Skuteczność i jakość w dowodzeniu

Jarosław Wołejszo

Skuteczność w dowodzeniu jest jednym z najważniejszych elementów przygotowania i prowadzenia działań militarnych i niemilitarnych. Skuteczność taką zapewniają między innymi zautomatyzowane systemy wspomagania dowodzenia i kierowania walką. One dostarczają informacji o przeciwniku jak i wojskach własnych. Od terminowości i aktualności tychże informacji zależy powodzenie w walce. W niniejszym artykule przedstawiono ważność zautomatyzowanych systemów kierowania i dowodzenia walką podczas planowania i prowadzenia współczesnych działań.

Wstęp

W XXI w. społeczność krajów wysoko rozwiniętych stało się społeczeństwem typowo informacyjnym w którym informacja nabrała ogromnej wartości. Stała się dobrem, bez którego bardzo ciężko osiągnąć sukces gospodarczy. Posiadanie aktualnej i wiarygodnej informacji, zdolność jej szybkiej obróbki i wymiany jest obecnie niezbędnym wyznacznikiem nowoczesności, a umiejętność jej sprawnego wykorzystania decyduje o sposobie postępowania w bliższej lub dalszej przyszłości.

Z tego względu coraz większego znaczenia nabiera przede wszystkim sprawna i szybka obróbka (przetwarzanie) informacji. Dotyczy to w głównej mierze organizacji i instytucji, których istnienie zależy od umiejętności przetwarzania posiadanych informacji. Szybki, niezakłócony i zrozumiały proces przetwarzania informacji jest gwarantem sprawnego działania i osiągnięcia sukcesu.

Gwałtowny zwrot nastawienia na informację jako dobra konsumpcyjnego o największej wartości zapoczątkowany został przez rozwój szeroko rozumianych technik informatycznych. Dzięki komputerom i oprogramowaniu na nich zainstalowanym zostało zainicjowane znaczne przyspieszenie wszelkiego rodzaju procesów decyzyjnych, wykorzystujących coraz większe

zasoby danych. Podejmowanie decyzji stało się obecnie dużo bardziej racjonalne, a ich trafność jest coraz większa.

Niemniej jednak, aby proces podejmowania decyzji (proces dowodzenia) z wykorzystaniem szeroko rozumianych technik komputerowych (w tym zautomatyzowanych systemów dowodzenia) był realizowany poprawnie niezbędne jest odpowiednie podejście do problemu potrzeb informacyjnych. Wsparcie informatyczne procesu podejmowania decyzji wymaga ustalenia, w pierwszej kolejności, powiązań informacyjnych występujących pomiędzy wszystkimi uczestnikami tego procesu. Ustalenie uczestników wymiany informacji jest niezbędne dla określenia potrzeb informacyjnych zautomatyzowanego systemu dowodzenia. Od jego prawidłowej identyfikacji zależy efektywność wykorzystania posiadanych zasobów informatycznych, a co za tym idzie także trafność i szybkość podejmowanych decyzji.

Wykorzystanie wiedzy z prakseologii do zwiększenia sprawności dowodzenia wynika z faktu, że w obu dziedzinach mówimy o sprawnym działaniu ludzi (żołnierzy) pamiętając, że prakseologia dotyczy sposobów ulepszania działań natomiast dowodzenie uczy, jak organizować i prowadzić wszelkiego rodzaju działania militarne i niemilitarne. Wszelkiego rodzaju działania żołnierzy na polu walki nie są działaniami organizacji, ale za przykładem T. Kotarbińskiego „(…) uczestnicy walki podobnie postępują w walce mikro-, jeden na jednego, i na wysokim szczeblu dowodzenia, w walce makro-, armia z armią[1]", zaświadcza o możliwościach wykorzystania wiedzy wynikającej z prakseologii do praktycznego zastosowania w dowodzeniu. Zarówno w prakseologii jak i dowodzeniu zależy przede wszystkim na sprawnym prowadzeniu działań zbrojnych i niezbrojnych. Dowódcy planując wszelkiego rodzaju operacje militarne i niemilitarne zwracają uwagę przede wszystkim, aby straty wśród żołnierzy były jak najmniejsze. Współcześnie użycie wszelkiego rodzaju wojsk możliwe jest w bardzo zmiennym i złożonym otoczeniu, a od sprawności użycia tychże wojsk zależy sukces. Jednym z elementów, które pozwolą osiągnąć sukces i przewagę względem przeciwnika jest posiadanie przez dowódców aktualnej informacji o przeciwniku i własnych siłach użytych do walki. Taką informację (bieżącą) zapewnia wspólny obraz operacyjny (*Common Operational Picture,* COP) z jednej strony jest warunkiem koniecznym do uzyskania indywidualnej oraz współużytkowanej świadomości przez uczestników walki, ale ze względu na różnorodność operacji w jakich siły zbrojne mogą uczestniczyć, musi być też widziany jako

[1] T. Kotarbiński, *Traktat o dobrej robocie*, Łódź, Zakład im. Ossolińskich we Wrocławiu, 1965.

zależny od sytuacji, a więc dynamiczny segment powiązań informacyjnych między elementami organizacji prowadzącej działania. Zatem, zawartość COP będzie różna dla różnych grup użytkowników, w różnych misjach czy różnych ich etapach, a spowodowane jest to dużą zmiennością w trakcie działań, zarówno w zakresie powiązań społecznych (różne grupy uczestników i relacje między nimi) oraz powiązań informacyjnych (zmienne potrzeby informacyjne zależne od realizowanych zadań przez poszczególnych użytkowników). Inne zapotrzebowanie na informację będą miały dowództwa i sztaby w trakcie działań wojennych o dużej intensywności, a inne w misjach stabilizacyjnych czy humanitarnych. W zależności od misji również zmieniał się będzie zakres powiązań społecznych – od współpracy między elementami ugrupowania sił zbrojnych, poprzez ośrodki kierowania cywilnymi organizacjami rządowymi do agend cywilnych, międzynarodowych organizacji pozarządowych. Wspólny obraz sytuacji operacyjnej już samym określeniem rodzi wiele odniesień wymagających wyjaśnienia i zdefiniowania. Samo „wspólny", czy tworzony wspólnie przez wszystkich walczących po jednej stronie, czy do wspólnego wykorzystania, czy też jedno i drugie. Tak jedno i drugie. Łatwiej jest zdefiniować „obraz sytuacji operacyjnej". W praktycznej pracy sztabów dowództw wszystkich szczebli i dowódców pododdziałów (bez sztabów) „obrazem sytuacji operacyjnej" jest rzeczywiste położenie sił i środków w terenie, na akwenie lub w powietrzu, rysowane na mapach z oznaczeniem ich stanu, rodzaju aktywności, działania. Takie położenie rysuje się na mapach sytuacyjnych z bezpośredniej obserwacji pola walki i meldunków, sygnałów i znaków przekazywanych przez podwładnych. Dany dowódca odbierając meldunki ocenia ich wiarygodność i w przypadkach wątpliwości żąda potwierdzenia, wysyła żołnierza do sprawdzenia, bądź osobiście udaje się do miejsca, z którego może uzyskać wyjaśnienie sytuacji. Rzeczywista sytuacja operacyjna jest dynamiczna po obu stronach, tyle, że o tej drugiej stronie – o przeciwniku, wiemy tyle ile zdołamy rozpoznać.

