od 2,5 do 3,5 mln USD, koszty rejestracji spółki armatorskiej w Panamie, na Bahamach lub na

Cyprze nie przekraczają 40 tys. USD

#### 4.2.4. Próba prognozy

Obecnie wydaje się, że zagrożenie żeglugi handlowej działaniami terrorystycznymi będzie rosło. Szczególne zagrożenie stwarza, sygnalizowane już, pozyskiwanie przez organizacje terrorystyczne i zorganizowane grupy przestępcze coraz bardziej zaawansowanych środków. Do chwili obecnej udaremniono co najmniej trzy próby pozyskania przez struktury pozapaństwowe miniaturowych okrętów podwodnych. Dwa nielegalne warsztaty wykryto w Kolumbii (w rejonie Bogoty i Kartageny), trzeci ujawniony został przez służby bezpieczeństwa wewnętrznego Malezji w okolicy miejscowości Pukhet. W Kolumbii pozyskaniem jednostek zainteresowane były kartele narkotykowe, które zamierzały je prawdopodobnie wykorzystać do przemytu substancji psychotropowych. Nie wyklucza to jednak, że miniaturowe okręty podwodne zbudowane w tajnych stoczniach narkotykowych baronów nie znalazłyby się po pewnym czasie na czarnym rynku broni. Czynnikiem decydującym o takiej ewentualności byłaby prawdopodobnie tylko cena, którą skłonny byłby zapłacić potencjalny nabywca. W Malezji prace z całą pewnością prowadzono na zlecenia Tamilskich Tygrysów.

Bardzo poważne następstwa przynieść może opanowanie przez organizacje ekstremistyczne technologii produkcji min morskich, co stało się już rzeczywistością w odniesieniu do Tamilskich Tygrysów. Może to zaowocować pojawieniem się tego uzbrojenia na „międzynarodowym czarnym rynku broni”. Jest to o tyle groźne, że ruch tamilski dysponuje pełną autonomią, nie jest on „ugrupowaniem – klientem” jakiegokolwiek państwa, w związku z czym jego kontrolowanie bezpośrednio lub pośrednio przez podmiot zewnętrzny jest praktycznie niemożliwe. W związku z czym o „podaży” wymienionych rodzajów uzbrojenia decydować będą wyłącznie potrzeby Tamilów. Nie można więc wy-

kluczyć sytuacji, że miny morskie wyprodukowane w *Wolnym Tamillandzie* zastosowane zostaną w innych rejonach świata. W ostatnich miesiącach pojawiły się ponadto informacje, że miny morskie pozyskały również inne ruchy ekstremistyczne. Na przykład Rewolucyjne Siły Kolumbii (FARC) miały je pozyskać o niezidentyfikowanych sponsorów zagranicznych, a kilka innych organizacji samodzielnie produkuje ładunki wybuchowa odpalane zdalnie z brzegu. Stwarza to zupełnie nową jakość w zakresie bezpieczeństwa morskiego, gdyż dotychczas użycia morskiej broni minowej było domeną państwa lub organizacji dysponujących poparciem służb państwowych. Obecnie miny mogą znaleźć się w obrocie pozostającym poza kontrolą państwowych służb specjalnych.

Z powyższych rozważań wynika, że obszary morskie, zarówno pozostające w obrębie suwerenności państw, jak i zaliczane do morza pełnego stać się mogą obszarem intensywnych, prowadzonych na dużą skalę i ze znacznym rozmachem działań terrorystycznych. Obecnie społeczność międzynarodowa nie jest przygotowana do stawienia czoła temu zagrożeniu. Dobitnie świadczy o tym – sygnalizowany już – wzrost przypadków ataków pirackich na statki. Oby nie okazało się więc, że dopiero kolejny spektakularny akt motywowanej politycznie przemocy, o katastrofalnych następstwach zainicjuje aktywne działania przeciwko już dziś widocznemu zagrożeniu.

## 5. WYBRANE PROBLEMY BEZPIECZEŃSTWA NATO I POLSKI W KONTEKŚCIE ZAGROŻEŃ ASYMETRYCZNYCH

Na początku lat 90-tych ubiegłego stulecia zaczęto dostrzegać coraz wyraźniej narastający potencjał militarnych zagrożeń asymetrycznych. Był to jeden z wyznaczników nowego pojmowania środowiska bezpieczeństwa wyłaniającego się w okresie po „Zimnej Wojnie”. Konsekwencją takiego postrzegania nowych zjawisk w obszarze bezpieczeństwa musi być próba odpowiedzi na powtarzające się, fundamentalne pytanie: jakich zagrożeń możemy się spodziewać na początku XXI wieku. Odpowiedź na to pytanie wykrystalizowała się w ostatniej dekadzie XX wieku. Po doświadczeniach jego pierwszej połowy, po dwóch wojnach światowych, w które zaangażowano olbrzymie potencjały ludzi i sprzętu, druga połowa XX wieku wykazała, iż mamy do czynienia ze zmianą hierarchii i rodzajów zagrożeń. Z kolei nowe doświadczenia wskazują, że zjawiska związane z rozszerzaniem się „wojny asymetrycznej” będą się nasilać, zaś jej podstawowym orężem będzie terroryzm. Istnieje więc konieczność nowego podejścia do tego zjawiska, gdyż terroryzm jest jednym z wielu niekonwencjonalnych wyzwań dla bezpieczeństwa. Co to oznacza?

Oznacza to, że w wiek XXI nie weszliśmy jak sto lat temu z teorią i praktyką przygotowującymi do wojny powszechnej (totalnej), a może nawet i kontynentalnej czy też regionalnej. Nie ten rodzaj wojny (konfliktu) należy postawić na pierwszym miejscu, czyli jako najbardziej prawdopodobny. Na pierwszy plan, co pokazały doświadczenia i wnioski ostatniej dekady lat dziewięćdziesiątych, wysunęły się różnego rodzaju konflikty ograniczone, lokalne, innymi słowy - bardzo często konflikty inne w swym charakterze niż dotychczasowa wojna w klasycznej postaci. Do tego należałoby dodać różnego rodzaju zagrożenia niemilitarne, a zwłaszcza te, które przyniosła ze sobą cywilizacja i postęp społeczny. Przykładem mogą być konflikty etniczne i religijne, przemyt narkotyków, masowe migracje, regionalna niestabilność, pranie brudnych pie-

niędzy, działania różnych bojówek oraz kradzież informacji. Nie jest też możliwe rozdzielenie terroryzmu od prania brudnych pieniędzy czy przestępczości zorganizowanej trudniącej się przemytem narkotyków. Innym przykładem wzajemnych powiązań są migracje. Wywołują one obawy o bezpieczeństwo wewnętrzne, mogą być też przyczyną ksenofobii i konfliktów w miarę jak zagrożone są dotychczasowe tradycyjne możliwości znalezienia pracy.

Nie sposób pominąć dzisiaj możliwości wystąpienia nagłego ryzyka związanego z użyciem i dalszym rozprzestrzenianiem broni masowego rażenia i środków jej przenoszenia. Należy podkreślić, że coraz liczniejsza jest grupa państw, w tym prowadzących politykę konfrontacyjną, bliskich wejścia w jej posiadanie. Jeżeli dodać do tego, że do dysponowania tą bronią dążą również skrajne ugrupowania polityczne, religijne, a nawet przestępcze, to możliwość ewentualnego jej użycia wykracza niekiedy już poza sferę wyobraźni. Przez ostatnie pół wieku dzięki strategii odstraszenia udało się uniknąć wojny nuklearnej. Uznano, że nie ma po co atakować, bowiem i atak, i kontratak miałyby dla obydwu stron miażdżące konsekwencje. Koncepcja ta została zapisana w 1972 r. w traktacie ABM (o kontroli rakiet balistycznych), w którym Stany Zjednoczone i Związek Radziecki zgodziły się ograniczyć do minimum zdolność swoich potencjałów militarnych. Limity ilości i rodzajów broni nuklearnej ustalono w taki sposób, by nie wykluczały one jednak możliwości ewentualnego starcia i wzajemnego się pokonania. Obecnie coraz częściej pojawia się postulat wprowadzenia nowej, jeszcze dalej idącej koncepcji strategicznej, zmierzającej w kierunku zapobiegania wojnom i konfliktom. Wiąże się to z koniecznością dalszego zmniejszenia nuklearnych potencjałów ofensywnych i zwiększenia rakietywnych potencjałów obronnych. Zaznaczyć należy, że nie jest to myślenie powszechne, bowiem rodzi ono nowe zagrożenia. Kilka krajów - w tym Korea Północna, Irak, Iran - pracują nad skonstruowaniem rakiet balistycznych i głowic nuklearnych. Niektóre z tych rakiet mogą zagrozić stacjonującym w zapal-

nym regionach świata wojskom amerykańskim, sojusznikom Stanów Zjednoczonych, a nawet terytorium amerykańskiemu. W konsekwencji należy więc w dalszym ciągu z największą powagą rozważać groźbę i możliwość użycia tej broni. Do tego dochodzą również zwiększone zainteresowania dostępem do broni masowego rażenia i jej użyciem przez terrorystów. Bin Laden stwierdził publicznie w udzielanych wywiadach, że jej pozyskanie uznaje za swój religijny obowiązek. Mimo iż użycie przez terrorystów broni nuklearnej wydaje się obecnie mało prawdopodobne to jednak niebezpieczeństwo takie istnieje. Terrorysty mogą otrzymać materiały bojowe lub broń od państw sympatyzujących, mogą ją wykraść ze słabo strzeżonych obiektów a nawet kupić od rozczarowanych lub słabo opłacanych naukowców czy strażników.

