

**Krzysztof Rokiciński**  
**Akademia Marynarki Wojennej**

## **MOŻLIWOŚCI ZASTOSOWANIA KONCEPCJI SIECIOCENTRYCZNOŚCI NA OBSZARACH MORSKICH RZECZYPOSPOLITEJ POLSKIEJ**

### **STRESZCZENIE**

W artykule przedstawione zostały rozważania z zakresu możliwości zastosowania koncepcji sieciocentryczności na obszarach morskich Rzeczypospolitej Polskiej. Dokonano tego po analizie idei tej koncepcji oraz na tle systemu bezpieczeństwa istniejącego w Regionie Bałtyckim.

Słowa kluczowe:

sieciocentryczność, bezpieczeństwo, Morze Bałtyckie, Rzeczpospolita Polska.

### **WSTĘP**

Nowe uwarunkowania prowadzenia działań związanych z szeroko rozumianym bezpieczeństwem wymagają pozyskiwania i przetwarzania danych z wielu źródeł, a następnie efektywnej dystrybucji informacji<sup>1</sup>. Konieczność zwiększenia efektywności tego procesu spowodowała powstanie koncepcji sieciocentryczności (ang. Network Centric Warfare – NCW). Autor przyjął do dalszych rozważań amerykańskie określenie sieciocentryczności, chociaż w innych krajach określa się ją najczęściej adekwatnie do koncepcji narodowych. Przykładem jest brytyjska koncepcja określana jako NEC (ang. Network Enabled Capability)<sup>2</sup>.

Wprowadzenie w życie koncepcji sieciocentryczności nie jest fanaberią, a koniecznością. W niniejszym artykule dokonana zostanie analiza możliwości

---

<sup>1</sup> W niniejszym artykule jako informacje będą rozumiane wcześniej uzyskane i odpowiednio przetworzone dane.

<sup>2</sup> L. Willet, *UK defines its network ethos*, „Navy International”, 2006, Vol. 111, No 4, pp. 50 – 55.

zastosowania tej koncepcji w odniesieniu do obszarów morskich Rzeczypospolitej Polskiej (RP) na tle uwarunkowań Regionu Bałtyckiego jako najważniejszego obszaru zainteresowania dla RP.

## POJĘCIE SIECIOCENTRYCZNOŚCI

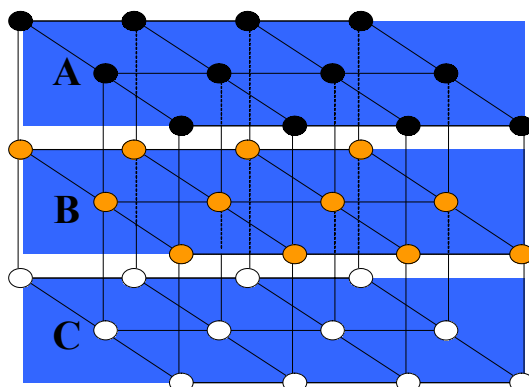
Analizując literaturę przedmiotu, można wyszczególnić wiele wątków i kontekstów koncepcji sieciocentryczności, co powoduje pewien chaos pojęciowy w tym zakresie<sup>3</sup>. Nie istnieje jednolita definicja NCW, a poszczególne kraje interpretują i wdrażają ją w różny, specyficzny dla siebie sposób. Tym samym realizacja techniczna tej koncepcji, nawet w państwach należących do tych samych sojuszy i organizacji lub blisko ze sobą współpracujących, napotyka na duże trudności.

Sprawne i skuteczne funkcjonowanie każdego systemu zależy więc od efektywności korelowania działań wszystkich służb wchodzących w jego skład. Ideą sieciocentryczności jest zwiększenie potencjału sił nie przez rozbudowę ilościową środków i stanu liczebnego, a bardziej racjonalne (efektywne) ich wykorzystanie przez decydentów (dowódców) dzięki posiadaniu aktualnej i wiarygodnej informacji oraz jej dystrybucję. Według jednego z twórców tej koncepcji J. Garstki podstawą jest założenie zwiększenia efektywności działań poprzez połączenie w globalną strukturę sieciową (ang. Global Information Grid) wszystkich jej składników, tj. ośrodków decyzyjnych, sensorów i efektorów. Ma to zapewnić, pomimo dużego rozśrodkowania, uzyskanie zsynchronizowanej czasowo i przestrzennie „świadomości sytuacyjnej” wszystkich uczestników sieci<sup>4</sup>. Oznacza to, iż teoretycznie tę samą informację powinien mieć każdy element w systemie. Ideę sieciocentryczności przedstawiono na rysunku 1.

---

<sup>3</sup> Por. G. I. Peterson, *The Father of Network-Centric Warfare. A Salute to Vice Admiral Arthur K. Cebrowski*, „Naval Forces”, 2001, No 1, p. 81; A. Stokalski, R. Kulicki, *C-commerce, C-government, NCW: Konwergencja doktryn i technologii*, X Konferencja „Automatyzacja Dowodzenia”, Jelenia Góra, czerwiec 2002, s. 2; R. Rugała, *Przyszłość morskich systemów wymiany danych w aspekcie koncepcji działań sieciocentrycznych*, X Sympozjum Wojskowej Techniki Morskiej, Puck, 19 – 20.10.2005, s. 4; A. Stokalski, *Sieciorcentryczna architektura zautomatyzowanych systemów dowodzenia – Bazowa Infrastruktura Informacyjna (Network-centric warfare – the base of infostructure)*, VIII Konferencja „Automatyzacja Dowodzenia”, Jelenia Góra, maj 2000, s. 4; R. Romba, S. Schäfer, *REACH BACK – Move information, not people*, „Europäische Sicherheit”, 2006, Nr 8, S. 48.

