SILNE I SŁABE STRONY KONCEPCJI DZIAŁAŃ SIECIOCENTRYCZNYCH

Janusz Kręcikij

Wojskowa Akademia Techniczna

Streszczenie. Zjawisko organizowania przestrzeni informacyjnej na potrzeby sił zbrojnych istnieje już od kilkunastu lat, i trend ten wciąż się nasila. Sprzyjają temu zarówno osiągnięcia technologii informacyjnych, jak i wyniesione z praktycznych zastosowań i rzeczywistych doświadczeń przekonanie, że technologie te mogą i powinny być głównym czynnikiem sukcesu współczesnych i przyszłych działań zbrojnych oraz szeroko rozumianego bezpieczeństwa narodowego. W połączeniu z tworzoną od kilku lat koncepcją działań sieciocentrycznych (Network Centric Warfare – NCW), wykorzystującą wiedzę zgromadzoną w sieciach internetowych i centrycznych do formowania i stosowania wielorodzajowej siły, działania zbrojne mogą się stać – i stają – nieporównywalnie bardziej efektywne. W pewnym uproszczeniu działania sieciocentryczne można opisać jako bazującą na przewadze informacyjnej koncepcję, według której wzrost siły bojowej jest generowany poprzez połączenie w sieć informacyjną sensorów, decydentów i systemów walki w celu osiągnięcia wspólnej świadomości, zwiększenia szybkości dowodzenia oraz tempa operacji, zwiększenia skuteczności uzbrojenia, odporności na uderzenia przeciwnika i stopnia synchronizacji działań. Zatem działania sieciocentryczne przekładają przewagę informacyjną na siłę bojową poprzez wydajne połączenia dysponujących wiedzą różnych jednostek organizacyjnych na polu (w przestrzeni) walki.

Czy jednak wspomniana koncepcja stanowi idealne panaceum na wszelkie wymagania współczesnych i przyszłych konfliktów i zagrożeń? Czy ma jakieś istotne słabe strony? A jeśli tak, to czy siła zalet jest w stanie zniwelować negatywne skutki ewentualnych wad lub niedociągnięć? Warto zatem zidentyfikować wyróżniki NCW, aby można było każde konkretne działanie określić terminem „ sieciocentrycznego" lub też nie – zakwalifikować do działań militarnych typowych dla ery przemysłowej. Wszystko to po to, aby realne stało się podjęcie próby określenia ewentualnych słabych stron koncepcji i w konsekwencji określenie zagrożeń z nich wynikających.

Wydaje się bowiem, że sieciocentryzm jako sposób prowadzenia działań (czy też szerzej – zarządzania bezpieczeństwem) charakteryzuje się licznymi i niezaprzeczalnymi zaletami, tworzącymi warunki do zdobycia i utrzymania przewagi w przestrzeni walki przy relatywnie niskich stratach i dużej szybkości działania. Jednocześnie nie można całkowicie lekceważyć słabych stron poruszanej koncepcji, gdyż takie po prostu są – jak w każdej innej wizji czy sposobie rozwiązywania sytuacji problemowych. Nie jest to z pewnością podstawa do negowania, odrzucania czy też lekceważenia NCW. Błędem byłoby jednak traktowanie jej jako swego rodzaju „świętego Graala". We współczesnym świecie, w dobie wysoce zintegrowanego i systemowego podejścia do problematyki bezpieczeństwa narodowego i międzynarodowego, sieciocentryzm pozostanie jego bardzo istotnym, ale jednym z wielu, filarem.

Truizmem byłoby stwierdzenie, że zjawisko organizowania przestrzeni informacyjnej na potrzeby sił zbrojnych już istnieje. Tak jest i trend ten wciąż się nasila. Sprzyjają temu zarówno osiągnięcia technologii informacyjnych, jak i wyniesione z praktycznych zastosowań i rzeczywistych doświadczeń przekonanie, że technologie te mogą i powinny być głównym czynnikiem sukcesu współczesnych i przyszłych działań zbrojnych. W połączeniu z tworzoną od kilku lat koncepcją działań sieciocentrycznych – wykorzystania wiedzy zgromadzonej w sieciach internetowych i centrycznych do formowania i stosowania wielorodzajowej siły, adekwatnie do sytuacji na polu walki, działania zbrojne mogą się stać nieporównywalnie bardziej efektywne. Nie wchodząc w tym miejscu w zbędne szczegóły, działania sieciocentryczne można opisać (ale nie zdefiniować!) jako bazującą na przewadze informacyjnej koncepcję prowadzenia działań, według której wzrost siły bojowej jest generowany poprzez połączenie w sieć informacyjną sensorów, decydentów i systemów walki (rys. 1) w celu osiągnięcia wspólnej świadomości, zwiększenia szybkości dowodzenia oraz tempa operacji, zwiększenia skuteczności uzbrojenia, odporności na uderzenia przeciwnika i stopnia synchronizacji działań. Zatem działania sieciocentryczne przekładają przewagę informacyjną na siłę bojową poprzez wydajne połączenia dysponujących wiedzą różnych jednostek organizacyjnych na polu (w przestrzeni) walki[1].

Istniejąca literatura fachowa stosuje do opisu działań tego rodzaju różne terminy, np.:

- network centric warfare,
- net-centric operations,
- network centric war.

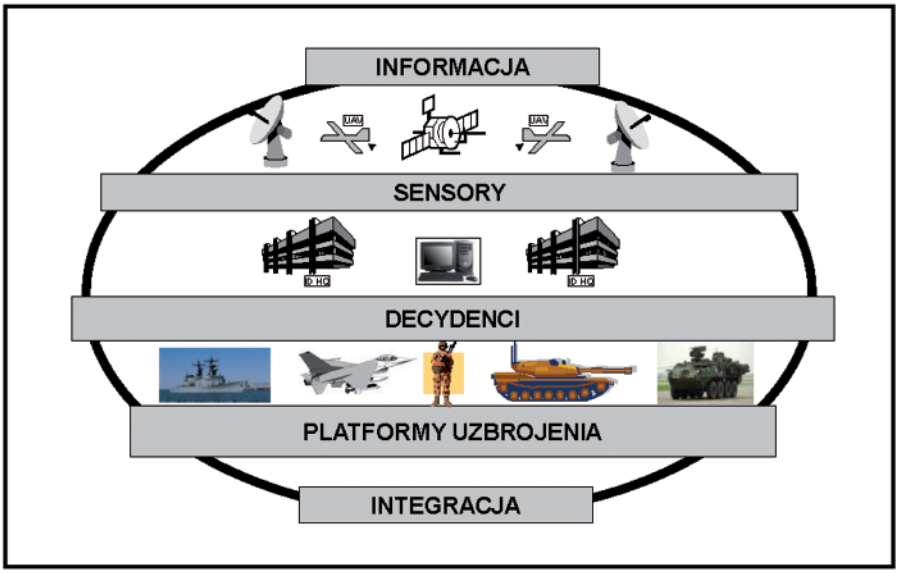
Spotkać można także określenia w rodzaju:

- walka zbrojna ery cyfrowej,
- walka wielowymiarowa,
- operacja połączona w środowisku rozproszonym,
- rozległa operacja połączona,
- połączone działania sił rozproszonych.