Wykorzystanie nowoczesnych technologii (zautomatyzowane systemy wspomagania dowodzenia i kierowania walką) do jakościowego przewartościowania sprawności dowodzenia poprzez automatyzację jego procesów może doprowadzić do stanu, w którym możliwie najwierniejszy obraz sytuacji operacyjnej pojawiał się będzie na wszystkich szczeblach dowodzenia z opóźnieniami niepozwalającymi na ucieczkę celów, obiektów i tym samym na efektywne ich rażenie.

Ta przesłanka musi dominować w rozwiązywaniu problemu wspólnego obrazu sytuacji operacyjnej. Z niej powinny wynikać podstawowe

wymagania, co do aktualności (terminowości), treści, sposobu prezentacji możliwości dystrybucji, selekcji i doboru według potrzeb użytkowników oraz przenoszenia sytuacji do oprogramowania obsługującego procesy planowania operacyjnego, ogniowego i logistycznego.

Odpowiedź, dla kogo ma być wspólny obraz to nie tylko sprawa wyobraźni, ale wynik analizy zasad sztuki wojennej oraz możliwości sił i środków ścierających się stron. Wspólny obraz sytuacji operacyjnej (COP) to tworzony wspólnie i jednocześnie przez wszystkich walczących po jednej stronie oraz przez ich źródła czujnikowe obraz wykorzystywany w dowodzeniu i kierowaniu. Idea jawi się jako zapis w serwerach zdefiniowanych informacji, które są jednoznaczne i niepowtarzalne. To jednorodna strukturalnie baza – umiejscowienia obiektów wraz z ich głównymi atrybutami. Dane po przetworzeniu przedstawią obraz sytuacji na ekranach stacji roboczych poszczególnych osób funkcyjnych danego organu dowodzenia, oczywiście po uzyskaniu przez te osoby funkcyjne uprawnień do odczytu danego obrazu.

Zautomatyzowane systemy dowodzenia w działaniach militarnych

Skuteczność wykorzystania nowych technologii w tym głównie narzędzi informatycznych zależy od sposobu organizacji wsparcia informatycznego procesu dowodzenia. Powinno być one rozpatrywane w dwóch płaszczyznach. Pierwsza z nich to wsparcie informatyczne (jako czynności decyzyjno-organizacyjne) realizowane na konkretne żądanie przez odpowiednie komórki sztabu i podległe im wyspecjalizowane siły.

Kolejna płaszczyzna wsparcia informatycznego dowodzenia polega na wykorzystaniu w procesie dowodzenia narzędzi informatycznych (instrumentów) wspomagających podejmowanie decyzji. Z prakseologii wynika, że „(...) przy pomocy niektórych instrumentów pracuje się bez porównania ekonomiczniej niż bez nich. (...) Rozmaite narzędzia i w ogóle narzędzia techniczne pozwalają w wybitnym stopniu minimalizować interwencję”[2]. Takimi środkami są m.in. zautomatyzowane systemy dowodzenia. To dzięki nim można skrócić cykl decyzyjny a tym samym osiągnąć przewagę nad przeciwnikiem. Tak dwojako rozumiane wsparcie informatyczne dowodzenia jest ze sobą bardzo ściśle powiązane. Wsparcie informatyczne powinno zapewnić właściwe funkcjonowanie posiadanych środków informatycznych w tym przede wszystkim zautomatyzowanych systemów dowo-

[2] *Ibidem*, s. 196

dzenia. Środki te będą funkcjonowały efektywnie tylko wtedy, gdy zostanie m.in. przeprowadzony w sposób poprawny proces identyfikacji powiązań i potrzeb informacyjnych.

Nie ulega wątpliwości, że wprowadzenie na szeroką skalę do wojsk tego rodzaju narzędzi wpłynie bezpośrednio i pośrednio na specyfiką sprawowania dowodzenia. Jednocześnie podkreślić należy, że w obszarze zainteresowania Sił Zbrojnych RP największe znaczenie ma wciąż rozwijany zautomatyzowany system wspomagania dowodzenia „C3IS Jaśmin", który poza swym głównym zadaniem – informatycznego wsparcia pracy dowódców i oficerów sztabów, ma w założeniach „spiąć" w całość inne funkcjonujące zautomatyzowane systemy walki i dowodzenia, pracujące na korzyść poszczególnych rodzajów wojsk. Oznacza to, że wspomniany system będzie odgrywał szczególną rolę w dowodzeniu najliczniejszym rodzajem Sił Zbrojnych naszego kraju.

Nie ulega wątpliwości, iż współczesne prowadzenie działań militarnych i niemilitarnych wymaga umiejętnego planowania i synchronizacji działań wielu szczebli dowodzenia oraz rodzajów wojsk. Posiadanie takich możliwości powiązane ze zdolnością do szybkiego przekazywania informacji stanowi zasadnicze uwarunkowanie zwiększenia efektywności i skuteczności sprawowanego dowodzenia. Jest to jednak możliwe tylko w przypadku dysponowania nowoczesnym, wysoce sprawnym zautomatyzowanym systemem wspierającym dowodzenie, pozwalającym na integrację wszystkich elementów ugrupowania bojowego zaangażowanych w prowadzone działania. Osiągnięcie celu działań w nowych uwarunkowaniach oraz użycie nowoczesnych systemów rozpoznania i rażenia jest praktycznie niemożliwe przy korzystaniu z „tradycyjnych" środków dowodzenia.

