

Editorial Introduction

Bernard P. Zeigler, Ph.D.
Editor-in-Chief

This issue marks the first in our third volume of *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology (JDMS)*. It is an occasion to step back and review the record of the first two volumes and look ahead to the future. To assist readers in a review, on the JDMS web site, <http://scs.org/pubs/jdms/issues.html>, and at end of this issue, we have published a table of all keywords employed by authors in the first two years of published articles together with the papers that mention each keyword. This should provide a perception at a glance on what has been published and the topics that have been covered. In a broader sense, the presentation should provide a first approximation to what characterizes the field of defense modeling and simulation, who are the participants, and what distinguishes this field from other fields in modeling and simulation and neighboring disciplines such as operations research and software engineering. As in the past, we invite your comments on what gaps there may be, what improvements might be needed, and where the future should bring us.

The current issue continues to explore new ground. Roger Smith opens up the issue with observations on the evolution of computer game technologies in the simulation training marketplace. In "Technology Disruption in the Simulation Industry," he employs notional models of disruptive technology dynamics to offer predictions on where virtual training simulators are heading. While not a simulation itself, most reviewers thought the article was significant for its insights on where the industry is heading and therefore where researchers and developers might wish to focus their energies. Let us know what you think.

Momen and Rozenblit, the authors of "Dynamic Decision Support in the Advanced Tactical Architecture for Combat Knowledge System," present a somewhat different view of the evolution of simulation support environments. They assert that modern military systems are demanding faster reactions and becoming more mobile. This implies that the difference between planning and execution will fade until the planning process appears to merge with the battle management process. The Advanced Tactical Architecture for Combat Knowledge System (ATAACKS) was earlier designed to incorporate both tools and algorithms for battlefield visualization. In the current article, ATAACKS is enhanced with an infrastructure based on the Discrete Event System Specification (DEVS) formalism to support rapid planning and decision making in dynamic battlefield environments. The article contrasts with Roger Smith's in that it brings into focus the need for advanced modeling and simulation methodologies to enable the advance of simulation technologies in addition to the hardware and general computer science advances that externally drive it forward.

Another article in this issue relates to methodological advances needed to support the new net-centric environments that are emerging. With the U.S. Department of Defense directing that all of its activities be migrated to the Global Information Grid (GIG) with its Service Oriented Architecture (SOA), the question of how to make this "stove-pipe" breaking transition happen comes front and center. In "Composable M&S Web Services for Net-Centric Applications," Tolk, Turnitsa, Diallo, and Winters note that although the Extensible Markup Language (XML) enables a new level of interoperability it is only a first layer upon which data sharing and service orchestration can be based. The authors developed a layered framework, the Levels of Conceptual Interoperability Model (LCIM), and methods of model-based data engineering to support semantically consistent service interoperation.

Finally, in "A Theoretical Model of Public Response to the Homeland Security Advisory System," Amy Ding employs differential equations to explore the dynamics of public perception of the information content of anti-threat warnings. How people perceive and respond to warnings may depend on a number of factors such as their reliability and frequency of occurrence. Reminiscent of the boy who cried wolf fairy tale, security advisory systems must be aware of the rise and fall of public credibility and attention to warnings and be designed according. Dynamic, predictive models may help.