<sup>4</sup> J. J. Garstka, *Theory and practise of Network Centric Warfare*, Materiały z konferencji „Conference Documentation from Network Centric Warfare Conference”, London, 10 & 11<sup>th</sup> September 2001.



Rys. 1. Idea koncepcji sieciocentryczności

*Opracowanie własne.*

Przedstawiona na rysunku 1. koncepcja sieciocentryczności jest wyidealizowana, niemniej stanowi doskonałą podstawę do dalszych rozważań. Analiza rysunku 1. dowodzi, iż koncepcja sieciocentryczności obejmuje praktycznie wszystkie elementy, które uczestniczą w różnym zakresie w poszczególnych przedsięwzięciach. Widoczne jest, że poszczególne płaszczyzny (oznaczone kolejno A, B i C) nie są połączone jak dotychczas jednym lub tylko kilkoma kanałami przesyłania informacji, a na zasadzie „każdy z każdym”. Niniejsze płaszczyzny mogą być odpowiednikiem na przykład poziomów kierowania państwem (centralny, wojewódzki i powiatowy), dowodzenia (strategiczny, operacyjny i taktyczny) czy sferami militarną i cywilną. Charakterystyczne jest, iż elementarnym składnikiem sieci może być nawet pojedyncza osoba (żołnierz), co jest jednym z filarów tej koncepcji. Oznacza to, że jest ona jednocześnie źródłem i odbiorcą informacji znajdującej się w sieci. W aspekcie sił morskich elementarnym składnikiem sieci jest zarówno jednostka pływająca, statek powietrzny, jak i brzegowy punkt obserwacyjny.

## **ORGANIZACJA SYSTEMU BEZPIECZEŃSTWA W REGIONIE BAŁTYCKIM**

Przedstawione powyżej zależności pozwalają na określenie płaszczyzn w aspekcie koncepcji sieciocentryczności w odniesieniu do systemu bezpieczeństwa państw leżących nad Morzem Bałtyckim, określanych dalej jako Region Bałtycki.

Państwa te należą do różnych systemów bezpieczeństwa, w którym wyróżnia się cztery poziomy:

- światowy;
- europejski;
- regionalny;
- narodowy.

Do **światowego systemu bezpieczeństwa** pod względem politycznym oczywiście zalicza się ONZ, do którego należą wszystkie państwa Regionu Bałtyckiego. Pod względem militarnym jest nim bez wątpienia NATO, do którego nie należą jedynie trzy państwa Regionu. Sytuacja ta może się wkrótce zmienić, gdyż w Finlandii trwa coraz bardziej intensywna dyskusja nad wstąpieniem do paktu NATO, który jest zainteresowany także specjalną umową ze Szwecją<sup>5</sup>. Ponadto wszystkie kraje Regionu należą do Interpolu (Międzynarodowej Organizacji Policji Kryminalnych), co w znaczący sposób podnosi stopień bezpieczeństwa społeczeństw w aspekcie niemilitarnym.

Znaczniejszy wpływ na bezpieczeństwo Regionu ma **współpraca w ramach Unii Europejskiej**, do której należy osiem państw, a ich wybrzeża obejmują 95% Morza Bałtyckiego. Sprzyja temu formowanie w ramach UE wspólnych narzędzi do zapewnienia bezpieczeństwa zewnętrznego (Europejskie Siły Zbrojne) i wewnętrznego (między innymi Europol). Trzeba tym samym spodziewać się, że wszelkie przedsięwzięcia państw Regionu będą pochodnymi przedsięwzięć UE i zostaną z nimi ściśle skorelowane.

Trzecim poziomem systemu bezpieczeństwa jest poziom **regionalny**, realizowany w ramach tzw. współpracy bałtyckiej. Składa się na nią szereg struktur współpracy międzyrządowej działających przede wszystkim pod egidą Rady Państw Morza Bałtyckiego (RPMB). Zakres korelowanej przez nią współpracy obejmuje aspekty bezpieczeństwa morskiego, zagrożeń dla środowiska naturalnego, katastrof przemysłowych, kontroli ruchu powietrznego, morskiego i granicznego oraz współpracy służb ratowniczych<sup>6</sup>. Ponadto prowadzonych jest wiele innych przedsięwzięć, z których można wymienić chociażby „Baltic Master” (międzynarodowy projekt dotyczący poprawy bezpieczeństwa morskiego poprzez integrowanie lokalnych

---

<sup>5</sup> Z kim ma się wiązać NATO, „Gazeta Wyborcza” z 22 listopada 2006, s. 9.

<sup>6</sup> Por. Wspólny Dokument Programowy Program Współpracy Przygranicznej Phare 2001 – 2006. Estonia, Litwa, Łotwa, Polska, lipiec 2001, rozdział 1.1.4.

i regionalnych przedsięwzięć w różnych aspektach) czy „Umbrella Operation” (przygotowanie do zwalczania i zapobiegania skutkom katastrof)<sup>7</sup>.

Każde z państw Regionu ma specyficzny system bezpieczeństwa **narodowego** różniący się od pozostałych sposobem podejścia do zapobiegania i zwalczania zagrożeń.

## RODZAJE ZAGROŻEŃ W REGIONIE BAŁTYCKIM

Istotnym czynnikiem tworzenia systemu bezpieczeństwa wpływającym bezpośrednio na koncepcję sieciocentryczności są obecne i prognozowane zagrożenia. W pewnym stopniu Bałtyk charakteryzuje się specyficznymi cechami w odniesieniu do pozostałych mórz, co zostanie wyspecyfikowane poniżej.

Po analizie obecnej i prognozowanej sytuacji na Morzu Bałtyckim można stwierdzić, że znacznie zmniejszyło się zagrożenie ze strony przeciwnika symetrycznego, a wzrosło ze strony przeciwnika asymetrycznego.