Z przedstawionych uwarunkowań wynika jednoznacznie, że współczesnym i przyszłym wymaganiom można będzie sprostać tylko w przypadku posiadania sprawnego systemu dowodzenia, z jednej strony koordynującego proces obiegu informacji, z drugiej zaś wspierającego podejmowanie decyzji, opartego na maksymalnym wykorzystaniu możliwości współczesnych technologii przetwarzania danych. Właśnie automatyzacja systemu dowodzenia będzie decydować o efektywności dowodzenia, a tym samym o uzyskaniu powodzenia w potencjalnym konflikcie zbrojnym.

Zalety wykorzystania nowoczesnych technologii w dowodzeniu

Wyniki analizy literatury przedmiotu i samej istoty koncepcji sieciocentrycznej (*Network Centric Warfare*, NCW – wojny sieciocentrycznej) pozwalają na stwierdzenie, że zdigitalizowane siły, wykorzystujące wszystkie zalety wynikające z zasad działań sieciocentrycznych, będą w stanie, poprzez właściwe wykorzystanie przewagi informacyjnej przeciwstawić się siłom przeciwnika ze skutecznością dotąd niespotykaną. Jako przykład posłużyć może ćwiczenie prowadzone przez Amerykanów w 2001 r. (a więc na wczesnym etapie rozwoju koncepcji NCW) na poligonie w Kalifornii, gdzie po stronie sił własnych działały dwie brygady 3 Dywizji Piechoty wspierane przez samoloty F-16 i A-10 Sił Powietrznych Gwardii Narodowej. Struktury te zostały „usieciowione" w stopniu dotąd nie spotykanym i spięte strukturą dowodzenia do działań połączonych. Dzięki temu samoloty Sił Powietrznych dysponowały przez cały czas aktualną informacją o sytuacji naziemnej, zapewniając jednocześnie wojskom lądowym dopływ informacji nieosiągalnych z innych źródeł rozpoznania. W konsekwencji, ćwiczące siły bez problemów pokonały silniejszego i bardziej doświadczonego przeciwnika.

Można zatem stwierdzić, a właściwie potwierdzić, że 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, że 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[3]:

1. Siły NCW mogą być mniej liczne niż dotąd (w relacji: zadanie do wykonania – siły niezbędne do wykonania zadania), zyskując nową jakość w zakresie szybkości i manewrowości, ze względu na fakt mniejszych potrzeb tak transportowych, jak i logistycznych. Zachowują jednocześnie zdolność do efektywnego działania, co więcej – przy mniejszych jego kosztach.
2. Działania NCW umożliwiają wdrożenie i stosowanie nowej taktyki. Podczas operacji w Iraku siły amerykańskie podczas natarcia stosowały formę manewru nazywaną „taktyką roju". Dzięki posiadaniu ciągłej informacji o tym gdzie znajdują się pozostałe własne woj-

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

ska, elementy ugrupowania bojowego mogły poruszać się w małych, samodzielnych formacjach, unikając koncentrowania dużej ilości sprzętu w jednym miejscu i ciasnego „łokieć w łokieć" ugrupowania bojowego[4]. Tak zorganizowany manewr przebiegał szybko, zaś jeśli 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 przewagi posiadania informacyjnej i wspólnej świadomości sytuacji na polu walki).

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 Centrum Operacyjnego, gdzie umieszczana 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.

Można stwierdzić, że z operacyjnego punktu widzenia do zasadniczych korzyści osiąganych poprzez wdrażanie sieciocentryzmu zaliczyć należy:

- mniejszą ilość sił (żołnierzy i sprzętu) niezbędną do wykonania zadania, co redukuje szeroko rozumiane koszty działań;
- „rozśrodkowanie" sił własnych które, działając w niewielkich zgrupowaniach, utrudniają przeciwnikowi skuteczne zlokalizowanie, identyfikację i rażenie;
- możliwość kontrolowania znacznie większego obszaru terenu przez relatywnie niewielkie siły własne, nie zmuszone do utrzymywania określonego, sztywnego szyku (ugrupowania) bojowego;
- zmniejszenie zagrożenia zadawania strat siłom własnym (*blue on blue*), 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 (*commander's intent*);

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

- łatwiejszą ocenę sytuacji (decydenci mają możliwość „widzieć" przestrzeń walki w czasie prawie rzeczywistym, będąc zasilanymi informacjami 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 zadania będą adekwatne do rzeczywistej sytuacji, nie zaś spóźnione, a tym samym błędne.

Wady wykorzystania nowoczesnych technologii w dowodzeniu

Założenia NCW, jak każdej nowej koncepcji czy idei, nie są 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 zarzutów wymienić należy[5]:

1. przywiązywanie przesadnej wagi do informacji – przecenianie informacji;
2. niedocenianie potencjalnego przeciwnika;
3. problemy z interoperacyjnością;
4. ograniczenia w przepływie informacji;
5. niepewność co do przyszłego panowania w przestrzeni kosmicznej;
6. niekontrolowany wypływ technologii informatycznych;
7. niebezpieczeństwo wynikające z zagrożeń asymetrycznych;
8. narażenie na ataki w cyberprzestrzeni;

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

Przywiązywanie przesadnej wagi do informacji – przecenianie informacji

Analiza ocen krytycznych wskazuje, że zdaniem części specjalistów transmisja informacji nie jest wystarczającym substytutem manewru na polu walki i konwencjonalnych możliwości bojowych. Podkreśla się ponadto, że przewaga informacyjna oraz szeroko dostępna świadomość sytuacji to nie jedyne, czy też najważniejsze, części składowe siły bojowej na polu walki. Pojawiają się również obawy, że pewność siebie wynikająca z przekonania, że dowódca wie wszystko co mu potrzebne do podjęcia decyzji, może spowodować początkowo lekceważenie, a ostatecznie całkowity zanik umiejętności analizy działań przeciwnika, stanowiącej podstawę wojskowego procesu decyzyjnego. Podkreśla się także, że siły zbrojne „zachłysnęły się" nowoczesnymi technologiami ery informacyjnej, ale jednocześnie nie przeprowadziły rzetelnej analizy ryzyka w zakresie rzeczywistego wdrożenia doktryny militarnej, opartej całkowicie na (uzależnionej od) tak zdobywanych i przesyłanych danych. Formowane są także zarzuty, że wzrost przetwarzanych informacji często prowadzi (wymusza) do jakościowych zmian w organizacji. To z kolei, co wskazuje praktyka zarządzania, nie zawsze owocuje zwiększeniem sprawności jej działania, zaś nadmierne zaufanie do skomplikowanych (a zdaniem krytyków zawodnych) systemów informacyjnych może prowadzić do nieprzewidywalnych problemów na realnym polu walki. Nie neguje się faktu, że niespodziewanie duża ilość informacji może kreować wiele nowych, nieprzewidywalnych wcześniej okazji działania. Jednak zdaniem niektórych ekspertów, może to prowokować dowódców do zmiany otrzymanych wcześniej zadań w tak dużym zakresie, który może generować poważne problemy. Jako przykład takiego niebezpieczeństwa podaje się, że pierwszym zauważalnym skutkiem cyfryzacji było wielokrotnie większe niż zazwyczaj (w podobnych sytuacjach) zużycie amunicji. Wpłynął na to fakt, że dowódcy „znaleźli się" w środowisku walki, w którym „roi się" od potencjalnych celów. Zamiast więc identyfikować i zwalczać obiekty rzeczywiście istotne z punktu widzenia działania, rażono wszystko, co znajdowało się w zasięgu posiadanych środków. To z kolei spowodowało konieczność gwałtownego odtwarzania zapasów, przeciążenie logistyki i ogólne trudności w logistycznym zasilaniu pola walki.

