16th ICCRTS

"Collective C2 in Multinational Civil-Military Operations"

Paper Title:
Simulating Marine Asymmetric Scenarios for testing different C2 Maturity Levels

Topic(s):
Modeling and Simulation

Name of Author(s)
Agostino G. Bruzzone, Marina Massei
MISS DIPTEM University of Genoa
Via Opera Pia 15, 16145 Genova, Italy
agostino@itim.unige.it; massei@itim.unige.it
www.itim.unige.it

Francesca Madeo, Federico Tarone
Simulation Team
Via Cadorna 2, 17100 Savona, Italy
madeo@simulationteam.com; tarone@simulationteam.com
www.simulationteam.com

Murat M. Gunal
Industrial Engineering Dept. Turkish Naval Academy
Tuzla, Istanbul, Turkey
MGUNAL@dho.edu.tr

Point of Contact
Agostino G. Bruzzone
agostino@itim.unige.it

Simulating Marine Asymmetric Scenarios for testing different C2 Maturity Levels

Agostino G. Bruzzone, Marina Massei
MISS DIPTEM University of Genoa
Via Opera Pia 15, 16145 Genova, Italy
Email {agostino, massei}@itim.unige.it - URL www.itim.unige.it

Francesca Madeo, Federico Tarone
Simulation Team
Via Cadorna 2, 17100 Savona, Italy
Email {madeo,tarone}@simulationteam.com - URL www.simulationteam.com

Murat M. Gunal
Industrial Engineering Dept. Turkish Naval Academy
Tuzla, Istanbul, Turkey
Email MGUNAL@dho.edu.tr

ABSTRACT

This research is devoted to experimentation, by using simulation, on a complex maritime scenario where it's possible to evaluate different strategies in NEC C2 M2 (Net Centric Command and Control Maturity Models). In this paper the authors propose an experimentation based on a simulation model related to an asymmetric scenario in maritime domain with special attention to piracy; in fact the authors developed a simulator, titled PANOPEA (Piracy Asymmetric Naval Operation Patterns modeling for Education & Analysis) to analyze new asymmetrical war theaters focusing on scenarios of marine warfare versus pirates in Aden Gulf for supporting different educational and training purposes.
PANOPEA reproduces a piracy scenario in the Horn of Africa, a very critical area in terms of pirates' attacks against cargo ships. This scenario includes navy vessels and helicopters, intelligence assets, ground bases, cargos as well as other boats (i.e. fisherman and yachts) and pirates hiding in the general traffic. The entities are directed by IA-CGF (Intelligent Agents Computer Generated Forces) and apply strategies for succeeding based on their scenario awareness. In addition, PANOPEA simulator allows different strategies to be modeled of C2 (Command and Control) due to the fact that the authors implemented into simulator different C2 Architectures, including hierarchical and edge solutions. PANOPEA tool supports the authors in making experimental analysis by modeling different C2 maturity levels and measuring the effectiveness and the efficiency of the proposed scenarios in order to investigate the agility of the C2 solutions and their influence in preventing attacks by implementing different policies and different organizational models

Today this scenario is quite interesting: in fact maritime security is a very critical aspect of the marine framework and extends the concept of asymmetric warfare within Marine Environment with new threats such as (Piracy, Conventional Terrorism, CBRN - Chemical, biological, radiological, and nuclear). Therefore the case proposed involves over 1000 units directed by intelligent agents, so modeling and simulation is critical to evaluate strategies in term of efficiency to prevent and mitigate threats by improving policies, sensors, equipment as well as C2 solutions that obviously affect detection, identification, decision making and scenario evolution.
The authors will present the results of their experimental analysis on the impact on system agility of both organizational model, hierarchical and edge in order to compare the two approaches.
.

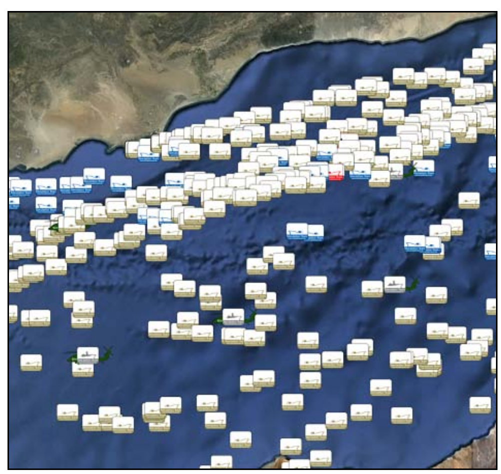

Figure 1 PANOPEA Scenario Dynamical Evolution in GIS

INTRODUCTION

The new warfare scenarios are characterized by new unconventional threats (i.e. terrorism, insurgency etc).
In maritime domain, piracy attacks are increasing over, in particular along Somalia Coast and in Arabian Sea.
In 2009, 406 piracy attacks are reported by the IMB (International Maritime Bureau) into the annual report and 217 episodes are attributed to Somalia pirates. Those attacks generate huge economic and social damages to the entire world due to the great value of goods moved by sea. In fact, in a pirate attack often the interests of many countries are affected: the state of the attacked vessel, hostage's countries, the State of the industrial company owner of the cargo and so on. Moreover, such attacks make surely global communications unsafe and produce the following effects:

- Increase rates of marine insurance and freight costs
- Increase environmental risks
- Increase danger to seafarer's lives because of the injury, killing or capture possibilities
- Consequently increase of goods prices for final consumers

Some important aspects are expected to increase their impact over next years in general as well in marine framework increasing on Asymmetric Threats:

- Economic Issues:
  - Moving European Region Social Economic Center of Gravity to South increasing maritime traffic with North Africa
  - Stabilization and Normalization Processes and Country Reconstruction Initiatives Overseas
  - Overseas Developing Areas Growth, Production/Demand & Sustainability Issues
- Technologies:
  - Opportunity to access more easily new knowledge Bases and information, for instance, for preparing and creating critical threats (i.e. Cyberspace)
  - Multiple opportunities to Access to Resources to develop WMD (i.e. smallpox, RDD)
  - IT & Web empowering the potential of individuals and small groups (i.e. C2 capabilities)
  - Increasing new reachable targets such as Oil Platform, Environmental Threats, Social Service
- Political Issues:
  - Political Instability on Critical Regions (i.e. Africa)
  - Evolution of Principle of Nations and Populations (i.e. Commercial States)
  - Evolution of new critical issues requiring changes on joint Defense and Homeland Security Budgets (i.e. natural resource issues: water)

Modeling and Simulation (M&S) are a strong support to evaluate Strategies in Threat Identification, Decision Making & Evolution Prediction:

- Once upon time it was used to identify threats based on Platform Detection, Identification and Classification
- Today in many case the same Platform is in use on multiple sides
- In some case the Platform is becoming a menace just based on own it is operating

Such kind of asymmetric threats need to be modeled due to the complexity of scenario in terms of entities involved, number of variables to be analyzed and dynamic evolution of threats behaviors.
The authors developed PANOPEA simulator to support operational planners in strategies analysis. They modeled different entities (i.e. cargo ships, frigate, pirates, intelligence etc.) by using Intelligent Agents for Computer Generator Forces (IA-GGF). These agents are able to drive units' behavior. Simulation with Computer Generated Forces managed by intelligent agents is the best way to consider scenarios with a large number of actors and parameters and provide a competitive advantage for using simulation in Planning & Operation Support respect existing tools and techniques.

