DISTRIBUTED VIRTUAL SIMULATION SUPPORTING DEFENSE AGAINST TERRORISM

Agostino G. Bruzzone[1,2], Marina Massei[1], Alberto Tremori[2], Marco Camponeschi[3], Letizia Nicoletti[3], Riccardo Di Matteo[3], Giulio Franzinetti[3]

[1] ***DIME University of Genoa***
Email: {agostino, massei}@itim.unige.it
URL: www.itim.unige.it

[2] ***CMRE***
Email: {bruzzone, alberto.tremori}@cmre.nato.int
URL: www. cmre.nato.int

[3] ***Simulationteam***
Email: {marco.camponeschi, letizia.nicoletti, riccardo.dimatteo, giulio.franzinetti}@simulationteam.com
URL: www.simulationteam.com

ABSTRACT

This paper propose an innovative MS2G (Modeling, interoperable Simulation and Serious Game) to address Defense Anti Terrorism (DAT) the solution proposed allows to access to a web application adopting SaaS (Simulation as a Service) paradigm over secure networks for experimenting and or exercising on this context. The possibility to investigate specific scenarios changing boundary conditions as well as hypothesis allows evaluating most effective actions for vulnerability reduction versus potential terrorist attacks. The use of intelligent agents allows executing automatically the scenario based on dynamically aggressive and defensive interactions; the proposed models present a virtual representation that immerse the user in an easy understandable framework supporting crowdsourcing among subject matter experts on DAT.

Keywords: *Defense Anti Terrorism, Intelligent Agents, Simulation, Crowdsourcing*

INTRODUCTION

Last fifteen years the terrorism represented one of the major issues for the Nations and the current situation is not really promising about the future; in facts actions from isolated groups fighting against authorities and government were extensively present along the last century (Hudson et al. 1999; Endes et al. 2002).
Therefore it is evident that the technology developments in several sectors increased the impact of the attacks as well as the vulnerability of the Nations. The evolution and diffusion of innovative communications, media and social networks further emphasized the impact of these elements (Matusitz 2013).
After the twin tower attack many Nations and International Organizations activated new research programs addressing terrorism that further evolved along last decade (Benney et al. 2009).

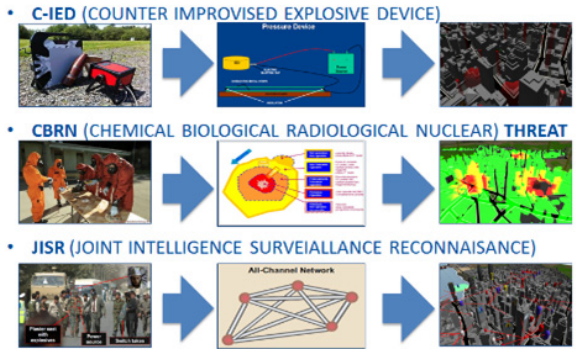

Figure 1 – DVx2 Scenarios and their Virtual Representation

In particular NATO established in 2004 the NATO DAT PoW (Defense Against Terrorism Program of Work) developing innovative solutions on different areas to face these threats; this paper proposes the development of innovative simulation solution based on MS2G (Modeling, interoperable Simulation and Serious Game) to address the complex sector of defense against terrorism and it was developed under NATO DAT PoW (Bruzzone et al.2014a); in addition the authors developed this simulator based on SaaS Paradigm (Simulation as a Service) in order to make it available over the web as a cloud service.
The main goal of this project was to evaluate vulnerability reduction versus terrorism in reference to the achievements of the NATO research on the area along last years (Bruzzone, Tremori 2014b).