Niedocenianie potencjalnego przeciwnika

Oponenci NCW podkreślają, że cała nowa koncepcja działań oparta jest na nieodpowiedzialnym niedocenianiu potencjalnego przeciwnika. Zauważa się, że jakiekolwiek możliwości strony przeciwnej w zwalczaniu lub zakłócaniu sensorów czy też blokowaniu przekazu informacji, są w zasadzie

całkowicie lekceważone. Na poparcie takiej tezy podawany jest fakt, że filozofia NCW, nowych technologii i sposobów ich stosowania jest publikowana całkowicie jawnie. Takie podejście do bezpieczeństwa daje więc potencjalnemu przeciwnikowi czas na systematyczną ocenę sytuacji i planowanie, jak znaleźć i wykorzystać słabe strony koncepcji.

Problemy z interoperacyjnością

Wśród ekspertów wojskowych pojawiają się wątpliwości, czy możliwe jest osiągnięcie rzeczywistej i pełnej interoperacyjności między rodzajami sił zbrojnych, niezbędnej dla prowadzenia rzeczywistych działań połączonych. Wątpliwości te wynikają ze świadomości różnic, jakie dzielą poszczególne rodzaje sił zbrojnych. Chodzi zarówno o rozbieżne zasady działania (taktyka, sztuka operacyjna), różnice w procedurach dowodzenia oraz możliwościach działania w konkretnych, specyficznych dla jednego rodzaju sił zbrojnych środowiskach. Stawiane są pytania, czy możliwe jest np. sprowadzenie do wspólnego mianownika doktryny marynarki wojennej, stworzonej do działań na morzu i wojsk lądowych, przewidzianych do walki w diametralnie różnym otoczeniu.

Ograniczenia w przepływie informacji

Kolejne pytania dotyczą obaw, czy istniejące środki transmisji informacji będą w stanie sprostać ciągle rosnącym wymaganiom sił zbrojnych. Dotychczasowe doświadczenia wykazują bowiem, że zdarzały się sytuacje, kiedy przepustowość kanałów informacyjnych okazywała się niewystarczająca. W takich przypadkach wojskowi operatorzy systemu „ręcznie" decydowali o priorytecie wysyłania wybranych danych. Powodowało to opóźnienia lub wręcz kasowanie danych, którym z konieczności nadano niższy priorytet. W połączeniu z nadmiernym zaufaniem do technologii prowadziło 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, traktowane są przez sceptycznych ekspertów jako bardzo poważne zagrożenia.

Niepewność co do przyszłego panowania w przestrzeni kosmicznej

Podkreśla się, że w chwili obecnej USA dominują w przestrzeni kosmicznej, która odgrywa niepoślednią rolę w koncepcji NCW. Przewaga ta była

bezwzględnie wykorzystana podczas dwóch wojen w Zatoce Perskiej oraz podczas działań w Afganistanie. Oponenci wskazują jednak, że było to możliwe, ponieważ strona przeciwna w ogóle nie wykorzystywała przestrzeni kosmicznej. W związku z tym, nie można mieć absolutnej pewności, że 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 lub w Chinach) i wykorzystywania zaawansowanych technologii.

Niekontrolowany wypływ (proliferacja) technologii informatycznych

Wzrost powszechnego dostępu do zaawansowanych technologii może doprowadzić do niekontrolowanego przepływu wiedzy i technologii w „niepożądane ręce". W konsekwencji stanowi to, zdaniem sceptyków, przesłankę do utraty globalnej przewagi w tym zakresie przez USA i może stanowić kolejne poważne zagrożenie dla koncepcji NCW, niwelujące jej silne strony. Takie samo zagrożenie związane jest ze stosowanym przez przedsiębiorstwa pracujące dla obronności *outsourcingiem* tym bardziej, że wiele zamówień na potrzeby sił zbrojnych realizuje się w Azji (m.in. w Chinach i Indiach). Już obecnie 80 proc. 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, można więc mówić o trendzie stopniowej utraty technologicznej suwerenności.

Niebezpieczeństwo wypływające z zagrożeń asymetrycznych

Wśród asymetrycznych zagrożeń, które mogą być kierowane przeciwko koncepcji NCW (w sensie neutralizacji sensorów lub innych działań zmierzających do zmniejszenia skuteczności zaawansowanego technologicznie uzbrojenia) wymienia się m.in.:

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

Zagrożenie to jest tym większe, że wśród już aresztowanych terrorystów znajdują się osoby, które studiowały (często w USA) na kierunkach związanych z zaawansowanymi technologiami. Oznacza to, że organizacje terrorystyczne mogą dysponować wiedzą, jak przy użyciu stosunkowo prostych lub niekonwencjonalnych środków wykorzystać słabe punkty koncepcji NCW. Nie można też wykluczyć zagrożeń w rodzaju:

- zakłócania sygnałów satelitarnych i radiowych;
- niszczenia (uszkadzania) na odległość instalacji komputerowych;
- włamań do systemów komputerowych (kradzież i modyfikowanie danych).

