

PARADYGMATY BADAŃ NAD BEZPIECZEŃSTWEM

**INFRASTRUKTURA KRYTYCZNA W PROCESIE
ZARZĄDZANIA W SYTUACJACH KRYZYSOWYCH**

Andrzej GAŁECKI
Anna KURKIEWICZ
Stanisław MIKOŁAJCZAK
(redakcja naukowa)

Poznań 2014

INFRASTRUKTURA KRYTYCZNA W PROCESIE ZARZĄDZANIA W SYTUACJACH KRYZYSOWYCH

PARADYGMATY BADAŃ NAD
BEZPIECZEŃSTWEM

INFRASTRUKTURA KRYTYCZNA W PROCESIE ZARZĄDZANIA W SYTUACJACH KRYZYSOWYCH

1

Andrzej GAŁECKI
Anna KURKIEWICZ
Stanisław MIKOŁAJCZAK
(redakcja naukowa)



Poznań 2014

Recenzje

prof. zw. dr hab. inż. Marian KOPCZEWSKI

Projekt okładki

Monika BRZOZOWSKA

Edycja tekstów

Agnieszka Maria TUREK

Skład komputerowy

Marta WALACHOWSKA

Copyright©2014by

 wydawnictwo Wyższej Szkoły Bezpieczeństwa
All rights reserved

ISBN: 978-83-61304-85-2



Wydawnictwo Wyższej Szkoły Bezpieczeństwa

ul. Orzeszkowej 1, 60-778 Poznań

tel. 61 851 05 18

e-mail: kierownik.wydawnictwa@wsb.net.pl

www.wsb.net.pl

Druk i oprawa:

Fabryka Druku sp. z o.o.
ul. Zgrupowania AK „Kampanos” 6
01-943 Warszawa
fabryka_druku@fabrykadruku.pl

Wydanie pierwsze
Druk ukończono w lipcu 2014 r.

SPIS TREŚCI

Wstęp (Andrzej GAŁECKI)	9
Rozdział I ZARZĄDZANIE KRYZYSOWE	11
<i>Zarządzanie kryzysowe jako istotny element kierowania współczesnym bezpieczeństwem narodowym</i> (Karina GÓRSKA, Anna ROŻEJ)	13
<i>Czynniki determinujące proces zarządzania kryzysowego</i> (Andrzej GAŁECKI)	27
<i>Integracja systemów wspomagania decyzji na potrzeby zarządzania kryzysowego</i> (Bartosz BIERNACIK)	37
<i>Kryzys, konflikt, terroryzm – fazy eskalacji zjawiska w kontekście sytuacji kryzysowej</i> (Michał A. DOMAŃSKI)	59
<i>Systemy informacyjne organizacji w zarządzaniu kryzysowym</i> (Maciej MARCZYK, Ilona ZIEMKIEWICZ-GAWLIK)	69
<i>Użycie sił zbrojnych w sytuacjach kryzysowych</i> (Barbara RATAJCZYK)	81
<i>Policja w systemie zarządzania kryzysowego</i> (Jerzy GAŚSIOROWSKI)	89
<i>Administracja publiczna w systemie zarządzania kryzysowego</i> (Monika TRYBÓŃ, Izabella GRABOWSKA-LEPCZAK, Marek KWIATKOWSKI)	117
<i>Udział organów administracji wojskowej w zarządzaniu kryzysowym</i> (Ryszard LELITO)	129
<i>Prawne uwarunkowania zarządzania kryzysowego na szczeblu powiatu</i> (Przemysław NIEMCZUK)	143
<i>Samorząd terytorialny w systemie bezpieczeństwa publicznego – szczebel powiatu</i> (Grzegorz NAKIELSKI, Piotr LIZAKOWSKI)	155
<i>Zadania straży gminnych/miejskich podczas sytuacji kryzysowych</i> (Agata DYBIOCH)	173
<i>Zabezpieczenie logistyczne policyjnych sytuacji kryzysowych</i> (Jarosław STRUNIAWSKI, Mariusz NEPELSKI)	183

<i>Plany zarządzania kryzysowego a działania policji</i> (Anna ROLKA)	193
<i>Determinanty funkcjonowania systemu zarządzania kryzysowego sił powietrznych</i> (Bogdan GRENDĄ)	203
<i>Zarządzanie kryzysowe w odniesieniu do śródlądowych zasobów wodnych i żeglugi śródlądowej</i> (Krzysztof ROKIĆIŃSKI)	219
Rozdział II	
INFRASTRUKTURA KRYTYCZNA	233
<i>Zagrożenia infrastruktury krytycznej państwa i obywateli</i> (Marian KOPCZEWSKI, Bartłomiej PAĆZEK)	235
<i>Wybrane problemy ochrony infrastruktury krytycznej</i> (Franciszek MROCZKO)	249
<i>Zadania administracji publicznej w świetle narodowego programu ochrony infrastruktury krytycznej</i> (Patrycja BRYCZEK, Tadeusz SZCZUREK)	267
<i>Zmiany klimatyczne i ich wpływ na bezpieczeństwo infrastruktury krytycznej</i> (Marian KOPCZEWSKI, Marek TOBOLSKI, Sławomir SKIBIŃSKI)	283
<i>Normatywne determinanty procedury rozpoznawania, wyznaczania i ochrony europejskiej infrastruktury krytycznej</i> (Mirosław TOKARSKI)	297
<i>The protection of the airport as a part of critical infrastructure</i> (Michaela MLYNÁROVÁ)	313
<i>Infrastruktura w bezpieczeństwie obywateli i państwa</i> (Stanisław DWORECKI)	317
<i>Szanse i zagrożenia związane z uodparnianiem infrastruktury krytycznej</i> (Agata TYBURSKA)	329
<i>Rola i zadania państwowej straży pożarnej w ochronie infrastruktury krytycznej</i> (Robert DANIŁOWICZ)	349
<i>Process of critical infrastructure elements assessment in a transportation sector</i> (Lucia ĎURANOVÁ)	363
<i>Wpływ działań Unii Europejskiej na ochronę infrastruktury krytycznej w krajach członkowskich</i> (Joanna ŚWIĄTKOWSKA)	373

Rozdział III

BEZPIECZEŃSTWO W SKALI NARODOWEJ	383
<i>Wybrane elementy bezpieczeństwa w oparciu o założenia Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (Marian KOPCZEWSKI, Dariusz SIENKIEWICZ)</i>	385
<i>Rola i zadania Marynarki Wojennej w kształtowaniu bezpieczeństwa państwa (Andrzej BURSZTYŃSKI)</i>	403
<i>Zintegrowany system ratowniczy elementem bezpieczeństwa wewnętrznego Rzeczypospolitej Polskiej (Marian KOPCZEWSKI, Marek TOBOLSKI)</i>	415
<i>Wpływ nowoczesnych technologii na bezpieczeństwo ekologiczne państwa (Edyta ŁOŃSKA, Jacek FABISIAK, Jarosław MICHALAK)</i>	427
<i>Zaawansowane technologie teleinformatyczne wspomagające projektowanie systemu ratowniczego (Paweł KĘPKA, Wiktor GAWROŃSKI)</i>	441
<i>Ochotnicze straże pożarne w krajowym systemie ratowniczo-gaśniczym (Barbara WĘGLARZ)</i>	451
<i>Działalność organów administracji publicznej na tle ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym jako element bezpieczeństwa narodowego (Izabela KOCOT-LIS, Tadeusz LIS)</i>	461
<i>Zakończenie (Andrzej GAŁECKI)</i>	471

WSTĘP

Bezpieczeństwo jest zależne od szerokiego spektrum czynników, wśród których, zarówno w skali narodowej, jak i globalnej, na czołowym miejscu znajduje się walka z terroryzmem.

Funkcjonujący w Polsce system bezpieczeństwa narodowego integruje siły zbrojne, służby, instytucje rządowe i samorządowe, a także inne podmioty prawne. Przeznaczenie tego systemu sprowadza się do zapobiegania i przeciwdziałania zagrożeniom zewnętrznym, zapewnienia bezpieczeństwa publicznego, prowadzenia działań ratowniczych oraz ochrony ludności i mienia w sytuacjach nadzwyczajnych. Podstawowym zadaniem podsystemu kierowania jest zapewnienie ciągłości podejmowania decyzji i działań w celu utrzymania bezpieczeństwa narodowego. Realizacja tego zadania jest możliwa dzięki prowadzeniu monitoringu źródeł, skali oraz rodzajów zagrożeń, które najogólniej można postrzegać w wymiarze militarnym i pozamilitarnym.

Jaki jest rezultat badań dotyczących bezpieczeństwa, w szczególności w obszarze zarządzania kryzysowego? Próbą odpowiedzi na to pytanie jest niniejsza monografia składająca się z dziewięciu zasadniczych rozdziałów.

Treści rozdziału pierwszego odnoszą się do zarządzania kryzysowego jako istotnego komponentu bezpieczeństwa narodowego. Sprecyzowano w nim obszar badawczy dotyczący determinantów procesu zarządzania kryzysowego. Ponadto wskazano potrzebę wykorzystania oraz integracji systemów wspomagania decyzji. Podkreślono istotną rolę sił zbrojnych, policji, straży miejskiej oraz samorządów terytorialnych w systemie zarządzania kryzysowego.

W kolejnej części niniejszej publikacji skoncentrowano się na określeniu znaczenia infrastruktury krytycznej dla poziomu bezpieczeństwa narodowego. Zwrócono tu szczególną uwagę na potencjalne zagrożenia i możliwości ochrony infrastruktury.

W następnym rozdziale zidentyfikowano pojęcie terroryzmu oraz zaprezentowano strategię działań terrorystycznych, a ponadto wskazano główne metody ich zwalczania. Wyróżniono różne aspekty występowania tego zjawiska, zarówno w obszarze kulturowym, jak i wyznaniowym.

W dalszej części rozdziału odniesiono się do cyberzagrożeń.

W rozdziale czwartym skupiono uwagę na różnych aspektach bezpieczeństwa międzynarodowego. Wyartykułowane w nim treści obejmują w głównej mierze system bezpieczeństwa europejskiego oraz bliskowschodniego. W tej części monografii zwrócono również uwagę na „aspekt gruziński” i prezentowaną w tym zakresie strategię i politykę bezpieczeństwa Unii Europejskiej, Stanów Zjednoczonych, Rosji oraz Polski.

Ważnym elementem monografii są spostrzeżenia koncentrujące się na bezpieczeństwie narodowym. Dominują tu efekty badań naukowych dotyczących problemów Strategii Bezpieczeństwa Rzeczypospolitej Polskiej. Wskazano w nim także na rolę Marynarki Wojennej RP, Zintegrowanego Systemu Ratowniczego oraz administracji publicznej na potencjał bezpieczeństwa państwa polskiego.