1. DAT APPLICATION FIELD AND SIMULATION

The DAT operational requirements and shortfalls has been addressed within 11 items in the DAT PoW instantiated by the Conference of National Armaments Directors (CNAD 2004 and following):

- Large-Body Aircraft Against Man-Portable Air Defense Systems (MANPADS)
- Protection of Harbors and Ports (HPP)

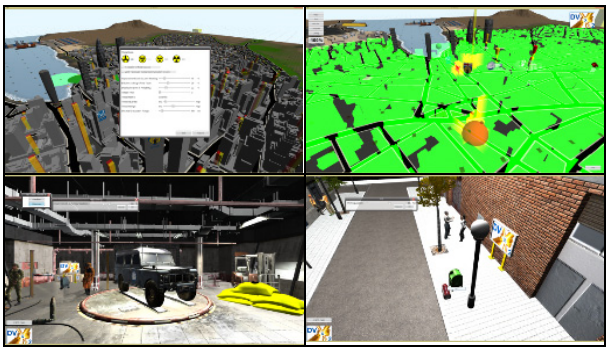

Figure 2 – DVx2 Virtual Representation of Scenario Parameters, Damages due to multiple attacks, Countermeasures Setting and *Hot Spot* on Attack Site (left up to right down)

- Protection of Helicopters from Rocket-Propelled Grenades RPGs
- Counter Improvised Explosive Devices (C-IEDs)
- Explosive Ordnance Disposal (EOD) and Consequence Management
- Precision Air-Drop Technology for Special Operation Forces, Detection
- Protection and Defeat of CBRN Weapons
- Technology for Intelligence, Surveillance, Reconnaissance and Target Acquisition (ISRTA)
- Defense against Mortar Attacks (DAMA)
- Protection of Critical Infrastructure (CIP)
- Non-Lethal Capabilities (NLC)

Simulation was identified as a solution for demonstrating and presenting virtually the achievements of the related researches carried out on this area along last 10 years; indeed an important benefit arising from using simulation is the possibility to provide subject matter experts (SME) with an interactive tool allowing to conduct experiments (Longo 2010; Longo 2012);
This capability becomes even more significant in case the innovative MS2G paradigm is applied, because the SME could access remotely the simulator and share not only results, but also hypotheses and scenario configuration to compare their assumptions and mutually validate their conclusions (Bruzzone et al.2014a).
This aspect for DAT is very important considering the complexity of the scenario, but also the heavy uncertainty over many factors; in facts, in terrorism, it is pretty difficult to have reliable statistics on attack probabilities, efficiency and effectiveness of attacks and defensive solutions (McKercher et al.2004).; this is not only due to the security issues, but even to the continuous evolving nature of these aspects that reduce the size of available samples as well as the possibility to conduct valid live experiments.
In 2002 there was a panel on M&S organized by MIMOS (Movimento Italiano Modellazione e Simulazione) where it was proposed the question about "*how simulation could support anti-terrorism considering the inventive and creativity of human beings in preparing attacks*" (MIMOS 2002); in such occasion Prof. Bruzzone stated that "*while it is impossible to predict terrorist attacks, it could be pretty feasible to simulate them, obviously not to support terrorist plans, but to evaluate vulnerability reduction achievable by alternative solution*".
This paper proposes DVx2 simulation that addresses exactly these issues after several years with benefits from currently available technologies and new methodologies (e.g. SaaS, MS2G).
Indeed simulation aims to create a consolidated benchmark for vulnerability reduction and accomplishment, based on the assessments made by experts. Considering the complexity and dimension of DAT it was obviously necessary to define bounds for the model development, indeed the authors decided to start the modelling working on three important elements of the above presented list: C-IED/EOD, CBRN, JISR (Bossomaier 2000; Bossomaier et al. 2009).
In facts simulation could be used to address multiple aspects from capability assessment to training; therefore a major innovative aspect, in this case, is the use of the MS2G for creating a distributed framework that could support crowdsourcing (Bruzzone et al. 2014a); in anti-terrorism crowdsourcing is a major issue devoted to allow the Subject Matter Experts to interact each other and to share estimations, ideas and solutions; it is evident the possibilities enabled by providing an interactive simulation environment that could be used over secure networks for this purpose; another aspect not to be neglected is the possibility to use these models for exploitation of the results among decision makers or general public; obviously all these issues should deal with the sensitive nature of some of the research and this paper address just public releasable information related to the conceptual modelling of the initiative.