Narażenie na ataki w cyberprzestrzeni

Oponenci koncepcji NCW podkreślają, że mimo licznych zabezpieczeń systemów teleinformatycznych, wciąż zdarzają się przypadki ataków hakerów, nierzadko zakończone powodzeniem. Nie można zatem wykluczyć sytuacji, w której państwo, strona przeciwna lub organizacja o charakterze niepaństwowym (przestępcza, terrorystyczna) 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 finezyjnie – 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 mniejszym lub większym stopniu charakter techniczny, podkreśla się niekiedy jeszcze jedną kwestię, osadzoną raczej w ludzkiej mentalności – jest to potencjalne zagrożenie dla sprawowania dowodzenia zgodnie z filozofią *mission command*. Ten styl dowodzenia opiera się na czterech filarach, z których decydujący mówi o inicjatywie podwładnych, nie ograniczanej przez przełożonych zbyt szczegółowymi instrukcjami (*micromanagement*). 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 odległych wydarzeń i obszarów zainteresowania dowódców niskich szczebli. Zjawisko to samo w sobie nie jest niczym złym. Doświadczenia wskazują jednak, że wielu wysokich dowódców próbuje ingerować w działania niskich szczebli dowodzenia, odbierając dowódcom tak potrzebną inicjatywę. W konsekwencji doprowadzić to może do sytuacji, w której podwładni przestaną odważnie reagować na zmienne realia pola walki i będą biernie czekać

na instrukcje „z góry". To zaś oznacza upadek koncepcji dowodzenia przez cele, która doskonale sprawdziła się w minionych konfliktach zbrojnych.

Podsumowując, walka (działania w środowisku) sieciocentryczna to odpowiedź sił zbrojnych na wyzwania ery informacyjnej. Teoria ta koncentruje się nie tyle na liczbie i jakości środków rażenia, co na sile możliwej do wygenerowania w wyniku efektywnego połączenia (sieciowania) elementów ugrupowania bojowego (decydentów, sensorów, systemów walki). Połączenie wszystkich sił prowadzących działania w jedną sieć informacyjną umożliwia uzyskanie wspólnej świadomości sytuacji i wygenerowanie jednolitego jej zobrazowania, dostępnego dla wszystkich uprawnionych użytkowników. Dysponując uaktualnianym w czasie rzeczywistym, jednolitym obrazem sytuacji, siły prowadzące walkę sieciocentryczną uzyskują przewagę informacyjną nad przeciwnikiem, co umożliwia im zwiększenie szybkości dowodzenia, tempa operacji, zwiększenie skuteczności uzbrojenia i odporności na uderzenia przeciwnika, a także lepszą synchronizację własnych działań.

Będzie sposobem prowadzenia działań, w którym siły zbrojne spięte siecią teleinformatyczną będą wykorzystywać przewagę informacyjną i pełną świadomość sytuacji (strategicznej, operacyjnej i taktycznej) do prowadzenia szybkich oraz skutecznych działań, pozwalających na pokonanie przeciwnika z możliwie najefektywniejszym i optymalnym ekonomicznie wykorzystaniem sił własnych.

Charakterystyka przykładowych zautomatyzowanych systemów dowodzenia w działaniach militarnych

Nazwa systemu	**LC2IS**
Kraj pochodzenia	**NATO**
Opis systemu	System LC2IS obsługuje wiele formatów standardowych interfejsów i protokołów, w tym: MIP-BL2, ADatP3 Rev 11 NFFI v 1.3, NVG 1.4 i 1.5. LC2IS składa się z szeregu zintegrowanych komponentów świadczących różne usługi niezbędne do przeprowadzenia planowania, koordynacji, przydział zadań, raportowania i oceny misji wojsk lądowych.

Nazwa systemu	**LC2IS**
Opis systemu	Szczegółowe obszary funkcjonalne dedykowane dla LC2IS to: • współpraca podczas planowania operacji lądowych • monitorowanie i ocena trwających działaniach lądowych • zapewnienie lądowego obrazu rozpoznania (RGP) • współpraca i synchronizacja • międzynarodowa integracja
Producent	NCIA (NATO Communications and Information Agency)
Referencje – wykorzystanie	ISAF (*International Security Assistance Force*)
Dedykowany poziom	Punkty dowodzenia
Interfejsy wymiany danych	NFFI MIP Baseline 2.0 MIP Baseline 3.1 OTH Goild ADatP-3 NVG 1.4

Źródło: opracowanie własne na podstawie: strona ćwiczenia CWIX https://tide.act.nato.int/cwix/ tłumaczenie autora (dostęp: 30 listopada 2017 r.).

Nazwa systemu	**CPOF (*Command Post of the Future*)** *Tactical Mission Command* (TMC)/*Maneuver Control System* (MCS)
Kraj pochodzenia	Stany Zjednoczone
Opis systemu	*Command Post of the Future* (CPOF) to oprogramowanie C2, które umożliwia dowódcy uzyskanie wysokopoziomowego przeglądu pola walki, współpracę z przełożonymi nad danymi otrzymywanymi w czasie rzeczywistym oraz zapewniającym platformę komunikacyjną. *Tactical Mission Command* (TMC) rozwija, integruje i zapewnia podstawowe wsparcie dla przeprowadzenia misji we współdzielonym środowisku; umożliwia dowódcom podejmowanie trafnych i efektywnych decyzji. Dostarcza funkcjonalności pozwalające na realizację w armii wizji stworzenia jednolitego środowiska przetwarzania na stanowiskach dowodzenia.

Producent	General Dynamics
Referencje – wykorzystanie	• Pierwsze wdrożenie dla Armii USA w Iraku w 1. dywizji kawalerzystów (1st Cavalry Division) w roku 2014 • Konsekwentnie wykorzystywany podczas wielu misji w Afganistanie • Brał udział w United States Joint Forces Command's Urban Resolve w roku 2015 • Wykorzystywany w Centrum Operacji Morskich USA od roku 2007
Dedykowany poziom dowodzenia	Kwatera dowodzenia, dowódcy oddziałów

Źródło: opracowanie własne na podstawie: https://fas.org/man/dod-101/sys/land/wsh2013/304.pdf; http://peoc3t.army.mil/mc/tmc.php tłumaczenie autora (dostęp: 30 listopada 2017 r.).