Zdaniem autora najważniejszym czynnikiem generującym **zagrożenia asymetryczne** w Regionie Bałtyckim jest sytuacja demograficzna<sup>8</sup>. W pasie nadmorskim wszystkich krajów znajdują się wielkie aglomeracje portowe (w tym pięć stolic), a w północnej części koncentruje się wręcz większość dużych miast. Powoduje to, iż przy takiej koncentracji przemysłu oraz ludności obszary te są niezwykle podatne na zagrożenia związane z zorganizowaną przestępczością, nielegalną imigracją, a także terroryzmem<sup>9</sup>. Ale paradoksalnie brak siły roboczej mogą odczuć nie bogate kraje Regionu Bałtyckiego, a ze względu na dużą emigrację zarobkową

---

<sup>7</sup> Materiały z konferencji „Can we control Baltic Sea”, Gdańsk, 7 – 8 listopada 2005 r. Szczegóły projektu można znaleźć na oficjalnej stronie internetowej projektu. Por. *Baltic Master. Maritime Safety Across Order. Project Information*, <http://www.balticmaster.org>, *Maritime Safety Umbrella Operation – MSUO*, [www.maritime-safety.org](http://www.maritime-safety.org).

<sup>8</sup> Wyszczególnienie dotyczy danych z 2005 roku i opracowane zostało na podstawie badań przeprowadzonych w: K. Rokiciński *Zagrożenia asymetryczne w Regionie Bałtyckim*, Warszawa 2006, s. 101 – 108.

<sup>9</sup> Ciekawe analizy zagrożeń dla miast (aglomeracji) portowych na przykładzie Gdyni i Sopotu można znaleźć między innymi w: K. Ficoń, *Identyfikacja zagrożeń rzeczywistych i potencjalnych dla miasta portowego na przykładzie Gdyni*, [w:], *Człowiek i technika w systemach bezpieczeństwa i ochrony*, red. K. Chwesiuk, A. Ostrokólski, J. Sadowiski, E. Kołodziński, IV Międzynarodowa Konferencja Naukowa „Zarządzanie kryzysowe”, Akademia Morska, Szczecin 2006, s. 89 – 100; R. Sadkowski, *Bezpieczeństwo Sopotu*, Bałtycki Kongres Bezpieczeństwa Europejskiego, Jurata 2006, s. 309 – 324.

raczej były państwa socjalistyczne. Wbrew obiegowym opiniom kształtowanym przez media najgorsza sytuacja pod względem demograficznym panuje właśnie w krajach byłego obozu socjalistycznego. Dowodzą tego wskaźniki urodzeń, zgonów, dzietność kobiet, a przede wszystkim przyrost naturalny (jest on dodatni tylko w Polsce). Zdaniem autora to właśnie sytuacja demograficzna będzie determinowała w przyszłości w Regionie Bałtyckim rodzaje i skalę występowania zagrożeń asymetrycznych<sup>10</sup>.

Mogą one spowodować falę masowej **nielegalnej imigracji** nie tylko do krajów „starej Unii”, ale przede wszystkim nowych członków, którzy, jak się wydaje, nie są na to przygotowani technicznie, proceduralnie, organizacyjnie, a co najważniejsze – mentalnie.

Nie mniej istotne zagrożenie niesie **zorganizowana przestępczość**, która w Regionie Bałtyckim może przyjąć następujące formy:

- produkcja i przerzut środków odurzających;
- kradzieże;
- przemyt<sup>11</sup>;
- organizacja nielegalnej imigracji;
- handel żywym towarem (szczególnie kobiety – prostytutka i dzieci – prostytutka oraz adopcje);
- pranie brudnych pieniędzy;
- zlecone zastraszanie, morderstwa i porachunki grup przestępczych;
- podrabianie pieniędzy i papierów wartościowych;
- przestępstwa przeciwko znakom towarowym (podrabianie produktów);
- kłusownictwo.

Szczególnie niebezpieczny jest „narkobiznes”, który stał się realnym zagrożeniem dla bezpieczeństwa wielu państw, zarówno z uwagi na charakter prowadzonej działalności, jak i sposób działania (korupcja, pranie brudnych pieniędzy, destabilizacja systemu finansowego itd.).

Wydaje się, że na obszarze Bałtyku należy liczyć się z aktami **terroryzmu**, których bezpośrednim celem nie będzie raczej zniszczenie (uszkodzenie) określonych obiektów. Wynika to z faktu, iż potencjalni terroryści nie są w stanie dokonać

---

<sup>10</sup> K. Rokiciński *Zagrożenia asymetryczne w Regionie Bałtyckim*, wyd. cyt., s. 101 – 108.

<sup>11</sup> Przykładem jest próba masowego przemytu 15 mln sztuk papierosów na barce z Kaliningradu w 2004 roku. Por. *15 milionów papierosów, 130 policjantów i barka*, „Gazeta Morska”, lokalny dodatek do „Gazety Wyborczej” z 30 czerwca 2004, s. 3.

wielu ataków, a jedynie spektakularnego aktu, co wynika z efektywnego systemu bezpieczeństwa oraz, jak na razie, małych możliwości rekrutacji potencjalnych sprawców<sup>12</sup>. Wynikiem działań terrorystycznych mogą być relatywnie duże straty, ale jednorazowe. Można więc stwierdzić, iż *de facto* celem aktów terroryzmu będzie stworzenie atmosfery zagrożenia, by wymusić decyzje polityczne czy ekonomiczne.

Przedstawiona powyżej ocena zagrożeń różni się od obszaru pozostałej części Europy, szczególnie południowej. Zdecydowanie wyżej stawia się tam na terroryzm (na co wpływa pamięć zamachu na pociąg podmiejski w Madrycie) oraz nielegalną imigrację<sup>13</sup>, a więc odwrotnie niż w Regionie Bałtyckim.