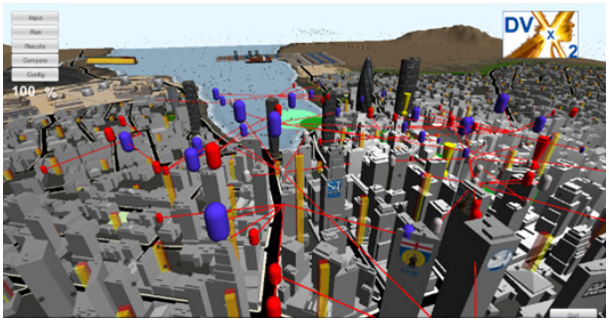

Figure 3 – Threat network presented in JISR module of DVx2

2. SIMULATION AND CROWDSOURCING AGAINST TERRORISM

The idea to create simulation models for anti terrorism (and even for conflicts management) has been investigated since many years and resulted pretty popular since September 11 (Mosca et al. 1996; Smith 2002; Petrova and Camponeschi 2002; Abrahams 2005; Oren and Longo, 2008; Bruzzone et al.2009a, 2009b).

In this case some the authors propose the use of simulation within an innovative paradigm corresponding to M2SG (Bruzzone et al. 2014a).
The authors developed the proposed simulator DVx2 (Distributed Virtual eXperience and eXercise) within specific areas (e.g. Counter Improvised Explosive Devices, CBRN, JISR) to address the DAT complexity by a modular approach as proposed in figure 1.
Indeed DVx2 simulator has been developed with the goal to collect knowledge and experience from anti-terrorism SME by applying the MS2G; the simulator combines interoperable simulation and web serious games to create a distributed environment where simulation could be delivered as a service. A major advantage in this case is based on the use of IA-CGF (Intelligent Agent Computer Generated Forces), developed by Simulation Team, for directing terrorists and defenders (Bruzzone et al.2011a, 2011b).