Największe obawy wywołuje broń biologiczna. W przypadku jej zastosowania należy się liczyć z niemożnością zidentyfikowania czasu i miejsca jej użycia, a skutki mogą być zauważalne dopiero po fakcie. Zakaźny charakter środków biologicznych wskazuje wyraźnie na znaczenie budowania systemu, który nie tylko tworzy możliwości przeciwstawiania się jednemu zagrożeniu, ale poradzi sobie z różnorodnymi sytuacjami.

Wydarzenia z 11 września 2001 r. i późniejsze ataki z wykorzystaniem bakterii węglika pokazały, że więcej uwagi i środków należy kierować na rozpoznawanie i ewentualną walkę z zagrożeniem terrorystycznym. Podkreślić należy, że do 11 września nie istniała zgodność poglądów dotyczących głównego zagrożenia Stanów Zjednoczonych. Niektórzy specjaliści liczyli się z ponownymi atakami terrorystycznymi na wojskowe obiekty USA za granicą. Inni uważali, że zagrożenie może przyjść z Chin. Zakładano również atak Korei Północnej na Południową, lub atak jakiegoś "państwa bandyckiego" na Stany Zjednoczone. Nawet obecnie, w obliczu zgody, że terroryzm jest największym zagrożeniem, niektórzy nadal spierają się, jaką może on przybrać formę.

NATO, w tym także Polska jako część systemu wojskowego sojuszu

musi się liczyć z możliwością ataku informacyjnego na strategiczną infrastrukturę narodową, szczególnie w okresie narastania kryzysu wojskowego (czy np. w fazie dokonywania przerzutu wojsk). Celami mogą stać się główne dziedziny gospodarki narodowej, w tym system bankowy i finansowy, sieć zasilania w energię elektryczną, sieć rurociągów gazowych i naftowych, system telekomunikacji oraz ogólnonarodowy i lokalne systemy komunikacji lądowej powietrznej i morskiej. Wszystkie te dziedziny strategicznej infrastruktury narodowej przechodzą gwałtowne przemiany, często o charakterze rewolucyjnym, w warunkach presji prywatyzacyjnej, globalizacyjnej i napływu różnorodnej techniki informacyjnej. Zagrożenia asymetryczna związane z tym problemem powinny być przedmiotem bieżącego planowania wojskowego i struktur (instytucji) odpowiedzialnych za funkcjonowanie kluczowych systemów infrastruktury państwa w warunkach kryzysowych.

Poważne zagrożenie może wystąpić ze strony hakerów<sup>94</sup> związanych z organizacjami i ugrupowaniami pozapaństwowymi (non-state actors), ale przede wszystkim ze strony obcych służb specjalnych. Obecnie nie można podać potwierdzonych i w pełni udokumentowanych przykładów poważnego zagrożenia dla struktur informacyjnych państwa (w tym wojska). Ocenia się jednak, że w perspektywie średnio- i długoterminowej mogą one zostać poddane działaniom IW o różnej formie, zasięgu i skali intensywności.

Przedstawione oceny i prognozy wskazują, że w pełni trzeba zgodzić się z poglądem, znajdującym odzwierciedlenie w polskiej strategii bezpieczeństwa i obronności, iż na początku XXI wieku w przeciwdziałaniu zagrożeniom dominować będą działania prewencyjno-stabilizacyjne, realizowane zawczasu, tzn. jeszcze w okresie pokoju. Istotą tych działań będzie zapobieganie na bieżąco występowaniu zewnętrznych zagrożeń polityczno-militarnych (kryzysowych i

---

<sup>94</sup> Osób specjalizujących się w nieuprawnionych „wejściach” (włamaniach) do komputerowych systemów informacyjnych.

wojennych) poprzez neutralizowanie ich potencjalnych przyczyn (źródeł) oraz stabilizowanie i umacnianie bezpieczeństwa.

W stosunku natomiast do grupy zagrożeń związanych z kryzysami, zwłaszcza polityczno-militarnymi, wyraźnie już dzisiaj daje się zauważyć, że będziemy mieli do czynienia z potrzebą jak najwcześniejszego i skutecznego ich opanowywania. Stąd też myślą przewodnią reagowania na kryzysy będzie: jak najszybsze opanowanie każdej sytuacji kryzysowej, zagrażającej interesom państwa lub społeczności międzynarodowej. Celem natomiast opanowania kryzysu będzie minimalizowanie jego skutków i przywrócenie stanu sprzed kryzysu bądź innego zadowalającego rozwiązania, a w szczególności zapobieganie przedrodzeniu się kryzysów w bezpośrednie zagrożenie wojenne.<sup>95</sup>

Śmiało więc można dziś postawić tezę, że istotą działań prewencyjno-stabilizacyjnych i reagowania kryzysowego będzie zapobieganie rozszerzaniu się sytuacji niebezpiecznych, które rodzą się w czasie pokoju, a skutkują w istocie wojną. Będą to działania dominujące na początku XXI wieku, które mieszczą się w strategii, którą można nazwać STRATEGIĄ ZAPOBIEGANIA.

Dopiero jakby na trzecim, ostatnim miejscu wymienia się możliwość wybuchu wojny na szerszą skalę, jako wynik nieopanowania w odpowiednim czasie kryzysów, wojen lokalnych (ograniczonych), oraz innych konfliktów. Nie należy też zupełnie wykluczyć możliwości rozszerzenia się kryzysu, konfliktu ograniczonego i przerodzenia ich w wojnę z użyciem broni jądrowej (BMR), obejmującej stopniowo swoim zasięgiem coraz większe połacie kuli ziemskiej. Na pewno trzeba mieć wiele wyobraźni, żeby dopuszczać możliwość jej wybuchu, ale trzeba też w pełni zdać sobie sprawę z tego, że mogą zaistnieć ku temu przesłanki, gdy tej wyobraźni nie ma się w ogóle. Można sądzić, że w dalszym ciągu pozostaje aktualna maksyma wojskowa, że dopóki jakaś broń znajduje się

---

<sup>95</sup> B. Balcerowicz, Cel: wola wroga, Czy grozi nam wojna światowa? Polityka nr 4 z dn. 22.01.2000.

w arsenałach (magazynach) państw, dopóty istnieje niebezpieczeństwo jej użycia.

Dla realizacji głównych zadań strategicznych, będących ukonkretnieniem współczesnej wojskowej myśli strategicznej, potrzebne są odpowiednie siły i środki. Właśnie w tym zakresie zachodzą na przełomie wieków olbrzymie zmiany. Mamy do czynienia z sytuacją, w której najważniejsza staje się jakość, nie ilość. Przemiany ilościowo-jakościowe, zwłaszcza przygotowywanie się do szybkiej reakcji powodują, że szczególnie pożądane stają się dziś jednostki lekkie, zdolne do natychmiastowego działania po przerzucie w rejony walki, a szczególnie efektywna staje się lekka broń precyzyjnego rażenia wraz z całym jej oprzyrządowaniem.

Wreszcie idea działań wspólnych, działań połączonych wszystkich rodzajów sił zbrojnych „dyktuje” dziś kształt struktur organizacyjnych i wyposażenia wojsk. Przewaga jakości poczynając od pancerzy czołgów, rakiet, systemów kierowania ogniem, możliwości zakłócania, a zwłaszcza możliwość użycia broni inteligentnych, jest nie do podważenia. Gigantyczny most powietrzny, po którym Amerykanom, Brytyjczykom i Francuzom udało się w rejonie konfliktu (Zatoka Perska) zgromadzić ok. 690 tys. żołnierzy z pełnym wyposażeniem też jest faktem. Była to w końcu największa operacja transportowa w dziejach ludzkości. Na pewno też sukces w operacji lądowej zapewniły aliantom lepsze systemy wykrywania celów i nowocześniejsze urządzenia noktowizyjne.