Można zatem przyjąć, iż tak zwana sieciocentryczność jest nie tylko koncepcją działań zbrojnych, lecz także projektem zarządzania systemem dowodzenia (w tym informacyjnym) sił zbrojnych oraz wspólną ideą dla programu ich dalszego rozwoju. Jeżeli przyjmie się, że w wyniku takiej transformacji siły zbrojne będą przekształcane (zgodnie z koncepcją sieciocentryczności) w organizację zdolną świadczyć usługi w zakresie militarnego niwelowania zagrożeń stabilizacji i bezpieczeństwa w skali globalnej, to ich strategiczna reorientacja (zmiana doktryny) będzie musiała uwzględniać także reorientację organizacyjną. Jeżeli taki jest rzeczywiście kierunek zmian, oznacza to, iż

[1] Por. Z. Maślak, *Informacje w obronie powietrznej. Potrzeby, wymagania, zagrożenia*, PWLiOP nr 7/2002, Warszawa 2002, s. 24.

w ramach transformacji niezbędne jest określenie długofalowych celów do osiągnięcia, wynikających z nich zadań oraz przewidywalnych skutków (konsekwencji).



Rys. 1. Istota koncepcji działań sieciocentrycznych – systemowa integracja decydentów, sensorów i platform uzbrojenia. Źródło: opracowano na podstawie prezentacji: *C31 Systems as Fundament fot Network Enabled Capabilities – The German Vision*

Rezultaty analiz dostępnych informacji tak z działań sojuszniczych, jak i narodowych pozwalają na stwierdzenie, jako swego rodzaju prawidłowości, iż wysiłki w tym zakresie koncentrowane są na:

- tworzeniu „sieci" informacyjnej, która połączy systemy rażenia, sensory i systemy dowodzenia, oraz zbudowaniu infrastruktury informatycznej pozwalającej na urealnienie struktury sił „sieciocentrycznych". Sieć ta ma w założeniach zapewniać również interoperacyjność informacyjną z potencjalnymi sojusznikami i koalicjantami;
- badaniu nowych technologii w zakresie sensorów pod względem ich możliwości współdziałania ze środkami rażenia i kierowania działania tych środków, zakres badań obejmuje przy tym: bezpilotowe środki latające, radary wysokiej częstotliwości, środki obserwacji rozmieszczone w przestrzeni kosmicznej oraz różnego rodzaju sensory naziemne;
- określeniu co, mając na uwadze człowieka-żołnierza, powinno ulec zmianie w zakresie doktryn, organizacji, kształcenia i szkolenia;
- przyspieszeniu procesu zmian i wprowadzaniu nowych technologii poprzez ciągłą i bliską współpracę na linii siły zbrojne–przemysł obronny;

- wdrażaniu podejścia systemowego, polegającego na założeniu, iż „usieciowienie" nie może ograniczać się tylko do wszystkich rodzajów sił zbrojnych, ale dla maksymalnego wykorzystania potencjalnych możliwości powinno objąć także elementy takie jak: doktryna, organizacja, szkolenie, inne moduły systemu bezpieczeństwa (Straż Graniczna, Policja, sojusznicy) tak, aby maksymalnie zintegrować wszystko to, co ma wpływ na potencjał obronny i bezpieczeństwo narodowe kraju;
- zapewnieniu wspólnej świadomości sytuacyjnej oraz, dzięki temu, zwiększeniu możliwości pełnego wykorzystania myśli przewodniej dowódcy w procesie dowodzenia;
- umożliwieniu pełnego dostępu do informacji, zakładając, iż wszyscy beneficjenci systemu mogą wprowadzać informacje do przestrzeni informacyjnej, pobierać je i wymieniać,
- wykorzystaniu efektu synchronizacji, który powinien zapewnić właściwe rezultaty działania poprzez maksymalizację pozytywnych skutków działań połączonych;
- stworzeniu możliwości wykonywania szerokiego spektrum zadań przez osiągnięcie zdolności do szybkiego generowania (formowania) sił i odpowiedniego do potrzeb konfigurowania sił zadaniowych;
- doprowadzeniu systemu dowodzenia do poziomu umożliwiającego sprawowanie dowodzenia w dynamicznych, ciągłych i trudno przewidywalnych działaniach;
- zapewnianiu odpowiedniego poziomu bezpieczeństwa informacji w przestrzeni informacyjnej.

Zaprezentowane główne kierunki działania wskazują również na bardzo interesujący i szczególnie aktualny aspekt wykorzystania zdolności sieciocentrycznych. Jest nim dążenie do maksymalnej integracji sił zbrojnych ery informacyjnej ze wszystkimi organami państwa, których działalność składa się na szeroko rozumiane bezpieczeństwo narodowe.

Czy jednak analizowana koncepcja stanowi idealne panaceum na wszelkie wymagania współczesnych i przyszłych konfliktów i zagrożeń? Czy ma jakieś istotne słabe strony? A jeśli tak, to czy siła zalet jest w stanie zniwelować negatywne skutki ewentualnych wad lub niedociągnięć? Aby odpowiedzieć na te pytania, rezultaty rozważań zostały zgrupowane w dwóch częściach. W pierwszej zawarto syntetyczne rezultaty badań ukierunkowanych na identyfikację wyróżników Network Centric Warfare. Zasadniczym celem prowadzonych badań i rozważań było zidentyfikowanie minimalnych warunków, które (w kontekście prowadzonych działań) muszą być spełnione (z innego niż techniczny punktu widzenia), aby można je było określić terminem „działań sieciocentrycznych", a tym samym odróżnić od działań militarnych typowych dla ery przemysłowej. Część druga koncentruje się na wcześniej

wspomnianych ewentualnych słabych stronach koncepcji, poszukując zagrożeń z nich wynikających.

Już wyniki badań wstępnych pozwoliły na konstatację, iż istniejące definicje działań sieciocentrycznych, funkcjonujące w dostępnej literaturze, nie należą do zbyt precyzyjnych. Tym bardziej celowe okazało się zidentyfikowanie konkretnych wyróżników NEC jako najprostszej drogi do określenia, czym są, a czym nie są tego rodzaju działania i zdolności.

Wyniki analizy literatury przedmiotu dają podstawę do stwierdzenia, iż wyróżnia się następujące zasady działań sieciocentrycznych. Są to[2]:

1. Dążenie do zdobycia w pierwszej kolejności przewagi informacyjnej.
2. Dostęp do informacji pochodzącej z różnych źródeł, zgodnie z potrzebami i specyfiką poziomu dowodzenia/rodzaju wojsk i sił zbrojnych.
3. Szybki cykl dowodzenia (Command and Control Cycle – C2 Cycle).
4. Samosynchronizacja.
5. Nielinearne pole (przestrzeń) walki.
6. Rozproszenie sił (rozumiane jako przeciwieństwo fizycznego i geograficznego zmasowania sił i środków).
7. Masowe użycie sensorów.
8. „Wykorzystywanie okazji".
9. Zmniejszenie różnic pomiędzy poziomami działań zbrojnych oraz granic pomiędzy rodzajami sił zbrojnych i wojsk.