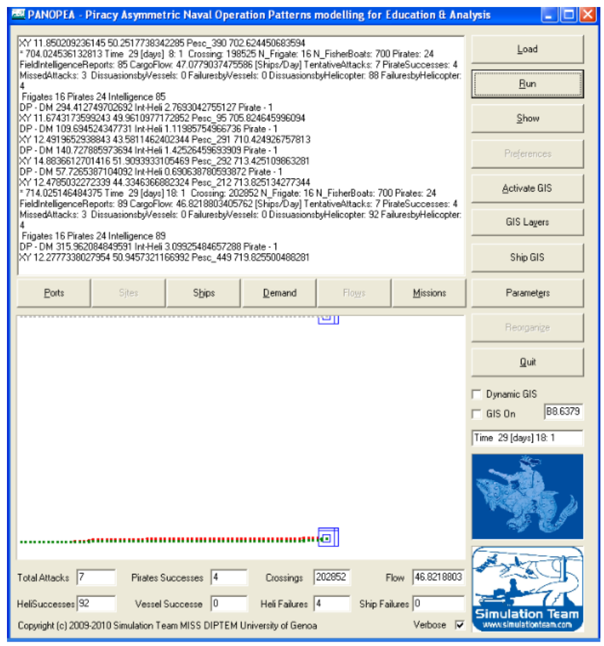

Figure 2 PANOPEA Main Graphic User Interface

STATE OF THE ART AND PIRACY OVERVIEW

The maritime piracy has become a critical issue in specific regions (for instance the Somalia coast) due to local factors such as political and socio-economical instabilities since 2006. Actually, the maritime piracy is not a new phenomenon, but changes in geographic "hot spots", the increased frequency of incidents and the severity of attacks are requiring to face the current maritime piracy situation in a more effective and efficient way.
Recent maritime piracy incidents, for instance, on the coast of Somalia, of the Gulf of Aden and of the Horn of Africa (HoA) have not only received significant attention from the media and the international community, but they were of

interest also for policy strategists and academic researchers as well.

Different models were developed to analyze the maritime traffic and to support maritime surveillance systems (Monperrus et al., 2008). Xiao et al. (2009) propose a framework of the Dynamic Data Driven Multi-Agent Simulation system in the maritime traffic domain.

Discrete-event simulation (DES) was used to simulate a typical port security, local, waterside-threat response model and to test the adaptive response of asymmetric threats in reaction to port-security procedures, while a multi-agent system (MAS) was used to provide the complex adaptive behaviors for the threats. Cover and dynamic path finding algorithms were used in Simkit to enhance the spatial interactivity of the agents (Chee Wan Ng . 2007)

A maritime counter-piracy scenario is modelled using the agent-based simulation platform MANA (Decraene J., 2010).

Vanek O. (2010) presents an agent-based simulation of the maritime traffic. The aim of the research was to simulate not only the legitimate maritime traffic, such as an intercontinental transportation, coastal fishing or recreational traffic, but also the illegitimate aspects, such as illegal fishing, waste dumping and maritime piracy.

A transit game model was developed to study the problem of a mobile agent trying to cross an area patrolled by a mobile adversary and to define an optimum route selection strategy in order to minimize the probability of hostile encounter (Vanek et al. 2010).

AgentC Testbed platform was developed by M. Jackob et al. (2010). It combines simulated vessel operation with a wide range of data sources on real-world maritime security. Vessel trajectories, obtained from the on line providers of AIS data (Automatic Identification System) are the first category of real-world data integrated into the testbed.

Naval Postgraduate School had used Simio services in 2010. Simio is a developer of 3D object-oriented simulation software which is aimed to model piracy defence strategies in order to study the prevention of piracy, illegal drug trafficking and increased security within ports, waterways and coastal areas.

The authors propose to introduce the concept of Net Centric Command and Control in piracy scenario in order to provide decisions makers with a tool able to reproduce different operational strategies and to support them in evaluating the best way to stop pirates' attacks.

NET CENTRIC COMMAND AND CONTROL MATURITY MODELS

The concept of Net-Centric was established in military sector and introduced in the early '90. This concept is used to describe an operational paradigm that exploits information and technological infrastructure to increase speed of command, resulting faster and more agile in carrying out operation and a sharing of knowledge. During recent years it was critical to consider how different C2 solutions are able to reproduce different maturity levels (i.e. conflicted, deconflicted, coordinated, collaborative and edge). Nowadays, the critical issue on this matter is to develop experiments to support investigation about characteristics of C2 solutions such as robustness, resilience, agility. A major concept related to NecC2M2 is represented by the idea that in the same scenario over time, it could make sense to have different C2 maturity levels evolving based on the needs. Another important aspect is to test critical conditions or events that requires to adapt the C2 maturity level.

PIRACY SCENARIO MODELING

There are two common definitions of piracy. The first, used by the IMO (International Maritime Organisation), derives from the U.N. Convention on the Law of the Sea (UNCLOS). It says that:

"Piracy consists of any of the following acts:

(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:

- on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft
- against a ship, aircraft, persons or property in a place outside the jurisdiction of any state

(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

(c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).

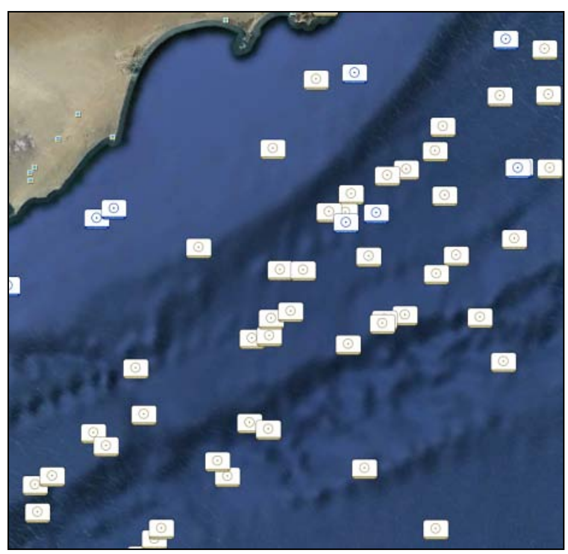

Figure 3.Details during PANOPEA Simulation

The IMB (International Maritime Bureau) offers another definition of piracy: "An act of boarding or attempting to board any ship with the apparent intent to commit theft or any other crime and with the apparent intent or capability to use force in the furtherance of that act".

Somalia is the country where the largest number of piracy organizations is located. The major reason is related to extremely hard social and economic conditions. In addition the poor control of local coast guard allows illegal acts (i.e. illegal fishing or waste discharge) and the strategic position for commercial traffics forced piracy acts.

