Analiza zdolności cybernetycznych za pomocą symulacji komputerowej

Andrzej Najgebauer
kierownik **Zespołu Modelowania, Symulacji i Informatycznego Wspomagania Decyzji w Sytuacjach Kryzysowych i Konfliktowych**
Instytut Systemów Informatycznych
Wydział Cybernetyki
Zespół: A. Najgebauer, R. Antkiewicz, Z. Tarapata, W. Kulas, D. Pierzchała, J. Rulka, M. Chmielewski, R. Kasprzyk, M. Dyk,

Plan prezentacji

- Prace Zespołu Modelowania, Symulacji i Informatycznego Wspomagania Decyzji w Sytuacjach Kryzysowych i Konfliktowych
- Projekt pt. Research and Development on the Application of Cyber Warfare Simulation for Decision Support (Wydział Cybernetyki WAT – Boeing Defense)
- Metodyka badań
- Klasyfikacja i środki działań cybernetycznych
- Symulator wariantów działań taktycznych
- Network Defense Trainer
- Środowisko gry symulacyjnej – federacja
- Eksperymenty symulacyjne operacji militarnych (działania kinetyczne i cybernetyczne (niekinetyczne))
- Podsumowanie

Dotychczasowe prace w zakresie symulacji działań bojowych i wspomagania decyzji

- **W WCY WAT od ponad 20 lat trwają prace w zakresie modelowania i symulacji procesów walki oraz metod wspomagana dowodzenia –** prezentowane systemy są efektem tych doświadczeń;
- Projekty zrealizowane w tym zakresie:
  1. PBR: System symulacyjnego wspomagania szkolenia operacyjnego **ZŁOCIEŃ** (2001-2003); wdrożenie w Centrum Symulacji i Komputerowych Gier Wojennych, AON, (2006-2008, B+R MON);
  2. PBR: Zautomatyzowane narzędzia wspomagania decyzji – system ekspercki pk. **GURU** (2004-2007, B+R MON);
  3. PBZ: Zaawansowane metody i techniki tworzenia świadomości sytuacyjnej w działaniach sieciocentrycznych (2007-2010, PBZ MNiSW);
  4. PR: Integracja systemów dowodzenia (2008-2010, PR MNiSW);
  5. PR: Symulacja działań bojowych w heterogenicznym środowisku wielorozdzielczej i rozproszonej symulacji (2008-2010, PR MNiSW);
  6. Asymmetric Threat Environment Analysis (**ATHENA**) – within multinational consortium for European Defence Agency (2010-2012);
  7. (2012-2015) DOBR/0069/R/ID1/2012/03 **System informatycznego wsparcia rozwoju zdolności oraz identyfikacji potrzeb operacyjnych Sił Zbrojnych RP**, Realizuje konsorcjum – Lider konsorcjum WAT

Dotychczasowe prace w zakresie symulacji sytuacji konfliktowych i działań antykryzysowych

- SEC5-PR-113700 Highway to Security: Interoperability for Situation Awareness and Crisis Management (HiTS-ISAC), "Requirements and Design of Automatic Alarms" (2006-2008) Projekt został zrealizowany przez międzynarodowe konsorcjum w składzie:
  EADS Defence and Security Systems SA, TeliaSonera, Swedish Defence Research Agency, EADS Secure Networks, TietoEnator ALISE, Denodo Technologies S.L. Hugin Expert A/S, Cybernetica AS, UAB "ERP, Saab AB (lider konsorcjum) MUT, Cybernetics Faculty. Projekt został sfinansowany z funduszy Unii Europejskiej
- PBZ-MNiSW-DBO-01/I/2007 nt. "Monitoring, identyfikacja i przeciwdziałanie zagrożeniom bezpieczeństwa obywateli" (2007-2008),
- **NATO MSG 026 pt. M&S Tools for Early Warning Identification of Terrorist Activities**. (2006-2007),
- PBZ-MIN/011/013/2004 pt.: Modele zagrożeń aglomeracji miejskiej wraz z systemem zarządzania kryzysowego na przykładzie m.st. Warszawy. (2006-2009),
- (2009) System Agregacji Raportów - Narzędzie Analityczne (SARNA) dla Rządowego Centrum Bezpieczeństwa. Projekt realizowany w Zespole naukowym modelowania, symulacji i informatycznego wspomagania decyzji w sytuacjach kryzysowych i konfliktowych,
- (2011-2014) PBR -K 15-047/2011/WAT, NCBiR, Nowoczesne technologie dla/w procesie karnym i ich wykorzystanie – aspekty techniczne, kryminalistyczne, kryminologiczne i prawne
- (2011-2013) PBR-K/15-033/2011/WAT, NCBiR, Opracowanie nowoczesnych stanowisk szkoleniowych zwiększających skuteczność działań ratowników KSRG
- (2012-2015) Wirtualny System Doskonalenia Taktyki Ochrony Granicy Państwowej oraz Kontroli Ruchu Granicznego, PBR NCBIR –konsorcjum, którego liderem jest WAT
- (2013- 2014) Projekt międzynarodowy, finansowany przez firmę **Boeing** (USA)"In Support of The NATO AWACS Program - Research and Development on the Application of **Cyber Warfare** Simulation for Decision Support