Pod pojęciem przewagi informacyjnej rozumie się zazwyczaj „…zdolność do zbierania, gromadzenia, przetwarzania, analizowania i dystrybucji informacji, utrzymania nieprzerwanego strumienia ich przepływu oraz pełnego jej wykorzystania, przy jednoczesnym posiadaniu możliwości wzbraniania przeciwnikowi prowadzenia podobnej działalności informacyjnej…"[3]. W takim kontekście istotą analizowanej zasady jest konsekwentne zdobywanie przewagi poprzez zapewnienie terminowości, dokładności oraz rzeczowości zdobywanej informacji. W rezultacie działania tego rodzaju powinny zapewnić:

- wymuszenie zwiększenia potrzeb informacyjnych przeciwnika przy jednoczesnym zmniejszeniu jego możliwości w zakresie dostępu do niezbędnych informacji oraz redukcję wiarygodności danych przez niego zdobytych;
- zapewnienie siłom własnym ciągłego dostępu do informacji poprzez właściwie zorganizowaną „przestrzeń informacyjną" oraz skuteczną ochronę własnych systemów informacyjnych, w tym sensorów;

[2] *The Implementation of Network – Centric Warfare*, Office of Force Transformation Office of the Secretary of Defense, Washington 2004, s. 8-10.

[3] JP 3-13 *Joint Doctrine for Information Operations*, Department of Defense, Washington 1998.

– zmniejszenie własnych potrzeb informacyjnych, szczególnie w zakresie ich objętości, poprzez wzrost zdolności pełnego wykorzystania usług wszystkich własnych „zbieraczy" danych.

Zasadniczym wymaganiem wynikającym z zasady dostępu do informacji pochodzącej z różnych źródeł jest zapewnienie pewnego, prostego i bezpiecznego dostępu do informacji dla wszystkich potrzebujących jej elementów własnego ugrupowania bojowego, w celu zapewnienia wymaganego poziomu wspólnej świadomości sytuacji operacyjnej/taktycznej. Wynikają z tego następujące potrzeby:

– stworzenie współdziałającej „sieci sieci", zasilanej w sposób ciągły wysoką jakościowo informacją ze wszelkich możliwych źródeł (tak rozpoznawczych, jak i wszystkich innych, które są dostępne);
– beneficjenci dostępnych informacji muszą być jednocześnie jej dostarczycielami, odpowiedzialnymi za wprowadzanie nowych danych bez opóźnień, zaś dostęp do informacji nie może być zależny od fizycznego położenia sił w przestrzeni walki;
– powszechny dostęp (własnych użytkowników) do informacji nie może kolidować z wymaganym właściwym poziomem ochrony sieci i informacji.

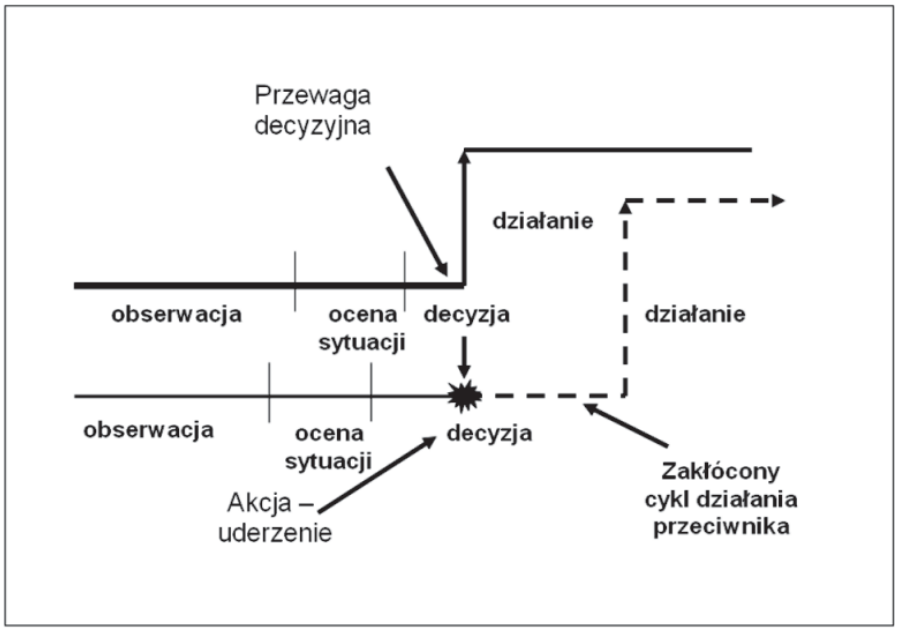
Istotą **szybkiego cyklu dowodzenia** jest zdolność wojsk własnych do wykorzystania przewagi informacyjnej poprzez przekształcenie jej w umiejętność tak szybkiej realizacji procesów i procedur dowodzenia, jaka byłaby niemożliwa przy wykorzystaniu typowych rozwiązań. Jednocześnie nie powinien zostać zwiększony poziom ryzyka decyzyjnego. Przy takim założeniu „szybki" cykl dowodzenia powinien:

– doprowadzić do przełożenia przewagi informacyjnej na przewagę decyzyjną, a w konsekwencji – na przewagę efektów działania,
– stworzyć pożądaną przez dowódców „od zawsze" możliwość działania „wewnątrz" cyklu decyzyjnego przeciwnika (rys. 2),
– zmniejszyć swobodę działania przeciwnika w zakresie wyboru alternatywnych opcji działania, zapewniając jednocześnie wojskom własnym możliwość wariantowania sposobów rozwiązywania problemów decyzyjnych.

Właściwe zrozumienie istoty „samosynchronizacji" (*selfsynchronization*) wymaga, dla uniknięcia nieporozumień leksykalnych i niepotrzebnego tworzenia nowych terminów specjalistycznych, wyjaśnienia różnic i zależności pomiędzy następującymi, już funkcjonującymi terminami:

– współdziałanie (*co-operation*),
– koordynacja (*co-ordination*),
– synchronizacja (*synchronization*).

Nie dążąc dla uproszczenia do cytowania licznych (i różnych) definicji w tych obszarach problemowych, celowe wydaje się wskazanie wyróżników przedsięwzięć kryjących się pod wymienionymi trzema terminami.



Rys. 2. Istota działania „wewnątrz" cyklu decyzyjnego przeciwnika. Źródło: opracowanie na podstawie J. Krecikij, *Działania siecioscentryczne. Wybrane problemy*

Zatem wyróżnikami współdziałania są:
- brak stosunku podległości pomiędzy podmiotami,
- działania uzgadniane dobrowolnie, jako samodzielne kompetencje stron,
- działania podejmowane do realizacji celu głównego uczestników.

Z kolei wyróżniki koordynacji określić można następująco:
- hierarchiczna zależność pomiędzy podmiotami koordynacji,
- realizowanie koordynacji na potrzeby wykonania określonego zadania w przestrzeni walki,
- koordynacja organizowana i kierowana jest przez szczebel nadrzędny dla realizacji celów pośrednich.

Wyróżniki synchronizacji:
- zależność organizacyjna lub funkcjonalna podmiotów synchronizacji,
- realizacja celów uczestników walki w czasie operacyjnym – czynnik czasu wyróżnikiem zasadniczym.