Prognozuje się, że w ciągu najbliższych 20 lat w światowej technice obronnej nastąpi przełom technologiczno-strategiczny. Na przyszłą strategię i taktykę coraz większy wpływ wywierać będą właśnie możliwości technologiczne. Wielu naukowców cywilnych i wojskowych przewiduje, że w ciągu najbliższych 15-20 lat będziemy mieli do czynienia z rewolucyjnymi zmianami w kilku dziedzinach. Do ważniejszych zalicza się bezprzewodowe sieci komputerowe, miniaturyzację i robotyzację wraz z gwałtownym rozwojem

nauk biologicznych i ich militarnym wykorzystaniem. Ważnymi pytaniami, jakie zadają sobie dziś specjaliści to: Czy lasery i energia kierowana znajdą szersze zastosowanie w najbliższej przyszłości? Czy realizacja zadań na polu walki zostanie w znacznym zakresie powierzona bezzałogowym jej środkom, które same rozpoznają cele, namierzają je, a następnie niszczą?

Najnowocześniejsze bronie, wchodzące już do wyposażenia żołnierza końca XX w. będą prawdopodobnie upowszechnione i doskonalone na początku nowego stulecia. Tak więc żołnierz początku XXI wieku będzie coraz częściej dysponował karabinkiem wyposażonym w kamerę video, kamerą na promienie podczerwone, dalmierzem laserowym i kompasem cyfrowym. Hełm żołnierza będzie posiadał noktowizor, urządzenie alarmowe, informujące go, że znalazł się w zasięgu wrogiego lasera, oraz miniaturowy ekran, wyświetlający mapy, rozkazy i obrazy z kamery video karabinu.

Olbrzymią karierę zrobią też zapewne wspomniane już wcześniej różnego rodzaju latające aparaty (pojazdy, samoloty) bezzałogowe, naszpikowane sensorami na światło dzienne i podczerwień, posiadające dalmierze laserowe i wysokiej jakości kamery nadzorujące, które „na żywo” będą przekazywać obrazy dowództwom. Modernizacji tej przyświeca cel ostateczny, którym ma być „przezroczyste” pole walki; takie pole walki na którym można będzie rozpoznać każdego wroga i skalkulować każde ryzyko. Już obecnie żołnierze sił szybkiego reagowania w Niemczech, Wielkiej Brytanii, a zwłaszcza USA trenują na takim przyszłym polu bitwy. Każdego żołnierza, czołg, transporter, wyposaża się w urządzenia do nawigacji satelitarnej, które pokazują na mapach położenie walczących wojsk. Zespoły „specjalistów” pracują nad systemami „człowiek – maszyna”, dążąc do zwiększenia siły uderzeniowej pojedynczego żołnierza. Nie ulega wątpliwości, że miniaturyzacja stała się kolejnym trendem powszechnym. Obecnie wymiary urządzeń – zarówno elektronicznych, jak mechanicznych – zmniejszają się w tempie 5,6 razy co dziesięć lat.

W najbliższych dekadach przewaga techniczna i technologiczna pozostanie jednym z podstawowych filarów doktryny obronnej każdego państwa, a opanowanie nowoczesnych rozwiązań w takich dziedzinach jak: radiolokacja, źródła energii, napędy, nokto- i termowizja, redukcja skutecznej powierzchni odbicia środków walki, nawigacja satelitarna oraz systemy przetwarzania i zarządzania informacją, wpływać będą na zmiany w uzbrojeniu i sposobach jego wykorzystania. Broń skonstruowana w oparciu o najnowsze osiągnięcia techniczne i technologiczne umożliwi zdobycie i utrzymanie asymetrycznej przewagi przy stosunkowo niewielkich stratach własnych. Nowe technologie pozwolą także na osiąganie celów wojskowych sposobami innymi od dotychczas przyjętych<sup>96</sup>, a zwycięstwo w przyszłym konflikcie uzyska ta strona, która szybciej potrafi odkryć możliwości, jakie one stwarzają.

W czasie pokoju przewaga technologiczna powinna być kluczowym elementem odstraszenia potencjalnego przeciwnika. Podczas kryzysów stwarza ona możliwość elastycznego reagowania władzom cywilnym oraz dowództwu wojskowemu, przy jednoczesnym sygnalizowaniu sojusznikom, że ich partner kontroluje sytuację. W czasie wojny przewaga technologiczna zmniejsza straty osobowe, sprzętu i uzbrojenia oraz zwiększa efektywność bojową wojsk. Dlatego w czasie, gdy redukowane są budżety wojskowe i postępuje zmniejszanie stanów osobowych sił zbrojnych, dbałość o inwestycje w dziedzinie techniki i technologii wojskowych powinny być przedmiotem troski i wręcz obowiązkiem każdego rządu. Dotyczy to zwłaszcza państw o mniejszym potencjale badawczo-rozwojowym sektora cywilnego i wojskowego. Ograniczone zapotrzebowanie rynku wewnętrznego jest zbyt małe, aby być motorem postępu technologicznego na potrzeby obronności pojedynczego państwa.

Większość wynalazków i nowoczesnych technologii inicjowały dotychczas laboratoria i zakłady pracujących na rzecz obronności, z reguły finansowa-

---

<sup>96</sup> Np. zastosowanie bezzałogowych samolotów bojowych w sytuacji, gdy potencjalne straty byłyby zbyt duże dla samolotów konwencjonalnych.

ne z budżetów obronnych. Obecnie, ze względu na redukcje stanów osobowych oraz cięcia budżetowe, coraz większy udział w finansowaniu postępu ma sektor cywilny. Proces ten działa na zasadzie swoistego sprzężenia zwrotnego, szczególnie w dziedzinie szeroko pojętej elektroniki, technik informacyjnych, czy biotechnologii. Przykładowo, komercyjny popyt na kamery wideo spowodował olbrzymią redukcję kosztów matryc CCD (Charged Coupled Detector), upowszechniając w ten sposób stosowanie elektrooptycznych układów naprowadzania i umożliwiając dalsze badania w tej dziedzinie. Podobny postęp jest obecnie oczekiwany w obszarze wojskowych zastosowań układów termowizyjnych.

Wysłuzony dogmat, iż „siła ognia jest potęgą” nadaje się już chyba do lamusa. Zastępuje go coraz częściej określenie, iż „potęgą jest informacja”. Niewątpliwie jesteśmy świadkami gwałtownego rozwoju potencjału informacyjnego, którego znamioną cechą jest początek ery informacyjnej w sztuce wojennej, która nadchodzi po erach biologicznej i mechanicznej.<sup>97</sup> Przyszła teoria sztuki wojennej musi więc znaleźć odpowiedź na pytania dotyczące takich kwestii, jak skuteczne oddziaływanie informacyjne na przeciwnika i dezorganizowanie jego systemów informacyjnych oraz zapewnienie sprawności własnym systemom informacyjnym.

Rosnące uzależnienie rozwiniętych państw od systemów informacyjnych i techniki informacyjnej zwiększa podatność tych państw na zagrożenia związane z wymiarem cybernetycznym operacji informacyjnych oraz z ich tradycyjnymi aspektami, takimi jak operacje psychologiczne i oddziaływanie na percepcję. Wielu ekspertów wskazuje, że narastanie procesu cyfryzacji przekłada się bezpośrednio na wzrost podatności na zagrożenia.

Oznacza to, że **dominacja w sferze informacyjnej staje się kluczowym obszarem, oddziałującym bezpośrednio na istotę i znaczenie walki**

---

<sup>97</sup> Koziej S., *Strategia i potencjał obronny Polski w warunkach członkostwa w NATO, AON*, Warszawa, s. 40.

**zbrojnej.** Podstawowym problemem są przy tym procesy dotyczące syntezy danych napływających z różnych źródeł podczas prowadzenia walki oraz zdolność do ich przetwarzania w czasie rzeczywistym.

Generalnie należy oczekiwać kontynuowania obecnych tendencji, zwłaszcza w zakresie tworzenia konstrukcji niemetalicznych, stosowania materiałów inteligentnych<sup>98</sup> oraz dalszej redukcji pozostawiania śladu<sup>99</sup>, umożliwiającego wykrywanie i identyfikację środków walki. Ocenia się jednak, iż źródłem głównego zagrożenia będzie w najbliższej przyszłości wzrost liczebności dobrze uzbrojonych samolotów bojowych obecnej generacji, w tym wyspecjalizowanych w zwalczaniu celów naziemnych, których piloci będą stosowali udoskonaloną, wspartą technicznymi środkami, taktykę walki.