Nazwa systemu	**Land Command Support System**
Kraj pochodzenia	Kanada
Opis systemu	LCSS jest systemem kanadyjskiej armii wspierającym operacje wywiadowcze (rozpoznawcze), planowanie i działalność operacyjną. Jest on aktywnie wykorzystywany zarówno w krajowych jak i zagranicznych operacjach
Producent	Thales
Referencje – wykorzystanie	Siły Zbrojne Kanady
Dedykowany poziom dowodzenia	Stanowiska dowodzenia

Źródło: opracowanie własne na podstawie: http://searchrecherche.gc.ca/rGs/s_r?q=lcss&langs=eng&cdn=mdndnd&st=s&num=10&st1rt=0&s5bm3ts21rch=x&Action=Search tłumaczenie autora (dostęp: 30 listopada 2017 r.).

Nazwa systemu	**Bowman** *Battlefield Situational Awareness Module* (BSAM) ComBAT
Kraj pochodzenia	Wielka Brytania
Opisu systemu	*General Dynamics* UK jest głównym wykonawcą i integratorem Bowman, taktycznego systemu C4I dla brytyjskich sił zbrojnych. Bowman zapewnia mechanizmy automatycznego dostarczania pozycji, nawigowania oraz system raportowania, który umożliwia stworzenie świadomości sytuacyjnej jednostek w całej cyfrowej strukturze dowodzenia.
Producent	General Dynamics (UK)
Referencje – wykorzystanie	Wielka Brytania (UK)
Dedykowany poziom dowodzenia	Wszystkie

Źródło: opracowanie na podstawie: http://www.defense-aerospace.com/articles-view/release/3/12726/gdc2-cability-for-uk-bowman-(nov.15).html; https://www.generaldynamics.uk.com/?s=bowman tłumaczenie autora (dostęp: 30 listopada 2017 r.).

Nazwa systemu	**BULL BMS**
Kraj pochodzenia	Francja
Opisu systemu	Wojska mogą funkcjonować w jednym systemie w ramach batalionów, umożliwia on tworzenie wspólnych zadaniowych sił taktycznych, które mogą wymieniać się informacją podczas wykonywania zadań. Funkcjonuje na stanowiskach dowodzenia, pojazdach jak i używane przez pojedynczych żołnierzy. Dostarcza dowódcom bieżącą informację o położeniu.
Producent	ATOS
Referencje – wykorzystanie	Według producenta może mieć zastosowanie w siłach zbrojnych państw UE
Dedykowany poziom dowodzenia	Stanowiska dowodzenia, pojazdy jak i żołnierze

Źródło: opracowanie na podstawie: https://atos.net/en/products/defense-mission-critical/battle-management-system?utm_source=/battle-management-system/&utm_medium=301 (dostęp: 30 listopada 2017 r.).

Nazwa systemu	**System Wspomagania Dowodzenia C3IS JAŚMIN** moduł HMS C3IS JAŚMIN moduł BMS C3IS JAŚMIN moduł DSS C3IS JAŚMIN moduł JFSS C3IS JAŚMIN Wszystkie powyższe są elementami **Sieciocentrycznej Platformy Teleinformatycznej JAŚMIN** obejmującej infrastrukturę sprzętową (m.in. Zintegrowane Węzły Teleinformatyczne JASMIN) i programową.
Kraj pochodzenia	Polska
Oryginalny opis systemu	SWD C3IS JAŚMIN jest rozwiązaniem programowym – systemem wspierającym (w tym automatyzującym) procesy: dowodzenia i zarządzania walką na wszystkich szczeblach, do poziomu żołnierza spieszonego włącznie. Jest skalowalnym systemem C4I (*Command Control, Communications, Computers, and Intelligence*), który oferuje dostępny i łatwy w obsłudze, a zarazem kompleksowy zestaw narzędzi. Jego unikalną i pierwszorzędną cechą jest fakt, że posiada w sobie wiele podsystemów, które bazują na uniwersalnym zestawie usług tego kompleksowego produktu. SWD C3IS JAŚMIN tworzy i istotnie zwiększa świadomość sytuacyjną wojsk, zwłaszcza dowództw i sztabów, a także umożliwia m.in. tworzenie Połączonego Obrazu Sytuacji Operacyjnej – POSO. Ponadto SWD C3IS JAŚMIN zwiększa bezpieczeństwo komponentów wojskowych i elementów wchodzących w ich skład, w tym żołnierzy oraz pojazdów. SWD C3IS JAŚMIN (w tym każdy jego moduł) może występować również jako rozwiązanie autonomiczne i pracować samodzielnie. W ramach Sieciocentrycznej Platformy Teleinformatycznej JAŚMIN funkcjonuje też oprogramowanie do zarządzania, konfigurowania i monitorowania.
Producent	TELDAT (PL)
Referencje – wykorzystanie	SZ RP
Dedykowany poziom	Dowolny szczebel – korpus, dywizja, brygada, batalion, kompania, pluton, drużyna

Interfejsy wymiany danych	MIP Baseline 2, 3 i 3.1, ADEM (Multilateral Interoperability Programme) oraz JC3IEDM (STANAG 5525) NFFI (NATO Friendly Force Information) V.1.3 (IP1, IP2), SIP3, HUB (STANAG 5527) ADatP-36 (FFI-XML-MTF) Plany i Rozkazy (STANAG 2014) ADatP-3, APP-11(C) Baseline 11C/F, 12.2, 13 i 14 (STANAG 5500) APP6-A, APP6-B (Symbolika taktyczna) MIL-STD-2525B, MIL-STD-2525C NVG (NATO Vector Graphics) 1.4 i 1.5 JIPS (JCOP Information Product Services) 0.5 i 0.6 JDSS (STANAG 4677) Link 16, JREAP C, SIMPLE (STANAG 5602), Link 11B VMF (Variable Message Format) (MIL-STD 6018B i MIL-STD 47001D change 1) ATP-45 (CBRN – Chemical, Biological, Radilogical and Nuclear) ADatP-37 – CID Server (STANAG 5528) OTH-GOLD WMS (Web Map Service) WFS (Web Feature Service) HLA – High Level Architecture (STANAG 4603) Battlefield Directory (STANAG 4644)

Źródło: opracowanie własne na podstawie: https://www.teldat.com.pl/. Autor podkreśla, że w SZ RP wdrożony jest system wspomagania i dowodzenia C3IS Jaśmin (ok. 1 tys. licencji). Tylko w Wielonarodowym Korpusie Północno–Wschodnim w Szczecinie funkcjonuje angielska wersja systemu wsparcia dowodzenia SZAFRAN.