Research and Development on the Application of Cyber Warfare Simulation for Decision Support

Integration of Polish MUT combat simulations „SWD_T” with NDT software – final Game

Głównym celem wspólnych badań było sprawdzenie za pomocą symulacji komputerowej oddziaływania cybernetycznego na przebieg operacji wojskowej w kontekście procesu decyzyjnego. Jedną z dwóch głównych części w tym programie badawczym był model symulacyjny pod nazwą „Model analizy koncepcji cybernetycznych” (ang. ‘Cyber Concepts Analysis Model’ (CyberCAM) firmy Boeing w kooperacji z firmą Scalable - aplikacja NDT). Drugą, symulator Wariantów Działań Taktycznych (SWDT) , pozwalający odwzorować skutki kinetyczne działań niekinetycznych (WCY, WAT.)

MS4DS team
MODELLING & SIMULATION FOR DECISION SUPPORT TEAM

Metodyka badań

1. Wg. „NATO Code of Best Practice for C2 Assessment” , należy wyznaczyć miary wydajności (Measures of Performance - **MoP**):
   - Liczba zaatakowanych cybernetycznie węzłów teleinformatycznych
   - Liczba ataków cybernetycznych scentralizowanych na siły przeciwnika (DOS) z rozkładem na węzły;
   - Liczba ataków zdecentralizowanych (DDOS) na przeciwnika
   - Liczba ataków szerokopasmowych (jamming)

Pozwalają one na bezpośrednie porównanie różnych typów cybernetycznych działań ofensywnych, wykonywanych w trakcie działań taktycznych lub przed.

2. Do oceny wpływu wydajności działań cybernetycznych na rezultaty działań bojowych wykorzystuje się wskaźniki „Measures of Force Effectiveness (**MoFE**)”:
   - straty własne,
   - straty przeciwnika,
   - tempo natarcia,
   - stopień realizacji przydzielonych zadań (wielkość zajętego obszaru itp.).

3. Badanie należy wykonać dla różnych scenariuszy ataków cybernetycznych w specjalnie skonstruowanym środowisku gry symulacyjnej

Klasyfikacja i środki działań cybernetycznych

- **Działania Cybernetyczne** – działania militarne mające na celu zmianę stanu elementów lub zasobów informacyjnych cyberprzestrzeni. Działania cybernetyczne są kombinacją działań w cyberprzestrzeni oraz fizycznego oddziaływania na elementy cyberprzestrzeni realizowanego w innych wymiarach działań militarnych.
- ***Zdolności cybernetyczne*** – dysponowanie przygotowanym personelem, procedurami, organizacją, narzędziami (uzbrojeniem) i doktryną umożliwiającymi prowadzenie działań cybernetycznych.
- **Działania cybernetyczne składają się z czterech komponentów:**
  - **Tworzenie świadomości sytuacyjnej w cyberprzestrzeni** (identyfikacja aktywności sojuszników i przeciwników w i poprzez cyberprzestrzeń, ocena zdolności cybernetycznych, ocena podatności na działania w cyberprzestrzeni)
  - **Obrona i ochrona cyberprzestrzeni** – polegają na rozwinięciu, operowaniu, zarządzaniu, ochronie, obronie i dowodzeniu własnymi elementami cyberprzestrzeni - Systemy (rozwiązania sprzętowo-programowe) **osłony kryptograficznej połączeń, generatory ruchu maskującego, Systemy detekcyjne (IDS), wykrywające miękkie działania rozpoznawcze i sondujące, usługi własnej, zaufanej „chmury”**, w tym usługi: magazynowania i współdzielenia plików, synchronizacji oraz magazynu haseł, **Silne mechanizmy uwierzytelniania, …**
  - **Walka cybernetyczna** – działania mające na celu wykrycie, zakłócenie, eksplorację lub zniszczenie elementów cyberprzestrzeni lub zasobów informacyjnych przeciwnika (**atak cybernetyczny, eksploracja cybernetyczna** - **Narzędzia ataków hakerskich różnych typów**, **Botnet** jako narzędzie skoordynowanych ataków przeciążeniowych
  - **Działanie wspierające (**Identyfikacja podatności **–** dotycząca cyberprzestrzeni własnej i przeciwnika, Opracowanie metod usuwania podatności we własnej cyberprzestrzeni, …)

