Henryk Kruszyński, Tomasz Ziemowit Kosowski

Sieciocentryczny aspekt współpracy cywilno wojskowej w działaniach kryzysowych

Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej nr 3, 119-135

2012

AUTOR
mgr inż. Henryk Kruszyński
mgr inż. Tomasz Ziemowit Kosowski

RECENZENT
płk prof. dr hab. inż. Jarosław Wołejszo

SIECIOCENTRYCZNY ASPEKT WSPÓŁPRACY CYWILNO-WOJSKOWEJ W DZIAŁANIACH KRYZYSOWYCH

Wstęp

Celem działania grup współpracy cywilno-wojskowej (CIMIC – *Civil-Military Co-Operation*) jest ustanowienie i utrzymywanie pełnej współpracy pomiędzy dowódcą wojskowym a środowiskiem cywilnym oraz koordynacja tych działań w obszarze odpowiedzialności, a także wspieranie tworzenia i ugruntowywania warunków służących osiągnięciu zakładanych celów operacji. Współpraca cywilno-wojskowa jest narzędziem umożliwiającym osiągnięcie wspólnych celów siłom reagowania, przeznaczonym do różnych zastosowań. Podczas działań zbrojnych jest jedynym niebojowym (niekinetycznym) narzędziem dowódcy w osiąganiu celów operacji. Najbardziej powszechny przykład takiej współpracy możemy odnaleźć w trakcie operacji kryzysowych, nie tylko związanych z konfliktami, lecz także przeprowadzanych podczas klęsk żywiołowych. Pomimo oczywistej potrzeby posiadania odpowiedniego narzędzia, które jednocześnie mogłoby wspierać zarówno cywili, jak i wojskowych, można zauważyć, że kanały komunikacyjne oraz współpraca z wojskiem są opracowywane w zależności od potrzeb, z wykorzystaniem dostępnych obecnie zasobów i panujących warunków sytuacyjnych. We wskazanych przykładowych planach prezentujących metodykę postępowania na wypadek zagrożenia kryzysem można znaleźć opisy użycia jedynie telefonów komórkowych i stacjonarnych do komunikacji[1]. Ciągłe zbieranie i rozpowszechnianie informacji, efektywna współpraca oraz świadomość sytuacyjna podczas sytuacji kryzysowej są czynnikami potrzebnymi do zapewnienia efektywnej kooperacji zarówno z wojskowymi, jak i cywilnymi organizacjami. Te czynniki mogą być osiągnięte poprzez analizę i zastosowanie doktryn i koncepcji North Atlantic Treaty Organization (NATO), jak na

[1] *Miejski plan reagowania kryzysowego. Plan główny. Załącznik nr 6.4*, Ośrodek koordynacyjno-informacyjny ochrony przeciwpowodziowej. Regionalny zarząd gospodarki wodnej w Krakowie, http://oki.krakow.rzgw.gov.pl/ [dostępne: 09.07.2012].

przykład NNEC[2], EU NEC[3] czy też CIMIC[4], oraz poprzez użycie najnowszych technologii informatycznych zarówno w zakresie sprzętu, jak i oprogramowania.

Współpraca cywilno-wojskowa w operacjach reagowania kryzysowego poza terytorium kraju

Współczesne operacje wojskowe mogą być prowadzone przy użyciu zgrupowań o składzie narodowym, sojuszniczym lub wielonarodowym. Operacje wielonarodowe z udziałem komponentów cywilno-wojskowych prowadzi się pod auspicjami Organizacji Narodów Zjednoczonych (ONZ), NATO, Unii Europejskiej (UE) lub Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE). Operacje tzw. spoza art. 5 *Traktatu waszyngtońskiego* coraz częściej nazywamy operacjami reagowania kryzysowego[5]. Są *to działania przy użyciu sił zbrojnych skierowane na usuwanie przyczyn sytuacji kryzysowych lub kryzysów zagrażających regionalnemu lub światowemu bezpieczeństwu oraz powodujących naruszenie praw człowieka*[6].

Operacje reagowania kryzysowego według NATO obejmują[7]:

- operacje ratowniczo-poszukiwawcze;
- operacje ewakuacyjne;
- świadczenie pomocy w przypadku katastrof lub klęsk żywiołowych;
- operacje wsparcia władz cywilnych;
- operacje egzekwowania sankcji i embarga;
- operacje wsparcia pokoju (utrzymanie pokoju, wymuszanie pokoju, zapobieganie konfliktom, tworzenie pokoju, budowanie pokoju, operacje humanitarne).

Działalność CIMIC w operacjach reagowania kryzysowego w SZ RP reguluje *Doktryna współpracy cywilno-wojskowej Sił Zbrojnych RP*[8], wydana na podstawie AJP-09.

---

[2] Zob. *NATO Network-Enabled Capability (NNEC) – Vision & Concept*, Supreme Allied Commander Transformation Organization, 2006.