Na kanwie prowadzonych badań, wyrażonych w postaci treści zawartych w następnym rozdziale, zaprezentowano rezultaty dotyczące bezpieczeństwa lokalnego. Główny kierunek badawczy został skoncentrowany na zagrożeniach i związanych z nimi zadaniach administracji samorządowej oraz jednostek ratowniczych.

Niewątpliwie istotnym elementem dociekań naukowych zawsze były i z pewnością pozostaną problemy edukacji dla bezpieczeństwa, postrzegane w aspekcie globalnym. W tym względzie na pierwszy plan wysuwają się problemy dotyczące bezpieczeństwa w procesie komunikowania, alokacji edukacji, jak również podejścia metodologicznego w analizowanym obszarze.

Nowe światło na problemy związane z bezpieczeństwem rzuca zastosowanie szerokiej perspektywy badawczej – podjęto bowiem badania w ujęciu psychologicznym, socjologicznym, pedagogicznym czy polityki społeczno-wychowawczej państwa. Rezultaty badań w tym zakresie zostały zaprezentowane w rozdziale 8 niniejszej monografii.

W ostatniej części zaprezentowano wielopłaszczyznową interpretację problemów bezpieczeństwa. Opisane wyniki odpowiadają specyfice szeroko rozumianego bezpieczeństwa w analizowanym obszarze badań.

Andrzej GAŁECKI

INTEGRACJA SYSTEMÓW WSPOMAGANIA DECYZJI NA POTRZEBY ZARZĄDZANIA KRYZYSOWEGO

Wstęp

Prezentowany materiał jest rozwinięciem prezentacji: „Integracja informacji w służbach publicznych na potrzeby reagowania kryzysowego”, wygłoszonej w ubiegłym roku w Poznaniu, w trakcie ubiegłorocznej edycji Konferencji „Paradygmaty badań nad bezpieczeństwem”. Wówczas głównym punktem ciężkości artykułu było wskazanie możliwości zintegrowania informacji przetwarzanych przez służby publiczne na potrzeby reagowania kryzysowego (Policja, PSP, ratownictwo medyczne itp.). Jednakże już wtedy wskazane zostały (wówczas jeszcze teoretyczne) możliwości integracji posiadanych systemów wsparcia decyzji (C3IS Jaśmin) z systemami symulacyjnymi (wówczas na przykładzie systemu VBS2). W tym roku potrzeba integracji informacji służb publicznych została uzupełniona o możliwości współpracy systemów wsparcia decyzji z różnymi systemami symulacji będącymi w posiadaniu SZ RP – odpowiednich dla różnych poziomów zarządzania kryzysowego. To było również głównym tematem tegorocznego wystąpienia. Dlatego w artykule autor pomija szczegółowy opis systemów wspomagania decyzji (C3IS Jaśmin, HMS Web portal, SharePoint i innych), których opis można znaleźć w ubiegłorocznych materiałach pokonferencyjnych.¹

Potrzeba integracji informacji w służbach publicznych

Działania związane z zarządzaniem kryzysowym wymagają gromadzenia, przetwarzania ogromnych ilości informacji i ich prezentowania (w odpowiednim miejscu i czasie – odpowiednio przygotowanych i w odpowiedniej formie) w różnych służbach publicznych, odpowiedzialnych za zarządzanie kryzysowe w Polsce. Wszystko to działa obecnie w pewnym zakresie do chwili, gdy informacje są w posiadaniu jednej ze służb. Problem pojawia się w momencie, w którym musi nastąpić wymiana informacji pomiędzy różnymi służbami – jak wskazują wyniki ubiegłorocznych badań – jest to szczególnie problem prawny, gdyż techniczne możliwości takiej integracji zostały już stworzone i szczegółowo przedstawione.

Dla przypomnienia – możliwe jest zintegrowanie informacji służb publicznych bez konieczności wymiany lub nawet instalacji jakichkolwiek nowych narzędzi informatycznych w poszczególnych służbach publicznych (co wiązałoby się z dużymi kosztami implementacji) na bazie dwóch rozwiązań:

1. Systemu HMS Web Portal – elementu sieciocentrycznej platformy teleinformatycznej Jaśmin. Narzędzie to powstało w wyniku prowadzonych przez producenta oprogramowania, firmą Teldat, wraz z Akademią Obrony Narodowej, badań naukowych w zakresie rozwoju systemów wsparcia

¹ B. Biernacik, J. Janczak, *Integracja informacji w służbach publicznych na potrzeby reagowania kryzysowego* (w:) *Paradygmaty badań nad bezpieczeństwem – Zarządzanie kryzysowe w teorii i praktyce*, Wydawnictwo Wyższej Szkoły Bezpieczeństwa. Poznań 2013, ISBN 978-83-61304-58-6, s. 53-72

dowodzenia w Wojskach Lądowych. Zasadniczą zaletą tego rozwiązania jest umożliwienie integracji informacji pochodzących z najróżniejszych systemów stosowanych przez służby publiczne. Można to zawęzić do realizacji zadań wynikających z reagowania kryzysowego, ale można to również potraktować szerzej, jako możliwość integracji informacji służb publicznych zarówno w kraju, jak i pomiędzy np. członkami Unii Europejskiej czy też państwami członkowskimi NATO. Narzędzie to może integrować informacje tworzone w różnych systemach i przechowywać je w jednym miejscu (na dyskach twardych serwera) umożliwiając jednocześnie dostęp do nich wszystkim użytkownikom posiadającym uprawnienia. Jest to możliwe, gdyż „rdzeniem” portalu HMS Web Portal jest system SharePoint firmy Microsoft, na bazie którego tworzony jest portal ekstrasietowy (posiadający wszystkie funkcje systemu SharePoint). Technologia firmy Microsoft umożliwia tworzenie bezpiecznych witryn w ramach intranetu lub ekstrasietu. Witryny te służą pracy grupowej i są miejscem, w którym użytkownicy mają szybki dostęp do niezbędnych danych do realizacji postawionych zadań. Będąc podłączonym do Internetu lub wewnętrznej sieci intranetu, niezależnie od miejsca pobytu, wszyscy członkowie zespołu, po podaniu hasła, mogą skorzystać z witryny SharePoint i wymieniać się w niej zadaniami, projektami, dokumentami i ogłoszeniami oraz swobodnie rozszerzać witrynę o kolejne podstrony. W ramach jednej platformy uzyskują możliwość korzystania z narzędzia, w którym można umieszczać dane z różnych źródeł. Jest to rozwiązanie dość popularne na świecie i zyskujące na popularności w Polsce (coraz więcej firm krajowych wykorzystuje tę platformę w swojej działalności, np. w wojsku m.in. w sieci MIL-WAN, w AON w WZiD jako Intranet);

2. Systemu SZK Web Portal – stanowiącego rozwojową wersję systemu HMS Web Portal. Dzięki temu możliwa jest technicznie pełna wymiana informacji pomiędzy wszystkimi elementami biorącymi udział zarówno w działaniach związanych z zarządzaniem i reagowaniem kryzysowym, jak również z działaniami w stanie kryzysu i wojny. Jest to możliwe dzięki wspólnym mechanizmom wymiany danych w obydwu systemach (System Zarządzania Kryzysowego oraz Platforma Sieciocentryczna Jaśmin). Wykorzystanie tego narzędzia umożliwia stworzenie wspólnej platformy dla służb publicznych, która z kolei daje możliwość lepszego wykorzystania posiadanego sprzętu i środków oraz zmniejsza ryzyko wielokrotnego wykonywania tych samych czynności przez różne służby. W efekcie obniżone zostaną również koszty prowadzonych akcji.

Obecnie w Siłach Zbrojnych RP trwają prace nad uzyskaniem **Połączonego Obrazu Sytuacji Operacyjnej (POSO)**, która będzie obejmowała informacje ze wszystkich rodzajów wojsk (Wojsk Lądowych, Wojsk Specjalnych, Marynarki Wojennej, Sił Powietrznych). Obraz ten należy jeszcze poszerzyć o informacje z sił sojuszniczych NATO oraz innych, współpracujących z nami. Taka integracja informacji na poziomie SZ RP możliwa jest właśnie dzięki wykorzystaniu rozwiązania HMS Web Portal.

Wykorzystanie w wojsku Platformy Sieciocentrycznej Jaśmin, w służbach publicznych Systemu Zarządzania Kryzysowego SZK Jaśmin pozwoli na uzyskanie jeszcze szerszego zakresu zintegrowanych informacji – **Połączonego Obrazu Sytuacji Służb Publicznych (POSSP)**, który obejmie również informacje ze wszystkich służb publicznych, krajowych i zagranicznych (w razie potrzeby). Wskazane są oczywiście prace nad poprawą stanu prawnego, który obecnie uniemożliwia wspólną pracę wszystkich służb odpowiedzialnych za realizację zadań wynikających z zarządzania kryzysowego.

Potrzeba integracji systemów informatycznych w służbach publicznych

O ile możliwe jest zintegrowanie informacji posiadanych przez różne służby od strony technicznej, to kolejnym ważnym aspektem, nad którym należy się zastanowić, jest stworzenie warunków do prowadzenia wspólnych ćwiczeń w ramach realizacji zadań zarządzania kryzysowego.

Taka możliwość została zidentyfikowana w trakcie prowadzonych badań, rozpoczętych od zbadania technicznych możliwości wymiany danych pomiędzy systemem wsparcia dowodzenia C3IS Jaśmin, a Symulatorem Działań Taktycznych AON/WAT na potrzeby prowadzonych w Wydziale Zarządzania i Dowodzenia Akademii Obrony Narodowej ćwiczeń wojskowych. Dalsze prace pozwoliły rozszerzyć zakres takiej współpracy z kolejnymi narzędziami, jak również zdefiniować szerszy zakres możliwego wykorzystania poszczególnych narzędzi symulacyjnych – na potrzeby realizacji ćwiczeń zarządzania kryzysowego.

I tak obecnie możliwa jest integracja m.in. z następującymi systemami symulacyjnymi (licząc od najwyższego poziomu ZK):

1. JTLS – symulacja konstruktywna;²
2. Symulator Działań Taktycznych AON/WAT – symulacja konstruktywna;
3. JCATS – symulacja konstruktywna;
4. VBS2 – symulacja wirtualna.³

1. System Symulacyjny Działań Połączonych JTLS⁴

JTLS – (ang. *Joint Theater Level Simulation*) System symulacyjny działań połączonych JTLS jest interaktywnym systemem symulacyjnym, modelującym działania Wojsk Lądowych, Sił Powietrznych, Marynarki Wojennej, a także Sił Specjalnych. Odzwierciedla kluczowe aspekty wojny z uwzględnieniem ogniw pozamilitarnych. Producentem systemu jest firma Rolands & Associates Corporation (<http://www.rolands.com>).