Pirates, generally leaves from their basis using four or five boats which are small and can reach speeds exceeding 30 knots. The type of boat is indistinguishable from local fisherman boats. For this reason, the detection of attackers is very hard for the armed forces that are responsible in the area for tackling the phenomenon. The boats carrying pirates usually go hunting for vulnerable vessels, with a low freeboard that travel below 15 knots during the day. Once target is defined, pirates usually coordinate an attack on two or three fronts simultaneously from several directions. Depending on the characteristics and compliance of the vessel victim of the attack, the pirates can go up and take command of a ship in less than 20 minutes after the first attack. Then the vessels are conducted near the coast or in some ports that are used by pirates as a base of operations.

Due to the strong impact of pirates' actions on the world economy, International Community reacted with the use of its naval units in the critical zones. The affected area is very large and, therefore, it is required a significant number of military units for an accurate control of the area.

Actually, different missions are kept in the Gulf of Aden such as:

- Combined Task Force 151
- Ocean Shield NATO mission
- UE Atlanta mission
- missions of other countries like Russia, China, India, Japan and Pakistan.

From an operational point of view, military units get two approaches to prevent the actions of the pirates:

- Escorting cargo ships in order to be ready to quickly opposite pirates approaching to the escorted cargo by using helicopters and special forces
- patrolling the area in order to identify possible suspect boats and prevent actions by pirates, even in this mode, the naval units may employ on-board helicopters and personnel belonging to special forces.

PANOPEA SIMULATOR

PANOPEA reproduces piracy activities for evaluating different strategies in NEC C2 M2. PANOPEA is a stochastic discrete event simulator integrated with IA-CGF (Intelligent Agent Simulation Computer Generated Force) developed by the authors.

The following actors and activities are modeled:

- **Pirates**, different attack modes are considered: Outrunning, Maintaining Innocent Speed, Following a Ship, Hiding between Ships, Swarming. The main characteristics of these units are: agile structure, knowledge of the sea area, support from local population and in some case from political structure.
- **Navy**, represented by strong coalition force patrolling the area. The command and control system is not so "agile" such as pirates' organization. Patrol modality: mostly frigate, helicopters & special force squads
- **Intelligence Agencies**, that represent critical support to the Navy to predict pirates attacks by using instruments and techniques such as: data analysis, special commandos, satellite and communication technologies
- **Local Authority**, it is critical, i.e. "Failure Nations": no stable government, but strong presence of gangs, warlords etc.

The table below is a synthesis of entities modeled by the authors. For each entity some characteristics are defined.

Cargo Ship	Frigate	Fisherman/Pirate Boat
– Name	– Name	– Name
– Nationality	– Nationality	– Nationality
– Speed	– Speed	– Speed
– Radar Max	– Radar Max	– Pirates (%)
– Eye Max	– Eye Max	– Attack Distance
– Communication Delays	– Communication Delay	– Attack Probability
– Number of Cargo Ship	– Number of Frigates	– Number of Fisherman boats
	**Helicopter** – Speed – Radar Max – Eye Max	

Figure 4. PANOPEA Example of Unit Parameters

Cargo Ships are devoted to goods transportation and daily thousands of cargo ships cross through Gulf of Aden. Cargo ships activities are synthesized into the conceptual model represented in Figure 5; each cargo chooses a path and proceeds in that direction to reach its destination. By using the radar (covering a range of 20 nautical miles), the cargo ship checks the presence of boats approaching. It proceeds towards the destination until radar alerts about the approaching of a vessel. In this case, ship's crew makes a second check within 8 nautical miles to evaluate if the vessel is or not a pirate ship. In the second case, it asks for help by radio.

The major characteristics of cargo ships are:

- Speed: 16 to 20 knots.
- Technology on board: VHF radio, GPS, radar system
- Other: no weapons on board, but sometimes contractors could be engaged.

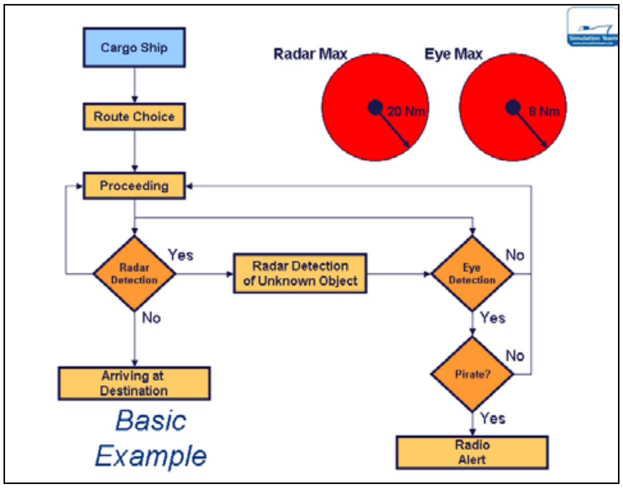

Figure 5.Basic Example for Cargo Ship

Cargo ship objective is to transport goods (general goods or gas or fuel, etc) by optimizing its route in order to reduce navigation time and costs. Some constraints are modeled: the chosen route is the shortest one; international rules often don't allow the private use of weapons.

Frigates are military ships aimed to patrol an assigned area or escort cargo ships. The main objective is to identify and block pirates. Frigates activities are regulated by Rules of Engagement, maritime laws and contracts with local authorities.

Frigate is critical in the piracy scenario due to the fact that it is the only adversary unit against pirates.

Generally a Frigate makes patrolling in an assigned area and along specific routes. If it detects a suspect fisherman boat, it is possible to intervene by using the helicopter or to make a control by the sea and, if it is necessary, to send Special Forces on board (see model in figure 6). Frigates may also to answer to an help request by a cargo ship. By making considerations about distance and time estimated to reach the cargo ship, the military ship choices if intervene by itself or by using helicopter.

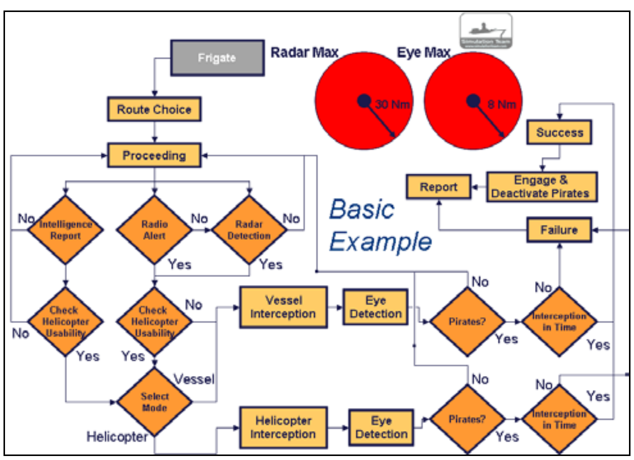

Figure 6. Basic Example for Ship Patrolling

The helicopter is assigned to a frigate and its goals are mainly: to patrol the area where the frigate has identified a suspicious fisherman boat; to intimidate pirates (the helicopter is a very effective means of deterrence); to shut off the boarded ship and to free the sailors taken in hostage as soon as possible.

Helicopter activities are regulated by Rules of Engagement. The helicopter is sent by the frigate to patrol a suspicious boat or to rescue cargo ship under attack. In the first case if the boat is a pirate boat, dissuading procedures are activated in order to stop pirates. In the second case helicopter can send raiders on the ship to arrest pirates and to free hostages.