Jeżeli zatem pod pojęciem „samosynchronizacji" jako zasady NCW rozumie się zwiększenie zdolności jednostek najniższych szczebli dowodzenia do działania niemal samodzielnie (w tym możliwości samodzielnego dostosowywania ich zadań do sytuacji), korzystając z dostępu do informacji (bazując jednak ciągle na myśli przewodniej dowódcy), oraz uzgadnianie wspólnych działań z „sąsiadami", niezależnie

od ich organizacyjnej podległości i fizycznej odległości, to przedsięwzięcia takie w polskiej terminologii wojskowej (*vide* wymienione powyżej wyróżniki) określić należy po prostu jako **współdziałanie**. Właściwe wykorzystanie tej możliwości i jednocześnie zdolności ma zapewnić:

- zwiększenie inicjatywy podwładnych, a tym samym zwiększenie tempa operacyjnego oraz zdolności do terminowego reagowania na zmiany w sytuacji,
- pełniejsze wykorzystanie zalet wynikających z zasady działania zgodnie z myślą przewodnią dowódcy, nie zaś sztywnym planem,
- możliwość błyskawicznego wykorzystywania na swoją korzyść gwałtownych zmian w sytuacji („wykorzystywanie nadarzających się okazji") oraz eliminację sztywnego, tradycyjnego podziału działań (operacji) na kolejne, ściśle określone fazy.

Głównym założeniem nielinearnego pola (przestrzeni) walki jest ostateczne przejście od działań o charakterze linearnym (rozumianych jako starcia wzdłuż ciągłej linii frontu i w bezpośredniej styczności z przeciwnikiem) do nielinearnych. Zakłada się zatem:

- przejście od fizycznego panowania nad terenem do kontroli nad nim w taki sposób, aby uniemożliwić jego wykorzystanie przez przeciwnika, przy równoległym utrzymaniu zdolności do generowania niezbędnego potencjału bojowego we właściwym miejscu i czasie,
- nielinearność działań zarówno w przestrzeni jak i w czasie, przy zachowaniu pełnej zdolności do (na żądanie – zgodnie z potrzebami) nasycenia przestrzeni walki niezbędnym potencjałem bojowym,
- zwiększenie stopnia integracji planowania i realizacji przedsięwzięć związanych z rozpoznaniem, działaniami bojowymi i wsparciem logistycznym, co powinno umożliwić osiąganie założonych efektów operacyjnych oraz poprawić zdolność do uzyskiwania czasowej przewagi, niezależnie od rozproszenia sił na dużym obszarze.

Rozproszenie sił (przeciwieństwo masowania). Zakłada się, że typowe dla klasycznych działań geograficzne (przestrzenne) rozumienie koncentracji (masowania) sił i środków musi zostać zastąpione koncentracją wysiłku na efektach (zamierzonych skutkach) działań. W takiej sytuacji:

- informacja, a w konsekwencji przewaga informacyjna, używana będzie dla osiągnięcia założonych skutków, co powinno pozwolić na zmniejszenie do minimum niezbędnej fizycznej koncentracji sił i środków w określonym rejonie,
- zwiększone zostanie tempo operacyjne, co utrudni przeciwnikowi skuteczne przeciwdziałanie posunięciom wojsk własnych.

Masowe użycie sensorów w swej istocie sprowadza się do szerokiego stosowania sensorów działających w sieci (przestrzeni) informacyjnej, rozmieszczanych

w różnych odległościach od sił własnych (platform bojowych), które zapewnią dopływ informacji niezbędnej dla osiągania założonych efektów operacyjnych. Takie wykorzystanie sensorów na niespotykaną dotąd skalę ma umożliwić:

- bardziej intensywną i przez to skokowo bardziej skuteczną działalność rozpoznania,
- stworzenie i utrzymanie warunków do wykorzystywania przewagi informacyjnej,
- wykorzystanie każdej platformy uzbrojenia jako sensora, począwszy od pojedynczego żołnierza, a na satelitach skończywszy (ang. *each platform is a sensor*).

Zasada „wykorzystywania okazji" sprowadza się do nabycia umiejętności wykorzystania pozytywnych skutków stosowania wszystkich innych zasad, w celu uzyskania zdolności sił własnych (głównie w aspekcie umiejętności dowódców) do szybkiej identyfikacji, adaptowania na swoje potrzeby i przekształcania we własne silne strony każdej zmiany w sytuacji, nawet jeśli konkretne wydarzenie w przestrzeni walki zostało zaplanowane i jest sterowane przez przeciwnika.

Istotą ostatniej zasady: zmniejszenia różnic pomiędzy poziomami działań zbrojnych oraz granic pomiędzy rodzajami sił zbrojnych i wojsk jest eliminacja formalnych i proceduralnych różnic pomiędzy rodzajami sił zbrojnych, w celu umożliwienia prowadzenia działań połączonych na możliwie najniższych szczeblach dowodzenia. Sprowadzenie „połączoności" na poziom dziś niespotykany ma ułatwić osiąganie szybkich i zdecydowanych efektów dzięki maksymalnemu wykorzystaniu zjawiska synergii. Cel ten ma być osiągnięty poprzez:

- zwiększenie zbieżności (podobieństwa) w szybkości przemieszczania, rozmieszczania i działania poszczególnych rodzajów sił zbrojnych,
- eliminację różnic proceduralnych (dotyczących np. organizacji, przemieszczania, rozmieszczania, zasilania) oraz funkcjonalnych (różnic w zasadach działań bojowych/operacyjnych, rozpoznania, funkcjonowania logistyki) rodzajów sił zbrojnych,
- zmniejszenie różnic strukturalnych, co jest warunkiem koniecznym stworzenia możliwości prowadzenia działań połączonych, nawet na poziomie kompanii/baterii/klucza lotniczego/okrętu.

Przeprowadzona, z operacyjnego punktu widzenia, szczegółowa analiza zasad NCW nie daje jednakże odpowiedzi na sformułowane wcześniej pytanie zasadnicze: co wyróżnia działania sieciocentryczne wśród działań zbrojnych typowych dla ery przemysłowej? Główną przyczyną takiej sytuacji jest fakt, iż niektóre z przedstawionych powyżej zasad odnieść można do sposobów działań już obecnie (a często i w przeszłości) stosowanych. Dogłębne rozpatrzenie istoty każdej z zasad pozwala jednakże na stwierdzenie, że za rzeczywiste wyróżniki działań/zdolności sieciocentrycznych uznać można zasady oznaczone numerami 2, 4, 6, 7 i 9. Istota tych wyróżników zobrazowana została w tabeli 1.

Tabela 1

Wyróżniki NCW w stosunku do działań militarnych ery przedinformacyjnej („klasycznych")

Działania typu NCW	**Działania typu „klasycznego"**
Powszechny dostęp do informacji wiarygodnej, terminowej i dokładnej.	Informacje zdobywane w sposób tradycyjny, czasochłonny, nieterminowy i niedokładny.
Samosynchronizacja (współdziałanie).	Synchronizacja organizowana przez szczebel nadrzędny.
Rozproszenie sił, skupianie efektów, a nie sił i środków.	Koncentracja sił i środków.
Masowe użycie sensorów (każdy element NCW ma być sensorem, od żołnierza do satelity).	Tradycyjne użycie sensorów, zwykle ściśle związanych z platformami uzbrojenia i obsługą.
Zacieranie granic pomiędzy poziomami działań, rodzajami SZ i wojsk.	Formalny i doktrynalny podział na rodzaje wojsk i SZ, sztywna systematyka poziomów działań.