[3] Zob. *Extract From The NEC Vision – EU NEC Vision Report*, www.eda.europa.eu [dostępne: 06.07.2012].

[4] Zob. *AJP-9., NATO Civil-Military Co-Operation (CIMIC) Doctrine*, NATO Standarization Agency, 2003.

[5] Zob. *AJP 3.4 –Allied Joint Doctrine for non-article 5 Crisis Response Operations*, NATO Standarization Agency, 2004.

[6] A. Czupryński, *Współczesna sztuka operacyjna*, AON, Warszawa 2009, s. 241.

[7] Zob. L .Elak, *Komponent cywilno – wojskowy w operacjach reagowania kryzysowego*, AON, Warszawa 2011.

[8] *DD/09 – Doktryna współpracy cywilno-wojskowej Sił Zbrojnych RP*, MON, Warszawa 2004.

Koncepcja współpracy wojsk lądowych i grup cywilnych nie jest nową ideą, jednakże do dziś rysuje się jako wyzwanie w zakresie metodologii wymiany informacji i poleceń. Interakcja i jej przebieg pomiędzy siłami militarnymi oraz środowiskiem cywilnym są kluczowe dla sukcesu operacji. Dowodzeniem i zarządzaniem są objęte siły, które współistnieją, bądź czasami są wręcz kreowane w kontekście wybranej misji z jasno zdefiniowanymi celami. Dowodzenie i zarządzanie obejmuje:

- narodowe i lokalne jednostki rządowe oraz pozarządowe;
- organizacje międzynarodowe;
- lokalne i narodowe siły reagowania oraz organizacje społeczne, takie jak: policja, straż miejska czy straż pożarna.

W obrębie jednostek wojskowych istnieją zespoły cywilno-wojskowe, które są ściśle zintegrowane w ogólną strukturę dowodzenia. Zespoły te stanowią integralną część planu dowódcy, egzystują w zakresie całościowej strategii przy jednoczesnym założeniu, że odpowiedzialności podczas przeprowadzania misji mogą być czasowo przekazane ze struktury wojskowej do cywilnej.

Zespoły CIMIC realizują swoje zadania poprzez:

- identyfikowanie i wymianę informacji dotyczącej wspólnie realizowanych celów;
- współpracę z podmiotami na odpowiednim poziomie i usuwanie konfliktów w przypadku nakładających się kwestii;
- zaangażowanie się w planowanie z odpowiednimi zespołami cywilów, ekspertów i zarządców, zarówno przed, jak i w czasie trwania operacji, oraz analizę i ewaluację wniosków i najlepszych praktyk po ich zakończeniu;
- pracę w zintegrowany sposób z pozostałymi rodzajami zespołów nad wszystkimi aspektami operacji;
- prowadzenie stałej oceny środowiska, w tym lokalizowanie regionalnych potrzeb w celu zidentyfikowania zasięgu zagrożenia i sposobu jego zlikwidowania;
- prace nad terminowym i sprawnym przekazaniem cywilnych odpowiedzialności do wojskowych, odpowiednich ekspertów, tak szybko jak to tylko możliwe;
- służenie wsparciem eksperckim dowódcy przez cały czas trwania misji i podczas etapu planowania.

W obrębie CIMIC nakreślono zasady, które wpływają na prowadzenie współpracy. Dotyczą one dwóch podstawowych kategorii:

- zasady wskazujące militarne kierunki działania CIMIC: dotyczą wewnętrznych wojskowych procesów, które umożliwiają rozwój planu wsparcia i regulują jego wykonanie;
- zasady wskazujące kierunki współpracy: wytyczne w zakresie ustanawiania oraz zarządzania efektywnymi relacjami cywilno-wojskowymi z cywilnymi jednostkami, organizacjami i ludnością.

Zadania grup CIMIC realizowane są w różnych fazach. W fazie preoperacyjnej grupy CIMIC przygotowują jednostki sił zbrojnych do panujących warunków. W tym zakresie następuje planowanie, do którego podstawowe informacje dostarczają grupy cywilne. Informacje te uwzględniają polityczną i kulturalną historię, lokalne i narodowe warunki, potrzeby miejscowej ludności, sposób przemieszczania się ludności, ekonomię terenów, cywilną infrastrukturę, a także obecność, możliwości i intencje wszelakich organizacji mogących wpływać na przeprowadzane operacje. Poza planowaniem zespoły CIMIC aktywnie uczestniczą w doradzaniu w strukturze dowódczej, przygotowaniu treningów oraz szkoleniach.