Równie ważne jest zagadnienie **wojny w „cyberprzestrzeni”**. Obszar Morza Bałtyckiego charakteryzuje się skupieniem dużego potencjału technologicznego i technicznego. Istnieje więc znaczna liczba celów, które mogą stać się obiektami ataków związanych ze sferą informacji. Szczególnie niebezpieczne dla sfery związanej z morzem jest nagromadzenie systemów informacyjnych (zbierania, dystrybucji i przetwarzania informacji), które z reguły są wzajemnie ze sobą powiązane, stanowiąc „słabe ogniwo” sieci. Tym samym można spodziewać się ataków na systemy militarne i cywilne, a zatem związane z gospodarką morską, od systemów kontroli ruchu po administrację państwową i sferę ekonomii.

W rozważaniach dotyczących zagrożeń należy podkreślić również skutki ewentualnej **katastrofy ekologicznej** na Morzu Bałtyckim. Wynika to ze specyfiki Bałtyku, gdyż całkowita wymiana wody trwa tu co najmniej 25 lat<sup>14</sup>. Znaczne zagrożenia dla ekosystemu Morza Bałtyckiego (a także ekonomii) generuje transport morski, szczególnie jednostki transportujące substancje niebezpieczne (ropę naftową, gaz ziemny, chemikalia, kopaliny itd.). Zagrożenie to doskonale ilustruje ruch tankowców na Bałtyku, gdyż dziennie na tym akwenie (na morzu i w portach) znajduje się od 150 do 200 takich jednostek. Wielkość przewożonego ładunku ropy wynosi obecnie ponad 80 mln ton rocznie, a prognozuje się, że w najbliższych latach

---

<sup>12</sup> Niektórzy autorzy zwracają jednak uwagę na fakt, że coraz częściej sprawcami aktów terrorystycznych nie są imigranci i ich potomkowie, a osoby wywodzące się z rdzennej ludności, które zostały oświecone określoną ideą, religią lub przekonaniem. Por. A. Pargeter, *Western converts to radical Islam: the global jihad's new soldiers?* „Jane's Intelligence Review” 2006, Vol. 18, No 8, pp. 20 – 26; G. Sorman, *Kim są terroryści i jak się ich pozbyć?*, „Dziennik. Polska, Europa, Świat” z 21 sierpnia 2006, s. 32.

<sup>13</sup> T. Szubrycht, *The security threats for Europe*, „Polish Journal of Environmental Studies”, 2005, Vol. 14, supplement 1, pp. 147 – 151.

<sup>14</sup> Wspólny Dokument Programowy Program Współpracy Przygranicznej Phare 2001 – 2006, wyd. cyt., rozdział 1.1.5.

może osiągnąć poziom nawet 150 mln ton<sup>15</sup>. Tylko na Zatoce Gdańskiej Służba Kontroli Ruchu Statków „VTS Zatoka Gdańska” obsłużyła w 2005 roku 7 678 jednostek pływających, a w tej liczbie 2 548 z ładunkami niebezpiecznymi<sup>16</sup>.

Sygnalizowanym ostatnio zagrożeniem związanym z tym problemem jest budowa Rurociągu Północnego (określanego także jako Wybörg – Greifswald).

Istotnym niebezpieczeństwem są masowo zatapiane w minionych latach **substancje toksyczne** oraz zapasy **broni chemicznej** po II wojnie światowej<sup>17</sup>. Jakość ich opakowań już jest zła, przez co stanowią swego rodzaju bombę ekologiczną o wielkiej mocy. Jeżeli rozkład tych substancji będzie trwał jak dotychczas w postaci odizolowanych źródeł skażeń, problem powinien rozwiązać się praktycznie sam<sup>18</sup>. W przeciwnym wypadku może skazić znaczny obszar Morza Bałtyckiego.

Reasumując, należy stwierdzić, iż w zakresie bezpieczeństwa Region Bałtycki charakteryzuje się:

- atrakcyjnością dla przeciwnika asymetrycznego (zarówno w aspekcie społecznym, a więc powodującym nielegalną imigrację, jak i zorganizowanej przestępczości oraz terroryzmu);
- dużym zagrożeniem katastrofami ekologicznymi ze względu na małe wymiary akwenu, długi okres wymiany wody oraz znaczny ruch jednostek pływających transportujących substancje szkodliwe, szczególnie ropę naftową i jej pochodne.

Przedstawione zagrożenia obrazują zakres i ilość informacji, które są niezbędne do prowadzenia działań w zakresie bezpieczeństwa. Wydaje się, że są to wystarczające determinanty uzasadniające wprowadzanie koncepcji sieciocentryczności.

---

<sup>15</sup> R. Wolf, *Ostsee wird zweispurig sicherer*, „TAZ-Bericht” z 28 lutego 2005, s. 8.

<sup>16</sup> AKTUALNOŚCI, 24.01.2006, *Nadzór i monitorowanie bezpieczeństwa ruchu statków w obszarze Służby Kontroli Ruchu Statków VTS Zatoka Gdańska w roku 2005*, <http://www.umgdby.gov.pl/pium/jednostka?menuId=2972&kodJednostki=rxm59jacv2.rsc9w4acv1 &id=12226> (11.08.2006).