Zastosowanie zautomatyzowanych systemów kierowania i dowodzenia w działaniach kryzysowych – wnioski i doświadczenie

Zarządzanie kryzysowe w Polsce regulowane jest głównie przez *ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*. Siły Zbrojne w ramach reagowania kryzysowego realizują wiele działań wymagających szerokiej współpracy cywilno-wojskowej. Należą do nich:

- współudział w monitorowaniu zagrożeń;
- wykonywanie zadań związanych z oceną skutków zjawisk zaistniałych na obszarze występowania zagrożeń;
- wykonywanie zadań poszukiwawczo-ratowniczych;
- ewakuowanie poszkodowanej ludności i mienia;

- wykonywanie zadań mających na celu przygotowanie warunków do czasowego przebywania ewakuowanej ludności w wyznaczonych miejscach;
- współudział w ochronie mienia pozostawionego na obszarze występowania zagrożeń;
- izolowanie obszaru występowania zagrożeń lub miejsca prowadzenia akcji ratowniczej;
- wykonywanie prac zabezpieczających, ratowniczych i ewakuacyjnych przy zagrożonych obiektach budowlanych i zabytkach;
- prowadzenie prac wymagających użycia specjalistycznego sprzętu technicznego lub materiałów wybuchowych będących w zasobach Sił Zbrojnych Rzeczypospolitej Polskiej;
- usuwanie materiałów niebezpiecznych i ich unieszkodliwianie, z wykorzystaniem sił i środków będących na wyposażeniu Sił Zbrojnych Rzeczypospolitej Polskiej;
- likwidowanie skażeń chemicznych oraz skażeń i zakażeń biologicznych;
- usuwanie skażeń promieniotwórczych;
- wykonywanie zadań związanych z naprawą i odbudową infrastruktury technicznej;
- współudział w zapewnieniu przejezdności szlaków komunikacyjnych;
- udzielanie pomocy medycznej i wykonywanie zadań sanitarno-higienicznych i przeciwepidemicznych;
- wykonywanie zadań ujętych w wojewódzkim planie reagowania kryzysowego[6].

W Polsce istnieje kilka poziomów administracyjnych (na poziomach państwa, województwa, powiatu i gminy – rysunek s. 98), które muszą wymieniać informacje między sobą. Ich zadania polegają na: przygotowaniu planów zarządzania kryzysowego; przygotowaniu struktur używanych w sytuacjach awaryjnych; przygotowaniu i zarządzaniu zespołami ludzkimi potrzebnymi do wykonania zadań uwzględnionych w planach zarządzania kryzysowego; zarządzaniu bazami danych potrzebnymi w procesie zarządzania kryzysowego; przygotowaniu rozwiązań w przypadku zniszczenia zakłócenia najważniejszych elementów infrastruktury; zapewnieniu koordynacji pomiędzy planami zarządzania kryzysowego a innymi planami stworzonymi na tego typu użytek przez uprawnione władze publiczne; ocenie i przewidywaniu

[6] *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,* Dz. U. z 2007r. Nr 89, Poz. 590, art. 25.

zagrożeń (potencjalnych i rzeczywistych) oraz nadzorze, kontroli i zarządzaniu zarówno podczas sytuacji kryzysowych, jak i planowania.

Na każdym poziomie informacyjnym proces zarządzania może być przeprowadzany podczas dwóch głównych etapów, gdy nie ma widocznych zagrożeń i sytuacja jest jedynie monitorowana oraz w odpowiedzi na jakiekolwiek zagrożenie.

Rysunek. Struktura węzłów w sieciocentrycznym systemie zarządzania kryzysowego

Źródło: TELDAT

Podczas sytuacji kryzysowej istnieje potrzeba generowania raportów co określony interwał czasowy. W tego typu raportach mogą być przekazywane przede wszystkim informacje o ważnych zdarzeniach i akcjach wyspecjalizowanych jednostek, w tym ratowniczych – np. straży pożarnej. Często natura tych raportów jest statystyczna, jednakże w pewnych przypadkach mogą zawierać pewne elementy opisowe, o charakterze bardziej szczegółowym. Raporty powinny być osiągalne, zgodnie z ustaloną polityką bezpieczeństwa dla wszystkich uprawnionych jednostek, które współdziałają w czasie przeprowadzanych misji, w tym: wojska, policji, straży pożarnej i ratownictwa medycznego oraz grup pomocy zorganizowanych wśród cywili.

Jednostki ratownicze są oddzielną gałęzią odpowiedzi na zagrożenia. Ich aktywność skupiona jest na polu, gdzie na podstawie otrzymanych rozkazów planują swoje zadania. Gromadzą również wszelkiego rodzaju informacje, które są następnie przekazywane zgodnie z obowiązującą strukturą przepływu. Aby zapewnić efektywną strukturę należy zbudować spójny i bardzo sprawny system zbierania, przetwarzania i dystrybucji informacji obejmujący wszystkie węzły informacyjne i ogniwa stanowisk dowodzenia. Najbardziej odpowiednim pojęciem stworzonym do opisu sposobu organizacji i prowadzenia działań, zarówno cywilnych, jak i wojskowych w przedstawionej strukturze jest ich sieciocentryzm. Pojęcie to nie odnosi się jedynie do prostego zastosowania techniki informatycznej, ale również do stworzenia złożonego systemu, który może zrewolucjonizować charakter działań. Wymaga on czegoś więcej niż tylko „zastrzyku" technologii informacyjnej w postaci infrastruktury informacyjnej. Aby efektywnie wykorzystać dostępną informację potrzebne są wspólne koncepcje operacji różnych służb (biorących udział w reagowaniu kryzysowym), wspólne metody i podejście w sprawach dowodzenia i zarządzania oraz formy organizacyjne, doktryny, struktury sił i wsparcie serwisowe. Dzięki skutecznemu połączeniu lub „sieciowaniu" odpowiednich węzłów rozproszonych w sposób geograficzny, możliwe jest współdzielenie informacji, co przyczynia się do rozwinięcia świadomości i współpracy celem osiągnięcia samo-synchronizacji.

System Zarządzania Kryzysowego[7] jest portalem hostującym wiele podstron łączących użytkowników z usługami wykonującymi dedykowane zadania. Portal umożliwia zdobywanie i dystrybucję informacji, która następnie może być poddana analizie. Wśród modułów na portalu wyróżnić można wyspecjalizowane w obsłudze poszczególnych komórek organizacyjnych, jak i stworzone pod pojedynczych użytkowników.