System ten jest przeznaczony do analizy, projektowania i oceny planów działania, oceny alternatywnych rozwiązań (wariantowanie działań bojowych), oraz analizy struktur jednostek bojowych z uwzględnieniem systemów walki. W Centrum Symulacji i Komputerowych Gier Wojennych (CSiKGW) AON wykorzystywany jest

² Symulacja konstruktywna – jej działanie oparte jest na komputerowym symulowaniu zachowań ludzi jak również sprzętu – wirtualny człowiek oraz sprzęt. Ten rodzaj symulacji związany jest bezpośrednio z symulacją analityczną.

³ Symulacja wirtualna – jest to rodzaj symulacji, w której operator działa przy wykorzystaniu symulowanego sprzętu – rzeczywisty człowiek, wirtualny sprzęt – do tej grupy symulatorów zaliczyć możemy np. trenażery. W symulacji wirtualnej użytkownik obserwuje graficzną reprezentację obszaru działań (np. na ekranie komputera, w specjalnych goglach, na wyświetlaczach trenażerów itp.) i jest jednocześnie jej elementem, bierze w niej czynny udział (w czasie rzeczywistym).

⁴ Więcej patrz: <http://csikgw.aon.edu.pl/index.php/pl/narzdzia/88-narzdzia.html>

do prowadzenia ćwiczeń wspomaganych komputerowo (CAX) (ang. *Computer Assisted Exercises*), poprzez wykorzystanie modeli działań bojowych do stworzenia w środowisku komputerowym środowiska operacyjnego dla elementów decyzyjnych podobnego, z jakim mogą się one spotkać na polu walki.

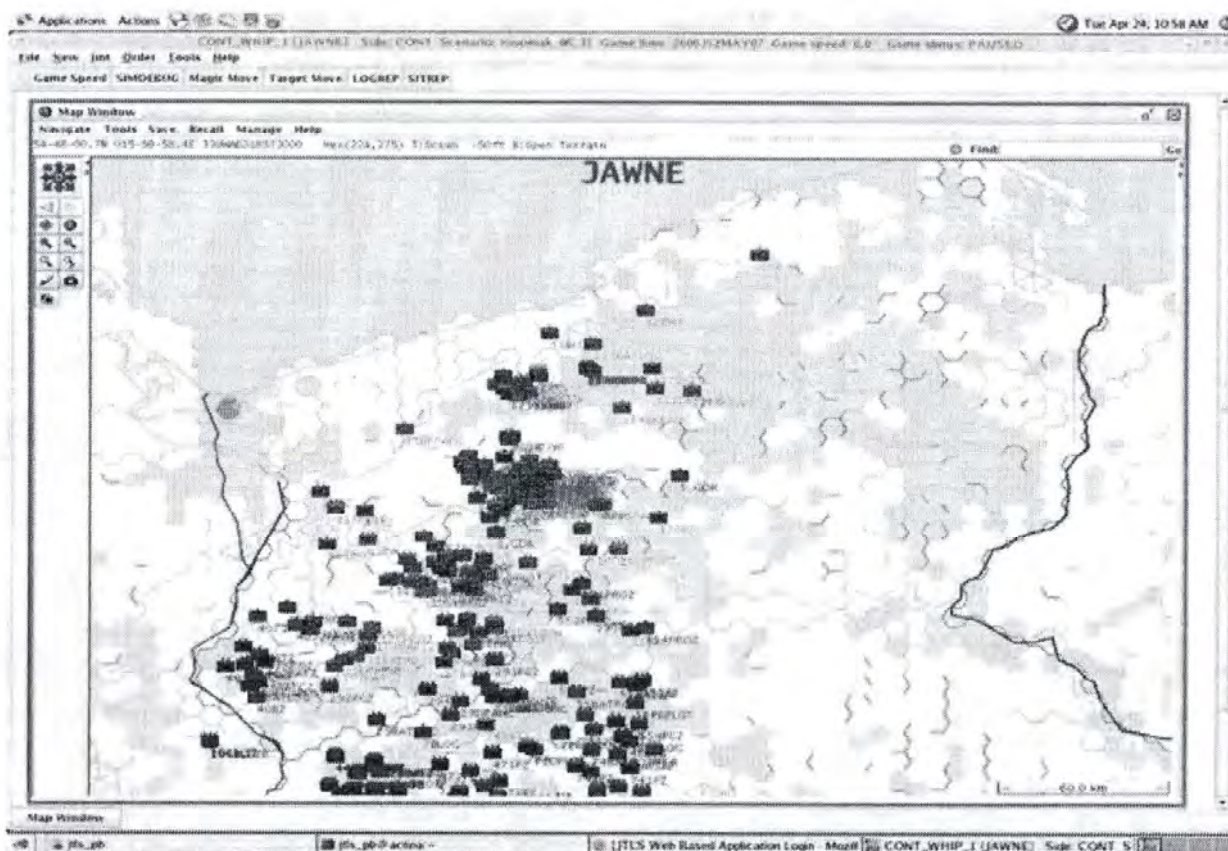
Możliwości operacyjne systemu

W JTLS istnieje możliwość tworzenia do 10 stron konfliktu zbrojnego, a każda ze stron konfliktu może być podzielona na dowolną liczbę podgrup sił tzw. frakcji. Jako frakcje, można modelować działania jednostek tego samego rodzaju sił zbrojnych bądź rodzaju wojsk (wojska zmechanizowane, pancerne, chemiczne, inżynieryjne, logistyczne itp.). Modelowane mogą być także ogniwa pozamilitarne jak np. grupy uchodźców. Relacje pomiędzy stronami mogą być asymetryczne i mogą być zmieniane przez ćwiczące strony w czasie gry, w zależności od potrzeb i scenariusza. Ćwiczący oddziałują na symulację interaktywnie poprzez wysyłanie rozkazów do jednostek, którymi dowodzą. Łańcuch dowodzenia definiuje się na etapie tworzenia bazy danych. Każda ze stron zdefiniowanych w grze znajduje się w określonej relacji z innymi stronami jako: przyjazna, neutralna, podejrzana lub wroga. Relacje stron określają sposób, w jaki jednostki jednej strony reagują na działania jednostki innej strony np. jednostka niszczy wykryte obiekty (inne jednostki, konwoje, środki transportu itp.) wtedy, gdy relacja z nią ustawiona jest jako „wroga”. Koncepcja symulacji w JTLS bazuje na zastosowaniu szeregu modeli cząstkowych, które określają zakres funkcjonalności oraz adekwatności modelu. Uzbrojenie i sprzęt wojskowy oraz stany osobowe modelowane są w JTLS w postaci tzw. systemów walki. W aktualnej wersji systemu istnieje możliwość modelowania 100 systemów walki. Każdy system walki opisany jest za pomocą wielu parametrów takich jak np. maksymalny skuteczny zasięg prowadzenia ognia, zdolności odzyskiwania i napraw uszkodzonego sprzętu, typ wymaganego paliwa i amunicji itp., które wykorzystywane są w trakcie symulacji. Systemy walki podzielone są na systemy do prowadzenia ognia bezpośredniego i pośredniego. JTLS umożliwia także modelowanie działania broni masowego rażenia.

Odwzorowanie terenu

W systemie JTLS podstawową jednostką opisu terenu jest obszar w kształcie sześcioboku foremnego nazywanego heksagonem (mapa heksagonalna) – rys. 1. Charakterystyka heksagonu to zbiór ściśle określonych parametrów dotyczących jego powierzchni oraz poszczególnych boków takich jak: pokrycie i ukształtowanie terenu (otwarty z drogami o dobrej przejezdności, otwarty z drogami o ograniczonej przejezdności, zalesiony, zalesiony z drogami o dobrej przejezdności, zalesiony z drogami o ograniczonej przejezdności, pustynny, pustynny z drogami o dobrej przejezdności, pustynny z drogami o ograniczonej przejezdności, miejski, ruiny, górski, teren górski z drogami o dobrej przejezdności, teren górski, słabe drogi, morze, małe wyspy), przeszkody terenowe (rzeka, fiord, wąwóz, rów przeciwczołgowy, teren niedostępny, wybrzeże morskie), maksymalna wysokość terenu oraz średnia głębokość akwenów morskich. System zapewnia możliwość prowadzenia ćwiczeń na obszarze o wymiarach 2000 x 2000 NM (1 NM = 1852 m).

Rysunek nr 1: Przykładowa sytuacja taktyczna w systemie JTLS.



Źródło: <http://csikgw.aon.edu.pl/index.php/pl/narzedzia/88-narzedzia.html>

System ten jest obecnie wykorzystywany do ćwiczeń z jednostkami na poziomie korpusu, dywizji, brygady (opcjonalnie) – a więc na poziomie największych jednostek wchodzących w skład SZ RP. Wynika to również z wspomnianej wcześniej dokładności systemu – jego rozdzielczości,⁵ która jest wystarczająca właśnie dla wspomnianych poziomów w SZ RP.

Stąd wykorzystanie tego systemu na potrzeby zarządzania kryzysowego należy rozpatrywać na poziomie krajowym, we współpracy z Rządowym Zespołem Zarządzania Kryzysowego oraz Rządowym Centrum Bezpieczeństwa (podległym Prezesowi Rady Ministrów – zapewniające obsługę Rady Ministrów, Prezesa Rady Ministrów, Zespołu i Ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz pełniące funkcję Krajowego Centrum Zarządzania Kryzysowego).

Współpraca JTLS powinna zostać zorganizowana w taki sposób, że osoby decyzyjne biorące udział w ćwiczeniu z jego wykorzystaniem nie byłyby zmuszone do obsługi kolejnego narzędzia informatycznego. Swoją pracę powinny nadal wykonywać w systemach używanych w pracy bieżącej, a dzięki zintegrowaniu przetwarzanych przez nich informacji np. poprzez wspomniane narzędzia HMS Web Portal lub SZK Web Portal powstaje możliwość integracji również z narzędziami symulacyjnymi. Stąd decyzje podjęte przez osoby funkcyjne w tych

⁵ A dokładnie o **rozdzielczości symulacji** – jest to wielkość określająca poziom detali, na jakim opisywany jest dany komponent systemu oraz jego zachowanie. dla każdego z opisywanych narzędzi rozdzielczość jest różna, tym większa im niższy poziom realizacji zadań zarządzania kryzysowego symuluje.