Pirate/ Fisherman boats are 4/5 meters long and their speed can reach 35 knots. Generally, fisherman boats sail at 10 knots while pirates boat are faster.

While the objective of fisherman boat is to fish, pirates objectives are:

- To attack cargo ship with the crew on board in order to ransom
- To loot goods on board cargo ships
- Don't be neutralized and / or arrested by the military forces

Once defined cargo ship target, pirate boat approaches it and tries the attack. Attack success is regulated by a probability based on the strategies of patrolling and control adopted by frigate.

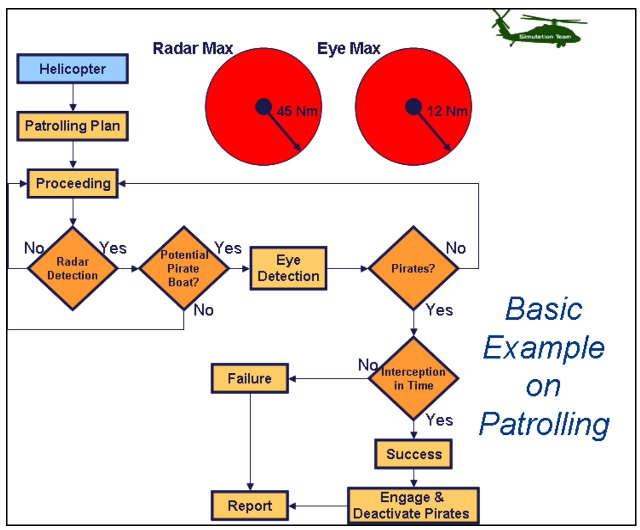

Figure 7.Basic Example for Helicopter Patrolling

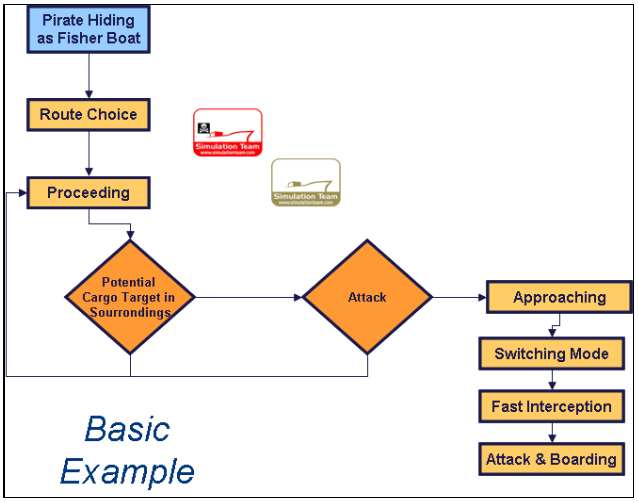

Figure 8.Basic Example for Pirate Hiding as a Small Boat

PANOPEA Simulator allows users to set several parameters such as ships speed (Cargo Average Speed, Frigate Cruise Speed and Full Speed radar range of view and eye range of view)

Cargo ship	
Number of Cargo Ships	Ships/day
Radar Max	Nm
Eye Max	Nm
Average Speed	Knots
Average Communication Delay	H
Average Boarding Time	H
Frigate	
Number of Frigate Ships	Ships
Radar Max	Nm
Eye Max	Nm
Cruise Speed	Knots
Full Speed	Knots
…Insp. Sampling	%
Intelligence	
Local Intelligence Detection Prob	%
Coalition Int. Detection Prob.	%
Helicopter	
Radar Max	Nm
Eye Max	Nm
Speed	Knots
Average Setup Time	H
Fisherman Boat/Pirates	
Number of Boats	Boats
Pirates	%
Attack Threshold	Nm
Attack Probability	%
Fisher Speed	Knots
Pirates Speed	Knots

Table 1. Parameters to be set in PANOPEA Simulator

In addition users are able to set Escorting and Inspecting modes in order to activate strategies about escort and inspections from frigates and helicopters and to define Simulation features:

- Simulation Duration
- Stochastic Influence
- Replications

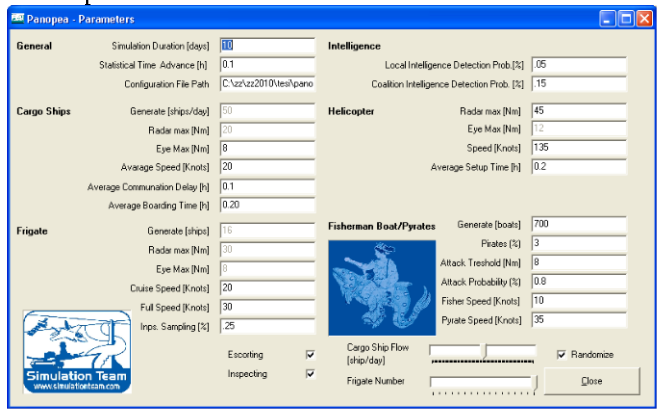

Figure 9 PANOPEA Synthetic Data for Boats and Vessels

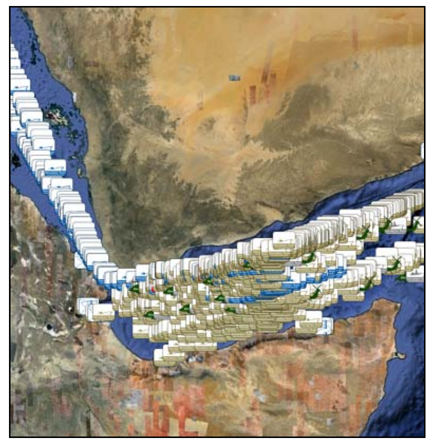
Figure 10. Integration of PANOPEA with Simplified GIS involving over 1'000 boats

The authors integrated the event discrete stochastic simulator with a simplified GIS (Geographic Information System) in order to visualize over 1000 boats that move around Aden Gulf, even by using military icons.

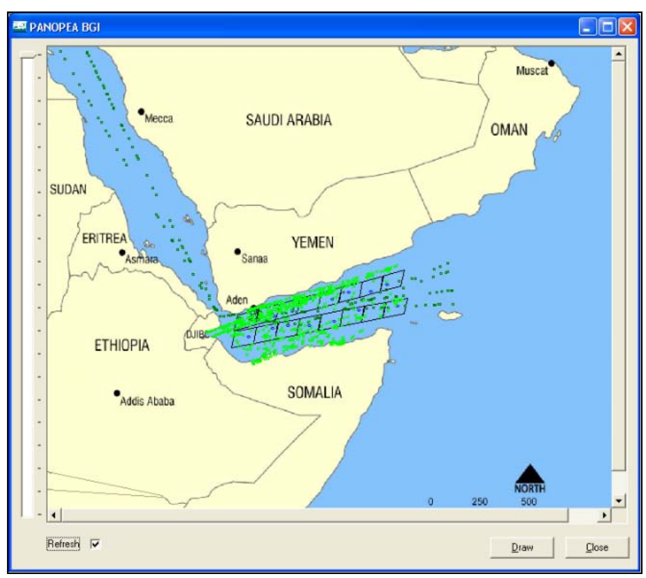

Figure 11. Zone Assignment and Corridors in PANOPEA Simulation

An additional function allows users to improve the visualization of ships routes and to setup the C2 strategy to be applied. Users are able to split the area to be controlled in different zones that are assigned to frigates, as reported in the window in Figure 11. In particular the strategy of creating a security corridor for cargo ships is visualized.
Finally, user is able to choose the desired organization model flagging the desired option in the C2 window (see figure 18).