Następną fazą dla zadań CIMIC jest faza operacyjna. Główną odpowiedzialnością w tym okresie jest stworzenie i zabezpieczenie jak największej liczby relacji z osobami cywilnymi. Należy wykazać się dbałością o komunikację, która musi być sprawna i efektywna na wszystkich poziomach, niezależnie od przyjętej infrastruktury. Ponadto informacje powinny być przekazywane w obie strony (pomiędzy jednostkami cywilnymi a wojskowymi), aby osiągnąć jak największą korzyść wzajemną. W tym zakresie wskazane jest branie pod uwagę różnych perspektyw oraz kultury ludności panującej na danym obszarze, aby poprawnie skoordynować przyszłe akcje. Faza przejściowa polega na jak najsprawniejszym przekazaniu władzy upoważnionym strukturom.

Współpraca cywilno-wojskowa na przykładzie ćwiczenia CWIX 2012

Jak co roku, również w 2012, Sojusznicze Dowództwo NATO ds. Transformacji (ang. Allied Command Transformation–ACT)[9] przeprowadziło kolejną edycję ćwiczenia zaprojektowanego, aby przynosić ciągły rozwój w dziedzinie interoperacyjności – NATO Coalition Warrior Interoperability eXercise (NATO CWIX). Program CWIX koncentruje się głównie na testowaniu i poprawie interoperacyjności NATO oraz krajowych systemów C4I, ze szczególnym naciskiem na te, które będą wdrażane w Siłach Odpowiedzi NATO (ang. NATO Response Force – NRF**)**[10] lub Wielonarodowych Połączonych Siłach Zadaniowych (ang. Combined Joint Task Force –

[9] Dowództwo utworzone w 2003 r. przeznaczone do prac w zakresie procesu transformacji zdolności Sojuszu.

[10] Utworzone w 2003 r. na podstawie postanowień szczytu w Pradze – NRF mają zapewnić zdolność do natychmiastowego reagowania w kontekście pojawiających się zagrożeń. Jest to wysoce mobilny i interoperacyjny zestaw sił utrzymywany w bardzo wysokim stopniu gotowości, zdolny do natychmiastowego przemieszczenia w region, gdzie będzie potrzebny do samodzielnego prowadzenia operacji przez 30 dni. Zob. *MC 477 Military Concept for the NATO Response Force*, North Atlantic Treaty Organization, Brussels 2003.

CJTF)[11]. Umożliwia on sprawdzenie techniczne systemów zarówno znajdujących się na wyposażeniu wojsk, jak i znajdujących się na etapie eksperymentalno-rozwojowym. Podczas tegorocznej edycji, podobnie jak co roku od 2008, testowany był System JAŚMIN. Wykonano kilkaset testów różnego rodzaju. Na uwagę w kontekście CIMIC zasługuje jednak test oznaczony numerem #1147[12]. Test został wykonany pomiędzy polskim Systemem JAŚMIN w wersji przeznaczonej na poziom taktyczny – Systemem Zarządzania Walką Szczebla Taktycznego – Battlefield Management System JAŚMIN (BMS JAŚMIN), a systemem francuskim Civil COP. Test przebiegł z użyciem protokołu NVG (ang. NATO Vector Graphics)[13], dzięki któremu systemy były w stanie wymienić się danymi operacyjnymi obejmującymi pozycje jednostek oraz ich charakterystykę.

Aby osiągnąć cele NNEC, należy się zmierzyć z problemem łączenia się sieci w sposób zautomatyzowany. Osiągnięcie tego celu wymaga implementacji bram wymiany informacji Information Exchange Gateways (IEG)[14], które zastąpią istniejące szczeliny powietrzne (ang. air gap), jednokierunkowe diody danych (ang. data diode), czy w rzadkich przypadkach istniejące niezarządzane dwukierunkowe połączenia. Z powyższego powodu zaimplementowano w sieciocentrycznej platformie teleinformatycznej JAŚMIN natowską koncepcję IEG. Na poziomie strategicznym zadaniem IEG jest wspierać proces konsultacji politycznych i umożliwić narodowe planowanie i bardziej efektywne ukierunkowanie operacji, a na poziomie operacyjnym wspierać dzienne planowanie operacyjne i zarządzanie. Natomiast na poziomie taktycznym, dzięki IEG, uzyskać można polepszenie prezentacji informacji dowódcom oraz lepsze zrozumienie ich intencji, możliwość współdzielenia danych między systemami wojskowymi i cywilnymi, rozproszoną współpracę oraz integrację sieciową czujników – sensorów.

Podczas CWIX 2012 kolejny raz przetestowano również możliwości IEG JAŚMIN. Bramy takie mogą być zastosowane do łączenia domen wojskowych i cywilnych (rys. 1. IEG JAŚMIN – przykład łączenia domeny cywilnej

[11] CJTF (Combined Joint Task Force), są wielonarodowymi, połączonymi, mobilnymi siłami stworzonymi do realizacji powierzonych misji. Koncepcja NATO zakłada posiadanie zdolnych do przerzutu sił zadaniowych, dostosowanych do wymagań operacji w myśl art. 5 Traktatu waszyngtońskiego oraz poza tym artykułem. Zob. B. Panek, *Operacje reagowania kryzysowego,* AON, Warszawa 2007, s. 28–31.