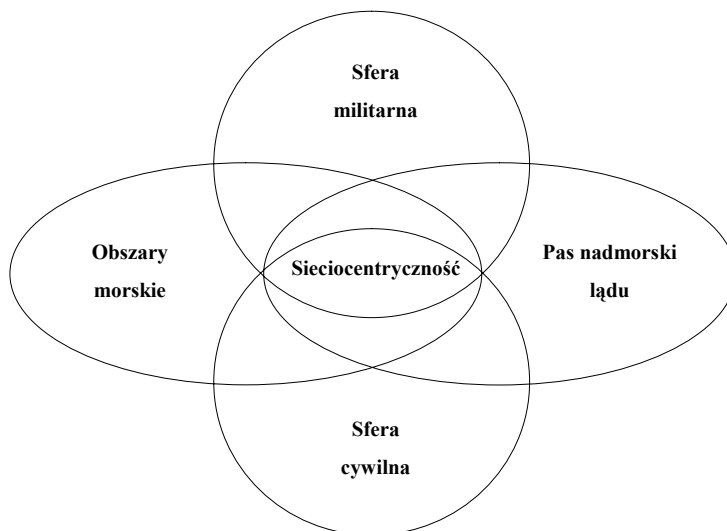
<sup>17</sup> Szczegółowo problem ten został opisany między innymi w: T. Kasperek, *Zagrożenia wynikające z zalegania amunicji chemicznej na dnie Bałtyku*, Bałtycki Kongres Bezpieczeństwa Europejskiego, Jurata 2006, s. 205 – 207; tenże, *Broń chemiczna zatopiona w Morzu Bałtyckim*, Wyd. Adam Marszałek, Toruń 1999, s. 5 – 9.

<sup>18</sup> Problem ten dotknął na przełomie lat 1996/1997 bezpośrednio terenu wybrzeża polskiego w rejonie Władysławowa. Por. Ł. Lipiński, K. Urbański, *Iperyty w rybackiej sieci*, „Gazeta Wyborcza”, dodatek lokalny „Gazeta Morska” z dnia 11/12 stycznia 1997, s. 1; W. Kuchanny, A. Rędzińska, *Półów skażony iperytem*, „Gazeta Wyborcza”, dodatek lokalny „Gazeta Morska” z dnia 13 stycznia 1997, s. 1.



## SIECIOCENTRYCZNOŚĆ W ASPEKCIE ZAGADNIENIŃ MORSKICH

Z powyższych rozważań wynika, że w aspekcie morza koncepcja sieciocentryczności musi obejmować dwa obszary funkcjonalne, a mianowicie narzędzia (sfera militarna i cywilna) oraz obszar (wodny i lądowy), co zilustrowano na rysunku 2.



Rys. 2. Współzależność obszarów funkcjonalnych w aspekcie koncepcji sieciocentryczności w odniesieniu do zagadnień związanych z morzem

*Opracowanie własne.*

W aspekcie bezpieczeństwa morza oraz pasa nadmorskiego krótki czas reakcji wymusza dostarczanie w odpowiednim czasie wiarygodnej informacji. W odniesieniu do systemu bezpieczeństwa wewnętrznego w znacznej mierze będzie dysponowała nią przede wszystkim sfera cywilna. Poniżej wyszczególnione zostaną zasadnicze międzynarodowe systemy cywilne dysponujące informacjami o sytuacji na morzu.

W zakresie nadzoru żeglugi istotnym elementem umożliwiającym stałe monitorowanie sytuacji, śledzenie jednostek pływających, a także dostarczanie informacji o ładunku, porcie docelowym, armatorze itd. są systemy **VTS (Vessel Traffic Service)**, **VMS (Vessel Monitoring System)** i **VTMIS (Vessel Traffic Management and Information Systems)**<sup>19</sup>.

---

<sup>19</sup> Szczegółowe informacje o statusie, zasadach i możliwościach tych systemów można znaleźć między innymi w: Międzynarodowa konwencja o bezpieczeństwie życia na morzu

Ponadto istnieją systemy pozycjonowania jednostek pływających oraz zgłaszania przez nie informacji o niebezpieczeństwie. System **SRS (Ship Reporting Systems)** służy do zgłaszania się statków oraz przekazywania im tras przejścia<sup>20</sup>, a **AIS (Automatic Identification System)** do automatycznej identyfikacji jednostek pływających<sup>21</sup>. Kolejnym przedsięwzięciem związanym z alarmowaniem przez jednostki pływające znajdujące się w niebezpieczeństwie jest system **SSAS (Ship Security Alert System)**<sup>22</sup>.

Szereg postanowień dotyczących powyższych systemów przyjęto w Londynie w grudniu 2002 roku na Dyplomatycznej Konferencji w sprawie Bezpieczeństwa Morskiego (Diplomatic Conference on Maritime Security). Następnie wprowadzono je w formie poprawek do rozdziału IX konwencji SOLAS (międzynarodowej konwencji o bezpieczeństwie życia na morzu z 1974 roku) w formie kodeksu ochrony, który przyjął nazwę Międzynarodowego Kodeksu dla Ochrony Statków i Obiektów Portowych (International Ship and Port Facility Code – ISPS)<sup>23</sup>. Intencją jego wprowadzenia jest ustanowienie skoordynowanego międzynarodowego systemu bezpieczeństwa realizowanego przez rządy, administrację lokalną, władze portowe i przemysł okrętowy w celu wykrywania zagrożeń oraz podejmowanie środków zapobiegawczych przeciwko incydentom dotyczącym statków i urządzeń portowych. Powoduje to, iż w celu wymiany informacji tylko pomiędzy nimi niezbędne jest wykorzystanie koncepcji sieciocentryczności.

---

„SOLAS” 1974 wraz z późniejszymi zmianami, Gdańsk 2002, rozdz. 5, prawidło 12, *Vessel Monitoring System*, <http://www.afma.gov.au/industry/vms/default.htm>, *Vessel Monitoring System (VMS) Information Website*, <http://www.glf.dfo-mpo.gc.ca/fm-gp/cp-cp/vms-ssn/index-e.jsp>, *The world's leading Vessel Traffic Management and Information Systems (VTMIS) and AIS Networks solutions provider*, <http://www.norcontrolit.com/>, *VTMIS – Vessel Traffic Management and Information Service*, <http://www.fma.fi/e/functions/trafficmanagement/?cat=gofrep&page=13042004>.