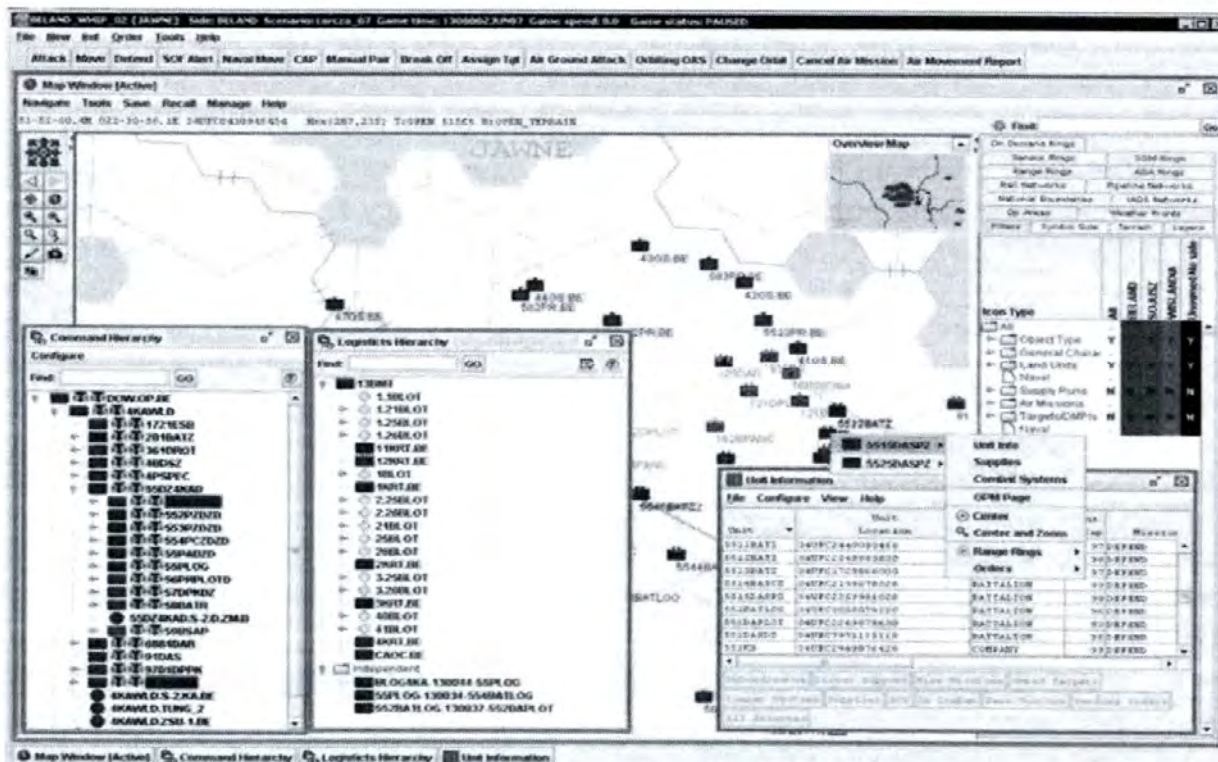
narzędziach można następnie przesłać do systemu JTLS, w którym nastąpi ich zasymulowanie – rys. 2.

Wyniki symulacji mogą być prezentowane zarówno w systemie JTLS z nałożonymi na nie np. mapami rastrowymi – rys. 3 lub ponownie przekazywane do systemu, w którym zostały opracowane i tam zaprezentowane. Druga opcja jest wersją przez autora preferowaną ze względu na wspomniane dążenie do ograniczenia ilości narzędzi informatycznych, których znajomość jest niezbędna do realizacji zadań przez osoby decyzyjne. Prezentowanie wyników symulacji w systemie JTLS ograniczone powinno być do osób nadzorujących przebieg ćwiczenia.

Integracja systemu JTLS z systemem C3IS Jaśmin została potwierdzona doświadczalnie w Akademii Obrony Narodowej w wyniku prób podjętych przez przedstawicieli CSiKGW oraz producenta oprogramowania – firmy Teldat. Stąd należy wskazać system JTLS jako narzędzie, które znacząco może podnieść poziom prowadzonych ćwiczeń zarządzania kryzysowego na najwyższym jego poziomie – krajowym.

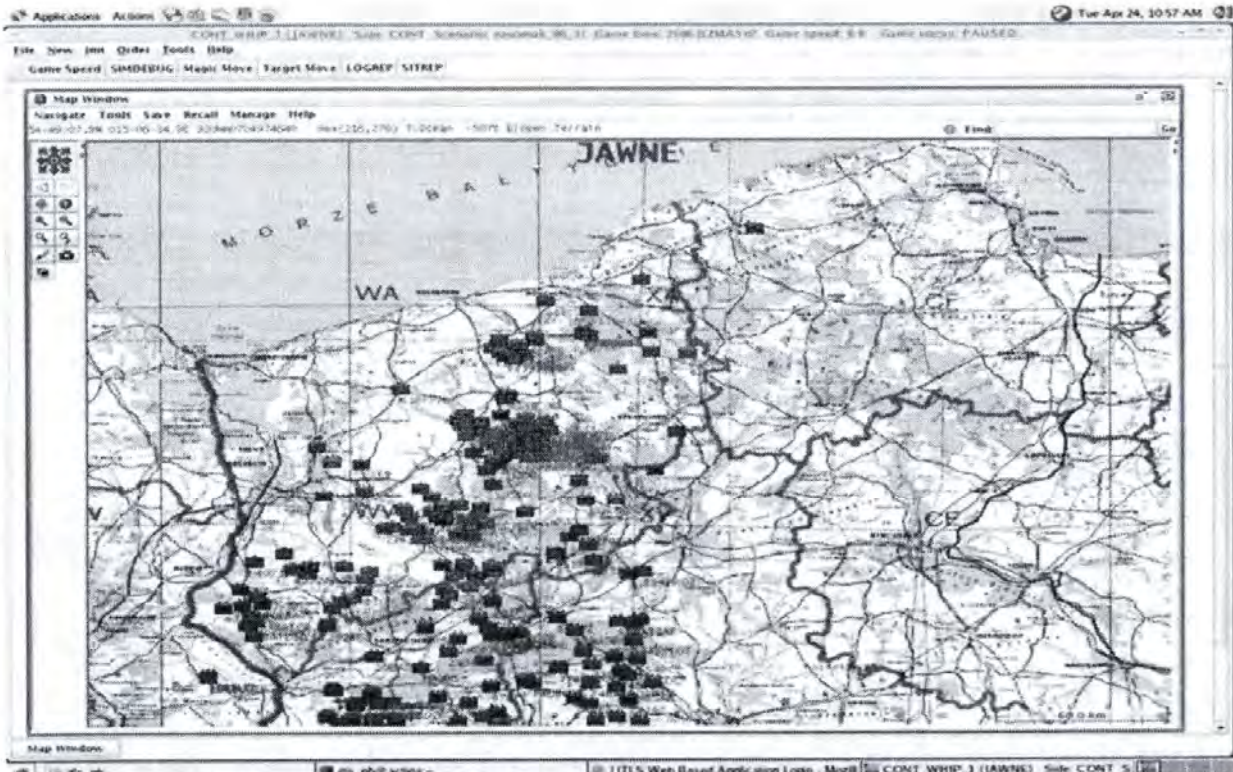
Z jednej strony używane jest przez cały czas narzędzie wykorzystywane do pracy bieżącej (unikamy używania systemów tylko okazjonalnie – w czasie ćwiczeń lub realizacji realnych działań), z drugiej zaś przebieg samego ćwiczenia wspomagany jest przez narzędzie symulacyjne, które wskazuje wszelkie słabości podjętych decyzji, ich przyczyny i skutki, które potem, w trakcie omawiania ćwiczenia, można zidentyfikować i wskazać, a przez to w przyszłości wyeliminować. Można również znaleźć ewentualne słabości realizowanych w trakcie ćwiczeń procedur.

Rysunek nr 2: Okno operatora systemu JTLS.



Źródło: <http://csikgw.aon.edu.pl/index.php/pl/narzdzia/88-narzdzia.html>

Rysunek nr 3: Wyniki symulacji w systemie JTLS zaprezentowane na podkładzie mapy rastrowej.



Źródło: <http://csikgw.aon.edu.pl/index.php/pl/narzedzia/88-narzedzia.html>

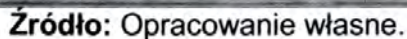
2. Symulator Działań Taktycznych AON/WAT

Symulator działań Taktycznych – jest to narzędzie stworzone przez konsorcjum: Wydział cybernetyki WAT oraz Wydział Zarządzania i Dowodzenia AON jako propozycja narzędzia symulacyjnego dla poziomu dowodzenia kompania – batalion (rys. 4.). W proponowanym rozwiązaniu wykorzystania systemów symulacyjnych na potrzeby zarządzania kryzysowego narzędzie to można by było wykorzystać na poziomie wojewódzkim, czyli w Wojewódzkich Zespołach Zarządzania Kryzysowego,⁶ oraz w Wojewódzkich Centrach Zarządzania Kryzysowego. Stanowiłoby to uzupełnienie i mogłoby współgrać z systemem JTLS, wykorzystywanym do ćwiczeń na wyższym poziomie.

Symulator Działań Taktycznych, stanowiący niejako punkt wyjścia do proponowanych rozwiązań doskonale sprawdził się (i sprawdza nadal) w trakcie realizowanych przez Wydział Zarządzania i Dowodzenia ćwiczeniach wojskowych z wykorzystaniem systemów wsparcia dowodzenia. Podobnie, jak to ma miejsce w przypadku systemu JTLS, możliwa jest wymiana danych pomiędzy systemem wsparcia dowodzenia C3IS Jaśmin, a Symulatorem Działań Taktycznych. W praktyce realizowane jest to w następujący sposób: sztab jednostki opracowuje warianty działania w systemie wsparcia dowodzenia C3IS Jaśmin. Następnie, wstępnie rekomendowany wariant, jest przesyłany do Symulatora, gdzie dokonywana jest jego symulacja (rys. 5.). Wyniki symulacji otrzymuje się w bardzo krótkim czasie, gdyż Symulator pozwala nawet na 60- krotne przyspieszenie

⁶ Wojewódzki Zespół Zarządzania Kryzysowego – organ pomocniczy wojewody powoływany przez wojewodę, który określa jego skład, organizację, siedzibę oraz tryb pracy.

Rysunek nr 4: Przykładowy wariant działania w Symulatorze Działań Taktycznych AON/WAT.