Wydatki na cele badawcze w dziedzinie technologii wojskowych koncentrować się będą na następujących zagadnieniach:

- możliwości wykonywania precyzyjnych uderzeń przeciwko przewidywanym celom ruchomym i stałym w każdych warunkach pogodowych i o każdej porze doby;
- opracowaniu systemów artyleryjskich i pocisków, które będą wykorzystane w lżejszych i bardziej mobilnych wozach bojowych, czołgach, okrętach nawodnych oraz statkach powietrznych;
- możliwości wykrycia, identyfikacji i zakłócenia czujników i urządzeń pracujących w zakresie częstotliwości radiowych i radiolokacyjnych oraz termo- i noktowizyjnych;
- opracowaniu urządzeń zakłócających i ostrzegających o opromienowaniu wiązką radiolokacyjną, które będą w stanie dostosować się w czasie rzeczywistym do zmieniających się zagrożeń;

<sup>98</sup> Np. materiałów z „pamięcią” magnetyczną.

<sup>99</sup> Inaczej „sygnatury” np. odbicia (echa) elektromagnetycznego, akustycznego itp.

- opracowaniu efektywnych metod wykrywania min i sposobów rozminowania na potrzeby operacji desantowania z morza;
- rozwijaniu systemów obrony przeciwlotniczej, przeciwrakietowej (także w odniesieniu do pocisków manewrujących o zmniejszonej skutecznej powierzchni odbicia promieniowania radiolokacyjnego oraz zmniejszonych śladach termicznych, akustycznych i innych), skutecznych w trudnych warunkach pogodowych i o każdej porze doby;
- możliwości zwalczania pocisków na każdym z odcinków toru lotu;
- możliwości obezwładniania lub zakłócania systemów C<sup>3</sup>I (Command, Control, Communication & Information) oraz nawigacyjnych przeciwnika;
- kontroli przestrzeni kosmicznej;
- możliwości rzeczywistego obezwładnienia systemów obrony przeciwlotniczej przeciwnika;
- możliwości zdobycia i utrzymania przewagi pod wodą;
- integracji (w czasie rzeczywistym) informacji z czujników pokładowych oraz dostępnej w ramach większych systemów oraz wykorzystanie jej do celów decyzyjnych, oceny wykonania zadania, opisu celów itp.;
- użyciu w różnych sytuacjach technologii właściwych dla „nieletalnych” środków obezwładniających.

Wydatki na cele badawcze w dziedzinie technologii wojskowych będą uwzględniać:

- dostępność – wszystkie nowe programy powinny uwzględniać możliwość zwiększanie efektywności uzbrojenia i wydłużanie jego re-

sursu technicznego, przy jednoczesnym zmniejszaniu kosztów wytwarzania i eksploatacji m.in. dzięki modernizacjom zaplanowanym już na etapie projektowania<sup>100</sup>;

- podwójne przeznaczenie – nowe programy muszą sprzyjać rozwojowi ogólnej bazy przemysłowej m.in. poprzez stosowanie technologii komercyjnych, a nowo opracowane technologie wojskowe powinny uwzględniać możliwość ich zastosowania w sektorze cywilnym;
- utrzymywanie krajowego potencjału badawczego i produkcyjnego – poprzez odpowiedni poziom (skalę) inwestycji; w przyszłości powinien on zapewnić centrom i ośrodkom decyzyjnym możliwość elastycznej reakcji w sytuacji zagrożeń asymetrycznych (większych od przewidywanych) oraz przy budżecie mniejszym od zakładanych potrzeb.

Liderem w dziedzinie wydatków na nowe technologie o potencjalnie wojskowym zastosowaniu będą Stany Zjednoczone, które przeznaczają na ten cel dwa razy więcej środków niż cała Europa (bez Rosji i państw b. ZSRR). Do liderów w dziedzinie inwestycji w badaniach nad rozwojem nowych technologii obronnych (asymetrycznych) należy Japonia, a w dłuższej perspektywie prawdopodobnie Chiny i Indie. Rosja będzie w najbliższych latach wykorzystywała (w swoisty sposób konsumowała) dorobek b. ZSRR, jednak w dłuższej perspektywie (20-30 lat) powinna ponownie dołączyć do grona liderów postępu technologicznego.

Różnica pomiędzy Stanami Zjednoczonymi i innymi państwami w wydatkach na cele badawcze i rozwój nowych technologii o zastosowaniu wojskowym będzie się powiększać, doprowadzając do powstania luki technologicznej. Może to w przyszłości uniemożliwić, lub poważnie zakłócić, prowadzenie wspólnych operacji w ramach NATO. W związku z tym dostęp do technologii

<sup>100</sup> Przykładem jest tu amerykański program wielozadaniowego samolotu bojowego *JSF* (Joint Strike Fighter).

amerykańskich będzie miał istotne znaczenie dla państw członkowskich paktu. Jednak, aby taki dostęp był możliwy, chcące uzyskać go państwo powinno zaoferować coś w zamian. Jest to szansa, a zarazem wyzwanie dla mniejszych państw, które mogą i w pewnym sensie muszą, wyspecjalizować się w wąskich dziedzinach określanych mianem *nisz technologicznych*.

Najwyższy poziom techniki, szczególnie w zakresie broni strategicznej, może pojawić się tylko w przypadku konfliktu z przeciwnikiem zaawansowanym technicznie i technologicznie. Jednak prawdopodobieństwo takiego starcia zostało w ostatnich latach znacząco zredukowane. Eksport nowych technologii umożliwia różnym, w tym niekoniecznie przyjaznym państwom, dostęp do uzbrojenia o dużym potencjale bojowym. Ogólnie oceniając, tanie uzbrojenie i technika wojskowa mogą wystąpić w wielu scenariuszach konfliktów zbrojnych, jednak koszty i formalno-prawne ograniczenia handlowe (antyproliferacyjne) będą w dalszym ciągu barierą w dotarciu importerów do nowej broni i związanych z nią technologii. **Największa skala proliferacji dotyczy techniki wojskowej o jedną generację starszą od techniki stosowanej obecnie przez najbardziej rozwinięte państwa świata.** Takie uzbrojenie jest udostępniane w dużych ilościach i po cenach znajdujących akceptację mniej zamożnych nabywców. **Oznacza to, że siły NATO nie będą opierać swojej przewagi na asymetrii ilościowej broni i środków technicznych, koncentrując się przede wszystkim na środkach i systemach zapewniających przewagę jakościową.**

Inne dylematy przełomu wieków, rzutujące na kształt przyszłości, zawierają się w wielu pytaniach, na które niełatwo będzie znaleźć jednoznaczną odpowiedź. I tak np. czy operacja „Pustynna Burza” była rzeczywiście pierwszą operacją wygraną z powietrza? Czy też prawdą jest, że odniesiono w niej zwycięstwo dzięki czołgom? Albo - czy siły zbrojne większości państw będą ewoluować ku armii czysto zawodowej, czy będzie to kombinacja mieszana, dostosowana do koncepcji powszechnej obrony narodowej?

Pod koniec XX wieku pojawił się kolejny, nienowoty zresztą poważny dylemat. Czy można wygrać wojnę tylko siłami powietrznymi? Po euforii skutecznych działań lotnictwa w Kosowie i Afganistanie przyszedł czas na podsumowania i refleksje. Dogmat o zwyciężaniu samym lotnictwem tak, jak teorię wojny powietrznej Douhet'a trzeba chyba ponownie wyrzucić na śmietnik. Wszystko bowiem wskazuje, że NATO w przyszłości również będzie zmuszone do prowadzenia działań na lądzie i właśnie przez wojska lądowe. Niemniej jednak daje się wyraźnie zauważyć, iż w ostatnich latach siły powietrzne są coraz nowocześniejszym i niezwykle skutecznym rodzajem sił zbrojnych, który w realizacji wielu zadań coraz częściej wyręcza, a nawet zastępuje wojska lądowe. To jednak, jaki kształt przybierze każda przyszła wojna zależeć będzie od konkretnej sytuacji, a zwłaszcza od celów jakie zostaną określone przez decydenckie gremia polityczne.