System Zarządzania Kryzysowego JAŚMIN wraz z SZK WPJ był w ćwiczeniach Pierścień 2012 używany podczas demonstracji możliwości połączenia jednostek cywilnych i wojskowych. W ramach demonstracji przygotowano scenariusz, w którym zidentyfikowano kilka węzłów, pełniących odpowiednie role:

- Urząd Wojewódzki w Szczecinie;
- Urząd Powiatowy w Drawsku Pomorskim;
- Komenda Państwowej Straży Pożarnej.

[7] Znajduje się w laboratorium zautomatyzowanych systemów kierowania i dowodzenia w Państwowej Wyższej Szkole Zawodowej im. Prezydenta Stanisława Wojciechowskiego w Kaliszu.

Węzły te wymieniały informacje między sobą oraz ratownikami, rozmieszczonymi na poligonie. Każdy z węzłów wyposażony był w serwer z aplikacją zawierającą dane operacyjne. Serwery są wykonane w technologii umożliwiającej ich swobodne przenoszenie zgodnie z bieżącym zapotrzebowaniem.

Ponadto, na wyposażeniu użytkowników i grup ratowników, działających w rejonie poligonu w Drawsku Pomorskim, znalazły się nowoczesne terminale T1000 i T4 oraz urządzenia Znacznik Ratownika. Na terminalach osadzono oprogramowanie, które umożliwiało zarządzanie bieżącą oraz planowaną sytuacją prowadzonej misji, wizualizację na podkładzie mapowym symboliki, zgodnie z obowiązującymi w administracji normami, przesyłanie wiadomości tekstowych oraz planów i rozkazów. Urządzenia Znacznik Ratownika umożliwiały przekazywanie bieżącego położenia każdego z biorących udział w akcji ratowników oraz pojazdów. Ponadto są w stanie przekazywać informacje o incydentach.

Zakończenie

Wspólny Obraz Operacyjny (COP) z jednej strony jest warunkiem koniecznym do uzyskania indywidualnej oraz współużytkowanej świadomości przez uczestników działań, ale musi być też widziany jako zależny od sytuacji, a więc dynamiczny segment powiązań informacyjnych między elementami organizacji prowadzącej działania. Zawartość COP będzie inna dla różnych grup użytkowników, w poszczególnych misjach czy ich etapach, a spowodowane jest to dużą zmiennością w trakcie działań, zarówno w zakresie powiązań społecznych (różne grupy uczestników i relacje między nimi) oraz powiązań informacyjnych (zmienne potrzeby informacyjne zależne od realizowanych zadań przez poszczególnych użytkowników).

Podsumowując dotychczasowe rozważania, system wspierający wytwarzanie i dystrybucję COP powinien udostępniać swojemu użytkownikowi następujące funkcje:

- możliwość pobierania danych zarówno źródłowych jak i przetworzonych przez podległe systemy C2 oraz przeprowadzania odpowiedniej fuzji tych danych;
- możliwość skupienia uwagi na dowolnym obszarze zainteresowania w obrębie całego świata, złożenia sobie obrazu operacyjnego rozgry-

wającego się w tym obszarze zdarzenia z informacji dostarczanych przez wszystkie dostępne źródła danych;
- możliwość zobrazowania planowanych i przeprowadzanych misji na wielu różnych poziomach szczegółowości, poczynając od szczegółowej perspektywy niezbędnej dla dowódów operacji do bardzo ogólnego zarysu operacji dla przywódców cywilnych;
- możliwość przetworzenia ogromnej ilości niepowiązanych ze sobą na pierwszy rzut oka danych źródłowych w mający znaczenie i sens operacyjny ciąg zdarzeń, który jest jasno zrozumiały dla użytkownika oraz może być animowany (odtwarzanie i predykcja zdarzeń) zarówno w przód jak i w tył w czasie;
- możliwość zobrazowania zarówno jakości jak i pochodzenia informacji, tak aby użytkownik był w stanie ocenić wartość i wiarygodność analizowanych danych;
- możliwość pracy grupowej wielu decydentów na wspólnym obrazie sytuacji operacyjnej oraz możliwość jego wzbogacania o dane wypracowane w toku indywidualnej analizy sytuacji przez poszczególnych użytkowników (*Shared Situation Awareness*).

Zautomatyzowany system wspomagania dowodzenia oddziałuje bezpośrednio na sprawowanie dowodzenia, mając szczególnie istotny wpływ na proces dowodzenia. Możliwości techniczne systemu tego rodzaju pozwalają na:
- urealnienie przepływu informacji między komórkami funkcjonalnymi stanowisk dowodzenia, pomiędzy stanowiskami dowodzenia danego poziomu dowodzenia oraz ze stanowiskami dowodzenia przełożonego, podwładnych i współdziałających elementów ugrupowania komponentu zadaniowego;
- urealnienie „świadomości sytuacyjnej", dając osobom funkcyjnym stanowiska dowodzenia obraz sytuacji w czasie zbliżonym do rzeczywistego;
- przyspieszenie i urealnienie procesów planowania poprzez możliwość wykonywania różnorodnych kalkulacji;
- porównywanie i rozważanie wariantów działania metodami symulacyjnymi;
- znaczne skrócenie czasu opracowywania dokumentów tekstowych i graficznych;
- prowadzenie wieloaspektowych analiz w procesie dowodzenia, łącznie z symulacją dla poszczególnych rodzajów działań wojsk lądowych;

- wyeliminowanie zasadniczej części ręcznie wykonywanych a wysoce czasochłonnych prac sprawozdawczo-meldunkowych.

Wymiana informacji w środowisku zautomatyzowanych systemów dowodzenia odbywać się będzie w trzech zasadniczych relacjach, a mianowicie:

- służbowych (hierarchicznych, rozkazodawczych, synchronizacyjnych) – związanych z podległością służbową („w dół" – rozkazy i „w górę" – meldunki);
- koordynacyjnych – związanych z wymianą informacji pomiędzy osobami funkcyjnymi wewnątrz dowództw (wewnętrzne więzi informacyjne) lub wymianą informacji w ramach specjalności, uzupełnianiem potrzebnych informacji pomiędzy specjalnościami na tym samym poziomie lub pomiędzy różnymi szczeblami z pominięciem przełożonych (zewnętrzne więzi informacyjne współdziałania);
- współdziałania – związanych z wymianą informacji pomiędzy poszczególnymi stanowiskami dowodzenia niemających zależności służbowych, a wynikających bezpośrednio z wykonywanego zadania.