[12] CWIX NATO, http://cwix.act.nato.int/portal/CWIX2012/2012TestCa/ [dostępne: 04.07.2012].

[13] Standard stosowany w systemach zobrazowania sytuacji operacyjno-taktycznej. Format danych NVG jest dokumentem XML. Dokument ten to zestaw podstawowych elementów graficznych, z których powstaje sytuacja taktyczna. Zob. http://tide.act.nato.int/tidepedia/index.php?title=NVG, [dostępne: 01.02.2011].

[14] Zob. M.A. Geistlinger*, Guidance document on the implementation of gateways for information exchange between NATO and external CIS communities*, AC/322(SC/4)N(2007)0007, NATO Consultation, Command and Control Agency, 2007.

i wojskowej). IEG może w takich przypadkach stanowić element brzegowy, uniemożliwiający wydostanie się niepowołanych informacji na zewnątrz, do grup systemów cywilnych. Ponieważ działa transparentnie, stąd użytkownicy z obu domen mogą nawet nie być świadomi jego istnienia.

Źródło: opracowanie własne.

Rys. 1. IEG JAŚMIN – przykład łączenia domeny cywilnej i wojskowej

Sytuacje kryzysowe na terytorium RP

Zarządzanie kryzysowe w Polsce regulowane jest głównie przez dwa dokumenty: *Ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* oraz *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 31 lipca 2009 r. w sprawie organizacji i funkcjonowania centrów powiadamiania ratunkowego i wojewódzkich centrów powiadamiania ratunkowego*.

SZ RP (głównie wojska lądowe) w ramach reagowania kryzysowego realizują szereg działań wymagających szerokiej współpracy cywilno-wojskowej. Należą do nich:

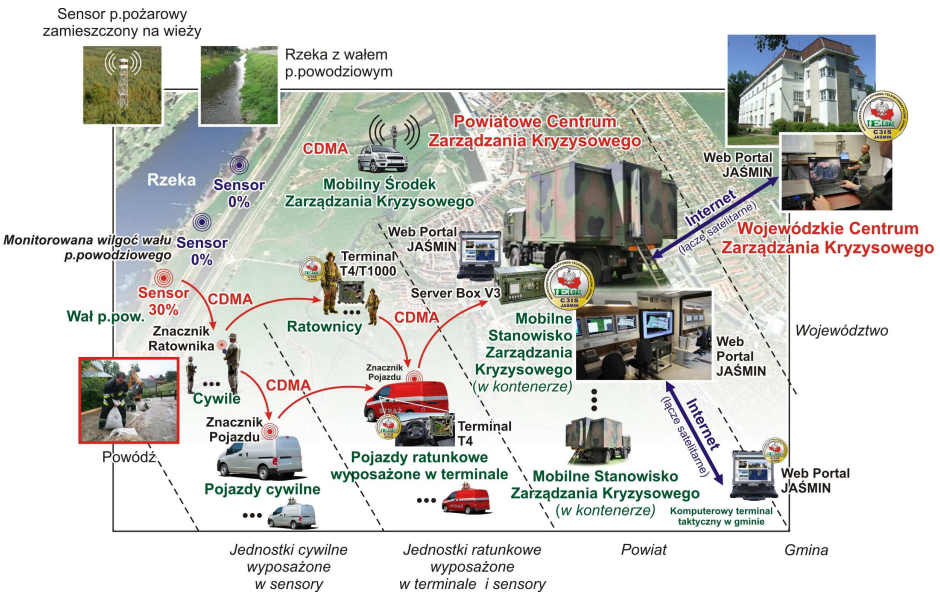
- *współudział w monitorowaniu zagrożeń;*
- *wykonywanie zadań związanych z oceną skutków zjawisk zaistniałych na obszarze występowania zagrożeń;*
- *wykonywanie zadań poszukiwawczo-ratowniczych;*
- *ewakuowanie poszkodowanej ludności i mienia;*

- *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*[15]*.*

W Polsce istnieje kilka poziomów administracyjnych, które muszą wymieniać informacje między sobą. Są to: kraj, województwo, powiat i gmina (rys. 2). 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 lub 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 zagrożeń (potencjalnych i rzeczywistych);
- nadzorze, kontroli i zarządzaniu zarówno podczas sytuacji kryzysowych, jak i planowania.

[15] Art. 25 *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,* Dz.U. z 2007 r. Nr 89, poz. 590.



Źródło: opracowanie własne.

Rys. 2. Struktura węzłów w sieciocentrycznym systemie zarządzania kryzysowego

Na każdym poziomie informacyjnym proces zarządzania może być przeprowadzany podczas dwóch głównych etapów:

- gdy nie ma widocznych zagrożeń i sytuacja jest jedynie monitorowana;
- w odpowiedzi na jakiekolwiek zagrożenie.