Źródło: J. Kręcikij, *Działania sieciocentryczne. Wybrane problemy*

Pozostałe z wymienionych zasad trudno postrzegać jako wyróżniki działań/zdolności NCW, ponieważ:

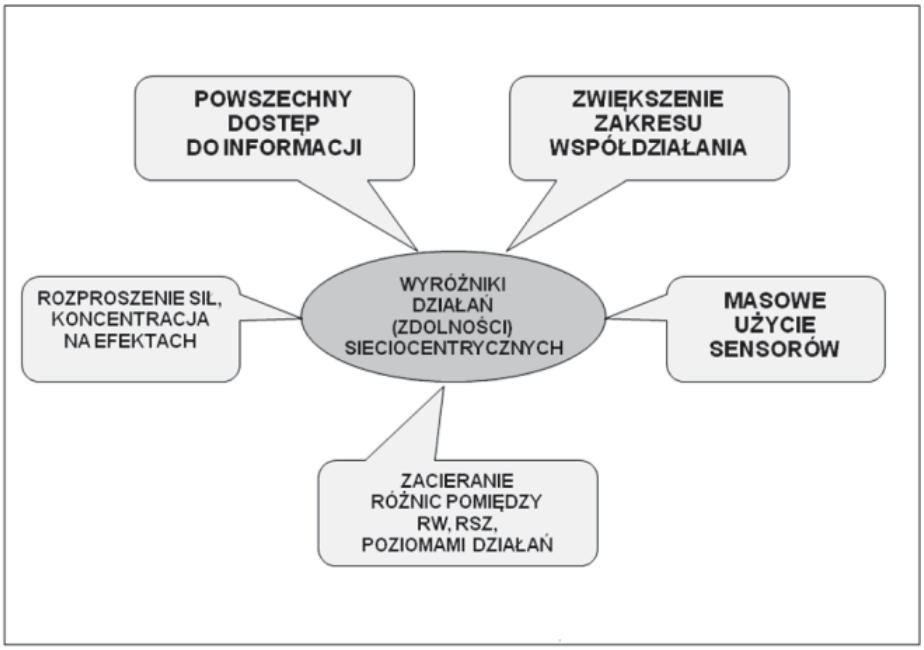
- dążenie do zdobycia w pierwszej kolejności przewagi informacyjnej nie jest założeniem nowym, znaczenie informacji dostrzegane było od zarania wojskowości, niezależnie od poziomu technologii jej przesyłania. Tradycyjnie w takiej sytuacji cytuje się Sun Tzu: „…kto zna przeciwnika i kto zna swoje siły, będzie zwyciężać w stu bitwach. Kto nie zna przeciwnika, ale zna własne siły, raz wygra, a raz przegra. Kto zna przeciwnika, ale nie zna własnych sił, będzie w niebezpieczeństwie w każdej bitwie…"[4];
- szybki cykl C2, nazywany także „dążeniem do działania wewnątrz cyklu decyzyjnego przeciwnika", również nie jest założeniem właściwym tylko dla NCW. Zapisy w tym zakresie funkcjonują w regulaminach walki wszystkich nowoczesnych armii;
- nielinearne pole (przestrzeń) walki „obecne" jest w teorii i praktyce działań zbrojnych od wielu lat i jest dość szeroko charakteryzowane w obowiązujących dokumentach doktrynalnych (regulaminach);
- „wykorzystywanie okazji", rozumiane jako zdolność podwładnych do wykazywania inicjatywy i umiejętności „wygrywania" sytuacji niespodziewanie pojawiających się na polu walki, stanowi jedną z podstaw filozofii dowo-

[4] Sun Tzu, *Sztuka wojowania*, cytat z pełnej wersji pracy dostępnej w Internecie pod adresem http://www.sonshi.com/sun3.html,

dzenia przez cele (ang. *mission command*, niem. *Führung Auftrag*), znanej i stosowanej w wielu armiach świata.

Podsumowując, wyniki przeprowadzonych badań pozwalają na konstatację, iż za operacyjne wyróżniki działań (zdolności) sieciocentrycznych uznać należy (rys. 3):

- powszechny (w zakresie uprzednio niespotykanym) dostęp do informacji wiarygodnej, terminowej i dokładnej,
- samosynchronizację (czyli szerokie współdziałanie) na najniższych możliwych szczeblach dowodzenia, a przez to gwałtowny wzrost autonomiczności działania niewielkich sił,
- rozproszenie sił w przestrzeni, skupianie efektów, a nie fizyczną koncentrację sił i środków,
- masowe (na niespotykaną dotąd skalę i w nowy zintegrowany sposób) użycie sensorów,
- zacieranie wyraźnych dotąd, organizacyjnych i proceduralnych granic pomiędzy poziomami działań, rodzajami SZ i wojsk.



Rys. 3. Operacyjne wyróżniki działań zdolności sieciocentrycznych. Źródło: J. Krecikij, *Działania sieciocentryczne. Wybrane problemy*

Każda nowa koncepcja ma swoich zwolenników i przeciwników. Network Centric Warfare nie jest wyjątkiem od tej zasady. Zwolennicy wskazują na wielkie korzyści, jakie niesie ze sobą wykorzystanie na niespotykaną dotąd skalę przestrzeni

informacyjnej. Krytycy wskazują słabe punkty, czy wręcz starają się wykazać nieprzydatność całej analizowanej idei. Celem dalszej części rozważań jest zatem porównanie ze sobą tych dwóch sprzecznych punktów widzenia, akcentując w obiektywny sposób mocne i słabe punkty koncepcji działań sieciocentrycznych.

Korzyści militarne

Rezultaty analizy literatury przedmiotu i samej istoty koncepcji NCW pozwalają na stwierdzenie, iż siły „usieciowione", wykorzystujące wszystkie zalety wynikające z zasad działań sieciocentrycznych, będą w stanie, poprzez właściwe wykorzystanie przewagi informacyjnej, przeciwstawić się siłom przeciwnika z niespotykaną dotąd skutecznością. Można zatem potwierdzić, iż przewaga nowego rodzaju sił wynika z dzielenia się informacją, dostępu do informacji i wynikającej z tych przedsięwzięć szybkości i rzeczywistej połączoności działania. Wyniki analiz literatury upoważniają do stwierdzenia, iż dopiero koncepcja NCW pozwala na maksymalne wykorzystanie wszystkich zalet płynących z głębokiego współdziałania rodzajów sił zbrojnych (działań połączonych), w tym także na niższych szczeblach dowodzenia. Prowadzone badania potwierdziły, że[5]:

1. Siły NCW mogą być mniejsze liczebnie niż dotąd (w relacji: zadanie do wykonania – siły niezbędne do wykonania zadania), zyskując nową jakość w zakresie szybkości i manewrowości, ze względu na fakt istnienia mniejszych potrzeb transportowych i logistycznych. Zachowują jednocześnie zdolność do efektywnego działania przy mniejszych jego kosztach.
2. Działania NCW umożliwiają wdrożenie i stosowanie nowej taktyki. Podczas operacji w Iraku siły amerykańskie w trakcie natarcia stosowały formę manewru nazywaną „taktyką roju". Dzięki posiadaniu ciągłej informacji o tym, gdzie znajdują się pozostałe własne wojska, elementy ugrupowania bojowego mogły poruszać się do przodu w małych, samodzielnych formacjach, unikając koncentrowania dużej ilości sprzętu w jednym miejscu i ciasnego „łokieć w łokieć" ugrupowania bojowego[6]. Tak zorganizowany manewr przebiegał szybko, jeśli zaś jeden z samodzielnych elementów uwikłał się w niebezpieczną sytuację, inne siły udzielały mu szybko pomocy, atakując przeciwnika ze wszystkich możliwych kierunków (co byłoby niemożliwe bez posiadania przewagi informacyjnej i wspólnej świadomości sytuacji na polu walki).