Wojna asymetryczna rozpoczęta zbrodnictwem zamachem 11 września 2001 r. będzie inna niż wszystkie inne. Rozwiązania militarne nie rozstrzygną palących problemów współczesnego świata, które dostarczają argumentów do działań terrorystycznych i przyczynią się do wzrostu desperacji i wszelkiego rodzaju zagrożeń na bazie fanatyzmów religijnych i ideologicznych. Oprócz rozwiązań siłowych społeczność międzynarodowa będzie musiała zbudować bariery powstrzymujące rozwój terroryzmu.

Spółeczeństwa demokratyczne wielokrotnie wychodziły obronną ręką z trudnych prób historycznych. Miejmy nadzieję, że w XXI wieku zwyciężą także z terroryzmem, a zwłaszcza złagodzą występującą w świecie asymetrię, która jest przyczyną nowych zagrożeń początku XXI wieku.

## ZAKOŃCZENIE

Działania asymetryczne są najbardziej skuteczne, gdy uzyskiwany efekt ma wymiar strategiczny, niezależnie od poziomu konfrontacji i skali podejmowanych przedsięwzięć. Intuicyjnie jednak, już z samej zasady asymetryczności wynika, że działania te są optymalne w sytuacjach gdy przedsięwzięcia o charakterze taktycznym czy operacyjnym dają efekt strategiczny, z wymownymi obecnie przykładami działań terrorystycznych włącznie.

Poziom operacyjny przedsięwzięć asymetrycznych obejmuje akcje szczebla regionalnego lub teatru działań wojennych (TDW). Przykładem takich działań była w ramach NATO operacja *Allied Force* (marzec-czerwiec 1999 r.), która poprzez destrukcyjne zaangażowanie serbskiej obrony powietrznej i selektywne ataki, wyłączyła ją ze skutecznego działania.

Koncepcja dysproporcjonalności efektów w porównaniu do zaangażowanych (lub możliwych do zaangażowania) środków pozwala na wyróżnienie pięciu wskaźników użytecznych w identyfikacji asymetryczności zantagonizowanych stron:

- skala rozbieżności interesów jako kluczowy czynnik w szacowaniu ich skłonności (poziomu zdecydowania) do podejmowania działań asymetrycznych;
- ustalenie, że pokonanie oponenta jest ostatecznym celem którejś ze stron konfliktu<sup>101</sup> oraz przekonanie, że jedynym sposobem jego osiągnięcia jest podjęcie działań asymetrycznych;
- oczekiwanie przez strony efektu strategicznego, przy jednoczesnym podejmowaniu działań na wszystkich trzech poziomach (taktycznym, operacyjnym i strategicznym);

---

<sup>101</sup> W krańcowym przypadku wszystkich stron tego konfliktu.

- uznawanie czynnika skuteczności za jedyne kryterium<sup>102</sup> warunkujące podejmowanie działań (operacji) asymetrycznych;
- nieuchronność wzrostu zagrożenia – jako wynik analizy dynamicznych procesów i zmian asymetryczności (jej narastania pomiędzy za-ntagonizowanymi stronami).

Wymienione wskaźniki sygnalizują również to, że nowatorski (często egzotyczny) sposób myślenia oraz niekonwencjonalne działania mogą doprowadzić podczas bezpośredniej konfrontacji stron do nieoczekiwanego sukcesu teoretycznie słabszej z nich, zwłaszcza gdy zastosuje ona nową broń i nowe zasady jej wykorzystania. Wiele z takich nowych rodzajów broni nadaje się do wykorzystania jako asymetryczny i bardzo skuteczny środek walki.

Przeprowadzone badania przez zespół autorski niniejszego opracowania pozwalają w zakończeniu stwierdzić, że w coraz wyraźniej zarysowującej się nowej erze globalizacji będziemy mieli do czynienia głównie z kampaniami, operacjami wojskowymi sprowadzającymi się do minimalnego ryzyka, z technologiami dowodzenia wirtualnego i w końcu z wojnami cybernetycznymi (być może bez rozlewu krwi). Natomiast w najbliższej i być może dalszej perspektywie wielkie niebezpieczeństwo czai się w zjawisku, które jest określane jako zagrożenia (działania) asymetryczne.

---

<sup>102</sup> Pomijanie np. czynnika moralnego, etycznego, prawnego itp.

## BIBLIOGRAFIA

1. *The asymmetric threat: can America be defeated?*, "Joint Force Quarterly" Autumn/Winter 1998-99.
2. The Atlantic Monthly; December 2001; *Fourth-generation warfare*; Vol. 288, No. 5; 48-50.
3. Bass B. M., *Leading in the Army After Next*, "Military Review", March-April 1998.
4. BIMCO Weekly News no.26, Shipping News 4425 June 1997,
5. Blackwill R. D. and Carter A. B., "The Role of Intelligence," in R. D. Blackwill et al., *New Nuclear Nations: Consequences for U.S. Policy* (New York: Council on Foreign Relation Press, 1993), 217 and 236-237.
6. Bennett Bruce (RAND Corporation), *Establishing a Baseline for New Force Planning Constructs – Comparing Analysis of QDR 1997*.
7. Bredow W., *Militär, Krieg und Nation – Zukunftsorientierte Überlegungen im Anschluß an Clausewitz* [w:] *Clausewitz und die Zukunft von Krieg und Militär*, Clausewitz-Information 2002, nr 1
8. *Changing the Defense: National Security in 21st Century*, [w:] Report of National Defense Panel, Washington, 1997.
9. Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002,
10. Grant Rebecca, *The Kosovo Campaign: Aerospace Power Made It Work* (Arlington, VA: Air Force Association, September 1999), 15.
11. Grange D.L. „Walka asymetryczna. Stara metoda, nowe troski”, ROA National Security Report, March 2001.
12. Hammes T. X., *The Evolution of War: The Fourth Generation*, [w:] [http:](http://)

defence and society.org.

- 13.Hoch M., *Krieg und Politik im 21. Jahrhundert* [w:] *Workshop Krieg im 21. Jahrhundert*, Clausewitz-Protokolle 2001, nr 1.
- 14.<http://www.bundesnachrichtendienst.de/faq/lexikon.htm>
- 15.Jane's Defence Weekly, 20 February 2002.
- 16.Jane's Fighting Ships 1999-2000.
- 17.Jane's Underwater Weapon Systems 1999-2000.
- 18.Joint Strategy Review, Washington, DC, [w:] The Joint Staff 1999.
- 19.Joint Vision'2010 oraz Joint Vision'2020.
20. Kelso F.B II, Building Blocks of Naval Power, USNI Proceedings 1992 nr 11,
- 21.Koziej S. *Rewolucja nuklearna*, „Polska Zbrojna”, 2002 nr 11.
- 22.Kubiak K., Wojna asymetryczna?, „Przegląd Morski”, 2002 nr 1.
- 23.Kubiak K., Piraci czy terroryści, Komandos 1996 nr 3.
- 24.Kupiecki R., *Powrót do NATO*, „Polska Zbrojna”, 2002 nr 11.
- 25.Kusovac Z., Stemming the flow of people – smuggling at sea, Jane's Navy International vol. 107, no 4, May 2002
- 26.Matthews L.J. Wstęp do „Wyzywając USA symetrycznie i asymetrycznie: Czy USA można pokonać?”, Strategic Studies Institute, July 1998
27. *Menaces asymetriques et leur parades*, “Defence Nationale”, 2002 nr 2.
28. Metz S., Johnson D.V., „Asymmetry and US military strategy”, USAWC, SSI, January 2001.
- 29.*Modern Conflict: The Reality. Slide Presentation*, [w:] <http://d-n-i.net>.
- 30.Obrien K., Nusbaum J., *Intelligence gathering asymmetric threats*, Jane's

Intelligence Review 2000.

31. Palm G., *Kapituliert der Staat?* /deutsch/ inhalt/co/11013/1.html
32. Pawłowski J., *Wybrane problemy bezpieczeństwa RP w kontekście walki z terroryzmem (Zagrożenia asymetryczne)*, rękopis wystąpienia w ramach międzynarodowej konferencji nt.: „Ewolucja polityki bezpieczeństwa i obrony państw Grupy Wyszehradzkiej 1997 – 2002”, AON 19–20 kwietnia 2002.
33. Piątkowski K., *Wojna asymetryczna*, „Komandos”, 2002 nr 3 i 4;
34. Piskozub A., *Przemiany kulturowe i cywilizacyjne w perspektywie społeczeństwa postindustrialnego i aspekty globalizacji kulturowej – uwarunkowania i wnioski*, [w:] *Polska na drodze do nowoczesnej cywilizacji*, t. II, Warszawa 1990.
35. Seller H.F., *Konfliktkonstellationen im internationalen System*, Österreichische Militärische Zeitschrift 1999, nr 5
36. Qiuo Liang, Xiangsui Wang, *Unrestricted Warfare*, [w:] [http: defence and society.org](http://defenceand.society.org)
37. *Reader Zentrum Führung Gemeinsamer Operationen*, Führungsakademie der Bundeswehr, Hamburg 2000.
38. Roth G, *Der Vernichtungsgedanke im militärischen Denken bei Carl von Clausewitz und Graf Alfred von Schlieffen* [w:] *Operatives Denken bei Clausewitz, Moltke, Schlieffen und Manstein*, Freiburg im Breisgau 1988
39. Rühle V., *Sicherheitspolitik nach dem 11. September: Herausforderungen für die Außenpolitik*, Deutsch-französisches Seminar der Konrad Adenauer-Stiftung, Roquebrune, 22. November 2001
40. Schreadley R. L., *Sea Lords*, USNI Proceedings 1970 nr 8;
41. Schreadley R. L., *The Naval War in Vietnam 1950 - 1970*, USNI Pro-

ceedings 1971 nr 5.