EXPERIMENTATION SCENARIO OVERVIEW

During the phase of the experimentation, the parameters in PANOPEA have been set as follows:

- Number of Merchant Ships: 50 [ships/day]
- Number of Frigate: 15
- Number of Fisher Boat: 700
- Attack Probability (%): 0.8
- Communication Delay: 0.1 [hours]
- Average Ship Speed: 20+/- 4 [Knots]
- Frigate Cruise Speed: 20 [Knots]
- Frigate Full Speed: 30 [Knots]
- Fisher boat Speed: 10 [Knots]
- Pirate boat Speed: 35 [Knots]
- Helicopter Speed: 135 [Knots]
- Attack Threshold: 8 [Nm]
- Local Intelligence Detection Prob. 0.05
- Coalition Int. Detection Prob. 0.15

Simulation outputs include:

- Total Reports from Cargo Ship
- Number of Frigate Successful Operations
- Number of Successful Operations due to Intelligence Reports
- Number of Pirate Successful Attacks

For the experimentation the Active Objects are synthesized below:

- **Cargo ship**
  - Speed: 16 – 20 knots.
  - Tecnology VHF radio, gps, radar system
  - No guns on board, but in some case shipowner engage contractors.
- **Frigate**
  - Speed: 18– 30 knots
  - Tecnology : Communication Systems , Sensors (Radars, IR, EO, ESM), gps
  - Armament: cannons, helicopters
- **Helicopter**
  - Speed : 150 - 200km/h
  - Tecnology: military communication systems, gps, Sensors (IR, EO, Radars)
  - Armament: special forces on board, machine gun
- **Generic boat**
  - Speed: 12 – 20 knots
  - A generic boat could represents both pirates (these are able to ramp up to 35 knots and armed with assault rifles, machine guns, grenades and rockets) or a civil traffic (i.e.fish boats)
- **Ground Radar systems**
  - Range of action: 20- 45 Nm
- **Satellite system**
  - Technologies: optical system, height tech cameras

Experimentation Results

The authors decided to evaluate and analyze two different C2 alternatives

- Conflicted C2: there is no distribution of information between or among the entities, all of the decision rights remain within each of the entities, and there are no interactions and common objectives (in a C2 sense) between or among the entities. The only C2 that exists is that exercised by the individual contributors over their own forces or organizations.
- Edge C2, all the entities are connected into a robust network and they are able to easy access and share information by continuous interactions. In Edge C2 the rights to decisions are broadly distributed.

In PANOPEA users are able to activate connections between:

- CoHQs: Coalition NATO Headquarter
- NHQs: National Headquarter
- LCG: Local Coast Gard
- CoaInt: Coalition Intelligence
- Operative units (Frigate Ships, Cargo)

Each connection is characterised by:

- Transmission time, required to comunicate the information along that link
- Information reliability, to measure the reliability of the transmitted information

In the hierarchical command and control setting, the coalition headquarters are in contact with: intelligence agencies, other headquarters and Operative units. Any form of action, then, is defined by the command chain hierarchy: each unit received orders by headquarters. In addition, each unit must report relevant information to HQs in order to allow them to manage the situation and to define appropriate strategies and actions. The goal is to prevent pirates attacks, increase gulf security, to measure efficiency, effectiveness and response time in forces deployment and reaction, by taking into consideration also boundary condition (i.e. weather, operating condition).

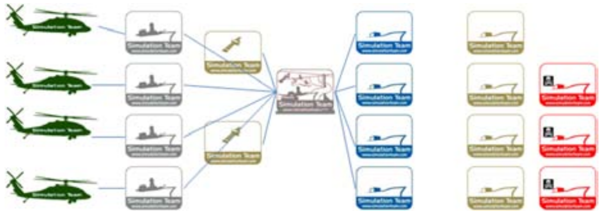

Figure 12. Example of Entity Connections

Edge C2 is a modern and sophisticated approach; this M2 (Maturity Model) is supported by an innovative technology component, in fact every entity is able to share information quickly and effectively. Edge Maturity Model aim is to ensure that all scenario entities are self-synchronized among them. A fundamental point is the knowledge sharing in order to let actors coordinated on theatre; it's clear that this approach is much more effective and keep the response speed to common enemy faster (i.e. Somali pirates). Otherwise, so widespread exchange of information could have a negative impact on field operations if not properly supervised and managed.

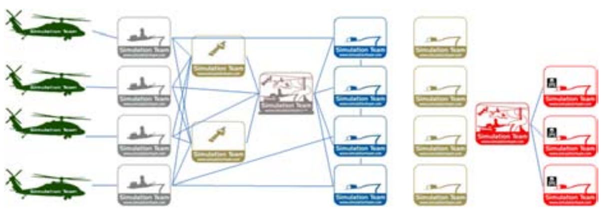

Figure 13. Different Example of Entity Connections

In PANOPEA it is possible to configure the Command and Control Hierarchy by clicking the button "C2GI" in PANOPEA interface and by creating the network connections among the various entities.

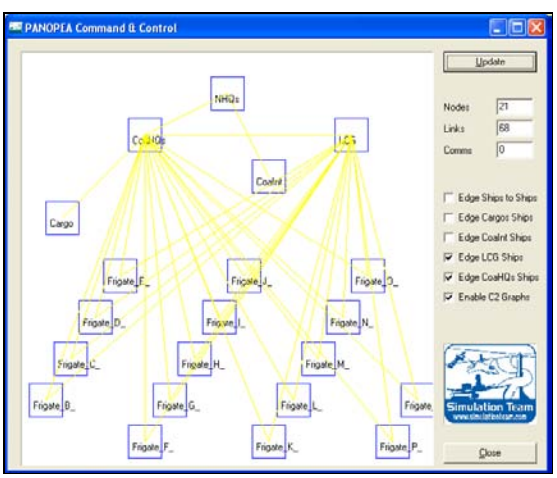

Figure 14. Modelling Data Distribution, Processing and Decision Allocation in PANOPEA

Due to the scenario complexity and the strongly not-linear level of the system, a careful experimental design is required in order to conduct a proper system analysis.
For this reason, the authors designed an experimental analysis to study simulator outputs in order to verify the stochastic influence on processes and to identify critical and significant parameters in terms of influence on costs.
In particular, the authors performed statistical analysis by using Mean Square Pure Error methodology (MSpE) in order to evaluate the experimental error and to measure the stochastic variables influence. That methodology allows to fix simulation length and to know results reliability based on confidence band.
The analysis was performed on the two scenarios proposed above (Hierarchical and Edge).
The authors made 5 simulation central runs in order to estimate MSpE, setting up inputs parameters on average values. In order to measure simulation results, the authors focused on foiled attacks by the vessels on the field.