[5] *Network Centric Warfare: Background and Oversight Issuer for Congress*, The Library of Congress, Washington 2004, s. 6-8.

[6] Które jest z założenia mało elastyczne i stanowi opłacalny cel dla uderzeń przeciwnika.

3. W znacznym stopniu ułatwione zostaje działanie na najniższych szczeblach dowodzenia, łącznie z pojedynczym żołnierzem. W wypadku sytuacji kryzysowej informacja o niej przekazywana jest do swego rodzaju „centrum operacyjnego", gdzie umieszczania jest w przestrzeni informacyjnej. Problem jest następnie rozwiązywany przez decydentów na takim poziomie dowodzenia (rodzaju wojsk, miejscu), który dysponuje odpowiednią informacją i właściwym potencjałem do jego neutralizacji.

Zatem z operacyjnego punktu widzenia do zasadniczych korzyści osiąganych poprzez wdrażanie NCW zaliczyć należy:

- mniejszą ilość sił (żołnierzy i sprzętu) niezbędną do wykonania zadania, co redukuje szeroko rozumiane koszty działań,
- rozproszenie sił własnych, które, działając w niewielkich zgrupowaniach, utrudniają przeciwnikowi skuteczne zlokalizowanie, identyfikację i rażenie,
- możliwość kontrolowania znacznie większego terenu przez relatywnie niewielkie siły własne, niezmuszone do utrzymywania określonego, sztywnego szyku (ugrupowania) bojowego,
- zmniejszenie zagrożenia zadawania strat siłom własnym (ogień bratobójczy – ang. *friendly fire*) dzięki znajomości lokalizacji wszystkich elementów własnego ugrupowania bojowego,
- doprowadzenie do rzeczywistego połączenia działań różnych rodzajów sił zbrojnych na bardzo niskich poziomach dowodzenia,
- mniejsze i bardziej mobilne organa dowodzenia (łatwiejsze do przerzutu, ochrony i obrony oraz maskowania, a także mniej kosztowne),
- pełne wykorzystanie możliwości wynikających z określania przez dowódców swojej myśli przewodniej (ang. *commander's intent*),
- łatwiejszą ocenę sytuacji (decydenci mają możliwość „widzieć" przestrzeń walki w czasie prawie rzeczywistym, są zasilani informacją o realnym położeniu i działaniu wojsk własnych i przeciwnika),
- możliwość podejmowania decyzji o mniejszym ryzyku (proporcjonalnie do ilości, jakości i terminowości posiadanych informacji),
- szybszy cykl dowodzenia, pozwalający realnie działać wewnątrz cyklu dowodzenia przeciwnika, co jest najprostszą drogą do przejęcia i utrzymania inicjatywy,
- dalszą decentralizację dowodzenia, co powinno skutkować wykazywaniem i wykorzystywaniem inicjatywy przez dowódców niższych szczebli, a w konsekwencji – pełniejsze wykorzystywanie zalet filozofii dowodzenia przez cele,
- szybsze doprowadzanie zadań do wykonawców, co spowoduje, że będą adekwatne do rzeczywistej sytuacji, nie zaś spóźnione, a tym samym – błędne.

Potencjalne niebezpieczeństwa i zagrożenia

Założenia NCW, jak każdej nowej koncepcji czy idei, nie są oczywiście wolne od słabych stron, których po dokładnej analizie literatury przedmiotu i samej idei sieciocentryzmu nie można nie zauważać i nie wolno lekceważyć. Wśród najczęściej spotykanych i wymienianych przez ekspertów wojskowych niedoskonałości wymienić należy[7]:

- przywiązywanie przesadnej wagi do informacji – przecenianie informacji,
- niedocenianie potencjalnego przeciwnika,
- problemy z interoperacyjnością,
- ograniczenia w przepływie informacji,
- niepewność co do przyszłego panowania w przestrzeni kosmicznej,
- niekontrolowany wypływ technologii informatycznych,
- niebezpieczeństwo wynikające z zagrożeń asymetrycznych,
- narażenie na ataki w cyberprzestrzeni.

Przywiązywanie przesadnej wagi do informacji – przecenianie informacji

Wyniki analizy ocen krytycznych pozwalają na konstatację, iż część specjalistów pozostaje przy twierdzeniu, że użycie sieci do transmisji informacji nie jest wystarczającym substytutem manewru na polu walki i możliwości bojowych w konwencjonalnym tego słowa znaczeniu. Podkreśla się ponadto, iż przewaga informacyjna oraz szeroko dostępna świadomość sytuacji nie są jedynymi czy też najważniejszymi składowymi siły bojowej na polu walki. Często pojawiają się również obawy, że pewność siebie wynikająca z przekonania o tym, iż dowódca wie wszystko, co mu potrzebne do podjęcia decyzji, spowodować może początkowo lekceważenie, a w końcu całkowity zanik umiejętności analitycznej oceny działań przeciwnika, stanowiącej podstawę wojskowego procesu decyzyjnego. Podkreśla się także, iż siły zbrojne niejako zachłysnęły się nowoczesną technologią ery informacyjnej, ale jednocześnie nie przeprowadziły rzetelnej analizy ryzyka w zakresie rzeczywistego wprowadzenia w życie doktryny militarnej opartej całkowicie na (uzależnionej od) tak zdobywanych i przesyłanych danych. Jako zarzuty formowane są także uwagi wskazujące, że zmiany w ilości informacji prowadzą (wymuszają) często do jakościowych zmian w organizacji. To z kolei, jak wskazuje praktyka zarządzania, nie zawsze owocować musi zwiększeniem sprawności jej działania, zaś nadmierne zaufanie do skomplikowanych (a więc, zdaniem krytyków, zawodnych) systemów informacyjnych prowadzić może do nieprzewidywalnych kłopotów na realnym polu walki. Nikt nie stara się negować faktu, iż niespodziewanie duża ilość informacji może kreować wiele nowych, nieprzewidywalnych wcześniej okazji działania. Jednakże

[7] *Network Centric Warfare: Background and Oversight Issuer for Congress*, The Library of Congress, Washington 2004, s. 9-14.

zdaniem niektórych ekspertów może to z kolei prowokować dowódców do zmiany otrzymanych wcześniej zadań w takim zakresie, który generować będzie poważne problemy. Jako przykład takiego niebezpieczeństwa podaje się często, że pierwszym naprawdę zauważalnym skutkiem digitalizacji było wielokrotnie większe niż zazwyczaj w podobnych sytuacjach zużycie amunicji. Wpłynął na to fakt, iż dowódcy nagle „znaleźli się" w środowisku walki, w którym aż „roiło się" od potencjalnych celów. Zamiast zatem identyfikować i zwalczać rzeczywiście istotne z punktu widzenia swojego działania obiekty, rażono wszystko, co tylko znalazło się w zasięgu posiadanych środków. To z kolei spowodowało konieczność gwałtownego odtwarzania zapasów, przeciążenie logistyki i ogólne trudności w logistycznym zasilaniu pola walki.