42.Schulz George P., *Turmoil and Triumph: My Years as Secretary of State* (New York: Charles Scribners Sons, 1993), 227-234.

43.Stahel A., *Null-Verluste Strategie und virtueller Krieg*, Österreichische Militärische Zeitschrift 2002, nr 3.

44.Steele R. D., *New craft of the intelligence*, [w:] Special Report of the Institute of Strategic Studies, US Army, February 2002.

45.Tofler H i A., *Wojna i antywojna*, Warszawa 1997

46.Webster's Third New International Dictionary of English Language, Springfield 1981,

## ZAŁĄCZNIKI

## Załącznik 1

*Zagrożenia asymetryczne, a przyszły Czteroletni Przegląd Obrony (ang. Quadrennial Defense Review – QDR); Autor: Kenneth F. MCKENZIE Jr.*

### Rozdział 1 *Co to jest walka asymetryczna?*

- Definicja asymetrii
- Charakterystyka nierówności interesów
- Wola przeciwnika obiektem działań
- Osiąganie skutków strategicznych na każdym poziomie wojny
- Znaczenie skuteczności
- Dynamika odpowiedzi na zagrożenia
- Rozważania kulturowe;
- Reakcja na postrzegane zagrożenia USA;
- Końcowy przykład – wojna tankowców w Zatoce Perskiej
- Wnioski

### Rozdział 2 *Typologia asymetrii – co, kto i kiedy*

Co – skala potencjalnych zagrożeń asymetrycznych

- broń jądrowa (wykorzystanie taktyczne, operacyjne i strategiczne) oraz wnioski jej dotyczące;
- broń chemiczna (wykorzystanie taktyczne, operacyjne i strategiczne) oraz wnioski jej dotyczące;
- broń biologiczna (wykorzystanie taktyczne, operacyjne i strategiczne) oraz wnioski jej dotyczące;
- operacje informacyjne (wykorzystanie taktyczne, operacyjne i strategiczne) oraz wykorzystanie impulsu elektromagnetycznego dużej wysokości (ang. High- altitude electromagnetic pulse - HEMP);
- inne koncepcje operacyjne (wykorzystanie taktyczne, operacyjne i strategiczne);
- terroryzm;

Kto – aktorzy regionalni, „państwa zbójce” oraz aktorzy nie państwowi;

Kiedy – prawdopodobieństwo w fazach kryzysowych

Wnioski

### **Rozdział 3 *Spojrzenie w lustro: gdzie są słabości asymetryczne Stanów Zjednoczonych***

- Miara konwencjonalnej przewagi wojskowej
- Jakie są operacyjne pojęcia dotyczące zdolności zawarte we „Wspólnej wizji 2010” (ang. Joint vision 2010);
- Jakie słabości opisuje wspomniany dokument;
- Ocena dotycząca ojczyzny;
- Wyliczenie celów dotyczących ojczyzny;
- Poddanie USA analizom
- Wymiar ilościowy analiz dot. USA – gdzie są cele?
- Analiza potencjalnych słabości

### **Rozdział 4 *Kategoryzacja zagrożeń***

- Jakie jest dziesięć zagrożeń asymetrycznych?
- Wnioski

### **Rozdział 5 *Wariant trudności przeciwstawiania się zagrożeniom asymetrycznym***

- Inicjatywy bieżące: stan na dzień dzisiejszy
- Podsumowanie bieżących inicjatyw
- Poprawiając – rozpoczęcie od trzech założeń
- Rekomendacje polityczne
- Akcje dla zminimalizowania słabości;
- Działania dla zaakcentowania mocnych stron;
- Działania w celu zapobieżenia efektom dysproporcji;
- Opcja trudności?

## Rozdział 6 *Wnioski*

### Tabele:

1. Zależności asymetryczne w zakresie żywotnych i mało żywotnych interesów USA oraz przeciwnika
2. Konwencjonalne możliwości działań uniemożliwiających lub opóźniających przerzut sił USA
3. Konwencjonalne możliwości działań uniemożliwiających lub opóźniających inwazję sił USA
4. Podsumowanie środków utrudniających dostęp siłom USA
5. Kwestia czasu: prawdopodobne zastosowania asymetrii w trakcie poszczególnych faz kryzysu
6. Miara efektywności koncepcji zamieszczonych we „Wspólnej wizji 2010” oraz niektóre potencjalne asymetrie
7. Czym jest ojczyzna? Przełamywanie stereotypów
8. Zestawienie dziesięciu zagrożeń asymetrycznych

***ASYMMETRY (Z FM 3-0 OPERATIONS)***

4-109. Asymmetry concerns dissimilarities in organization, equipment, doctrine, capabilities, and values between other armed forces (formally organized or not) and US forces. JFCs arrange symmetrical and asymmetrical actions to take advantage of friendly strengths and enemy vulnerabilities, and to preserve freedom of action. Engagements are symmetric if forces, technologies, and weapons are similar; they are asymmetric if forces, technologies, and weapons are different, or if a resort to terrorism and rejection of more conventional rules of engagement are the norm. In one sense, there are always asymmetries between forces: differing circumstances lead to differing military structures. Asymmetry becomes very significant, perhaps decisive, when the degree of dissimilarity creates exploitable advantages. Asymmetric engagements can be extremely lethal, especially if the target is not ready to defend itself against the asymmetric threat. Asymmetry tends to decay over time as adversaries adapt to dissimilarities exposed in action. In a larger sense, asymmetric warfare seeks to avoid enemy strengths and concentrate comparative advantages against relative weaknesses. The following tactical and operational examples illustrate the dynamic nature of asymmetry.

4-110. Third Army forces in the Gulf War were equipped with second-generation thermal sights. Iraqi units depended upon older, far less capable active infrared and light amplification systems. In engagement after engagement, US, British, and French armor destroyed Iraqi units, who could only return ineffective fire. At the system level, the advanced armor on the US and British tanks resisted the occasional hit from Iraqi fire, while friendly rounds immediately destroyed their targets. At tactical levels, Army forces exploited asymmetry in terms of equipment and organization.

4-111. In 1999, Serbian forces in Kosovo faced unrelenting aerial bombardment by North Atlantic Treaty Organization (NATO) air forces. As the air operations intensified, NATO refined its strike techniques while the Serbs applied techniques learned by the Iraqis during the Gulf War. Over time, the Serbs became very proficient at using decoys and concealment. Although they were unable to prevent losses, Serbian units protected most of their ground combat systems from this asymmetric attack. Thus, the asymmetric advantage conferred by advanced air power over ground elements decayed over time.

4-112. At the operational level in the Gulf War, USCENTCOM exploited the inherent flexibility of sea power and amphibious assault to threaten the Iraqi forces in Kuwait with a major strike from the Persian Gulf. Lacking a navy, the only possible operational response by the Iraqi high command was to shift six

divisions to coastal defense. The coalition ground offensive enveloped and destroyed these Iraqi forces, which were fixed by the threat of amphibious assault.

4-113. The likelihood of asymmetric attack increases with the continued conventional dominance of US forces at sea, on land, in the air, and in space. Such attacks may only disrupt tactical activities briefly; however, the operational and strategic consequences, particularly in stability operations and support operations, may be far-reaching. In Beirut, Lebanon, in 1983, and again at Khobar Towers, Saudi Arabia, in 1996, massive truck bombs destroyed portions of US military compounds, with heavy loss of life. Both attacks demonstrated asymmetry in terms of equipment and values. In addition, each was a political act of terrorism taken against a military objective. The risks of asymmetry multiply with the threat of WMD.