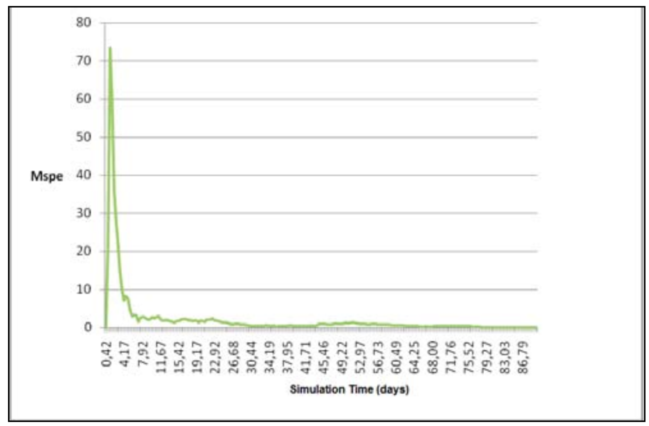

Figure 15. Mean Square pure Error on Attack Preventions versus Simulation Duration

Due to this analysis it was possible to define the simulation time length: approximately 30 days.
In addition, in order to perform sensitivity analysis, different factors are considered (see Table 2) in order to identify those which have major effects and influence on results. As reported in the table, these factors are evaluated in a predefined range in order to find correlations among independent variables and their combined effect.

Id	Fattore	Range
A	Local Intelligence	5% - 15%
B	Coalition intelligence	10% - 25%
C	Pirates Ships	3% - 7%
D	Cargo flow	min - max
E	Military Vessels	min - max

Table 2. Factors for the experimental analysis

The authors defined a Central Composite Design (CCD) experimental project composed by a 2k factorial part (in which each factor has two levels corresponding to the maximum and minimum range) and central replications.

Considering:

- n0: central replications on the reference values by changing the seed of pseudo-random numbers;
- 2k factorial replications to evaluate the effect of variables and their combinations (k = 5 variables);

Supposed that the experimental error is uniformly distributed within the ranges tested, it is possible to calculate the number of the minimum simulation runs:

n0 + 2k = 5 +25 = 37

Otherwise, if the hypothesis above is rejected, the experiment will require 160 runs:

n0 * 25 = 160

By using Simul8 for Design of Experiments, Anova (Analysis of Variance) Results for the Traditional Scenario are the following:

Source	Sum of Squares	df	Mean Square	F Value	p-value Prob > F	
Model	551.3778	31	17.78638	19.46467	0.0018	significant
A-Li	26.76681	1	26.76681	29.29247	0.0029	
B-Ci	0.268889	1	0.268889	0.294261	0.6108	
C-Pirates	63.28125	1	63.28125	69.25234	0.0004	
D-cargo f	0.21125	1	0.21125	0.231183	0.6509	
E-frigate	351.125	1	351.125	384.2564	< 0.0001	
AB	2.10125	1	2.10125	2.29952	0.1899	
AC	0.027222	1	0.027222	0.029791	0.8697	
AD	1.742222	1	1.742222	1.906615	0.2259	
AE	13.78125	1	13.78125	15.08162	0.0116	
BC	0.586806	1	0.586806	0.642175	0.4593	
BD	0.000139	1	0.000139	0.000152	0.9906	
BE	1.075556	1	1.075556	1.177043	0.3275	
CD	0.245	1	0.245	0.268118	0.6267	
CE	49.50125	1	49.50125	54.17209	0.0007	
DE	0.116806	1	0.116806	0.127827	0.7353	
ABC	0.067222	1	0.067222	0.073565	0.7971	
ABD	8.405	1	8.405	9.198079	0.0290	
ABE	0.586806	1	0.586806	0.642175	0.4593	
ACD	0.116806	1	0.116806	0.127827	0.7353	
ACE	2.067222	1	2.067222	2.262281	0.1929	
ADE	1.868889	1	1.868889	2.045233	0.2121	
BCD	0.035556	1	0.035556	0.038911	0.8514	
BCE	1.650139	1	1.650139	1.805843	0.2368	
BDE	0.390139	1	0.390139	0.426952	0.5423	
CDE	0.18	1	0.18	0.196984	0.6757	
ABCD	9.03125	1	9.03125	9.88342	0.0256	
ABCE	0.18	1	0.18	0.196984	0.6757	
ABDE	7.475556	1	7.475556	8.180934	0.0354	
ACDE	0.390139	1	0.390139	0.426952	0.5423	
BCDE	0.035556	1	0.035556	0.038911	0.8514	
ABCDE	8.066806	1	8.066806	8.827973	0.0311	
Residual	4.568889	5	0.913778			
Lack of Fit	0.263111	1	0.263111	0.244426	0.6469	not significant
Pure Error	4.305778	4	1.076444			
Cor Total	555.9467	36				

Figure 16. Analysis of Variance (ANOVA)

The Analysis is focused on the variables influence, in fact, as reported within Table in Figure 16, for each variable and their interactions it was performed a significant Test in order to be able to know which variables disrupt objective function more.

In addition, the authors performed also the first and the second Fisher Tests to be sure that the experimental project was developed correctly.

The first concerns with the significance of the regression test and formulate two hypotheses:

- H0: All regression coefficients are zero (β1 = β2 = ... = βn = 0);
- Ha: there is at least a βi != 0.

In this case the hypothesis H0 is rejected with a probability of 5% error (α), and then accepts the hypothesis Ha. There is therefore an independent variable among the five listed above that explains the observed variation in the response.

Both tests were successful. As result of this experimental analysis, the Authors identified relevant and significant variables:

- A (local intelligence level)
- C (pirates percentage)
- E (military vessels number)
- AE
- CE
- ABD
- ABCD
- ABDE
- ABCDE

AE, CE, ABD, ABCD, ABDE, ABCDE represent combined effects.

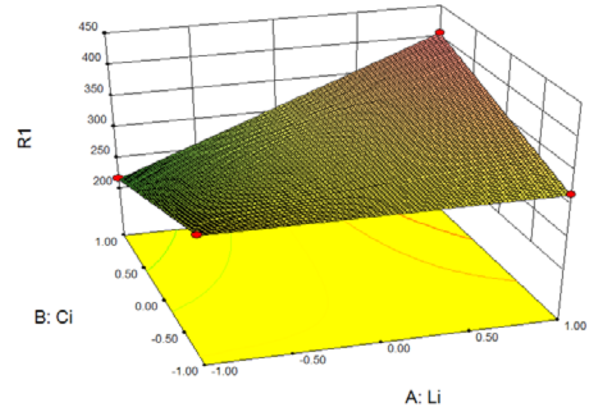

Figure 17. Response Surface in traditional scenario

The response surface, reported in the Figure 17, is a meta-model that allows by setting values of the different variables to have directly results without simulation help.

The authors adopted the same approach to analyze Edge Scenario in order to be able to compare the proposed two cases.