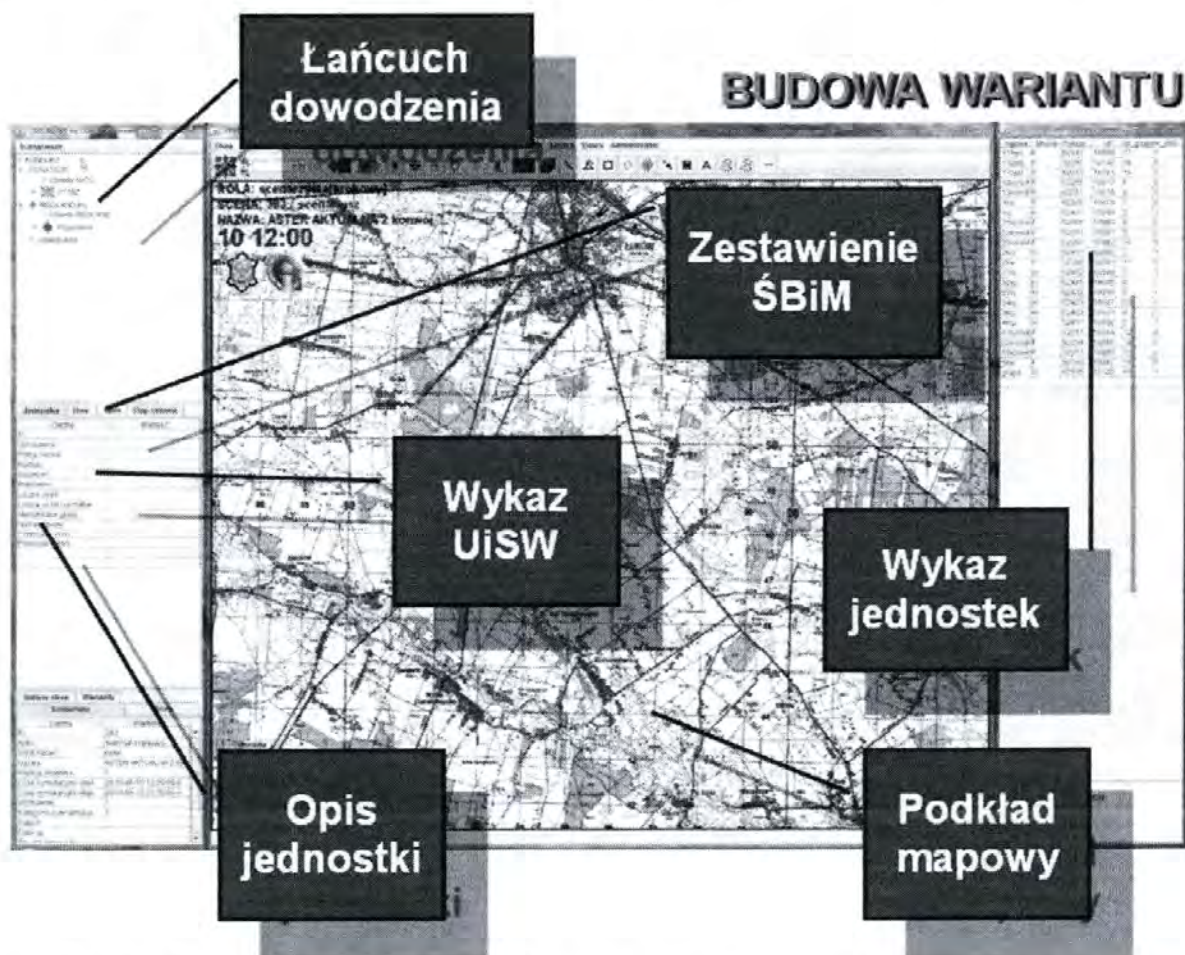
SYMULACJA WARIANTU



W związku z tym, że jest to narzędzie dopiero w fazie propozycji symulatora poziomu taktycznego możliwa jest jego rozbudowa o funkcjonalności związane z działaniami służb publicznych, charakterystycznymi dla poszczególnych z nich specyficznymi potrzebami informacyjnymi. Jednakże pomimo faktu, że jest to narzędzie stworzone specjalnie na potrzeby SZ RP możliwe jest jego wykorzystanie na potrzeby ZK, gdyż w obecnej wersji umożliwia on m.in.:

- tworzenie własnych wariantów działania (rys. 6) lub zaimportowanie ich z systemu C3IS Jaśmin;
- uwzględnienie podczas symulacji wariantów działania następujących cech:
 - danych terenowych (widzialność, przekraczalność, ukształtowanie terenu itp.);
 - położenia i wyposażenia sił własnych oraz przeciwnika;
 - parametrów posiadanego sprzętu;
 - możliwości rozpoznania zarówno przeciwnika przez wojska własne, jak i wojsk własnych przez przeciwnika;
 - modeli walki dla środków rażenia bezpośredniego i pośredniego;
 - parametrów posiadanej amunicji.
- dokonanie porównania różnych wariantów działania oraz wspiera proces podejmowania decyzji przez dowódcę.

Rysunek nr 6: Okno operatora w Symulatorze Działań Taktycznych AON/WAT umożliwiające tworzenie (lub importowanie) wariantów działania.



Źródło: Prezentacja dla Ministra Obrony Narodowej, w trakcie wizyty w WZiD AON.

Oczywiście, nie wszystkie z wymienionych cech są niezbędne w ZK, niemniej jednak wytrawny czytelnik zauważy, że niewielkie modyfikacje pozwolą na jego pełniejsze wykorzystanie również w innych służbach publicznych niż wojsko.

A wszystko znów mogłoby być zrealizowane niemal identycznie, jak w scenariuszu z wykorzystaniem systemu JTLS – osoby podejmujące decyzje pracują na swoich systemach, dzięki możliwości ich integracji z systemami HMS Web Portal lub SZK Web Portal informacje trafiają do Symulatora Działań Taktycznych, a następnie wynik symulacji ponownie jest przesyłany do systemów wykorzystywanych przez decydentów. Dzięki temu nie ma konieczności uczenia ich kolejnych narzędzi informatycznych.

W tym scenariuszu pojawia się jednak pewna nowość, wynikająca z niższego poziomu na którym prowadzone będą ćwiczenia, a dająca dodatkowe możliwości decydentom (ale i obowiązki). Mowa o (wspomnianej wcześniej) możliwości dopracowania wariantu działania przed jego ponownym przesłaniem do systemów wsparcia decyzji. W pierwszym scenariuszu, z wykorzystaniem systemu JTLS, nie wskazywano takiej możliwości – tam wyniki symulacji na bieżąco są przekazywane do systemu wsparcia dowodzenia. W jednym i drugim przypadku mamy do czynienia z symulacją konstruktywną, polegającą na symulowaniu zachowań ludzi i sprzętu przez narzędzie informatyczne. W wypadku wykorzystania Symulatora Działań Taktycznych ćwiczenia z nim prowadzone miałyby nieco inny charakter, gdyż wspiera on głównie symulację podejmowanej decyzji w trakcie planowania jej wykonania, a nie w trakcie jej realizacji – stąd różnica w scenariuszach wykorzystania. Do podobnego działania jak w przypadku systemu JTLS, ale na niższym poziomie ZK należy wykorzystać inne narzędzia symulacyjne – systemy JCATS oraz VBS2.

W tym scenariuszu należy przewidzieć współpracę decydentów biorących udział w ćwiczeniu z operatorami Symulatora w trakcie „dopracowywania” wariantu działania przed podjęciem ostatecznej decyzji o jego zatwierdzeniu. Stąd można wskazać, że jest to scenariusz o tyle trudniejszy, że wymaga poznania przez osoby ćwiczące specyfiki narzędzia symulacyjnego w takim zakresie, aby być w stanie w pełni wykorzystać jego możliwości. Inny jest również charakter prowadzonych ćwiczeń z jego wykorzystaniem – wspierający bardziej część planistyczną ćwiczenia.

3. System symulacji wirtualnej JCATS

JCATS (ang. *Joint Conflict and Tactical Simulation*) to symulator pozwalający na symulowanie najróżniejszych scenariuszy działania, pozwalający wykreować niemal każdą sytuację, z jaką można się zetknąć. Jest narzędziem bardzo podobnym do omówionego wcześniej systemu JTLS, z tą różnicą, że jest znacznie dokładniejszy, tzn. że ma znacznie większą rozdzielczość symulacji.

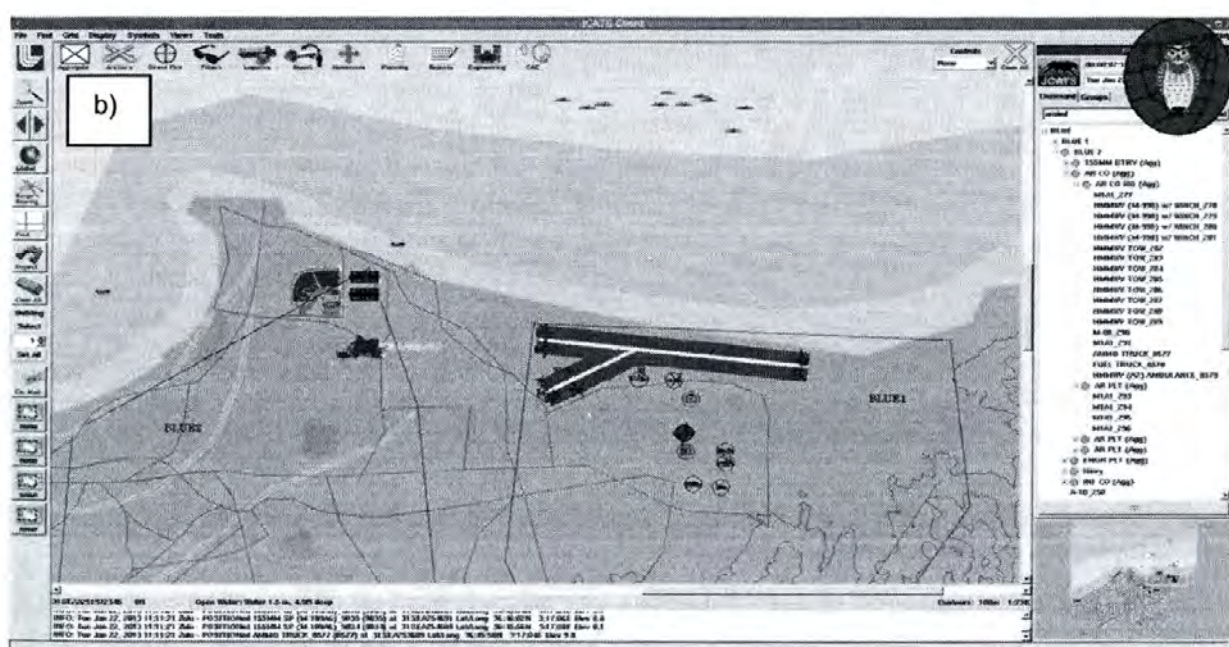
System może stworzyć ponad 60 tysięcy różnego rodzaju sytuacji rozgrywających się na cyfrowych mapach na obszarze około 700 kilometrów kwadratowych (rys. 7.). Jest w stanie wiernie odzwierciedlić potyczki, akcje odbijania zakładników czy działania antyterrorystyczne. Można w nim uczyć się również ewakuacji medycznej.