Podczas sytuacji kryzysowej istnieje potrzeba generowania raportów w określonym interwale czasowym. 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 wspólnie 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 one 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 in-

formacji obejmujący wszystkie węzły informacyjne i ogniwa stanowisk dowodzenia. Na rys. nr 2 przedstawiono jeden z wariantów takiego systemu. 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 wspólnej świadomości i współpracy celem osiągnięcia samosynchronizacji.

Realizacja współpracy cywilno-wojskowej podczas ćwiczenia Pierścień 2012

W dniach 15–30.05.2012 roku Akademia Obrony Narodowej (AON), przy współpracy pododdziałów: 100 batalionu łączności, 12 batalionu dowodzenia z 12 Dywizji Zmechanizowanej, batalionów dowodzenia 12 Brygady Zmechanizowanej i 7 Brygady Obrony Wybrzeża, wspieranych przez specjalistów z Centrum Wsparcia Mobilnych Systemów Dowodzenia Wojsk Lądowych (CWMSD) realizowała zadania na rzecz ćwiczenia Pierścień 2012[1617]. Ćwiczenie to odbywa się co roku, jednak po raz pierwszy od kilku lat, zorganizowane zostało z bardzo dużym rozmachem w warunkach poligonowych. Wzięło w nim udział 280 studentów i wykładowców AON oraz ponad 400 żołnierzy. Rozwinięto ponad 150 stanowisk Systemu JAŚMIN i środków łączności, które pracowały w warunkach polowych w Drawsku Pomorskim. Funkcjonowało 150 terminali roboczych oraz 37 serwerów utrzymywanych w ciągłym działaniu i sprawności.

Przebieg ćwiczenia był zgodny z tematem sprawdzenia wykorzystania zautomatyzowanych systemów wsparcia dowodzenia i aplikacji wspomagających proces dowodzenia oraz doskonalenia umiejętności współpracy oficerów z terenowymi organami administracji wojskowej i samorządowej. Ostatni punkt – współpraca ze Starostwem Powiatowym w Drawsku Pomorskim,

[16] *Pierścień'12 – Warunki polowe (by Piotr Przyborowski)*, http://www.youtube.com/ watch?v=Nkd8GSrLx_E&feature=plcp [dostępne: 09.07.2012].

[17] *Pierścień'12 – Warunki polowe*, http://www.aon.edu.pl/pl/component/content/article/187-wydarzenia/2179-piercie-12-warunkipolowe [dostępne: 09.07.2012].

które w swojej siedzibie zorganizowało spotkanie uczestników Pierścienia 2012 z przedstawicielami lokalnych służb: Straży Pożarnej i Policji oraz przedstawicielami władz: Wojewody, Starosty Powiatowego i Wojewódzkiego Sztabu Wojskowego, przebiegał dzięki zastosowaniu, po raz pierwszy w historii ćwiczenia, systemu przeznaczonego do pod zastosowania CIMIC. Rolę tego systemu pełnił System Zarządzania Kryzysowego (SZK) JAŚMIN.

System Zarządzania Kryzysowego JAŚMIN (SZK JAŚMIN) opiera się na komponentach znanego w Wojsku Polskim Systemu Wspomagania Dowodzenia C3IS JAŚMIN, działającego na bazie Sieciocentrycznej Platformy Teleinformatycznej JAŚMIN. SWD C3IS JAŚMIN projektowany i budowany był zgodnie z zasadami NATO Network Enabled Capability, EU Network Enabled Capability oraz architektury zorientowanej usługowo (ang. Service Oriented Architecture – SOA[18]), która z nich wynika. Te same reguły zostały zastosowane w Systemie Zarządzania Kryzysowego C3IS JAŚMIN, w efekcie możliwe było wykorzystanie tej samej, wielokrotnie testowanej i sprawdzonej infrastruktury komunikacyjno-bazodanowej, co w systemie SWD C3IS JAŚMIN. Dzięki temu SZK JAŚMIN ma możliwość swobodnej komunikacji z innymi systemami wojskowymi (oraz oczywiście z SWD C3IS JAŚMIN) z użyciem wielu znanych, ustandaryzowanych protokołów operacyjnych, takich jak np. Data Exchange Mechanism B2 i B3[19] lub też NATO Friendly Force Information[20].

System Zarządzania Kryzysowego Web Portal JAŚMIN (*SZK WPJ*) 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 zarówno wyspecjalizowane w obsłudze poszczególnych komórek organizacyjnych, jak i stworzone pod pojedynczych użytkowników.

System wspiera różne rodzaje dedykowanych komponentów odpowiedzialnych za różny obszar zainteresowań. Użycie serwisów dyktowane jest

[18] SOA – koncepcja tworzenia systemów informatycznych, w której główny nacisk stawia się na definiowanie usług spełniających wymagania użytkownika. Usługą określa się tu każdy element oprogramowania, mogący działać niezależnie od innych oraz posiadający zdefiniowany interfejs, za pomocą którego udostępnia realizowane funkcje. Sposób działania usługi jest w całości zdefiniowany przez interfejs ukrywający szczegóły implementacyjne, niewidoczne i nieistotne z punktu widzenia klienta.