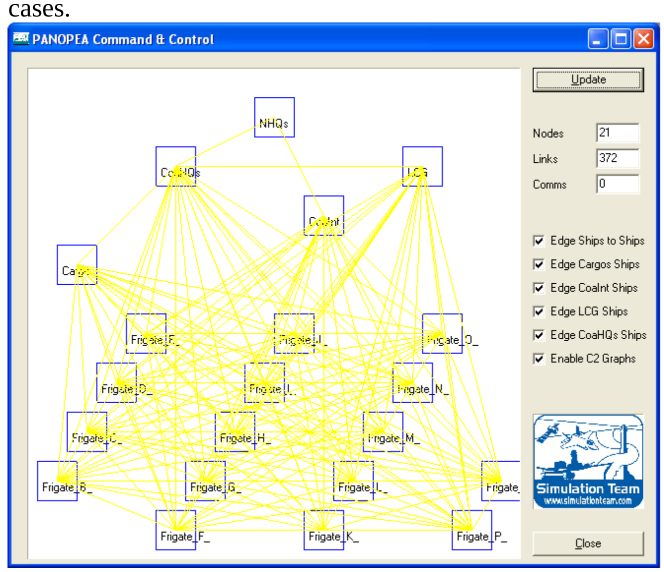

Figure 18. Edge Scenario

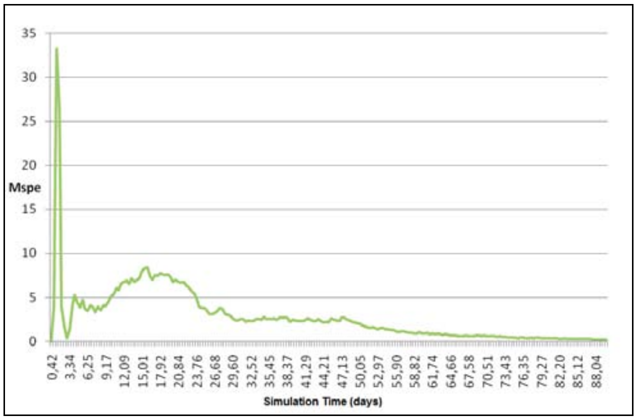

Figure 19. Mean Square pure Error Computation

In the C2 Edge Scenario:

Source	Sum of Squares	df	Mean Square	F Value	p-value Prob > F	
Model	1594.051	31	51.42099	51.16562	0.0002	significant
A-Li	0.564453	1	0.564453	0.56165	0.4873	
B-Ci	22.08355	1	22.08355	21.97387	0.0054	
C-Pirates	118.3876	1	118.3876	117.7996	0.0001	
D-cargo f.	0.316675	1	0.316675	0.315103	0.5988	
E-frigate	1246.461	1	1246.461	1240.27	< 0.0001	
AB	0.495842	1	0.495842	0.493379	0.5138	
AC	0.609592	1	0.609592	0.606565	0.4713	
AD	7.588759	1	7.588759	7.55107	0.0404	
AE	2.751467	1	2.751467	2.737802	0.1589	
BC	7.883759	1	7.883759	7.844604	0.0380	
BD	1.925703	1	1.925703	1.916139	0.2249	
BE	15.65668	1	15.65668	15.57892	0.0109	
CD	0.66605	1	0.66605	0.662742	0.4526	
CE	110.8188	1	110.8188	110.2685	0.0001	
DE	0.099384	1	0.099384	0.09889	0.7659	
ABC	0.002509	1	0.002509	0.002496	0.9621	
ABD	3.093828	1	3.093828	3.078463	0.1397	
ABE	0.675703	1	0.675703	0.672347	0.4495	
ACD	6.615703	1	6.615703	6.582847	0.0503	
ACE	2.77105	1	2.77105	2.757288	0.1577	
ADE	11.66043	1	11.66043	11.60251	0.0191	
BCD	5.267717	1	5.267717	5.241555	0.0707	
BCE	8.62855	1	8.62855	8.585697	0.0326	
BDE	2.058759	1	2.058759	2.048534	0.2118	
CDE	0.408759	1	0.408759	0.406729	0.5517	
ABCD	1.0573	1	1.0573	1.052049	0.3521	
ABCE	0.009453	1	0.009453	0.009406	0.9265	
ABDE	2.144175	1	2.144175	2.133526	0.2039	
ACDE	6.737509	1	6.737509	6.704047	0.0489	
BCDE	5.376467	1	5.376467	5.349765	0.0687	
ABCDE	1.233759	1	1.233759	1.227631	0.3183	
Residual	5.024956	5	1.004991			
Lack of Fit	3.030845	1	3.030845	6.079591	0.0693	not significant
Pure Error	1.994111	4	0.498528			
Cor Total	1599.076	36				

Figure 20. ANOVA Analysis

The Authors by using this methodology found relevant and significant variables for this scenario:

- B (coalition intelligence presence)
- C (pirates percentage)
- E (military vessels number)
- AD
- BE
- BC
- CE
- ADE
- BCE
- ACDE

The results of this analysis underline that the edge configuration is more expensive than the other one, but it seems to be more effective in terms of foiled attacks number.

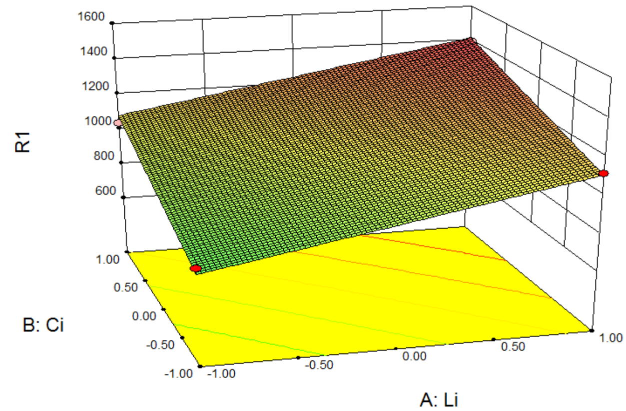

Figure 21. Response Surface

CONCLUSION

The paper proposes an approach for experimenting the influence of different parameters on the efficiency and effectiveness of C2 solutions; the main goal of this research is to test different Net C2 M2 models in order to evaluate and quantify the effectiveness and efficiency among different approaches by taking into consideration independent variables correlations respect target functions. Considering the problem nature complexity, this is devoted not to extract general directions (that are strongly influenced by boundary conditions and constraints), but to demonstrate the potential of using M&S in supporting analysis of different C2 maturity models.

PANOPEA simulator is a useful tool for the evaluation of different C2 strategies and the analysis of different scenarios. Anyway additional improvements will be provided in order to consider other C2 Levels (i.e. cooperative or de-conflicted).