Przeznaczenie symulatora

- Wspomaganie rozważania wariantów działania wojsk lądowych na etapie planowania działań
  - Kompleksowa ocena:
    - wojsk własnych i przeciwnika
    - terenu
  - Symulacyjna weryfikacja wariatów działania w zakresie:
    - stopnia realizacji zadań
    - strat potencjałów własnych i przeciwnika
- Szkolenie sztabów i wojsk
- Badanie skuteczności systemów uzbrojenia
- Weryfikacja efektywności procedur dowodzenia

Edytor scenariuszy

- Budowa łańcucha dowodzenia:
  - szablony jednostek
  - podległość jednostek
  - położenie
- Stawianie zadań
- Słowniki UiSW:
  - zasięgi rażenia
  - prawdopodobieństwa niszczenia
  - parametry taktyczno-techniczne
- Słowniki ŚO
- Słowniki ŚBiM
- Baza danych terenowych
- Baza danych o sieci drogowej

Opis symulatora

Opis symulatora

Opis symulatora

Edycja elementów zadania z wykorzystaniem interfejsu graficznego

Edycja położenia jednostek za pomocą interfejsu graficznego

- Model walki lądowej
  opisuje dwa uzupełniające się procesy:
  - strzelania ;
  - przemieszczania;

- Proces niszczenia podczas walki bazuje na rozszerzeniu modelu Lanchestera;

Network Defense Trainer (*NDTrainer*) : *„System symulacyjny (LVC) do implementacji zaawansowanych środowisk działań cybernetycznych, wykorzystywanych do treningów tzw. cyberwojowników. W odróżnieniu od innych aplikacji może zarówno współdziałać z innymi symulatorami oraz z rzeczywistymi systemami. Aby skutecznie wykorzystać właściwości NDT należy stworzyć federację aplikacji do wykonania złożonego eksperymentu szkoleniowego lub badawczego.*

Środowisko do gry

Ogólna postać scenariusza taktycznego

- Opis ogólny;
- Sytuacja geopolityczna w regionie;
- Analiza terenu
- Klimat i pogoda
- Opis ogólny konfliktu
- Początkowa sytuacja taktyczna
- Struktura sił
- Pełna sytuacja

Ogólny opis

- Hipotetyczny scenariusz zakłada użycie sił zbrojnych koalicji w scenariuszu kinetycznego i intensywnego konfliktu. Siły koalicji składają się z jednostek z: 1land, 2land, 3land. W operacji przedstawione dalej granice konfliktu znajdują się na terytorium kraju BLUE.
- Kraj BLUE ma klimat zmienny,
- Obszar operacji (AoO) pokrywa wschodnią część państwa BLUE koło granicy z państwem Red.
- Ugrupowanie koalicyjne zawiera wszystkie państwa członkowskie koalicji.
- Siły koalicyjne sformowane są w postaci dywizji wielonarodowej MNDIV.
- Siły koalicyjne działają zgodnie z umowami międzynarodowymi.
- Państwo Red kumuluje swoje siły w 2 lokalizacjach koło : BARANOVICHI i BREST. Red planuje działania blisko granicy z wykorzystanie ataku cybernetycznego.
- MNDIV planuje obronę terytorium i ewentualne kontruderzenie.