4-114. Asymmetric attacks pose dilemmas to both friendly and enemy forces. Countering asymmetric attacks requires the disadvantaged side to alter rules of engagement, organization, doctrine, training, or equipment. The higher the echelon, the longer it takes to remedy an enemy asymmetric advantage. To reduce the vulnerability to asymmetric attacks and to minimize their effects, Army organizations, training, and equipment emphasize flexible employment in diverse situations. Protective measures, such as physical security and OPSEC, lessen the effects of asymmetry. A credible NBC defense capability at the tactical level deters the use of WMD. Commanders must anticipate asymmetries and take preventive measures that reduce adversary advantages. Commanders identify and exploit friendly capabilities that pose asymmetric challenges to the enemy force, even as Army forces act to counter hostile asymmetric threats. Asymmetric attacks pose dilemmas to both friendly and enemy forces. Countering asymmetric attacks requires the disadvantaged side to alter rules of engagement, organization, doctrine, training, or equipment. The higher the echelon, the longer it takes to remedy an enemy asymmetric advantage. To reduce the vulnerability to asymmetric attacks and to minimize their effects, Army organizations, training, and equipment emphasize flexible employment in diverse situations. Protective measures, such as physical security and OPSEC, lessen the effects of asymmetry. A credible NBC defense capability at the tactical level deters the use of WMD. Commanders must anticipate asymmetries and take preventive measures that reduce adversary advantages. Commanders identify and exploit friendly capabilities that pose asymmetric challenges to the enemy force, even as Army forces act to counter hostile asymmetric threats.

*Cykl: Studia z dziedziny asymetrii*

***WOJNY WEWNĘTRZNE – ponowne przemyślenie problemu oraz reakcje***

*(Raport specjalny Instytutu Studiów Strategicznych SL USA (ISS), wrzesień 2001; autor: Max G. Manwaring)*

### ***Streszczenie robocze***

Zakończenie Zimnej Wojny nie przyniosło końca konfliktom wewnętrznym lub regionalnym oraz korzystania z oczekiwanej dywidendy pokoju. Obecnie ponad połowa państw wspólnoty międzynarodowej znajduje się w obliczu z tym lub innym typem małych wojen asymetrycznych (np. partyzanckich). Działania powstańcze, wojny wewnętrzne oraz inne działania na małą skalę (ang. SSC – small-scale contingencies) są najbardziej prawdopodobnym typem konfliktu w ramach nowego porządku światowego. Jest prawie pewne, że wcześniej czy później, Stany Zjednoczone zostaną wciągnięte, pośrednio lub bezpośrednio w wiele z takich konfliktów. Ponadto jest pewne to, że żalosne wnioski wietnamskie wypaczają i zamazują amerykański sposób myślenia o partyzanckich walkach powstańczych. W rezultacie mamy do czynienia z sytuacją, w której nie są uwzględniane wnioski poziomu strategicznego po Wojnie Wietnamskiej i po setkach małych konfliktów, jakie wybuchły w ostatnich kilkunastu latach.

Te lekcje nie zostały jednak utracone dla nowych aktorów politycznych wyłaniających się na współczesnej wielobiegunowej arenie bezpieczeństwa globalnego. Ironią jest to, że strategie opracowywane z myślą o ochronie i rozwijaniu interesów przez licznych nowych graczy sceny politycznej są inspirowane myślą unikania lub niweczenia przeważających konwencjonalnych sił wojskowych w ramach istniejącego globalnego chaosu. Im większe zdolności bojowe

go, że istnieje potrzeba powrotu do spraw podstawowych. Fakt, że SZ USA nigdy nie zostały pokonane na polu walki w Wietnamie zaciemnia kolejny ważny fakt tej wojny. Chociaż siły amerykańskie nigdy nie przegrały bitwy, to w gruncie rzeczy Vietcong i jego Północnowietnamscy sojusznicy osiągnęli cele strategiczne, okazując się zwycięzcami. Amerykanie byli przekonani, że prowadzą wojnę o ograniczonym zasięgu przeciwko tradycyjnemu przeciwnikowi – ubranemu w czarne piżamy. Zagrożenie z jakim Południowy Wietnam oraz Stany Zjednoczone miały do czynienia nie było ani tradycyjne ani ograniczone. Raczej Vietcong, na innym poziomie i ubrany w swoje komiczne czarne piżamy – prowadził niekonwencjonalne przygotowania do przejęcia władzy w państwie.

Taka rzeczywistość zabiera nas z powrotem do miejsca, gdzie się wszystko zaczęło. Chodzi o odpowiedź na pytanie: „Jak Stany Zjednoczone mogły wygrać wszystkie bitwy w Wietnamie, lecz przegrać wojnę?” Odpowiedź jest natychmiastowa. Przywódcy amerykańscy nie potrafili zastosować w odniesieniu do tego konfliktu fundamentalnych zasad teorii wojskowej i strategii. Mówiąc precyzyjniej:

- oceny w zakresie natury konfliktu były niewłaściwe;
- zostało zignorowane i było niezrozumiałe środowisko strategiczne w ramach którego prowadzona była wojna;
- zasadnicze środki ciężkości nie były starannie lub stale oceniane, porządkowane według priorytetów i rozważane w kategoriach nie wojskowych (np. socjalno – politycznych);
- nie było doceniania prymatu uczciwości oraz moralnego uzasadnienia wspierania działań przeciw partyzanckich;
- te fundamentalne zasady nie zostały uwzględniane i postrzegane przez pryzmat strategiczny umożliwiający zrozumienie i prowadzenie wojny.

Decydujące znaczenie posiada unifikacja tych wniosków. Instrumenty potęgi narodowej muszą być zorganizowane, szkolone oraz wyposażone w obrębie możliwości budżetowych. Jednak takie działania muszą być poprzedzone jasnym i logicznym kierunkiem politycznym. Powinny ponadto być określone: struktura, role, zadania oraz strategia, mające zapewnić osiągnięcie określonych celów politycznych. Jest to fundamentalna zasada, obowiązująca dla współczesnych i przyszłych konfliktów, tak samo jak było to w przeszłości.

**Wnioski z 69 wojen wewnętrznych, toczonych od zakończenia II Wojny Światowej. Przejściowe „zasady” prowadzenia gry na arenie współczesnego bezpieczeństwa światowego.**

W połowie lat 80. praktycy oraz akademicy cenili jako ważne rozpoczęcie działań zmierzających do niwelowania tzw. syndromu wietnamskiego oraz zrozumienia różnic powodujących różnice w kwestii odnoszenia zwycięstw lub przegrywania asymetrycznych wojen partyzanckich. Zamiarem było zwiększenie możliwości odniesienia sukcesów we współczesnych i przyszłych konfliktowych sytuacjach wewnętrznych oraz wniesienia większego wkładu do ochrony i rozwijania narodowych interesów USA w warunkach rosnącego braku stabilności globalnej. Jednym z takich wysiłków, nigdy nie opublikowanym oficjalnie, było opracowanie zainicjowane w 1984 roku przez zastępcę szefa sztabu SL, generała Maxwella Thurmana.

Rezultaty większości prac naukowo-badawczych są dostępne w zbiorach Archiwum Bezpieczeństwa Narodowego w Waszyngtonie. Nie zawierają one żadnych rewelacji. Proponują strategię bezpieczeństwa oraz sposoby zarządzania zasobami w wymiarze narodowym i międzynarodowym. Ważne jest jednak, że badania wskazują na to iż każda skuteczna strategia przyjęta w okresie

ostatnich 50 lat i stosowana przez dowolną stronę konfliktu, brała pod uwagę następujące wymiary strategiczne, związane z kategoriami wojny wewnętrznej.

Zaliczyć do nich można:

- „wojnę sprawiedliwą” w celu ataku lub obrony w imię moralnego prawa do istnienia reżimu;
- bardziej tradycyjne policyjno-wojskowe „wojny z wystrzałami” między walczącymi stronami;
- „wojny” w celu odizolowania walczących stron od ich źródeł zaopatrzenia wewnętrznego i zewnętrznego;
- blisko związane z powyższym „wojny na utrzymanie kursu”, oznaczające udzielania stałego i długotrwałego wsparcia sojuszniczego;
- „wojny” wywiadów i informacyjne;
- „wojny” dla unifikacji wielostronnych, wielowymiarowych oraz wielu organizacyjnych elementów w jeden skuteczny wysiłek.

Należy zauważyć, że zastosowanie tych dynamicznych elementów w jedną skuteczną strategię obejmuje realną wizję strategiczną oraz politykę bazującą na fundamentalnych zasadach przedstawionych w poprzedniej sekcji.