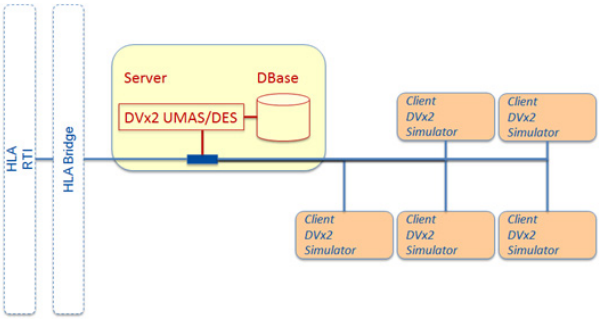

Figure 4 – DVx2 Architecture

The agents allows to carry out several runs automatically extending the experimentation capabilities of the simulator; so by this approach the SMEs could use DVx2 to test the effect of independent variables and assumption on the vulnerability reduction; DVx2 is pretty efficient currently so it is possible to conduct these experimentations interactively by investigating several configurations and analyzing immediately the results in the virtual environment.
DVx2 presents the situation in terms of 3D visualization of the town at high level as well as the distribution of damages, casualties, evacuation areas (see figure 2); all these parameters evolve dynamically during the run to allow understanding of the events, therefore in usual experimentation due to the high ratio fast time simulation this could be not appreciated. Special 3D detailed scene are generated to reproduce *hot spots* used for proposing the SME attack sites and/or possibility to change the parameters by clicking on virtual objects.
Indeed simulation results in terms of scenario configuration, risk analysis and key performance indexes about vulnerability reduction are stored in the cloud; this database allows the creation an up-to-date knowledge reference respect DAT that is populated by dynamic experimentation of SME over multiple scenarios. Indeed the DVx2 synthetic environment is currently focused on specific issues related to C-IED (Counter Improvised Explosive Devices), JISR (Joint Intelligence, Surveillance and Reconnaissance) and CBRN (chemical, biological, radiological, nuclear);.
Mixed scenario could be developed combining the different aspects indeed DVx2 uses IA-CGF to simulate dynamically the evolution of the threat network as proposed in figure 3.
DVx2 has been developed to address just some specific elements of these DAT PoW however it is evident that interoperability approach to the modeling allows to add other simulators or meta-models to extend its validity to new areas or to modulate its resolution and details towards specific elements (Kuhl et al.1999).
Within the specific case addressed the DVx2 allows the users to set parameters and to finalize decisions, while the simulator evaluates risks and impacts in term of vulnerability reduction. The DVx2 virtual world is used also to propose final results within an effective representation and allowing players to understand at glance the results of the simulation. DVx2 is implemented as web based serious game able to operate over secure networks; it was also investigated the possibility to activate a special release for NATO users on DBNL (Distributed Networked Battle Labs) for technological tests, therefore DBNL not classified network current planning reduced the priority of this initiative (Siegfried et al. 2014). It is important to outline that DVx2 conceptual model was developed considering High Level Architecture (HLA) as reference interoperability standards for future extensions and reuse as a distributed federate within large federation of simulators (Bruzzone et al.2011).
In addition, through a proper authorization scheme and access levels, the users could access the DVx2 Dbase and compare dynamically their experiments with others carried out by colleagues based on different assumptions; this allows to understand how much conservative or optimistic are their hypothesis as well as to evaluate the efficiency and effectiveness of the different alternatives on the simulated scenarios.
In this way DVx2 turns into a very effective support for Crowdsourcing and for interactive distributed experimentation; obviously the simulator has also a great potential as tool to be used for education and training (Tremori et al.2012); indeed use of simulation could support the development of virtual distributed exercise (Raybourn 2012)
So the use of MS2G in this context is expected to provide a consolidated approach and benchmark for new DAT capability; DVx2 could evaluate the accomplishments of DAT initiatives in terms of vulnerability reduction, for future planning and recognition of accomplishments, while the distributed nature of this approach allows to empowering SME networks.
The DVx2 general structure and architecture is based on the combination of stochastic discrete event simulation with Intelligent Agents playing the role of terrorists as well as that one of the DAT resources (Hill 1996; Banks 1998; Bruzzone et al. 2011b). DVx2 user accesses to this simulation service and he is enabled to define the

actions, assets, policies; he could select the hypotheses to be adopted in relation to the different DAT scenarios.
The Intelligent Agent Computer Generated Forces direct the terrorist actions and countermeasures during the whole simulation and by simulation are measured evolution risks as well as the vulnerability reduction (Bruzzone et al. 2011a); indeed the simulator estimates damages, costs as well as casualties and allows comparing different alternatives and/or estimations by SME.
DVx2 addressed VV&A (Verification, Validation and Accreditation) by informal techniques and dynamic experimentation; indeed the approach for development and validation is based on lean simulation concept (Bruzzone, Saetta 2002). In facts the validation of the correctness of the conceptual models respect the Simuland (the framework simulated by our computer models) should be checked by engaging simulation experts in the review process (Balci et al.1996; McLeod 1982); in addition it is necessary to verify the consistent implementation of the software code respect the conceptual models (Balci et al.2011). From this point of view the SME and CMRE Simulation Experts conducted face validation and dynamic test on DVx2 in order to address these issues (Amico et a. 2000);.
The DVx2 Architecture is based on Simulation as a Service Architecture that enables users to experience the DVx2 serious game directly on the web via a web browser by downloading a plug in (Guo, Bai, Xu 2011; Tsai et al.2011); this solution results flexible respect the Operating System in use. To guarantee full access to all potential users a stand-alone version to run locally or within a web browser framework was developed to test the GUI (Graphic User Interface) as well as the simulation engine and also for use from workstations that are operating within secure networks with heavy restrictions on internet access.
For these purposes the architecture includes conceptual element such as DVx2 User Management and Access System (UMAS) and the DVx2 Discrete Event Simulator (DES) as proposed in figure 4.
The DVx2 UMAS should be devoted to provide game users as well as game administrators with an easy to use system to create and manage users' accounts. The DVx2 UMAS was initially developed by using PHP while the main database used to store data (both user data as well as simulation input/output data) were implemented by using MySQL. As first step, two main roles were created as part of the DVx2 UMAS: the Administrator User and the Player User.
The DVx2 DES is a simulator (written in JAVA programming language) that takes care of the game evolution according to a stochastic discrete event simulation that depends on the variables and parameters set-up (made by the player users at Client level).
Finally the DVx2 architecture could also include an external bridge to IEEE 1516 HLA federation of simulators. This part of the architecture is devoted to guarantee the possibility (for future developments) to connect the DVx2 serious game as a federate of an HLA federation of simulators; the HLA Bridge was not integrated in the current release.
By this approach the DVx2 users compare the results achieved by changing parameters and by adopting different hypotheses working distributed over the web; this approach allows to investigate large set of alternatives through an interactive approach enabling crowdsourcing (Bruzzone et al. 2012; Elfrey 2006).
In terms of implementation the decision to enable use of Virtual World over the web through a browser introduced some computational efficiency constraint as well as aspects related to band availability; so during the development of DVx2 emerged the importance to provide the user with interactive and effective control of the virtual representation to represent the results. Due to the high volume of data the final structure of DVx2 was forced to consider the requirements to operate on the web and to be more interactive, so several models were moved from DVx2 DES to the original DVx2 GUI that evolved into a real simulator as proposed in the following structure that represent the final architecture proposed for the simulation.
This solution is effective in case of multiple SMEs running independent simulators, while in case of multiplayer interactive simulations this approach requires to enhance the DVx2 DES to enable this capability; in the DVx2 current release, the different users are enable to run multiple scenarios in competition, for instance as replication for testing reliability versus stochastic factors and for measuring resilience and robustness as well as for changing assumptions and parameters, therefore the intelligent agents play each run separately and the comparison is just on initial and final results.
DVx2 supports the processes and game logic depicted in figure 5; obviously in stand-alone respect crowdsourcing DVx2 is addressing just the simulation part, avoiding to take care of profile management and Dbase integration.