Istotne jest, że symulator ten, podobnie jak ma to miejsce w Symulatorze Działań Taktycznych, uwzględnia nie tylko charakterystykę obszaru, w którym odbywa się symulacja, ale także symuluje możliwości techniczne symulowanego

w scenariuszu sprzętu: pojazdów, uzbrojenia, itp. (rys. 8 i 9). Uwzględnia także takie parametry jak ilość paliwa, amunicji, zapasów żywności (i wiele innych). Jest również w stanie ocenić wytrzymałość operatorów biorących udział w symulacji.

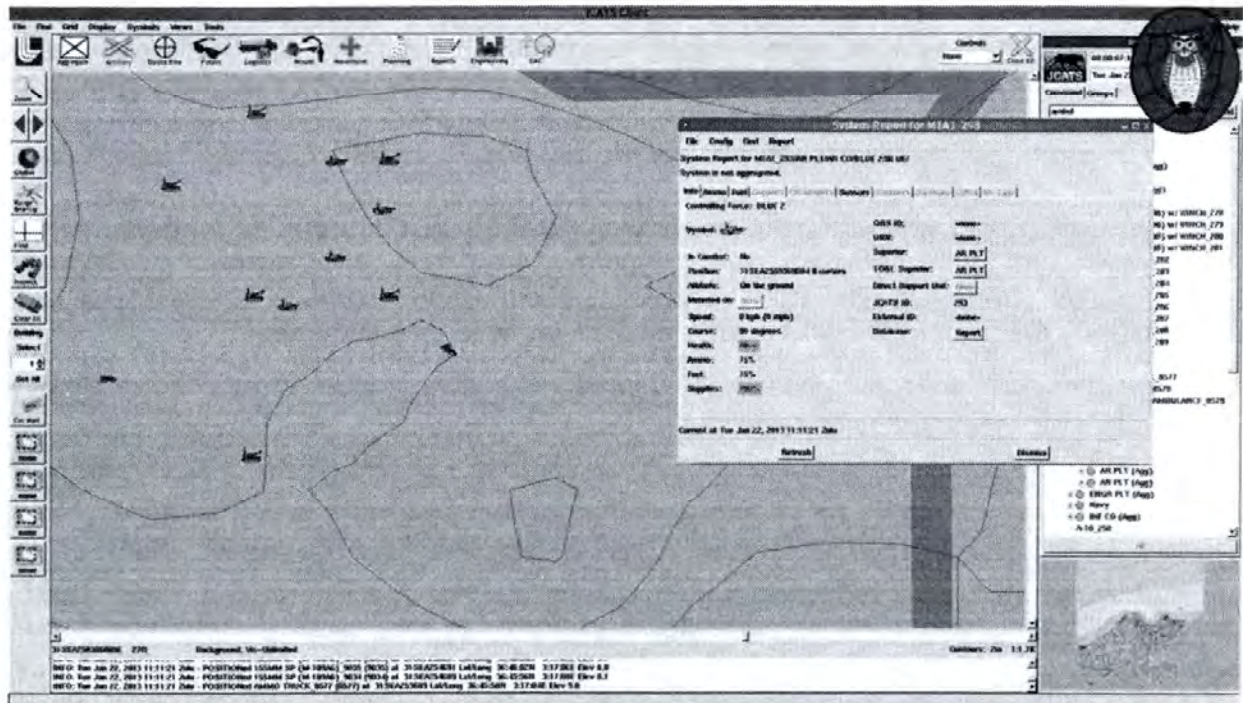
JCATS służy do weryfikowania możliwości wykonania zaplanowanych wariantów działania przez dowódców. Dzięki symulacji w czasie rzeczywistym możliwe jest skonfrontowanie planów i zadań postawionych podwładnym przez przełożonych.

Rysunek nr 7: Okno operatora w symulatorze JCATS. Widoczny na podkładzie map wektorowych fragment scenariusza przygotowany przez specjalistów z CWMSD na ćwiczenie „GRONOST@J-13”: a) obszar obejmujący fragment obszaru ćwiczeń; b) przybliżony obszar lotniska wraz z rozmieszczonym w terenie sprzętem.



Źródło: Materiały CWMSD.

Rysunek nr 8: Na podkładzie mapowym widoczne jest rozmieszczenie sprzętu. W dodatkowym oknie widoczne są informacje o czołgu o oznaczeniu M1A1-293.



Źródło: Materiały CWMSD.

Rysunek nr 9: Przykład postawionych zadań poszczególnym pojazdom. Na czerwono widoczny jest wskazany do zniszczenia samolot strony przeciwnej konfliktu.



Źródło: Materiały CWMSD.

Jest to narzędzie wykorzystywane do szkoleń przez Amerykanów od 2010 roku, a więc stosunkowo nowe. JCATS jest również na wyposażeniu SZ RP wykorzystuje je Centrum Wsparcia Mobilnych Systemów Dowodzenia

Wojsk Lądowych w Białobrzegach. Od niedawna specjaliści z CWMSD mogą samodzielnie przygotowywać scenariusze działań w tym systemie, uzyskali bowiem wszelkie certyfikaty od producentów oprogramowania. Miało to miejsce w trakcie ćwiczenia „GRONOST@J-13”, które odbyło się w dniach od 22 do 26 września 2013 roku na terenie Ośrodka Szkolenia Poligonowego Wojsk Lądowych w Wędrzynie. Wydział Symulacji CWMSD brał udział w projektowaniu, planowaniu i przygotowaniu ćwiczenia dowódczo-sztabowego wspomaganego komputerowo 7 batalionu z 17 Wielkopolskiej Brygady Zmechanizowanej (17WBZ).⁷

System ten może z powodzeniem być zasilony nie tylko danymi sprzętu wojskowego, ale również będącego na wyposażeniu pozostałych służb publicznych. Co więcej (i było to już wspomniane rok temu przy okazji omawiania systemu VBS2) można również symulować sprzęt niebędący jeszcze w użytkowaniu, a np. planowany do zakupu lub będący w trakcie projektowania.

Stąd system ten doskonale sprawdziłby się do ćwiczeń z zakresu ZK na poziomie powiatowym, w Powiatowych Zespołach Zarządzania Kryzysowego⁸ oraz Powiatowych Centrach Zarządzania Kryzysowego.

W wypadku tego systemu scenariusz jego wykorzystania jest niemal identyczny z pierwszym przypadkiem, systemem JTLS, tyle, że na niższym poziomie ZK. Stąd nie ma potrzeby dalszego jego opisywania, gdyż podobnie, jak to ma miejsce w przypadku systemu JTLS umożliwia on decydentom korzystanie z narzędzia, z którego korzystają na co dzień – natomiast wyniki ich pracy są weryfikowane przez symulator – system JCATS, który w czasie rzeczywistym daje odpowiedź, w jaki sposób podjęta decyzja wpływa na rozwój scenariusza ćwiczenia.

Jest to możliwe dzięki zastosowaniu w JCATS podobnych standardów wymiany danych, jak w przypadku systemu JTLS. Wspomniany JTLS oraz C3IS Jaśmin są w stanie wymieniać pomiędzy sobą dane, stąd domniemywać należy, że będzie to również możliwe i w tym przypadku.⁹

Jest to zatem system stwarzający podobne wymagania dla organizatorów ćwiczenia, co system JCATS, jednak na niższym poziomie ZK.

Znacznie ciekawiej prezentuje się ostatni z omawianych scenariuszy – wykorzystanie systemu VBS2 – systemu symulacji wirtualnej.

4. System symulacji wirtualnej VBS2

Ostatnim omawianym narzędziem symulacyjnym jest system VBS2 (*ang. Virtual Battle Space 2*), produkowany przez Czeską firmę Bohemia Interactive.

Jest to narzędzie o największej rozdzielczości z omawianych w artykule, stąd jego wykorzystanie powinno być planowane na poziomie gminnym (oraz ewentualnie na poziomie powiatowym – zamiast systemu JCATS).

⁷ Więcej na ten temat patrz: <http://www.army.mil.pl/index.php/aktualnosci/5529-jcats-z-cwmsd-podczas-certyfikacji>. oraz http://www.17wbz.wp.mil.pl/pl/66_792.html

⁸ Powiatowy Zespół Zarządzania Kryzysowego – organ pomocniczy powołany przez Starostę, który określa jego skład, organizację, siedzibę oraz tryb pracy.

⁹ Połączenie systemu C3IS Jaśmin z systemem JCATS jest planowane w najbliższej przyszłości w trakcie ćwiczeń wojskowych z wykorzystaniem obu systemów (w trakcie prowadzonych przez autora badań) w AON.

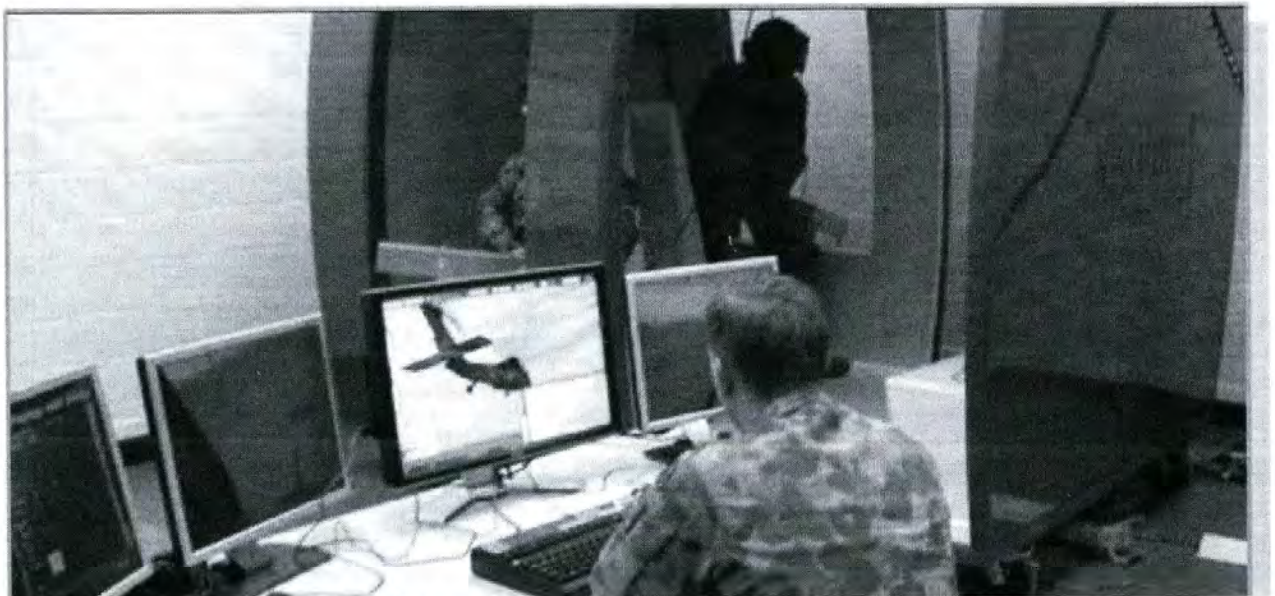
Działanie systemu polega na tym, że operator zasiadający np. przed monitorem komputera (możliwe są różne scenariusze wykorzystania systemu – od najprostszych, ograniczających się tylko do komputerów, na których jest zainstalowany system – rys. 10, do bardziej skomplikowanych, gdzie wykorzystuje się np. trenażery sprzętu lub specjalny strój dla osób uczestniczących w symulacji – rys. 11 i 12) porusza się w czasie rzeczywistym na mapach cyfrowych wybranego terenu.

