Mission Assurance Challenges within the Military Environment

Scott Musman, MITRE Corporation, McLean, VA, USA
Michael R. Grimaila, Air Force Institute of Technology, Wright-Patterson AFB, OH, USA

ABSTRACT

Virtually all modern organizations have embedded information and communication technologies into their core processes as a means to increase operational efficiency, improve decision quality, and reduce operational costs. However, this dependence can place the organizational mission at risk when an incident occurs that compromises a cyber resource critical to the success of the organizational mission. In this paper, the authors examine the challenges of developing and maintaining a mission-wide understanding of organizational mission risk within military environments. Specifically, they examine the concept of mission assurance, discuss various factors which must be taken into account when describing military missions, analyze the four primary types of representations used to capture mission-to-cyber relationships, and highlight the complexities of documenting cyber dependencies for the purpose of achieving mission assurance.

Keywords: Cyber Mission Assurance, Embedded Information and Communication Technologies, Mission Assurance, Mission-to-Cyber Relationships, Risk Management

INTRODUCTION

The benefits of embedding Information and Communications Technologies (ICT), also known as “cyberspace”, into core business processes are well understood as a means to increase operational efficiency, improve decision quality, and reduce costs. As a consequence, cyber security continues to grow in importance within the military community as modern military operations have become more dependent upon ICT. Given the enormous challenges facing cyber security, it has been considered that a more focused problem is to secure computing resources in the context of the missions that they support rather than just treat them as a collection of disjoint system focused security objectives (Hale, 2010). Within the military community, there has been a disconnection between the personnel who are responsible for securing the ICT and the personnel who are responsible for performing mission activities (Grimaila, 2008). Personnel on the mission side of operations are rarely aware of how cyber resources contribute to the success of their mission activities and people on the ICT side rarely understand which cyber resources support which missions or mission activities (Hale et al., 2010).

One of the fundamental goals of any organization is to assure the success of its mission objectives. Organizations typically address this...
risk through enterprise-wide risk management activities that focus on the explicit identification of risks so that control measures can be selected to mitigate mission risk to an acceptable level given budgetary constraints (ISO 31000, 2009; Whitman & Mattord, 2010). This type of focused planning is most successful in static business process environments, when all stakeholders participate, resources critical to the success of the organizational operations can be enumerated, and the projected scenarios are representative of the possible futures experienced by the organization. In contrast, military missions often involve dynamically changing, time-sensitive, complex, cooperative, and coordinated ventures between multiple organizations (e.g., units, services, agencies, coalition partners) who may not share in a complete view of their role within the overall mission (Alberts & Hayes, 2006). Since each participating organizational unit is resourced and managed as a separate entity, the enterprise-wide approach to assuring the mission is significantly more complex.

Recently, there has been an intense focus to formalize the concept of “Mission Assurance” (MA) within the United States (US) Department of Defense (DoD). Surprisingly, very little research has focused on the fundamental problem of how to describe and relate military mission requirements to cyber dependencies. Existing MA analysis rely on implicit assumptions that relate cyber and mission (i.e. it is usually safe to say that more resilient, less vulnerable cyber resources will tend to lead to more resilient mission systems). However, decision quality MA analysis requires a more formal, explicit description of missions, systems, resources and dependencies. In this paper, we examine the concept of Mission Assurance and present challenges of attaining it in military environments.

BACKGROUND

What is a “Mission?”

The meaning of the word “mission” can vary greatly based upon the context in which it is used. An organization’s mission statement is a clear, concise written statement that identifies and differentiates the organization’s purpose. The mission statement provides “the framework or context within which the company’s strategies are formulated” (Hill et al., 2008). The context of “mission” implies an enduring set of objectives defined at the strategic level. In order to fulfill these objectives, units within the organization execute day-to-day activities to accomplish the overall strategic mission.

In contrast, DoD Joint Publication 1-02 defines mission for the military as (JP 1-02, 2009):

1. The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore;
2. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task;
3. The dispatching of one or more aircraft to accomplish one particular task.

This definition is single-task focused: implies simple, limited duration and tractable complexity; and is measured by goal attainment. However, Donley (1995) identified that within the DoD a mission is more broadly defined as “integrating many activities around a common theme or purpose” which is at odds with the JP 1-02 definition. While “mission” frequently appears in military publications, it is rarely explicitly defined which results in confusion and misunderstandings (Alberts & Dorofee, 2005; Hale, 2010). One of the problems in discussing Mission Assurance is the lack of a standardized, canonical, widely accepted definition for the word “mission.”

What is “Mission Assurance?”

Although there are several definitions for the term “Mission Assurance”, they all have a common characteristic: they are techniques to improve the likelihood of mission success (DODD 3020.40, 2010; AFDD 3-12, 2011). Mission Assurance (MA) should be viewed as a continuous process whose purpose is to assure the capabilities and infrastructure necessary to
Related Content

Risk Factors to Retrieve Anomaly Intrusion Information and Profile User Behavior
[www.irma-international.org/article/risk-factors-retrieve-anomaly-intrusion/1418/](http://www.irma-international.org/article/risk-factors-retrieve-anomaly-intrusion/1418/)

Communication Improvement and Traffic Control Based on V2I in Smart City Framework
[www.irma-international.org/article/communication-improvement-and-traffic-control-based-on-v2i-in-smart-city-framework/203682/](http://www.irma-international.org/article/communication-improvement-and-traffic-control-based-on-v2i-in-smart-city-framework/203682/)

Self-Calibrating Source Synchronous Communication for Delay Variation Tolerant GALS Network-on-Chip Design
[www.irma-international.org/chapter/self-calibrating-source-synchronous-communication/74249/](http://www.irma-international.org/chapter/self-calibrating-source-synchronous-communication/74249/)

Modified Lease Auction: Proposal of a New System for Efficient Assignment of Radio-Spectrum Resources
[www.irma-international.org/chapter/modified-lease-auction/29816/](http://www.irma-international.org/chapter/modified-lease-auction/29816/)

Employing Content Validity Approach for Improving the Content of Broadband Adoption Survey Instrument
[www.irma-international.org/chapter/employing-content-validity-approach-improving/20448/](http://www.irma-international.org/chapter/employing-content-validity-approach-improving/20448/)