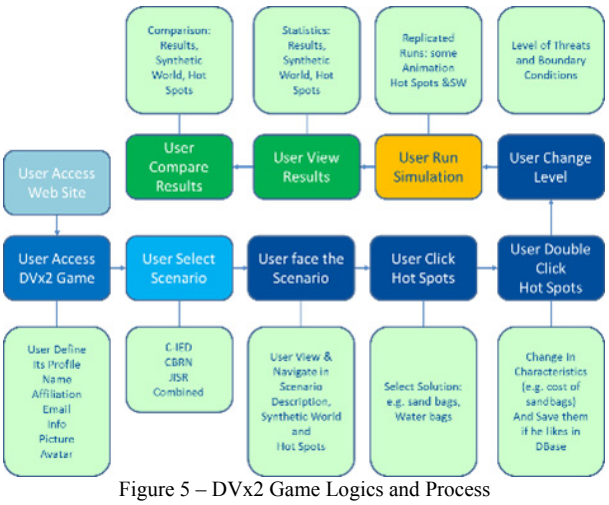

Figure 5 – DVx2 Game Logics and Process

In the current implemented release of DVx2, the user accesses to the DVx2 environment by selecting the game alternatives and then he proceeds in preparing and

analyzing the simulation runs; these activities are carried out within the DVx2 virtual framework while the results are proposed both in numerical and graphical forms.
DVx2 implements different target functions that allows providing an interactive assessment of impact of the DAT PoW achievements in terms of vulnerability reduction; in such sense the use of simulation allows to estimate a large spectrum of target variables able to provide a complete picture of the vulnerabilities respects many alternatives. Therefore for crowdsourcing just main variables are available in the Virtual 3D GUI for the user in order not to confuse him with too many factors. For instance in this case among parameters estimated by the simulator it was possible to collect: Casualties, wounded people, Reaction Time, Suspicious /Cleaned Area, Evacuation Time, Total Evacuation Costs, Success Rate, Correct Evacuation Range.
DVx2 demonstration success leads forward to the opportunity to use it for experiments devoted to reinforce its validity and create accreditation among SME community; indeed it is valuable to conduct experiments to measure the effectiveness by working with experts; indeed it is a strategic advantage to have access to a simulation framework that enable the capability to share and evaluate crucial interactive experimentation over DAT scenarios the community of expert for creating a dynamic repository of the related knowledge.