Teren

FE
ŁOMŻA
OSTROŁĘKA
BIAŁYSTOK
Zambrów
Łapy
Równina
BIELSK PODLASKI
Puszcza
Białowieska
Puszcza
Kamieniecka
Czarna Białostocka
Sokółka
Kolno
Morki
Choroszcz
Wasilków
Czerwony
Bór
Wyszki
Mazowieckie
Ostrów
Mazowiecka
Hajnówka
Piska

Teren

SYMULATOR-2
Okna
Komponenty komunikacji
Role
G:Wspomaganie
Słowniki
Mapa
File
Control
Navigate
Layers
Administrator
1:193 995
Lat, Lon (52,847, 22,77) - x, y (645,318)

Ogólny opis konfliktu

Początkowa sytuacja taktyczna

Sytuacja taktyczna

- ENEMY FORCES [H]
  - 2BZ
    - 21bz
      - 212kz
- COALITION [F]
  - 3BZ
    - 31bz
    - 32bz
      - 321kzmot
        - Z. [1] G. [ASAP] P. [-]
          - E [1] T [ASAP - ASAP]
          - E [2] T [ASAP - ASAP]
      - 322kzmot
        - Z. [1] G. [ASAP] P. [-]
          - E [1] T [ASAP - ASAP]
          - E [2] T [ASAP - ASAP]
      - 323kzmot
        - Z. [1] G. [ASAP] P. [-]
          - E [1] T [ASAP - ASAP]
          - E [2] T [ASAP - ASAP]
    - 33bcz
    - 34bcz
    - 35kdow

Struktura sił

Skrót	Liczba	Norma
KTO Rosomak	30	30
Granatnik RGP-7	57	57
BWP-1	30	30
kbkAK	643	643
PT-91	70	70

Skrót	Ilość	Ilość log.	Norma
Amo PG-15W do 2A28 ...	720	0	720
Amo 3WOF22 do 2A46 ...	700	0	700
Amo OG-15W do 2A28 ...	480	0	480
Amo PG-7M do RPG-7	285	0	285
Ppanc pk 9M14 Malutka	120	0	120
Amo do NSW 12,7x107 ...	21 000	0	21 000
Amo do PKT 7,62x54 mm	222 500	0	222 500
Amo APFSDS-T do arm...	7 500	0	7 500
Amo do kbkAK 7,62x39 ...	77 160	0	77 160
Amo 3WBK7 do 2A46 P...	1 120	0	1 120
Amo 3WBM3 do 2A46 P...	1 120	0	1 120
Olej napedowy	134 850	0	134 850

Struktura sił

Skrót	Liczba	Norma
Granatnik RGP-7	27	27
BWP-1	30	30
kbkAK	373	373
PT-91	9	9

Skrót	Ilość	Ilość log.	Norma
Amo PG-15W do 2A28 ...	720	0	720
Amo 3WOF22 do 2A46 ...	90	0	90
Amo OG-15W do 2A28 ...	480	0	480
Amo PG-15W do 2A28 ...	720	0	720
Amo 3WOF22 do 2A46 ...	90	0	90
Amo OG-15W do 2A28 ...	480	0	480
Amo do PKT 7,62x54 mm	78 000	0	78 000
Amo do kbkAK 7,62x39 ...	44 760	0	44 760
Amo 3WBK7 do 2A46 P...	144	0	144
Amo 3WBK7 do 2A46 P...	144	0	144
Amo 3WBM3 do 2A46 P...	144	0	144
Olej napedowy	28 110	0	28 110

Pełna sytuacja taktyczna

WARIANT 1

Sytuacja początkowa:

- Dowódca sił niebieskich ma informacje o jednej kompanii sił czerwonych na trasie 32 batalionu.
- Dowódca sił niebieskich rozkazuje 32 batalionowi zaatakować przeciwnika.

Rozwój scenariusza:

1. 32 batalion zbliża się i atakuje przeciwnika. Pozostałe siły niebieskie wykonują swoje zadania.
2. 32 batalion odkrywa podczas ataku koncentrację 2 dodatkowych kompanii czerwonych i wysyła meldunek do dowódcy niebieskich.
3. Dowódca niebieskich rozkazuje 2 dodatkowym batalionom wesprzeć atak.

Spodziewane wyniki:

- Komunikacja między elementami sił niebieskich działa bez przeszkód.
- Siły niebieskie wygrywają z małymi stratami.
- Siły niebieskie osiągają z sukcesem cel operacji.

WARIANT 2

Sytuacja początkowa:

- Dowódca sił niebieskich ma informacje o jednej kompanii sił czerwonych na trasie 32 batalionu.
- Dowódca sił niebieskich rozkazuje 32 batalionowi zaatakować przeciwnika.

