Chapter VI

The Game of Defense and Security

Michael Barlow, University of New South Wales, Australia

To stimulate creativity, one must develop the childlike inclination for play ...

Albert Einstein

Abstract

This chapter covers the emerging area of the use of commercial off-the-shelf (COTS) computer games for military, defense and security purposes. A brief background is provided of the historic link between games and military simulation, together with the size and scope of the modern computer game industry. Considerable effort is dedicated to providing a representative sample of the various defense and security usages of COTS games. Examples of current usage are drawn from a range of nations including the United States (U.S.), Australia, Denmark, Singapore and Canada. Coverage is broken into the three chief application areas of training, experimentation and decision-support, with mention of other areas such as recruitment and education. The chapter highlights the benefits and risks of the use of COTS games for defense and security.
purposes, including cost, acceptance, immersion, fidelity, multi-player, accessibility and rapid technological advance. The chapter concludes with a discussion of challenges and key enablers to be achieved if COTS games are to obtain their true potential as tools for defense and security training, experimentation and decision-support. Aspects highlighted include the dichotomy between games for entertainment and “serious” applications; verification, validation and accreditation; collaboration between the games industry and defense; modifiability, interoperability; quantifying training transfer; and a range of technological challenges for the games themselves.

Introduction

Games and warfare have a long association — venerable and even ancient games, including Go (called Wei Chi in China), chess (really a family of related games including European, Chinese — Xiang Chi, Japanese — Shogi, Korean — Changgi, Thai — Makruk, Burmese — Sittuyin and the Indian forerunner Shatranj) and Owari (from Africa — also spelled Awale and Warri), are abstract models of military conflict. Many have been used for teaching some of the principles of warfare, while others, such as the game of Kriegsspiel¹, were created and utilized directly as a military teaching tool.

The computer game as a genre is just more than 40 years old. Perhaps not surprisingly, the first known game — Spacewars — was of battle, between two spaceships (BBC, 2001). In the 40 years since Spacewars, computer games have gone from 2K (byte) programs written by enthusiasts to immersive, multi-media products developed by large teams and which support an international industry with a revenue estimated to be in excess of $15 billion per year. A typical modern game provides a swath of features — immersive 3D and multi-media content (audio, video, story); increasing degrees of interactivity with a simulated world; an intuitive and well-designed user interface; sophisticated “artificial intelligence (AI)” (computer-controlled) opponents and allies; multi-player capabilities in collaborative and opposed scenarios; and scenario building and editing capabilities (some even provide their own programming language or Application Programming Interface, or APF²).

If the abstracted board games of the past have offered utility as tools to the military; then what potential exists in the sophisticated COTS games of today
Related Content

Why Risk-Research is More Prominent in English Speaking Countries in the Digital Society

Secure Knowledge Management: Influencing the Development of Human Knowledge Sharing Networks
[www.igi-global.com/article/secure-knowledge-management/138275?camid=4v1a](www.igi-global.com/article/secure-knowledge-management/138275?camid=4v1a)

Fostering SCADA and IT Relationships: An Industry Perspective
[www.igi-global.com/article/fostering-scada-relationships/69769?camid=4v1a](www.igi-global.com/article/fostering-scada-relationships/69769?camid=4v1a)

Web Defacements and Semantic Attacks
[www.igi-global.com/chapter/web-defacements-semantic-attacks/25670?camid=4v1a](www.igi-global.com/chapter/web-defacements-semantic-attacks/25670?camid=4v1a)