### **Przyszłość asymetrycznych wojen wewnętrznych. Niektóre znaki na drodze ku przyszłości**

Ponieważ nawet rozsądne siły zbrojne muszą przygotować się na wojnę konwencjonalną, oznaczoną jako małego prawdopodobieństwa lecz wysokiego ryzyka, jest wysoce możliwe, że Prezydent oraz Kongres Stanów Zjednoczonych będą w przyszłości wymagali uczestnictwa w małych konfliktach we-

wewnętrznych o charakterze partyzanckim. Takie wojny będą nosiły nowe nazwy, posiadały nowe motywy oraz nowe poziomy gwałtowności – będzie stanowiło to tylko nowe elementy starego problemu. Tym niemniej, czy będą one nazywane „Wojnami o dzbanek na herbatę”, „Wojnami zakamuflowanymi”, „Wojnami bez granic”, „Operacjami innymi niż wojna” lub jeszcze inaczej, przyszłe wojny partyzanckie mogą być określane przez najmniejszy wspólny nominalny motyw. Jako mające związek z przymusem, obojętnie czy są one oceniane jako „powstania duchowe”, „powstania komercyjne” lub jeszcze inne, wojny partyzanckie stanowią zorganizowaną formę użycia siły lub przymusu nie militarne, względnie groźby użycia siły w celu stawiania oporu, dokonania zmian lub przewrotu urzędującego rządu oraz doprowadzenie do zmian politycznych.

Jest niekiedy strasznie pomyśleć o implikacjach jaki mogą pociągnąć za sobą działania partyzanckie z użyciem broni masowego rażenia, środków walki elektronicznej oraz informacyjnej. W ten oto sposób, chociaż obecne i przyszłe konflikty asymetryczne mogą zastawiać różne pułapki, należy pamiętać o wnioskach z przeszłości. Najnowsze doświadczenia można widzieć przez perspektywę toczących się obecnie konfliktów. Oznacza to:

- moralna legitymacja pozostaje najważniejszą zasadą okresu od zakończenia II Wojny Światowej. Można tu wymienić jako przykłady problem Kurdów w Iraku, Iranie, Turcji i Rosji od około 1961 roku do dnia dzisiejszego; Sierra Leone od 1991 roku; Front Wyzwolenia Islamskiego w Algierii od 1992; a także Czeczenia od 1999 roku;
- adekwatne użycie siły wojskowej stanowi ciągle zasadniczy element w określaniu sukcesów lub porażek w działaniach przeciw partyzanckich. Charakterystyczna jest nieadekwatność ciężkiego uzbrojenia oraz tradycyjnego szkolenia w wysiłkach strony peruwiańskiej wobec ugrupowania Świetlisty Szlak oraz w przypadku

Etiopii;

- logiczna potrzeba izolowania walczących stron od źródeł zaopatrzenia jest oczywista w szeregu przypadków wojen toczonych obecnie. Przykład stanowią Kolumbia i Czeczenia. W Kolumbii sojusz partyzancki obejmujący również handlarzy i przemytników narkotyków wspiera hojnie bojowników zapewniających ochronę operacji narkotykowych. W Czeczenii oraz wcześniej w Afganistanie, wojna przeciwko dominacji rosyjskiej nie byłaby możliwa bez znaczącej pomocy zewnętrznej innych państw oraz politycznych aktorów pozarządowych;
- w związku z tym, potrzeba „pozostawania na kursie” utrzymuje się. Bez zewnętrznej pomocy i wsparcia wewnętrznego, IRA nie mogłaby skutecznie funkcjonować w Irlandii Północnej. Podobnie, Kurdowie z Bliskiego Wschodu nie byłiby w stanie prowadzić akcji na rzecz wyzwolenia narodowego;
- wywiad i informacja stają się jeszcze bardziej ważne niż kiedykolwiek dla odniesienia sukcesu lub porażki we współczesnej wojnie partyzanckiej. Niektórzy spierają się o to, czy niepowodzenie operacji USA i ONZ stabilizujących pokój w Somalii było skutkiem braku właściwych źródeł osobowych. Z drugiej strony, jako jedyny przykład, kampanie informacyjne stanowiły klucz do sukcesu powstańców ruchu Zapatystów w Meksyku;
- jedność wysiłku stanowi ostatnią zasadę o jakiej będzie tutaj mowa. Wystarczy stwierdzić, że wiele problemów operacji pod egidą ONZ w Kongu (UNOC), operacji ONZ w Somalii (UNOSOM II), operacji ONZ w byłej Jugosławii oraz działań NATO w Bośni i Kosowie wypływa z braku jedności wysiłków różnych uczestni-

ków.

Tak samo jak w przeszłości, czynniki te znajdują swój wyraz w dowolnej strategii i faworyzują sukces. W przypadku braku jednego elementu, lub obecności w słabej formie, prawdopodobieństwo odniesienia sukcesu jest minimalne.

### **Dwie zaawansowane reguły strukturalne odnoszenia sukcesu na globalnej arenie bezpieczeństwa**

Dwie charakterystyki asymetrycznych zagrożeń partyzanckich zostały określone jako szczególnie znaczące. Po pierwsze, planiści obronni dnia dzisiejszego nie mogą dokładnie wiedzieć jaki rodzaj zagrożenia pojawi się i jakie działanie może okazać się skuteczne. Po drugie, skuteczność zagrożeń asymetrycznych odnoszących skutek, prędzej czy później będzie zmniejszała się, w miarę dopasowywania się do nich. Niektórzy twierdzą, że dzięki maksymalizacji koncepcyjnej, organizacyjnej zdolności adaptacyjnej oraz elastyczności, Stany Zjednoczone mogą zapewnić sprostanie powstającym zagrożeniom asymetrycznym, przyspieszając proces dzięki któremu zagrożenie staje się nieznaczne lub nieskuteczne. Inaczej mówiąc, w okresie płynności strategicznej oraz asymetrii tak jak to ma miejsce dzisiaj, aktor polityczny opracowujący nowe koncepcje i unifikujący strukturę organizacyjną, będzie to robił lepiej i szybciej niż przeciwnik osiągnie zdecydowaną przewagę.

Biorąc pod uwagę realia dnia dzisiejszego, możliwość niepowodzenia w przygotowaniu się na małą wojnę (np. partyzancką) jest niezaprzeczalna. Przy najmniej są dwa zasadnicze imperatywy kulturalne i organizacyjne:

- **Ocena przywódcy.** W tym kontekście występuje kilkanaście zasadniczych wymagań edukacyjnych i kulturalnych dotyczących

modyfikacji szablonów myślenia kategoriami Zimnej Wojny i rozwijania ocen przywódczych wymaganych dla skutecznego sprostania sytuacjom wojen wewnętrznych: kompleksowym, zdominowanym politycznie, wielowymiarowym, wielo kulturowym. Studiowanie wojen konwencjonalnych zawsze służyło jak zasadnicze przygotowywanie się przywódców związanych z wojną. Studiowanie „niekonwencjonalnych” wojen asymetrycznych jest nie mniej ważne.

- **Jedność wysiłku.** Działania na dowolnym poziomie osiągną przejrzystość strategiczną oraz maksymalną efektywność w rezultacie zintegrowania planowania poziomego i pionowego oraz właściwej implementacji od samego początku. Oznacza to zintegrowanie horyzontalnego planowania politycznego (np. wielonarodowego) oraz operacji z pionowym narodowym planowaniem polityczno-wojskowym (np. interagencyjnym w USA) i operacji. Osiągnięty zostaje efekt synergizmu w uzyskiwaniu uzgodnionej wizji politycznej. Są to dwa zasadnicze mechanizmy organizacyjne niezbędne dla eliminowania „strategicznej dwuznaczności”, „działań ad-hoc” oraz „ślimaczenia się działań”.

## **Wnioski**

To są wnioski, które należało wyciągnąć z doświadczeń USA w Wietnamie oraz analizy dużej liczby ostatnich przypadków relatywnie małych wojen (np. partyzanckich). Wartość idei lub „reguł” wynikających z tych doświadczeń osadza się na ich przydatności jako koncepcyjne ramy, w których można umieszczać dane pochodzące ze specyficznych sytuacji oraz je rozumieć. Jeśli przywódcy amerykańscy i innych państw uważają te idee nie tylko jako zasady,

lecz traktują je na serio, mogą być wtedy zdolni do przetransponowania odwagi na polu walki, przewagi logistycznej oraz sukcesów taktycznych w zwycięstwo strategiczne na obecnej i przyszłej arenie globalnego bezpieczeństwa asymetrycznego.

*Tłumaczenie robocze: kmdr Piotr Gawliczek*