[19] MIP B2 i B3 – mechanizmy wymiany danych opracowane w ramach międzynarodowego programu *Multilateral Interoperability Programme*. Zob. www.mip-site.org [dostępne: 10.07.2012].

[20] Standardy wymiany danych używane do monitorowania położenia wojsk własnych i sprzymierzonych. Zob. *NATO Friendly Force Information – STANAG 5527*, NATO Consultation, Command and Control Agency, 2009.

obecnie mocno wykorzystywanymi możliwościami Web 2.0[21], blogami i stronami Wiki[22]. Każdy komponent (zwany WebPartem) został zaprojektowany tak, aby w pełni zaspokoić potrzeby jednostki organizacyjnej mającej do czynienia z konkretnymi typami zadań:

- Video Streaming Web Part: daje możliwość otrzymania strumienia video od ratowników oraz z bezpilotowych środków rozpoznania;
- Web Operational Client: realizuje wsparcie procesu koordynowania pracy całej załogi w odniesieniu do danych operacyjnych, planów, dostarczania map, operacji dziennych, mapy sytuacyjnej;
- Mail Web Part: daje możliwość edycji, otrzymywania oraz wysyłania wiadomości e-mail do predefiniowanych kontaktów z Contacts Manager WebPart, umożliwia tworzenie wielu skrzynek odbiorczych i automatyczne filtruje przychodzącą pocztę;
- Contacts Manager Web Part: umożliwia zarządzania kontaktami oraz późniejsze użycie ich podczas wysyłania i odbierania wiadomości, dokumentów i plików. Kontakty mogą reprezentować zarówno jednostki logiczne, jak i pojedynczych użytkowników;
- Calendar Web Part: daje możliwość tworzenia i zarządzania zadaniami ustalonymi na konkretne terminy, przydzielonymi do użytkowników lub jednostek logicznych;
- Collaboration Web Part: pozwala na tworzenie, edycje i zarządzanie wszelkiego rodzaju dokumentami, z możliwością współpracy w grupie jednostek lub użytkowników, daje możliwość użycia szablonów i generowania raportów różnego typu;
- Documents View Web Part: umożliwia podgląd i edycję wszelkiego rodzaju dokumentów Microsoft Office;
- File Explorer (rys. 3.8): daje możliwość zarządzania plikami z poziomu WebPortalu, wysyłania ich do wskazanych odbiorców;
- Message Communication Web Part: posiada możliwość wysyłania i odbioru wiadomości tekstowych przy użyciu własnego protokołu (Battlefield Replication Mechanism – BRM[23]) oraz JCHAT[24];
- Documents Exchange Web Part: daje możliwość wysłania wszystkich dokumentów, przygotowanych w innych WebPartach z użyciem różnych protokołów.

---

[21] Określenie serwisów internetowych, w których działaniu podstawową rolę odgrywa treść generowana przez użytkowników danego serwisu. Zob. O'Reilly, *What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software*, http://oreilly.com/web2/archive/what-is-web-20.html, 2005 [dostępne: 09.07.2012].

[22] Typ serwisu internetowego, w którym treść można tworzyć i zmieniać w prosty i szybki sposób, z poziomu przeglądarki internetowej, za pomocą prostego języka znaczników.

[23] Protokół wymiany danych z użyciem łączy radiowych. Zob. H. Kruszyński, *BMS JAŚMIN-mobilny NCW*, Świat Radio nr 2/2012, s. 18–20.

[24] Komunikator taktyczny oparty o protokół XMPP, stosowany w sieciach koalicyjnych NATO.

Źródło: opracowanie własne.

Rys. 3. Web Portal JAŚMIN

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.

Węzły te wymieniały informacje między sobą oraz ratownikami, rozmieszczonymi na poligonie. Każdy z węzłów wyposażony był w serwer, na którym osadzono SZK WPJ oraz infrastrukturę bazodanową SZK JAŚMIN dla danych operacyjnych. 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, produkcji firmy TELDAT. Na terminalach osadzono oprogramowanie klienckie SZK JAŚMIN, 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 Znaczniki Ratownika są w stanie przekazywać informacje o incydentach.