REFERENCES

- Alberts D. S., (2002), "Information Age Transformation", revision June 2002, CCRP Publication Series
- Alberts David S., Gartska J.J., Stein F.P. (2000) "Net Centric Warfare", CCRP, Washington
- Alberts David S., Hayes Richard E., (2006) "Understanding Command and Control", Washington: CCRP, fig. 11, p. 35
- Alberts D.S., Hayes R.E. (2003) "Power to the Edge", CCPR Publications, Washington D.C.
- Alberts, D.S. (2007) “Agility, Focus, and Convergence: The Future of Command and Control.” The Int. C2 Journal, Vol. 1, No. 1, 1-30
- Alberts, D.S. (2008) “NATO NEC C2 Maturity Model Overview,” Draft for Peer Review, SAS-065 Study Group, 2008.
- Anderson N. (2006) "Are iPods shrinking the British vocabulary?", Ars Technica On-Line Magazine, December 15

- Bruzzone A.G., Cantice G., Morabito G., Mursia A., Sebastiani M., Tremori A. (2009) "CGF for NATO NEC C2 Maturity Model (N2C2M2) Evaluation", Proceedings of I/ITSEC2009, Orlando, November 30-December 4
- Bruzzone A.G. (2008) "Human Behavior Modeling: Achievement & Challenges", Invited Speech at SIREN Workshop, Bergeggi, Italy, June 6th
- Bruzzone A.G., (2007) "Challenges and Opportunities for Human Behaviour Modelling in Applied Simulation", Keynote Speech at Applied Simulation and Modelling, Palma de Mallorca
- Bruzzone A.G., Viazzo S., Massei M., BC (2004) "Modelling Human Behaviour in Industrial Facilities & Business Processes", Proc. Of ASTC, Arlington, VA, April
- Bruzzone A.G., Massei M., Simeoni S., Carini D., B.M. (2004) "Parameter Tuning in Modelling Human Behaviours by Using Optimization Techniques", Proceedings of ESM, Magdeburg, Germany, June
- Bruzzone A.G., Figini F. (2004) "Modelling Human Behaviour in Chemical Facilities and Oil Platforms", Proceedings of SCSC, San Jose
- Bruzzone A.G., Mosca R., Simeoni S., Massei M., B.M., B.C., (2004) "A Methodology for Estimating Impact of Different Human Factor Models on Industrial Processes", Proceedings of EUROSIM, Paris, France, September
- Bruzzone A.G., Page E., Uhrmacher A. (1999) "Web-based Modelling & Simulation", SCS International, San Francisco, ISBN 1-56555-156-7
- Bruzzone A.G., Giribone P. (1998) "Decision-Support Systems and Simulation for Logistics: Moving Forward for a Distributed, Real-Time, Interactive Simulation Environment", Proc. of the Annual Simulation Symposium IEEE, Boston
- Bruzzone A.G., Giribone P. (1998) "Quality Service Improvement by Using Human Behaviour Simulation", Proceedings of ESM, Manchester, UK, June
- Bruzzone A.G. (1996) "Object Oriented Modelling to Study Individual Human Behaviour in the Work Environment: a Medical Testing Laboratory ", Proc. of WMC, San Diego, January
- Cantice G. (2008) "Serious Games Serious Experimentations?", Proc. of SeriGamex, November
- Chee Wan Ng, Arnold H. Buss, John Hiles, (2007) "Discrete-event Simulation with Agents for Modeling of Dynamic Asymmetric Threats in Maritime Security Naval" Naval Postgraduate School, Monterey, California, Thesis approved for public release
- CTA (2002) "Agents for Net-Centric Warfare and Time Critical Targets", CTA Technical Report
- Decraene J., Anderson M., Low M. Y. H., “Maritime Counter-Piracy Study using Agent-Based Simulations”, In Proceedings of the 2010 Annual Simulation Symposium. pp. 82-89, April 11-15, 2010, Orlando, FL, USA
- Fogel D. (2005) "Volutionary Computation-toward a new philosophy of machine intelligence", IEEE Press series on Computational Intelligence
- Goldstein J. (2007) "Trial in Absentia Is Ordeal for Veteran Who Was Cleared by U.S. in a Killing", NY Sun, July 16
- Jakob M., Vanek O., Urban S., Benda P., Pechoucek M.,(2009) "AgentC: Agent-based Testbed for Adversarial Modeling and Reasoning in the Maritime Domain (Demo)", In Proceedings of The Ninth International Conference on Autonomous Agents and Multiagent Systems, July
- Krulak C.C. (1999) "The Strategic Corporal: Leadership in the Three Block War" Marines Magazine
- Ladner R., Petry F. (2005) "Net-Centric Web Approaches to Intelligence and National Security", Springer, NYC
- Ladner R., Warner E., Petry F., Katikaneni U., Shaw K., Gupta K., Moore P. (2009) "Web Services: Evolving Techniques in Net-Centric Operations", Proceedings of MTS/IEEE OCEANS,
- Liddy L. (2005) "The Strategic Corporal: Some Requirements in Training and Education", Australian Army Journal, Volume II, Number 2, 139-148
- Mavrakis D., Kontinakis N. “A queueing model of maritime traffic in Bosporus Straits” Simulation Modelling Practice and Theory 16 (2008) 315–328, Elsevier
- Molagh J. (2009) "How Afghanistan's Little Tragedies Are Adding Up", Time, May 26
- Moniz D. (2002) "Afghanistan’s Lessons Shaping New Military", USA Today, October 7
- Monperrus M., Jaozafy F., Marchalot G., Champeau J., Hoeltzener B., JézéquelJ. (2008) “Model-driven Simulation of a Maritime Surveillance System” Proceedings of the 4th European Conference on Model Driven Architecture Foundations and Applications (ECMDA'2008), Springer.
- Mosca R., Viazzo S., Massei M., Simeoni S., Carini D., B.C. (2004) "Human Resource Modelling for Business Process Re-Engineering",Proceedings of I3M2004, Bergeggi, Italy, October
- Patton M.S. (2003) "ES2: Every Soldier is a Sensor", The Washington Post, November 5
- Ray D.P. (2005) "Every Soldier Is a Sensor (ES2) Simulation: Virtual Simulation Using Game Technology", Military Intelligence Professional Bulletin
- Reverberi A. (2006) "Human Behavior Representation & Genetic Algorithms Characteristics Fitting", Invited Presentation on Piovra Workshop, Savona, February 7

- Sang Hoo Baea, Jay Pil Choib (2006) "A model of piracy", Elsevier, Information Economics and Policy Volume 18, Issue 3, September 2006, Pages 303-320
- Urban S., Jakob M., Pechoucek M.,(2010) "Probabilistic modeling of mobile agents’ trajectories", In Proceedings of the International Workshop on Agents and Data Mining Interaction (ADMI 2010), May.
- Vanek O., (2010) "Agent - Based Simulation of the Maritime Domain", 14th International Student Conference on Electrical Engineering. CVUT, Fakulta elektrotechnicka, May
- Vanek O., Bosansky B. and Jakob M., Pechoucek M. (2010), “Transiting Areas Patrolled by a Mobile Adversary”, Proceedings of 2010 IEEE Conference on Computational Intelligence and Games.
- Viazzo S., B.M., B.C. (2005) "Human Behavioral Models For M&S Applications", Proceedings of ESS2005, Marseille, 20-22 October
- Warne L., Ali I., Bopping D., Hart D., Pascoe C. (2004) "The Network Centric Warrior: The Human Dimension of Network Centric Warfare", Tech.Report DSTO, Edinburgh, Australia
- Xiao Y., Zhang H., Li S., (2009) "Dynamic Data Driven Multi-agent Simulation in Maritime Traffic," iccae, pp.234-237, International Conference on Computer and Automation Engineering (iccae 2009)