Oponenci NCW podkreślają często, iż cała nowa koncepcja działań oparta jest tak naprawdę na nieodpowiedzialnym niedocenianiu potencjalnego przeciwnika. Zauważa się bowiem, iż jakiekolwiek możliwości strony przeciwnej w zwalczaniu/zakłócaniu sensorów czy też blokowaniu przekazu informacji są w zasadzie całkowicie lekceważone. Na poparcie takiej tezy podawany jest często fakt, iż cała filozofia NCW, nowych technologii i sposobu ich stosowania jest całkowicie jawnie publikowana. Takie podejście do bezpieczeństwa daje zatem potencjalnemu przeciwnikowi czas na systematyczną ocenę sytuacji i planowanie, jak znaleźć i w jaki sposób wykorzystać słabe strony koncepcji.

Problemy z interoperacyjnością wiążą się z wątpliwościami wśród ekspertów wojskowych, czy możliwe jest osiągnięcie rzeczywistej i pełnej interoperacyjności pomiędzy rodzajami sił zbrojnych, niezbędnej dla prowadzenia rzeczywistych działań połączonych. Wątpliwości te wynikają ze świadomości różnic, jakie dzielą poszczególne rodzaje sił zbrojnych. Chodzi tu zarówno o rozbieżne zasady działania (taktyka, sztuka operacyjna), różnice w procedurach dowodzenia oraz możliwościach działania w konkretnych środowiskach, specyficznych dla jednego rodzaju sił zbrojnych. Niejednokrotnie stawiane jest pytanie, czy możliwe jest sprowadzenie do wspólnego mianownika doktryny np. marynarki wojennej, stworzonej do działań na morzu, i wojsk lądowych – przewidzianych do walki w diametralnie innym otoczeniu.

Kolejny pojawiający się w literaturze problem to ograniczenia w przepływie informacji. Wiążą się one z obawą, czy linie transmisji informacji będą w stanie sprostać ciągle rosnącym wymaganiom sił zbrojnych. Dotychczasowe doświadczenia pokazują bowiem, iż rzeczywiście zdarzały się sytuacje, kiedy kanały informacyjne okazywały się za mało przepustowe. W takich przypadkach wojskowi obsługujący system „ręcznie" decydowali o priorytecie wysyłania danych informacji. Powodowało to opóźnienia lub wręcz kasowanie danych, którym z konieczności nadano niższy priorytet. W połączeniu z nadmiernym zaufaniem do technologii doprowadzało to do sytuacji, w których dowódcy podejmowali decyzje na podstawie położenia i działania przeciwnika zobrazowanego na ekranach monitorów swoich stacji roboczych. Tymczasem w wyniku niedrożności kanałów informacyjnych i opóźniania

przesyłu niektórych danych generowana tam sytuacja była nieprawdziwa. Tego typu wydarzenia, połączone z utratą umiejętności analitycznych (po co prowadzić staroświecką ocenę sytuacji? Przecież wiem wszystko, co mi potrzeba), traktowane są przez sceptycznych ekspertów jako bardzo poważne zagrożenia.

W aspekcie niepewności co do przyszłego panowania w przestrzeni kosmicznej specjaliści podkreślają, iż w chwili obecnej USA dominuje w kosmosie, który odgrywa niepoślednią rolę w koncepcji NCW. Przewaga ta była bezwzględnie wykorzystana podczas dwóch wojen w Zatoce Perskiej oraz działań w Afganistanie. Głosy oponentów wskazują jednak na fakt, iż było to możliwe, ponieważ strona przeciwna w ogóle nie wykorzystywała przestrzeni kosmicznej. W związku z tym nie można mieć absolutnej pewności, iż tak korzystna sytuacja będzie się powtarzać w każdym następnym konflikcie. Wręcz przeciwnie, należy oczekiwać i być przygotowanym do starcia z przeciwnikiem znacznie mniej opóźnionym technologicznie, który będzie dysponował zaawansowanymi możliwościami walki elektronicznej czy chociażby precyzyjnego ataku na naziemne instalacje satelitarne. W sytuacji zagrożeń asymetrycznych nie można wykluczyć sytuacji wynajęcia przez organizacje terrorystyczne łączy satelitarnych czy też zakupienia (np. w Rosji czy w Chinach) i wykorzystywania zaawansowanych technologii.

Wzrost powszechnego dostępu do zaawansowanych technologii może doprowadzić do niekontrolowanego przepływu wiedzy i technologii informatycznych w „niepożądane ręce". W konsekwencji stanowi to, zdaniem sceptyków, przesłankę do utraty globalnej przewagi w tym zakresie przez USA i kolejne poważne zagrożenie dla koncepcji NCW eliminujące jej silne strony. Eksperci wskazują, że takie samo zagrożenie związane jest z szeroko stosowanym przez przedsiębiorstwa pracujące dla obronności outsourcingiem, tym bardziej iż wiele zamówień na potrzeby sił zbrojnych lokowanych jest w Azji, w tym w Chinach i Indiach. Już obecnie 80% podzespołów do źródeł zasilania stosowanych w amerykańskich rakietach oraz pociskach kierowanych pochodzi z zagranicy, zaś części do produkcji przyrządów obserwacji nocnej niemal w całości są importowane.

Wśród asymetrycznych zagrożeń, które mogą być skierowane przeciwko koncepcji NCW (w sensie neutralizacji sensorów lub innych działań zmierzających do zmniejszenia skuteczności zaawansowanego technologicznie uzbrojenia), najczęściej wymieniane są następujące:

- samobójcze ataki bombowe,
- używanie cywili jako żywych tarcz,
- siły nieregularne, koncentrujące się tylko na wykonaniu konkretnego uderzenia i natychmiast rozpraszające się w przyjaznym im środowisku,
- użycie „brudnych bomb" radioaktywnych,
- użycie broni biologicznej lub chemicznej.

Zagrożenie to jest, zdaniem specjalistów, tym większe, że wśród już aresztowanych terrorystów znajduje się wiele osób, które studiowały (często w USA) na

kierunkach związanych z zaawansowanymi technologiami. Oznacza to, iż organizacje terrorystyczne mogą dysponować wiedzą, jak przy użyciu stosunkowo prostych lub niekonwencjonalnych środków wykorzystać słabe punkty koncepcji NCW. Nie można też wykluczyć niebezpieczeństw w rodzaju:

- zakłócania sygnałów satelitarnych,
- niszczenia na odległość instalacji komputerowych,
- włamań do systemów komputerowych.