Ponieważ najbardziej istotnym elementem w tego typu przekazywaniu danych jest szybka i niezawodna ich dostawa, niezwykle istotne staje się wybranie odpowiedniego medium transmisyjnego. Takie medium musi zapewniać odpowiednią jakość transmisji oraz (zazwyczaj) dobrą przepływność. Wśród środków radiowych należało więc zwrócić uwagę na sieci komórkowe (na przykład technologię CDMA[25]) ze względu na największą powszechność, bardzo duże pokrycie oraz możliwość łatwego dodawania mobilnych węzłów rozszerzających zasięgi. Stąd też zarówno terminale klienckie T4 i T1000, jak i urządzenia Znacznik Ratownika wyposażono w modemy CDMA. Mogą one pracować również z innymi środkami łączności. Techniczna specyfikacja terminali obejmuje wiele nowoczesnych rozwiązań i odpowiada aktualnie obowiązującym standardom obliczeniowym (Rys. 3). Najważniejszymi cechami wyróżniającymi je na obecnym rynku są: mała waga, dotykowy ekran LCD, modem CDMA, umożliwiający komunikację z użyciem sieci komórkowych oraz technologii łączności bezprzewodowej WIFI i Bluetooth. Zawierają wbudowaną jedną lub dwie kamery, w zależności od wersji. Posiadają odpowiednią pojemności baterii, dzięki którym mogą długo funkcjonować podczas wykonywania zadań. Dzięki spełnianiu odpowiednich norm dotyczących kompatybilności elektromagnetycznej i wymagań środowiskowych możliwe jest używanie ich w różnego rodzaju ciężkich warunkach klimatycznych. Przeżywają upadek z wysokości około 1 metra i są w stanie pracować w wodzie na głębokości około 1 metra.

W ramach platformy sprzętowej SZK JAŚMIN opracowano i wykorzystano podczas ćwiczenia poniższe elementy (rys. 4):

- 6 sztuk Terminali T1000 (w tym zewnętrzne baterie, kamery, zasilacze, rozgałęźniki interfejsów USB/RJ);
- 5 sztuk Terminali T4 (w tym kamery, zasilacze, stacje dokujące);
- 15 sztuk Znaczników Ratownika.

[25] Standard sieci komórkowych Code Division Multiple Access (ang.), w którym używa się metody dostępu do medium transmisyjnego, polegającej na przypisaniu poszczególnym użytkownikom korzystających z tego samego kanału do przesyłania danych, sekwencji rozpraszających, dzięki którym odbiornik jednoznacznie zidentyfikuje przeznaczoną dla niego transmisję. Zob. J. Bannister, P. Mather, S. Coope, *Convergence Technologies for 3G Networks: IP, UMTS, EGPRS and ATM*, John Wiley & Sons Ltd., 2004.

Źródło: opracowanie własne.

Rys. 4. Terminale Taktyczne T4, T 1000 oraz Znacznik Ratownika lub Pojazdu

Podczas odegrania zaplanowanego scenariusza ćwiczebnego węzły wymieniały się informacjami różnego typu oraz zakresu, w tym:

- wstawiano na podkładzie mapowym symbole graficzne, wizualizowane w systemie zgodnie ze standardami obowiązującymi dla jednostek organizacyjnych administracji państwowej[26];
- przesyłano dane ze znaczników ratownika umożliwiające ich lokalizację w przestrzeni, z użyciem własnego protokołu;
- przesyłano pliki pomiędzy węzłami SZK WPJ;
- tworzono plany i rozkazy, z użyciem Collaboration WebPart, który umożliwił jednoczesną pracę wielu osób nad jednym dokumentem, stworzonym na bazie przygotowanego wcześniej szablonu. Po rozdzieleniu zadań koordynator dokonywał recenzji oraz zatwierdzenia i przesyłał tak stworzone dokumenty do odpowiednich odbiorców.

W zakresie integracji z różnymi źródłami danych na bieżąco pobierano automatycznie strumień video pochodzący z bezzałogowego samolotu rozpoznania oraz w sposób ciągły wymieniano dane w obu kierunkach z Sys-

[26] Zob. *Decyzja nr 13 Ministra Spraw Wewnętrznych i Administracji z dnia 28 stycznia 2008 r. w sprawie wprowadzenia do użytku Zestawu zasadniczych umówionych znaków operacyjnych właściwych dla komórek organizacyjnych Ministerstwa Spraw Wewnętrznych i Administracji oraz jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych i Administracji*, 2008.

temem Wspomagania Dowodzenia C3IS JASMIN, który wykorzystywany był w tym samym czasie przez uczestników ćwiczenia w wojskowej jego części. Należy wspomnieć, że system ten, wraz z platformą sprzętową JAŚMIN cieszył się dużym zainteresowaniem również wśród studentów kursów anglojęzycznych: Advanced Operational Strategic Course i Higher Operational Tactical Course. Akademicki Pierścień jest jednym z kolejnych (po Borsuku 2010 i Dragonie) ćwiczeń, na których wykorzystywany był System Zarządzania Komponentami/Modułami Bojowymi – HMS (ang. Headquarter Management System) JAŚMIN, jednocześnie pierwszym, na którym dokonano integracji ze służbami cywilnymi z wykorzystaniem systemu teleinformatycznego SZK JAŚMIN (rys. 5).