CONCLUSIONS

The new proposed approach based on MS2G is enabling crowdsourcing and data mining through combined use of M&S, IA and SG, so it becomes possible to involve a large number of people to keep up-to-date their know-how through interactive and engaging serious games.
This allows collecting data and information that are used to populate databases useful to better understand the different expert hypotheses as well as related to consequences estimated by the simulation. The authors focused this analysis on specific areas of DAT PoW and the related scenarios were useful to test the concepts as well as to investigate how M&S, IA, SG and immersive technologies could be effective in this environment.
An important follow up guaranteed by MS2G approach is the capability to create an interactive distributed simulation that could be effective for being used for training, education, dissemination, capability assessment, testing and experimentation by different users; for instance in DVx2 has an interesting potential in terms of general purpose for being applied in training and education for both over military and civil personnel, as well as for the diffusion of NATO DAT PoW Achievements.
A major benefits of DVx2 is the possibility to Support to Development of New Concepts and Solutions by Virtual Interoperable Testing; in similar way DVx2 could be used for the development of New Capabilities for Strategic Scenario Evaluation by New Simulation Models

ACKNOWLWDGMENTS

The authors thank the CMRE and NATO HQs for the support provided to this research; a special thank for the NATO DAT PoW, its coordination office and project teams and managers that contributed in model definition and validation.

REFERENCES

- Abrahams A., Boisot M., Bharathy Gnana (2005) “Simulating the Knowledge Transfer Dilemma: Lessons for Security and Counter-Terrorism”, Proceedings of SCSC, CherryHills, NJ, July
- Amico Vince, Guha R., Bruzzone A.G. (2000) "Critical Issues in Simulation", Proceedings of Summer Computer Simulation Conference, Vancouver, July
- Balci O., Glasow P., Muessig P, Page E.H., Sikora J., Solick S.,Youngblood S. (1996) "DoD Verification, Validation and Accreditation (VV&A) Recommended Practices Guide", Defense Modeling and Simulation Office, Alexandria, VA, November
- Banks J. (1998) “Handbook of Simulation: Principles, Methodology, Advances, Applications, and Practice”, John Wiley and Sons, NYC
- Bossomaier T, A.G. Bruzzone, M. Massei, D. Newth, J. Rosen (2009) “Pandemic dynamic object and reactive agents”, Int. Workshop on Modelling and Applied Simulation, Puerto de la Cruz, Tenerife
- Bossomaier T., Green G.D. (2000) “Complex Systems”, Cambridge University Press, Cambridge
- Benney R., Henry M., Lafond K., Meloni A., Patel S. (2009). "DoD New JPADS Programs & NATO Activities", Proceedings of 20th AIAA Aerodynamic Decelerator Systems Technology Conf. and Seminar, Seattle, WA, May 4-7
- Bruzzone A.G., Saetta S. (2002) "LESNEX: Lean Simulation Network of Excellence", Proceedings of Harbour Maritime Modeling and Simulation Conference, Bergeggi Italy, October 3-5, pp. 179-186
- Bruzzone, A., Cunha, G., Elfrey, P., & Tremori, A. (2009a). Simulation for education in resource management in homeland security. In Proceedings of the 2009 Summer Computer Simulation Conference (pp. 231-238). Society for Modeling & Simulation International. July
- Bruzzone, A. G., Cunha, G., & Tremori, A. (2009b). Intelligence and Security as a Framework