<sup>20</sup> Międzynarodowa konwencja o bezpieczeństwie życia na morzu „SOLAS” 1974 wraz z późniejszymi zmianami, wyd. cyt., rozdz. 11, *Mandatory Ship Reporting System for Northern Right Whales*, <http://www.nmfs.noaa.gov/pr/shipstrike/msr/> (13.11.2006).

<sup>21</sup> Międzynarodowa konwencja o bezpieczeństwie życia na morzu „SOLAS” 1974 wraz z późniejszymi zmianami, wyd. cyt., rozdz. 5, *What is the Automatic Identification System (AIS)?*, US Coast Guard Navigation Center, <http://www.navcen.uscg.gov/enav/ais/default.htm> (13.11.2006).

<sup>22</sup> *Gefahrenabwehr. Alarmsystem zur Gefahrenabwehr auf dem Schiff (Ship Security Alert System – SSAS)*, <http://www.bsh.de/de/Schifffahrt/Berufsschifffahrt/Gefahrenabwehr/SSAS.jsp> (13.11.2006), *Summary of the IMO ISPS Code / SOLAS XI-2/6*, [http://www.satamatics.com/ssas/ssas\\_ship\\_security\\_alert\\_system\\_regulations.htm](http://www.satamatics.com/ssas/ssas_ship_security_alert_system_regulations.htm) (28.12.2005).

<sup>23</sup> *International Ship & Port Facility Security (ISPS) Code, Amendments to SOLAS*, London 2003.

## SYSTEM BEZPIECZEŃSTWA MORSKIEGO RP

Adekwatnie do opisanych rozważań konieczna jest charakterystyka i ocena systemu bezpieczeństwa morskiego RP w aspekcie wykorzystania koncepcji sieciocentryczności. W tym celu zostaną przedstawione zasadnicze narzędzia, jakimi dysponuje RP.

Siły morskie RP składają się z dwóch wyraźnie wyodrębnionych elementów: Marynarki Wojennej RP ze swoimi systemami dowodzenia (ŁEBA, MCCIS i TACTICOS) oraz elementów pozamilitarnych należących do sfery cywilnej, która obejmuje również urzędy i służby państwowe oraz gospodarkę. Istotną rolę odgrywają urzędy morskie, które realizują zadania związane ze sprawowaniem jurysdykcji oraz egzekwowaniem prawa na polskich obszarach morskich. Jednym z istotnych zadań jest monitorowanie sytuacji w zakresie ekologii oraz kierowanie akcjami w przypadku wypadków i katastrof, których efektem jest skażenie środowiska. Należy podkreślić, że w ich skład wchodzi inspekcje państwa portu (Port State Controls), które wprowadziła do struktur ustawa z 15 stycznia 2004<sup>24</sup> celem nadzoru nad przestrzeganiem wymagań w stosunku do załóg i jednostek pływających poruszających się po wodach należących do członków Unii Europejskiej<sup>25</sup>. Polski Rejestr Statków (PRS) przeznaczony jest do kontroli stanu technicznego jednostek pływających, a zagadnieniami związanymi z rybołówstwem zajmuje się Inspekcja Rybołówstwa.

Bezpieczeństwo ruchu na polskich obszarach morskich zapewniają systemy „VTS Zatoka Gdańska” i „VTS Zatoka Pomorska”, tam, gdzie żegluga jest szczególnie intensywna i występuje duże prawdopodobieństwo kolizji. Ratowaniem życia i mienia na morzu zajmuje się Morska Służba Poszukiwania i Ratownictwa (MSPiR), która w tym zakresie ściśle współpracuje z MW RP, wydzielając do tego zadania śmigłowce ratownicze oraz okręty dyżurne. Ponadto MSPiR ma siły i środki do zwalczania skutków katastrof ekologicznych.

Przykładem systemu noszącego już obecnie pewne znamiona sieciocentryczności, służącego do monitorowania ruchu statków i przekazywania informacji, jest System Wymiany Informacji Bezpieczeństwa Żeglugi (SWIBŻ). Łączy on zobrazowanie mapy elektronicznej oparte na bieżącej informacji nautycznej, informację

---

<sup>24</sup> Ustawa o zmianie ustawy o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej oraz o zmianie niektórych innych ustaw z 18 grudnia 2003, DzU, 2004, nr 6, poz. 41.

<sup>25</sup> Rozporządzenie ministra infrastruktury z 26 kwietnia 2004 w sprawie podawania do publicznej wiadomości informacji dotyczących statków o obcej przynależności poddanych inspekcji, DzU, 2004, nr 101, poz. 1044.

z Automatycznego Systemu Identyfikacji (AIS) oraz bazy danych Służby Kontroli Ruchu Statków. Pozwala to na skuteczny nadzór nad ruchem statków przewożących ładunki niebezpieczne, nad skomplikowanymi holowaniami oraz działalnością Morskiej Kopalni Ropy Naftowej „Petrobaltic”. Wspomaga również działania związane z wykrywaniem niebezpiecznych sytuacji w polskich obszarach morskich, takich jak awarie statków, nieprzestrzeganie stref bezpieczeństwa wokół instalacji hydrotechnicznych, ruch tankowców jednokadłubowych itp. Już dziś system łączy ponad 40 użytkowników z różnych instytucji (między innymi Marynarki Wojennej RP, Straży Granicznej, izb celnych oraz MSPiR) i jest platformą wymiany informacji z centrami zarządzania kryzysowego na poziomie wojewodów, a także Centrum Reagowania Kryzysowego Ministerstwa Transportu i Budownictwa<sup>26</sup>.