Rysunek nr 10: Symulacja w systemie VBS2 w najprostszej wersji – system zainstalowany na komputerach i obsługiwany przez operatorów.



Źródło: Opracowanie własne na podstawie materiałów firmy SPECOPS.

Rysunek nr 11: Symulacja w systemie VBS2 w wersji najbardziej rozbudowanej – system zainstalowany na specjalnie przygotowanych trenażerach – na pierwszym planie widoczny operator scenariusza – tzw. „nadzorca”, w tle ćwiczący operatorzy.



Źródło: Opracowanie własne na podstawie materiałów firmy SPECOPS.

Dzięki odpowiednio przygotowanym mapom 3D operator ma wrażenie działania w terenie bardzo zbliżonym do rzeczywistego. Wierne odwzorowanie rzeźby terenu odgrywa bardzo ważną rolę w działaniach prowadzonych zarówno przez wojsko, jak i przez inne służby publiczne (PSP, Policja).

Symulacja z wykorzystaniem tego systemu ma nieco inny charakterom wcześniej omawianych symulatorów, chociażby ze względu na to, że jest to system wirtualnej symulacji, a nie symulacji konstruktywnej.

Rysunek nr 12: Symulacja w systemie VBS2 w wersji najbardziej rozbudowanej – system zainstalowany na specjalnie przygotowanych trenażerach.



Źródło: Opracowanie własne na podstawie materiałów firmy SPECOPS.

Scenariusz z wykorzystaniem systemu VBS2 na potrzeby ZK można sprowadzić do połączenia systemów wykorzystywanych przez decydentów w trakcie realizacji zadań ZK z systemami HMS Web Portal lub SZK Web Portal i systemem VBS2. Różnica polega jednak na tym, że system VBS2, jak wspomniano wcześniej, jest systemem najdokładniej oddającym rzeczywistość w wersji wirtualnej i wymaga realizacji zadań (stawianych przez dowódców) przez operatorów z największą dokładnością w czasie rzeczywistym. Oznacza to, że przy wykorzystaniu tego narzędzia schodzimy na najniższy możliwy poziom symulacji – pojedynczego sprzętu, konkretnego ratownika biorącego udział w akcji itp. Oczywiście system jest tak skonstruowany, że można wykorzystać w tworzonym scenariuszu dowolną ilość osób rzeczywiście biorących udział w ćwiczeniu, a pozostałe osoby niezbędne do jego realizacji powierzyć odgrywaniu przez sam symulator. Tak więc, mając przygotowany jeden scenariusz, można go ćwiczyć na wiele sposobów – w pełnej, częściowej lub bardzo okrojonej obsadzie etatowej – w zależności od możliwości i rozmachu ćwiczenia. Co więcej, ten sam scenariusz można rozgrywać w najróżniejszych warunkach meteorologicznych, wyposażenia itp. Ponadto, scenariusz rozgrywany nawet przy tych samych warunkach wstępnych, dzięki zastosowaniu mechanizmom nigdy nie przebiega w taki sam sposób. Dlatego nie ma niebezpieczeństwa ćwiczenia tych samych scenariuszy w sposób rutynowy – uczestnicy ćwiczenia za każdym razem będą musieli się zmagać z innym rozwojem sytuacji. Jest to niewątpliwa zaleta tego narzędzia i jeden z najważniejszych atutów (nie jedyny).

Jego wykorzystanie z jednej strony byłoby podobne do poprzednich przykładów (systemów: JTLS, Symulatora Działań Taktycznych czy systemu JCATS) – dla osób podejmujących decyzję, gdyż one, również i w tym przypadku powinny pracować przy wykorzystaniu swoich systemów. Również tutaj, dzięki ich integracji z HMS Web portal lub SZK Web Portal dane byłyby przesyłane do systemu symulacyjnego, w tym wypadku do VBS2.

Na tym jednak podobieństwa się kończą, gdyż w tym scenariuszu pojawia się potrzeba prowadzenia wirtualnej symulacji w czasie rzeczywistym (przypomnijmy – w tym wypadku jest to typowa symulacja wirtualna). Muszą ją prowadzić operatorzy w systemie symulacyjnym. Stanowią oni element realizujący stawiane w scenariuszu zadania, a więc wykonawców. Stąd, w tym przypadku, wynika potrzeba dodatkowego przeszkolenia osób odpowiedzialnych za realizację zadań w systemie ZK na poziomie gminnym i/lub powiatowym i jemu podległym w obsłudze systemu VBS2. Osoby decydujące o sposobie działania mogą nadal brać udział w ćwiczeniach przy wykorzystaniu jedynie narzędzi stosowanych na co dzień, jedynie zintegrowanych systemami HMS Web Portal lub SZK Web Portal.

Przykład takiej integracji dwustronnej stanowią ostatnie ćwiczenia prowadzone obecnie w WZiD w AON, w zakładzie autora. Polega to na łączeniu systemu VBS2 z systemem C3IS Jaśmin (relacja dwukierunkowa – decyzja dowódców z C3IS Jaśmin ma wpływ na symulację w VBS2 i odwrotnie – rozwój symulacji operatorów VBS2 przekłada się na sytuację w C3IS Jaśmin) – rys. 13 i 14.

Rysunek nr 13: Integracja systemu VBS2 z systemem C3IS Jaśmin. Na zdjęciu widoczny jest obraz z systemu VBS2 (skrajny prawy ekran) oraz odwzorowanie tej sytuacji w systemie C3IS Jaśmin na ekranie komputera (laptop pod tym ekranem).



Źródło: Opracowanie własne.

Rysunek nr 14: Inne ujęcie sytuacji z rys. 13.



Źródło: Opracowanie własne.

Należy również pamiętać o tym, że potrzebni będą również specjaliści, którzy pomogą (w porozumieniu z przedstawicielami organów ZK) przygotować odpowiednie scenariusze do systemu symulacyjnego.

Reasumując rozważania nad tym scenariuszem należy podkreślić, że jest on zdecydowanie bardziej skomplikowany w realizacji niż poprzednie dwa, ze względu na charakter systemu (wirtualna symulacja), jak również na sposób jego realizacji (czas rzeczywisty) oraz poziom dokładności symulowanych elementów (do pojedynczych pojazdów, osób, a terenu do kilku metrów). Jest również bardziej czasochłonny w przygotowaniu i musi obejmować również szkolenia dla operatorów symulatora. Dobrze, aby jego użytkownikami były osoby realnie wykonujące stawiane przez PZZK dlatego, że wraz z rosnącą liczbą przeprowadzonych ćwiczeń będzie wzrastało ich doświadczenie (nie tylko w obsłudze symulatora, ale przede wszystkim w sposobie działania na zaistniałe sytuacje).

Tak prowadzone ćwiczenia będą miały wymierne korzyści dla wszystkich elementów biorących udział w ZK. Z jednej strony umożliwią bowiem prowadzenie ćwiczeń w sytuacjach bardzo trudnych lub nawet, ze względów prawnych niemożliwych do przeprowadzenia w realnym świecie. Z drugiej strony każde takie ćwiczenie wymagające zaangażowania wielu służb będzie pozytywnie wpływać na świadomość decydentów (jak mają się zachować w danej sytuacji) oraz osób odpowiedzialnych za realizację zadań.

Przypominając nieco materiał ubiegłoroczny należy podkreślić, że system VBS 2:

- umożliwia pokazanie tego, czego nie można zobaczyć;
- pozwala zasymulować to, czego nie można wykonać;
- daje możliwość wypróbowania takich rozwiązań, które z różnych powodów (np. prawnych) nie są obecnie możliwe;
- weryfikuje teoretyczne założenia w wirtualnej rzeczywistości, w realiach czasu rzeczywistego.

System VBS 2 składa się z wielu modułów, które pozwalają m.in. na (rys. 15 i 16):

- tworzenie dowolnych obszarów (terenu), na których będą rozgrywane symulacje;
- tworzenie dowolnych scenariuszy działania, które w dodatku w trakcie trwania symulacji operator nadzorujący przebieg szkolenia może dowolnie modyfikować utrudniając lub ułatwiając szkolonym wykonanie zadania;
- tworzenie nowych rodzajów sprzętu – również takich, które nie są jeszcze na wyposażeniu służb lub są w trakcie badań;
- analizę wyników szkolenia wraz z pełną statystyką tego, co poszczególni uczestnicy wykonali w trakcie symulacji.