Oponenci koncepcji NCW podkreślają niebezpieczeństwo narażenia na ataki w cyberprzestrzeni. Twierdzi się, nie bez powodu, że pomimo iż militarne systemy komputerowe są zabezpieczane na wiele sposobów, wciąż zdarzają się przypadki ataków hakerów, nierzadko zakończone powodzeniem. Nie można zatem wykluczyć możliwości, iż państwo – strona przeciwna – lub organizacja o charakterze niepaństwowym (np. Al-Qaida) uzyska zdolność do penetracji przestrzeni informacyjnej. Tego rodzaju atak mógłby przynieść nieprzewidywalnie groźne skutki dla działań sieciocentrycznych, dając z jednej strony możliwość zakłócania przepływu informacji (który jest istotą NCW) lub, działając bardziej wyrafinowanie, jej fałszowania. W połączeniu z wymienionymi wcześniej słabymi punktami sytuacja taka, zdaniem oponentów, doprowadzić może do paraliżu sił działających zgodnie z literą koncepcji NCW.

Poza wymienionymi powyżej zagrożeniami, mającymi w większym lub mniejszym stopniu charakter techniczny, podkreśla się niekiedy jeszcze jedno, osadzone raczej w mentalności ludzkiej – jest to potencjalne zagrożenie dla sprawowania dowodzenia zgodnie z filozofią „mission command". Ten styl dowodzenia opiera się na czterech filarach, z których decydującym jest inicjatywa podwładnych, nieograniczana przez przełożonych zbyt szczegółowymi instrukcjami. Oznacza to, że przełożony określa podwładnemu, co i w jakim celu ma wykonać, nie ingerując bez potrzeby w sposób realizacji zadania. Powszechna świadomość sytuacji na polu walki daje przełożonym, często wysokich szczebli dowodzenia, szczegółową wiedzę na temat tego, co dzieje się bardzo daleko i interesuje dowódców niskich szczebli. Zjawisko to samo w sobie nie jest niczym złym. Doświadczenia wskazują jednak, iż wielu wysokich dowódców nie może się oprzeć sposobności ingerowania w działania niskich szczebli dowodzenia, odbierając dowódcom tak potrzebną zawsze inicjatywę. W konsekwencji doprowadzić to może do sytuacji, że podwładni przestaną odważnie reagować na zmiany sytuacji w przestrzeni walki i będą biernie czekać na instrukcje „z góry". To zaś oznacza upadek koncepcji dowodzenia przez cele, która doskonale sprawdziła się w ostatnich konfliktach zbrojnych.

Konstatując, sieciocentryzm jako sposób prowadzenia działań charakteryzuje się licznymi i niezaprzeczalnymi zaletami, tworzącymi warunki do zdobycia i utrzymania przewagi w przestrzeni walki przy relatywnie niskich stratach i dużej szybkości działania. Jednocześnie nie można nie dostrzegać słabych stron

analizowanej koncepcji, gdyż takie po prostu istnieją – jak w każdej innej wizji czy sposobie rozwiązywania sytuacji problemowych. Czy jednak z tego powodu należy koncepcję NCW odrzucić czy też lekceważyć? Oczywiście nie, ale błędem byłoby również traktowanie jej jako swego rodzaju „świętego Graala". We współczesnym świecie, w dobie wysoce zintegrowanego i systemowego podejścia do problematyki bezpieczeństwa narodowego i międzynarodowego, sieciocentryzm pozostanie jego bardzo istotnym filarem, ale jednym z wielu.

LITERATURA:

1. D.S. Alberts, J.J. Garstka, F.J. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, Department of Defense, Washington 2000.
2. D.S. Alberts, J.J. Garstka, R.E. Hayes, F.J. Stein, *Understanding Information Age Warfare*, Department of Defense, Washington 2001.
3. "Journal of Defence Science" 9/2003, Ministry of Defence, London 2003.
4. JP 3-13 *Joint Doctrine for Information Operations*, Department of Defense, Washington 1998.
5. J. Kręcikij, *Działania sieciocentryczne. Wybrane problemy*, AON, Warszawa 2008.
6. J. Kręcikij, *Istota działań sieciocentrycznych*, „Zeszyty Naukowe AON" nr 4 (65), Warszawa 2006.
7. J. Kręcikij, *Podejmowanie decyzji w działaniach sieciocentrycznych. Ewolucja czy rewolucja?*, PTM, Warszawa 2010.
8. J. Kręcikij, J. Wołejszo (red. nauk.), *Uwarunkowania działań sieciocentrycznych determinujące organizację i funkcjonowanie systemu dowodzenia*, AON, Warszawa 2008.
9. Z. Maślak, *Informacje w obronie powietrznej. Potrzeby, wymagania, zagrożenia*, „Przegląd Wojsk Lotniczych i Obrony Powietrznej" nr 7, Warszawa 2002.
10. Materiały z konferencji naukowej Instytutu Zarządzania i Dowodzenia AON nt. *System dowodzenia w środowisku sieciocentrycznym*, (w:) „Zeszyty Naukowe AON" nr 3(68) A, Warszawa 2007.
11. *Network Centric Warfare: Background and Oversight Issues for Congress*, The Library of Congress, Washington 2004.
12. E. Smith, *Effect Based Operations*, Department of Defense, Washington 2002.
13. R. Szpakowicz, *Wojna w Iraku a koncepcja wojny sieciocentrycznej*, „Przegląd Wojsk Lotniczych i Obrony Powietrznej" nr 11, Warszawa 2003.
14. Sun Tzu, *Sztuka wojowania*, http://www.sonshi.com/sun3.html.
15. *The Implementation of Network – Centric Warfare*, Office of Force Transformation Office of the Secretary of Defense, Washington 2004.
16. T. Węgierski, *Strategiczna reorientacja sił zbrojnych*, „Przegląd Sił Powietrznych" nr 5, Warszawa 2005.

The strengths and weaknesses of the operations in centralised network concept

Abstract. The trend of organizing the information space for the needs of armed forces is visible last couple of years and still continues, mainly because of the IT technologies achievements. The main popular believe is that high technologies can be and should be the main factor of common and future military activities, since positive impact on the widely understood national security. Technology, and growing with it last few years Network Centric Warfare Concept (NCW) became a unison, in which the knowledge gathered in nets is used to form a kind of multi-force military activities that could be proven – as they are now – much more effective. Simply speaking, NCW could be described as information superiority based concept, in which the combat power growth is generated by connecting into common information net: sensors, decision makers and combat platforms to achieve a common situation awareness, speed C2 and operations tempo, increase weapon effectiveness, resistance to enemy strikes and level of operations synchronization. In other words NCW transfers information superiority into combat power by efficient connectivity of having different knowledge units which exist in the battlefield (battle dimension). But is the concept mentioned above an ideal panacea for all requirements of present and future conflicts and threats? Does it have any important weaknesses? And if any, is the result of strong points able to cover negative results of eventually existed weak points? That is why it is worth to identify specifics of NCW. Thanks to that it would be possible to classify each military (or national security) operation as a network centric or not – as an old time style industrial era activity.