Postępem w zakresie sieciocentryczności jest budowa Krajowego Systemu Bezpieczeństwa Morskiego (KSBM-I) finansowanego ze środków UE w ramach „Strategicznego Programu Operacyjnego – Transport” wraz z tworzonym przez Straż Graniczną programem „Zarządzanie Granicą” (Zintegrowanym Zautomatyzowanym Systemem Radiolokacyjnego Nadzoru Obszarów Morskich)<sup>27</sup>. Podstawową formą kontroli obszarów morskich w ramach tego programu będzie obserwacja techniczna prowadzona z posterunków rozmieszczonych wzdłuż wybrzeża. Mają one przysyłać informacje do lokalnych ośrodków Straży Granicznej, a te do Centralnego Ośrodka Nadzoru. Dane z posterunków radiolokacyjnych będą weryfikowane i uzupełniane o informacje z urzędów morskich (AIS, VTS, VTMS, VMS) oraz Centrum Kontroli Rybołówstwa<sup>28</sup>.

W odniesieniu do bezpieczeństwa ekologicznego w aspekcie współpracy bałtyckiej interesujący jest program SWEPOL, który nosi także pewne cechy sieciocentryczności. Dotyczy on satelitarnego wykrywania zanieczyszczeń olejowych na obszarze Bałtyku Południowego. Ze strony szwedzkiej w programie uczestniczy straż przybrzeżna (Kustbevakning), a polskiej – Urząd Morski w Gdyni, Inspektorat Ochrony Środowiska oraz Centrum Bezpieczeństwa Morskiego („VTS Zatoka Gdańska”), pełniące rolę polskiego Centrum Koordynacyjnego (ang. Command Centre)<sup>29</sup>.

---

<sup>26</sup> AKTUALNOŚCI, 24.01.2006, *Nadzór i monitorowanie bezpieczeństwa ruchu statków w obszarze Służby Kontroli Ruchu Statków VTS Zatoka Gdańska w roku 2005*, wyd. cyt., (11.08.2006).

<sup>27</sup> 02.12 – 03.12.2004, Konferencja ERB-Seagull „Działania na rzecz zrównoważonego wzrostu w Euroregionie Bałtyk”, warsztaty nt. „Bezpieczeństwo morskie – jaką rolę może odegrać Euroregion Bałtyk?”, <http://www.umgd.gov.pl> (03.09.2005).

<sup>28</sup> R. Rugała, *Sieciocentryczna architektura Zautomatyzowanego Systemu Dowodzenia Marynarki Wojennej*, X Sympozjum Wojskowej Techniki Morskiej, Puck, 19 – 20.10.2005, s. 12.

<sup>29</sup> *Nowoczesne sposoby wykrywania zanieczyszczeń olejowych na Bałtyku*, <http://www.umgd.gov.pl/pium/jednostka?menuId=2972&kodJednostki=rxm59jacv2.rsc9w4acv1&id=12226> (13.08.2006).

## WNIOSKI

Reasumując rozważania zawarte w artykule, można stwierdzić, że elementami składowymi koncepcji sieciocentryczności muszą być wszystkie systemy, które się wzajemnie uzupełniają i determinują swoje istnienie. Obecnie systemy kierowania i dowodzenia wykazują jednak dużą różnorodność oferowanych rozwiązań. Każde z nich jest kierowane dla wybranej grupy użytkowników i obciążone specyfiką uwarunkowań doktrynalnych danego państwa<sup>30</sup>.

Na obecnym etapie wprowadzania koncepcji sieciocentryczności można zidentyfikować przeszkody w zakresie obszarów morskich:

- brak bezpiecznych połączeń oraz niski stopień interoperacyjności;
- brak zrozumienia kluczowych aspektów zachowań ludzkich i wynikających z organizacji działań zgodnie z nowoczesnymi koncepcjami;
- brak lub zbyt wolny rozwój technologicznych inwestycji związanych z NCW.

Wprowadzenie rozwiązań sieciocentrycznych pociąga za sobą również zwiększenie ich podatności na oddziaływanie przeciwnika zarówno symetrycznego, jak i asymetrycznego (cyberterroryzm).

W odniesieniu do możliwości zastosowania koncepcji sieciocentryczności w RP problemy z tym związane obrazują raporty dotyczące przygotowania administracji do działań w sytuacjach kryzysowych:

- brak klarowności i jednoznaczności w zakresie kierowania i organizacji;
- skomplikowane i niejednoznaczne procedury;
- brak ujednoliconej sfery definicyjnej;
- niezadawalający obieg informacji niezbędnej do prowadzenia działań i nieprzerwanego prognozowania zagrożeń<sup>31</sup>.

Należy podkreślić, że koncepcja sieciocentryczności pojawiła się stosunkowo niedawno i jest raczej zbiorem wytycznych do realizacji aniżeli gotowym

---

<sup>30</sup> P. Sienkiewicz, *Systemy kierowania*, Warszawa 1989, s. 128.

<sup>31</sup> Informacja o wynikach kontroli numer P/97210 i P/97211 dotyczącej przygotowania administracji zespolonej do działań w sytuacjach kryzysowych, raport Departamentu Obrony Narodowej i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli, Warszawa, maj 1998; Informacja o wynikach kontroli numer P/02/074 dotyczącej przygotowania administracji zespolonej do działań w sytuacjach kryzysowych, raport Departamentu Obrony Narodowej i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli, Warszawa, wrzesień 2003.

rozwiązaniem<sup>32</sup>. Raczej sugeruje ona kierunki rozwoju systemów kierowania oraz dowodzenia na najbliższą przyszłość i przez to nie należy spodziewać się jej szybkich, znaczących efektów. Jest to proces, którego cel nie zostanie nigdy osiągnięty, a będzie jedynie coraz bardziej zbliżał się do ideału. Odnosi się to także do możliwości wprowadzenia tej koncepcji w Polsce. Wydaje się, że będzie to proces powolny, ale systematyczny ze względu na coraz większe zrozumienie korzyści płynących z posiadania elementów, które są i w krótkim czasie mogą zostać połączone.