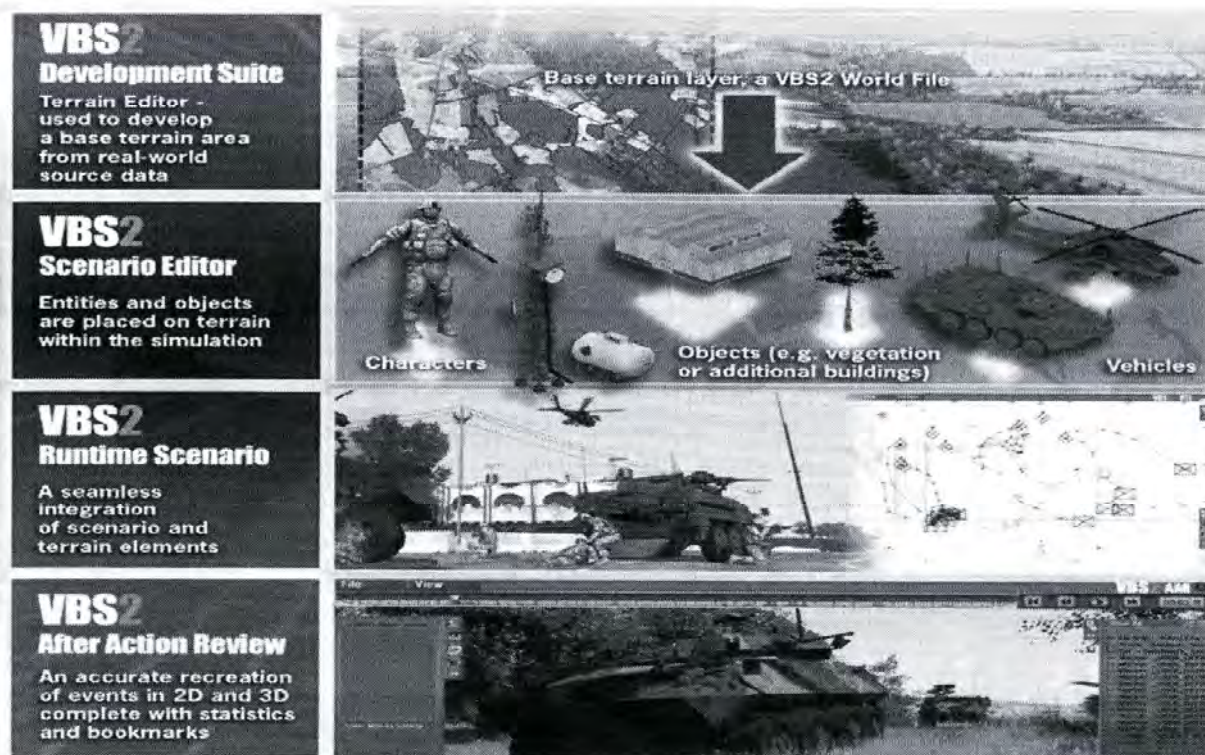
Rysunek nr 15: System VBS 2 – elementy składowe systemu.



Źródło: Opracowanie własne na podstawie materiałów firmy SPECOPS.

Pomysł na wykorzystanie systemu oraz jego zintegrowania z systemami wsparcia dowodzenia wykorzystywanymi w Wojsku Polskim zrodził się kilka lat temu. Obecnie, dzięki możliwościom technicznym oferowanym przez system C3IS Jaśmin, taka integracja jest możliwa.

Rysunek nr 16: System VBS 2 – elementy składowe systemu.



Źródło: Materiały firmy SPECOPS.

Daje to możliwość szkolenia w jednym czasie żołnierzy, operatorów sprzętu specjalistycznego oraz dowódców. Każdy ze szkolonych będzie wykorzystywał etatowe wyposażenie (żołnierz: karabin i umundurowanie, operator sprzętu: etatowe „stanowisko pracy” – z tą różnicą, że w trenażerze, a nie w realnym czołgu czy pojeździe, a dowódca będzie korzystał w tego samego narzędzia, z którego korzysta w trakcie ćwiczeń (i w trakcie kryzysu lub wojny) – z systemu wsparcia dowodzenia.

Informacje będą wymieniane pomiędzy tymi systemami a wyniki symulacji będą się przekładać na informacje przekazywane dowódcom. Z kolei decyzje dowódców będą wpływały na dalszy rozwój scenariusza w trakcie symulacji.

Tak stworzone środowisko ćwiczeń przygotowane dla wojsk należy poszerzyć o służby publiczne. Pozwoli to na ćwiczenie takich scenariuszy zdarzeń, które być może nigdy nie będą miały miejsca (awarie zapór wodnych, przerwanie wałów przeciwpowodziowych, awarie elektrowni, ataki terrorystyczne na np. infrastrukturę krytyczną państwa i wiele innych).

Podsumowanie

W opinii autora opisane scenariusze wykorzystania różnych, dostępnych obecnie na rynku, jak i w SZ RP, narzędzi symulacyjnych w połączeniu z systemem integrującym wszystkie służby publiczne pozwala na uzyskanie bardzo wielu korzyści, z których do najważniejszych należy zaliczyć m.in.:

1. Znaczne obniżenie kosztów ćwiczeń, poprzez umożliwienie m.in. działania na znaczne odległości bez konieczności przemieszczania się ćwiczących do rejonu ćwiczeń (dzięki wydajnym łączom Internetowym jest to obecnie możliwe bez większych trudności);

2. Ułatwienie ich przygotowania i przeprowadzenia specjalistom z zakresu informatyki i łączności (w zależności od ćwiczącego znacznie zmniejsza się ilość wykorzystywanych narzędzi informatycznych, a dzięki stosowaniu systemu HMS Web Portal lub SZK Web Portal jako integratora unikamy problemów z rozdzielczością poszczególnych symulatorów;¹⁰
3. Uniknięcie komplikacji związanych z koniecznością opanowania przez decydentów wielu nowych narzędzi informatycznych (co gorsza używanych jedynie w trakcie ćwiczeń) na rzecz jednego systemu, używanego na co dzień oraz w trakcie ćwiczeń (i najważniejsze – w trakcie działań).

Wskazane są dalsze prace w kierunku umożliwienia współpracy służb publicznych w celu stworzenia Wspólnego Obrazu Sytuacji Służb Publicznych, gdyż tylko taki obraz jest w stanie oddać w pełni to, co dzieje się na obszarze prowadzonych działań (szczególnie na terenie kraju).

Autor dołoży wszelkich starań, aby kontynuować badania w tym kierunku i rozwijać ideę integracji informacji oraz systemów wsparcia decyzji w służbach publicznych. Ma również nadzieję, że następna Konferencja będzie okazją do zaprezentowania kolejnych doświadczeń, zdobytych w trakcie planowanych na ten rok ćwiczeń w WZiD AON oraz w SZ RP.

Bibliografia

1. Biernacik B., *Wybrane aspekty wykorzystania narzędzi informatycznych w procesie zapewnienia bezpieczeństwa teleinformatycznego organizacji*, (w:) Człowiek wobec problemów bezpieczeństwa w XXI wieku, Wyzwania dla nauk społecznych wynikające z zagrożeń współczesnego świata, t. 3, red. A. Piotrowski, M. Ilnicki. Poznań 2012
2. Biernacik B., *Wsparcie informatyczne procesów informacyjnych w podstawowej jednostce organizacyjnej uczelni wojskowej*, AON. Warszawa 2013
3. Biernacik B., *Characteristics of C3IS JASMINE and SBOTSS ZLOCIEN Command Supporting Systems*, opracowanie w programie – Smart Information for Mission Success (SIMS), dla EDA (European Defence Agency), 2010 r.
4. Biernacik B., *Wnioski z wykorzystania zautomatyzowanych systemów wsparcia dowodzenia w wybranych ćwiczeniach organizowanych przez Akademię Obrony Narodowej w latach 2010-2011*, II Konferencja Łączności i Informatyki: Ewolucja wojskowych systemów teleinformatycznych oraz Lessons Learned w świetle misji pokojowych i stabilizacyjnych, 23-24 marca 2011 r. Sieradz 2011
5. Biernacik B., *A Way Towards The Common Operation Picture Using Command Supporting Systems*, 8th NATO LCM Conference, Life Cycle Management in NATO. The Basis for Interoperability and Cost Optimisation, 24-25 stycznia 2012, Bruksela

¹⁰ Temat rozdzielczości poszczególnych symulatorów sam w sobie jest tematem na bardzo obszerne opracowanie, dlatego nie będzie szczegółowo omówiony w tym artykule.

6. Biernacik B., *Możliwość wykorzystania HMS Web Portal na potrzeby zarządzania kryzysowego*, materiały z Sympozjum naukowego Zakładu Systemów Teleinformatycznych nt. „Systemy teleinformatyczne w zarządzaniu kryzysowym”, 11 stycznia 2012 roku, AON. Warszawa 2012
7. Biernacik B., *Wybrane aspekty wykorzystania narzędzi informatycznych w procesie zapewnienia bezpieczeństwa teleinformatycznego organizacji*, (w:) Człowiek wobec problemów bezpieczeństwa w XXI wieku, Wyzwania dla nauk społecznych wynikające z zagrożeń współczesnego świata, t. 3 red. A. Piotrowski, M. Ilnicki. Poznań 2012
8. Dela P., Biernacik B., Pilarski G., *Współpraca mobilnej sieci teleinformatycznej szczebla taktycznego z sieciami użytku publicznego w sieciocentrycznym wymiarze pola walki*, praca naukowo-badawcza pod kierunkiem płk. dr inż. P. Deli, AON. Warszawa 2008
9. Janczak J., *Informatyczne systemy wspomagania zarządzania*, AON. Warszawa 2011
10. Janczak J., Biernacik B., *Zintegrowane systemy informacyjne (dowodzenia wojskami i kierowania środkami walki) w działaniach taktycznych wojsk lądowych*, AON. Warszawa 2010, Praca badawczo-rozwojowa pod kier. dr hab. inż. Józefa Janczaka
11. Lidwa W., *Zarządzanie w sytuacjach kryzysowych*, AON. Warszawa 2010
12. Majewski T., Biernacik B., Frącik K., *System wykorzystania w procesie dydaktycznym informatycznego wspomagania procesu dowodzenia na Wydziale Zarządzania i Dowodzenia*, AON. Warszawa 2010
13. Materiały Teldat: www.teldat.com.pl
14. Materiały ze strony AON: www.aon.edu.pl
15. Materiały informacyjne firmy SPECOPS
16. Muchewicz K., Kruszyński H., Piotrowski M., Palka R., Kosowski T.Z., *Technologia WEB Portali we wspomaganiu pracy komórek sztabu z uwzględnieniem procesu tworzenia obrazu z rozpoznania*, Referat na Sympozjum Naukowym na temat: Nowe kierunki w rozpoznaniu Sił Zbrojnych RP, 1 grudnia 2011, AON. Warszawa.

Zasadniczy wpływ na bezpieczeństwo i szeroko rozumiane funkcjonowanie państwa wywiera niezakłócone działanie infrastruktury krytycznej (IK). Od sprawności tej infrastruktury zależy również bezpieczeństwo obywateli, poprawne funkcjonowanie organów administracji publicznej, a także wielu instytucji i innych organizacji gospodarczych. Już z tych przesłanek wynika, jak ważnym problemem jest identyfikacja zagrożeń i właściwe zaplanowanie i realizacja ochrony IK. Współcześnie występujące zagrożenia dla bezpieczeństwa państwa mają charakter rozwojowy co do rodzaju, źródeł pochodzenia, jak i natężenia czynników destrukcyjnych. Wynika to z wielu uwarunkowań zewnętrznych i wewnętrznych funkcjonowania naszego państwa oraz z rozwoju technologicznego, procesów globalizacji itp. Z powyższego wynika, że ochrona IK powinna być ciągle rozwijana i doskonała, stosownie do zmieniających się uwarunkowań i aktualnych zagrożeń.

prof. dr hab. inż. Franciszek MROCZKO