Źródło: opracowanie własne.

Rys. 5. Nieodfiltrowana sytuacja bojowa przekazywana do SZK JAŚMIN

Na uwagę zasługuje fakt, że zarówno system SZK JAŚMIN (używany w części cywilnej ćwiczenia), jak i HMS JAŚMIN (używany w części wojskowej ćwiczenia) konfigurowany i instalowany był z użyciem narzędzia – aplikacji Zarządzanie Modułami JAŚMIN (produkcji firmy TELDAT), która umożliwia zdefiniowanie danych i ustawień za pomocą diagramów, na których rysuje się urządzenia, oprogramowanie i ich połączenia, następnie generuje osadzaną na platformie konfigurację.

Podsumowanie

W artykule przedstawiono możliwości realizacji koncepcji CIMIC z użyciem systemu teleinformatycznego cechującego się właściwością sieciocentryczności. Dane zbierane z wielu miejsc ulegają przetwarzaniu w węzłach do tego przeznaczonych, które współdziałają ze sobą w osiąganiu wspólnych celów. Dzięki skutecznemu połączeniu odpowiednich węzłów rozproszonych w sposób geograficzny możliwe jest współdzielenie informacji, co przyczynia się do rozwinięcia wspólnej świadomości i współpracy w celu osiągnięcia samosynchronizacji.

Podczas ćwiczenia Pierścień 2012 wykorzystano system dedykowany dla współpracy cywilno-wojskowej, którego zadaniem było wspomożenie realizacji zadań przez grupy związane z CIMIC. Z sukcesem zrealizowano zaplanowany scenariusz, który obejmował zarówno wymianę danych przez sieć CDMA, wizualizację odpowiednich symboli przeznaczonych dla zastosowań administracyjnych, tworzenie planów i rozkazów w ramach pracy grupowej, jak również integrację i swobodny przepływ informacji między SZK JAŚMIN a istniejącym i wielokrotnie sprawdzonym w wojsku systemem wojskowym JAŚMIN, w tym przypadku głównie HMS JAŚMIN. Zweryfikowano poprawność architektury oraz fakt, że system spełnił oczekiwania użytkowników.

Podczas ćwiczeń zintegrowano rozwiązanie z dedykowanym osprzętem: terminalami T4, T1000 i urządzeniami Znacznik Ratownika, z których wszystkie wyposażono w modemy CDMA. Potwierdzono zasadność korzystania z szeroko dostępnych sieci komórkowych, udało się także bez zastrzeżeń i w czasie rzeczywistym monitorować położenie grup, informować o incydentach oraz przesyłać dokumenty.

Dokonano integracji zarówno SZK JAŚMIN, jak i Systemu HMS JAŚMIN z bezzałogowym środkiem rozpoznania, poprzez wizualizację strumienia video, który dostarczał. Zarówno w SZK WPJ, jak i dedykowanych aplikacjach klienckich możliwy był ponadto podgląd strumienia z kamer montowanych na hełmach żołnierzy biorących udział w misji.

Podczas ćwiczenia CWIX, edycji 2012, sprawdzono możliwość wymiany informacji między systemem wojskowym, BMS JAŚMIN a systemem francuskim, odpowiadającym jednostce cywilnej. Wykorzystano protokół NVG, z którego pomocą udało się przesłać pozycję i charakterystyki jednostek. Jednocześnie System BMS JAŚMIN był w stanie pobrać dane z użyciem wielu innych protokołów sprawdzonych podczas tych ćwiczeń. Ograniczenia współpracy cywilno-wojskowej, wynikające z konieczności zachowania bezpieczeństwa teleinformatycznego systemów, można zapewnić, stosując rozwiązania, takie jak np. Information Exchange Gateway, zalecane przez NATO.

Podsumowując, dzięki elementowi sieciocentryczności, w tym przypadku konkretnie Systemu JAŚMIN i jego architekturze zorientowanej usługowo (Service Oriented Architekcture), możliwe jest osiągnięcie pełnej integracji pomiędzy grupami cywilno-wojskowymi. Ponadto z wykorzystaniem gotowych infrastruktur komunikacyjnych sprawdzonych wielokrotnie w systemach wojskowych, integracja ta staje się niezwykle łatwa do wdrożenia.

CENTRIC NETWORK ASPECT OF CIVIL MILITARY COOPERATION IN CRISIS OPERATIONS

Abstract: Civil Military Cooperation (CIMIC) is a notion which defines the necessity of effective cooperation between civil and military services. The most common example of such cooperation can be found in crisis response operations conducted during calamities, natural disasters or conflicts.

The article features the way of applying the JAŚMIN System and its components to coordinate activities of groups of people or information domains. The legitimacy of creating system solution has been analysed, which due to its effective data acquisition from many sources is capable of information support for conducting joint operations and missions and significantly increase its effectiveness through higher synchronization of operations.