for Applying Serious Games. Proceedings of Serixgame, Civitavecchia, November.
- Bruzzone, A. G., Tremori, A., Tarone, F., & Madeo, F. (2011a). Intelligent agents driving computer generated forces for simulating human behaviour in urban riots. International Journal of Simulation and Process Modelling, 6(4), 308-316.
- Bruzzone, A.G., Tremori, A., Massei, M., (2011b), "Adding Smart to the Mix," Modeling, Simulation & Training: the International Defense Training Journal, 3, 25-27
- Bruzzone A.G., Marques H.C., Cantice G., Turi M. (2012) "Innovative C2 and Simulation for Crowdsourcing as Force Multiplier", Proceedings of EMSS2012, Wien, September
- Bruzzone A.G., Massei M., Tremori A., Longo F., Nicoletti L., Poggi S., Bartolucci C., Picco E., Poggio G. (2014a) "MS2G: simulation as a service for data mining and crowd sourcing in vulnerability reduction", Proc. of WAMS2014, Istanbul, Turkey
- Bruzzone A.G., Tremori A. (2014b) "Modelling and Simulation and Serious Games for Anti-Terrorism: Crowdsourcing within the SMEs Community", CMRE Report, La Spezia, December
- Elfrey, P. (2006) "Imagine Moving Off the Planet", Key Note Speech at Summer Computer Simulation Conference, Calgary, Alberta Canada, July
- Enders, W., & Sandler, T. (2002). Patterns of transnational terrorism, 1970–1999: alternative time-series estimates. International Studies Quarterly, 46(2), 145-165.
- Guo S., Bai F., Hu X (2011) "Simulation software as a service and Service-Oriented Simulation Experiment", Procededings of IEEE International Conference on Information Reuse and Integration, August, pp.113-116
- Hill David (1996) "Object-Oriented Simulation", Addison Wesley, Reading MA
- Hudson, R. A., & Majeska, M. (1999, September). The sociology and psychology of terrorism: Who becomes a terrorist and why? Washington, DC: Federal Research Division, Library of Congress.
- Kuhl F., Weatherly R., Dahmann J. (1999) "Creating Computer Simulation Systems: An Introduction to the High Level Architecture", Prentice Hall, NYC
- Longo F. (2010). Design And Integration Of The Containers Inspection Activities In The Container Terminal Operations. International Journal of Production Economics, vol. 125(2); p. 272-283, ISSN: 0925-5273, doi: 10.1016/j.ijpe.2010.01.026.
- Longo F (2012). Supply chain security: an integrated framework for container terminal facilities. International Journal of Simulation & Process Modelling, vol. 7, p. 159-167, ISSN: 1740-2123, doi: 10.1504/IJSPM.2012.049154
- Matusitz, J. A. (2013). Terrorism & communication: A critical introduction. Loa Angeles: Sage.
- McKercher, B., & Hui, E. L. (2004). Terrorism, economic uncertainty and outbound travel from Hong Kong. Journal of Travel & Tourism Marketing, 15(2-3), 99-115.
- McLeod J. (1982) "Computer Modeling and Simulation: Principles of Good Practice", SCS, San Diego
- Mosca, R., Bruzzone, A. G., & Costa, S. (1996). Simulation as a support for training personnel in security procedures. SIMULATION SERIES, 28, 251-255.
- MIMOS (2002) "Panel on M&S" MIMOS Annual Meeting, Turin
- Ören T., Longo F., (2008). Emergence, anticipation and multisimulation: Bases for conflict simulation Proceedings of the 20th European Modeling and Simulation Symposium, EMSS 2008, pp. 546-555
- Raybourn, E.M. 2012. Beyond serious games: Transmedia for more effective training & education, Proc. DHSS2012, Rome, Italy
- Siegfried, R., van den Berg, T. W., Cramp, A. J., & Huiskamp, W. (2014, January). M&S as a Service: Expectations and Challenges. In 2014 Fall Simulation Interoperability Workshops (SIW), 8-12 September 2014, Orlando, Florida, USA, 248-257. SISO.
- Smith, R. (2002, March). Counter terrorism simulation: a new breed of federation. In Proceedings of the Spring 2002 Simulation Interoperability Workshop.
- Tremori A., Baisini C., Enkvist T., Bruzzone A.G., Nyce J. M. (2012), "Intelligent Agents and Serious Games for the development of Contextual Sensitivity", Proceedings of AHFE 2012, San Francisco, US, July