## BIBLIOGRAFIA

- [1] *15 milionów papierosów, 130 policjantów i barka*, „Gazeta Morska”, lokalny dodatek do „Gazety Wyborczej” z 30 czerwca 2004.
- [2] *Baltic Master. Maritime Safety Across Order. Project Information*, <http://www.balticmaster.org>.
- [3] Ficoń K., *Identyfikacja zagrożeń rzeczywistych i potencjalnych dla miasta portowego na przykładzie Gdyni*, [w:], *Człowiek i technika w systemach bezpieczeństwa i ochrony*, red. K. Chwesiuk, A. Ostrokólski, J. Sadowiski, E. Kołodziński, IV Międzynarodowa Konferencja Naukowa „Zarządzanie kryzysowe”, Akademia Morska, Szczecin 2006.
- [4] Garstka J. J., *Theory and practise of Network Centric Warfare*, materiały z konferencji „Conference Documentation from Network Centric Warfare Conference”, London, 10 & 11<sup>th</sup> September 2001.
- [5] Kasperek T., *Broń chemiczna zatopiona w Morzu Bałtyckim*, Wyd. Adam Marszałek, Toruń 1999.
- [6] Kasperek T., *Zagrożenia wynikające z zalegania amunicji chemicznej na dnie Bałtyku*, Bałtycki Kongres Bezpieczeństwa Europejskiego, Jurata 2006.
- [7] *Maritime Safety Umbrella Operation – MSUO*, [www.maritime-safety.org](http://www.maritime-safety.org).

---

<sup>32</sup> Według programu rozwoju sił zbrojnych USA *Joint Vision 2020* realizacja przedsięwzięć NCW będzie trwała co najmniej 25 lat, a przypuszczalnie dłużej. Wymagać będzie ona niekonwencjonalnych rozwiązań i zastosowania technologii, o których w tej chwili nie mamy jeszcze pełnego wyobrażenia. Por. R. Rugała, *Sieciocentryczna architektura Zautomatyzowanego Systemu Dowodzenia Marynarki Wojennej – marzenia czy potencjalna możliwość?*, XI Konferencja Naukowa „Automatyzacja Dowodzenia”, Pieczęta, 24 – 26 września 2003, s. 3.

- [8] Pargeter A., *Western converts to radical Islam: the global jihad's new soldiers?* „Jane's Intelligence Review”, 2006, Vol. 18, No 8.
- [9] Peterson G. I., *The Father of Network-Centric Warfare. A Salute to Voice Admiral Arthur K. Cebrowski*, „Naval Forces”, 2001, No 1.
- [10] Rokiciński K., *Zagrożenia asymetryczne w Regionie Bałtyckim*, Warszawa 2006.
- [11] Romba R., Schäfer S., *REACH BACK – Move information, not people*, „Europäische Sicherheit”, 2006, Nr 8.
- [12] Rugała R., *Przyszłość morskich systemów wymiany danych w aspekcie koncepcji działań sieciocentrycznych*, X Sympozjum Wojskowej Techniki Morskiej, Puck, 19 – 20.10.2005.
- [13] Sadkowski R., *Bezpieczeństwo Sopotu*, Bałtycki Kongres Bezpieczeństwa Europejskiego, Jurata 2006.
- [14] Sorman G., *Kim są terroryści i jak się ich pozbyć?*, „Dziennik. Polska, Europa, Świat” z 21 sierpnia 2006.
- [15] Stokalski A., Kulicki R., *C-commerce, C-government, NCW: Konwergencja doktryn i technologii*, X Konferencja „Automatyzacja Dowodzenia”, Jelenia Góra, czerwiec 2002.
- [16] Stokalski A., *Sieciocentryczna architektura zautomatyzowanych systemów dowodzenia – Bazowa Infrastruktura Informacyjna (Network-centric warfare – the base of infostructure)*, VIII Konferencja „Automatyzacja Dowodzenia”, Jelenia Góra, maj 2000.
- [17] Szubrycht T., *The security threats for Europe*, „Polish Journal of Environmental Studies”, 2005, Vol. 14, supplement 1.
- [18] Willet L., *UK defines its network ethos*, „Navy International”, 2006, Vol. 111, No 4.
- [19] Wolf R., *Ostsee wird zweispurig sicherer*, „TAZ-Bericht” z 28 lutego 2005.
- [20] Wspólny Dokument Programowy Program Współpracy Przygranicznej Phare 2001 – 2006. Estonia, Litwa, Łotwa, Polska, lipiec 2001.
- [21] *Z kim ma się wiązać NATO*, „Gazeta Wyborcza” z 22 listopada 2006.
- [22] AKTUALNOŚCI, 24.01.2006, *Nadzór i monitorowanie bezpieczeństwa ruchu statków w obszarze Służby Kontroli Ruchu Statków VTS Zatoka Gdańska w roku 2005*, <http://www.umgdy.gov.pl/pium/jednostka?menuId=2972&kodJednostki=rxm59jacv2.rsc9w4acv1 &id=12226>.
- [23] *Can we control Baltic Sea*, materiały z konferencji, Gdańsk, 7 – 8 listopada 2005.

## **ABSTRACT**

The paper considers possibilities of using the network centric concept in maritime areas of Poland. The idea is analysed taking into consideration the existing security system in the Baltic Region.

Recenzent kmdr dr hab. Mariusz Zieliński, prof. AMW