Rozwój scenariusza:

1. Siły czerwone wykonują atak cybernetyczny DOS podczas marszu sił niebieskich.
2. 32 batalion atakuje przeciwnika po osiągnięciu odpowiedniej odległości. Pozostałe siły realizują swoje zadania.
3. 32 batalion odkrywa podczas ataku koncentrację 2 dodatkowych kompanii czerwonych i wysyła meldunek do dowódcy niebieskich.
4. Siły czerwone hakują system C2 dowódcy niebieskich i uniemożliwiają mu komunikację.
5. Dowódca niebieskich rozkazuje 2 dodatkowym batalionom wesprzeć atak.

Oczekiwane wyniki:

- Dowódca niebieskich otrzymuje tylko częściową informację o ruchu swoich sił.
- Dowódca niebieskich nie może wysłać rozkazów do jednostek, które miały wesprzeć 32 batalion.
- 32 batalion zostaje zniszczony przez siły czerwonych.
- Siły niebieskie nie osiągają celu operacji.

WARIANT 3

Sytuacja początkowa:

- Dowódca sił niebieskich ma informacje o jednej kompanii sił czerwonych na trasie 32 batalionu.
- Dowódca sił niebieskich rozkazuje 32 batalionowi zaatakować przeciwnika

Rozwój scenariusza:

1. Siły czerwone wykonują atak cybernetyczny DDOS podczas marszu sił niebieskich.
2. 32 batalion atakuje przeciwnika po osiągnięciu odpowiedniej odległości. Pozostałe siły realizują swoje zadania.
3. 32 batalion odkrywa podczas ataku koncentrację 2 dodatkowych kompanii czerwonych i wysyła meldunek do dowódcy niebieskich.
4. Siły czerwonych hakują system C2 niektórych kompanii niebieskich.
5. Dowódca niebieskich rozkazuje 2 dodatkowym batalionom wesprzeć atak.

Spodziewane wyniki:

- Dowódca niebieskich otrzymuje tylko częściową informację o ruchu swoich sił.
- Tylko część jednostek niebieskich otrzymuje rozkaz o wsparciu 32 batalionu.
- 32 batalion zostaje zniszczony przez siły czerwonych.
- Siły niebieskie nie osiągają celu operacji.

WARIANT 4

Sytuacja początkowa:

• Dowódca sił niebieskich ma informacje o jednej kompanii sił czerwonych na trasie 32 batalionu.

• Dowódca sił niebieskich rozkazuje 32 batalionowi zaatakować przeciwnika.

Rozwój scenariusza:

1. Siły czerwonych wykonują atak radioelektroniczny - zakłócanie.
2. 32 batalion atakuje przeciwnika po osiągnięciu odpowiedniej odległości. Pozostałe siły realizują swoje zadania.

Spodziewane wyniki:

• Dowódca niebieskich traci kontakt z batalionami 32 i 33.

• 32 batalion zostaje zniszczony przez siły czerwonych.

• Siły niebieskie nie osiągają celu operacji.

Rozgrywanie

Idea badania działań cybernetycznych w konflikcie zbrojnym

Eksperymenty symulacyjne – warianty działań

Przypadek A	**BLUFOR**	**Atak konwencjonalny**
	OPFOR	**Odpowiedź konwencjonal – bez ataku cybernetycznego**
Przypadek B	**BLUFOR**	**Atak konwencjonalny**
	OPFOR	**Scentralizowany Atak DoS**
Przypadek C	**BLUFOR**	**Atak konwencjonalny**
	OPFOR	**Zdecentralizowany atak DoS**
Przypadek D	**BLUFOR**	**Atak konwencjonalny**
	OPFOR	**Zakłócanie szerokopasmowe**

Wyniki– Straty BLUFOR / OPFOR

Podsumowanie

1. Zespoły Wydziału Cybernetyki WAT stanowią gotowe do działania zaplecze eksperckie i naukowe w zakresie:
   - modelowania i symulacji działań bojowych;
   - planowania, przeprowadzania i obróbki wyników eksperymentów symulacyjnych oraz ćwiczeń wspieranych komputerowo;
   - systemów wspomagania decyzji w planowaniu i dowodzeniu operacjami.
2. Prezentowany symulator wariantów działań SWD_T jest gotowym demonstratorem technologii. Symulator był z powodzeniem wykorzystywany w realnych ćwiczeniach wojskowych do symulacji działań kinetycznych i demonstracji skutków działań niekinetycznych i różnych metod rozpoznania obrazowego.