Chapter 5

The Social Design of 3D Interactive Spaces for Security in Higher Education: A Preliminary View

Shalin Hai-Jew
Kansas State University, USA

ABSTRACT

Immersive spaces offer a unique set of security challenges related to human, data, learning facilitation, and virtual environment risks. Security risks may originate from people, the technology, or a mix of unintended synergistic effects; they may originate from intentional, unintentional, and accidental actions. Understanding the risk environment will be important for those who use persistent, immersive 3D spaces for teaching and learning. Based on the current research and direct experiences in educational immersive spaces, this chapter will first define the security risks and offer real-world examples. Then, it will look at various potential social design interventions. “Social design” refers to protective measures created through awareness-raising among all participants, policy creation and implementation, human facilitation of teaching and learning in immersive spaces, and other efforts to improve and maintain the security for the socio-technical system, the institution of higher education, the learners, the faculty, and the larger cyber-sphere. These social design endeavors, one part of a larger 360 degree security approach, will improve security but never fully attain “perfect security” (a condition of no-risk). This chapter will include an international survey of instructors who teach in 3D immersive spaces to solicit their ideas about security and the social design of protective measures.

INTRODUCTION

With growing affordances for information transfer through the carrying capacity of the Internet, and the greater sophistication of 3D immersive technologies, many higher education courses, learning experiences and training exercises have moved to immersive 3D spaces. Learners themselves demonstrate a growing sophistication and comfort in such spaces, in the 15 years that virtual environments have been existent (Cikic, Grottke, Lehmann-Grube, & Sablatnig, 2008).
This increase in the use of persistent and immersive virtual worlds provides many affordances for online learners. 3D spaces offer opportunities for spatial reasoning. They offer opportunities for multi-way communications among human learners, with automated (often very human-like) AI-agents. With their own digital physics and ecologies, the virtual environments may be dynamic and interactive; they may offer dynamic modeling of complicated systems with many changing elements and interactions (Colella, 2000). Here, the learning may be multi-sensory, full-surround, and focused within a particular context for situated learning. Learners may explore spaces for experiential discovery-learning; they may make decisions and see the results of those decisions in a simulation. They may collaborate with peers and consult with subject matter experts (SMEs). They offer persistence over time, for truly longitudinal learning and relationship-building.

These affordances in complex, interconnected socio-technical systems offer plenty of opportunities for security lapses and compromises. These risks may originate from the social aspects (the learners, the exchanged information, and the facilitation of teaching and learning) and the technological ones (the virtual environment, the scripted robots, and virtual creatures). These hazards may come from purposive attacks, unintended actions, accidents, and unintended synergies that may occur with combined actions. The origins of these risks are several-fold. The nature of 3D immersive spaces themselves carries inherent risks. Lapses may occur at any point of connectivity to the immersive spaces, and the more the connection points, the more potential there are for unintended risks. Security here may be understood in a multi-faceted and broad sense. This chapter will address what is socially controllable and what may have to be addressed through policy and technology (through design and the deployment of various technologies for systems maintenance, surveillance, record-keeping, and the maintenance of order). The social design aspect will touch on issues of educational policymaking and enforcement, instructional facilitation, and technological oversight.

**SOME CAVEATS**

If security and surveillance are at one end of a continuum, at the other end would be the need for individual privacy protections. In M. Andrejevic’s dystopian nightmare of a “digital enclosure,” every human action is captured digitally and recorded (Andrejevic, 2007), in a panopticon society. Every person is theoretically trackable in wired and wireless spaces, and “black” information skimmers are alleged to be able to capture all electronic communications and sort through them for targeted messages and data (Bamford, 2008). The erosion of privacy is not the only concern. There are also risks of fomenting an unintended us-vs.-them between learners and the outside world beyond the confines of the controlled, private learning space.

Another caveat relates to the control-serendipity continuum. While control is sometimes linked with safety and security, excessive control leads to risks—of authoritarian approaches to a public architecture, of lack of chance-encounters, and of a lack of serendipity. There’s potency in the interactions of the real moment that is unplanned:

*The gesture has a spontaneity, a freedom, an unfiltered physicality in its instantaneous choice. There is a depth of communication in this moment—the split second of a photograph, the subtle timing of a comedian. These instants are not planned or contrived but quickly communicated through a developed intuition (Schkolne, 2002, p. 371).*

Immersive spaces capture creativity in motion and mediate the transfer of complex knowledge.

This chapter will explore the research on security issues in immersive spaces and involve live actual security incidences in educational immersive learning spaces. This will offer some
Related Content

Issues and Applications of Internet Traffic Modelling
www.igi-global.com/chapter/issues-applications-internet-traffic-modelling/16863?camid=4v1a

Basic Concepts on RIAs
www.igi-global.com/chapter/basic-concepts-on-rias/117375?camid=4v1a

A Security Framework for Networked RFID
www.igi-global.com/chapter/security-framework-networked-rfid/63547?camid=4v1a

www.igi-global.com/chapter/low-loss-energy-aware-routing/63554?camid=4v1a