Chapter 9
Developing a Military Cyber Maturity Model for Multi-Domain Battle Mission Resilience and Success

David Ormrod
Australian Centre for Cyber-Security, University of New South Wales at the Australian Defence Force Academy, Canberra, Australia

Benjamin Turnbull
Australian Centre for Cyber-Security, University of New South Wales at the Australian Defence Force Academy, Canberra, Australia

ABSTRACT

Modern military forces rely heavily on cyber-enabled systems; for logistics, communication, and control. Modern military platforms are heavily integrated with computing capability. This integration and reliance will only increase over time. Modern military operations require the support of flexible, responsive and resilient cyber-capabilities. Current information system security models and information assurance constructs seek to achieve information assurance, a high degree of certainty in the confidentiality, integrity and availability of cyber-systems supporting combat operations. However, this approach assumes that an information assurance approach is a complete and comprehensive defense. History though, has proven otherwise. This work argues that the information assurance approach, whilst a worthy goal, is not reflective of the lessons of history or warfare. Specifically, this work outlines the need for, and introduces The Military Cyber-Maturity Model, a pragmatic model that assumes a technically capable and intelligent adversary. This model assumes the possibility of an adversary utilizing an unknown vulnerability to attack the system, and expends resources to minimise the impact of the successful attack rather than relying entirely on an impregnable defense. This approach extends beyond the assumption that a cyber-attack immediately causes mission failure, by recognizing that each cyber-attack has different requirements and outcomes and will affect different assets and processes. The Military Cyber-Maturity Model seeks to model business continuity through a high degree of cultural change, embedded work practices that

DOI: 10.4018/978-1-7998-2466-4.ch009

parallel analogue and digital work practices with deceptive counterintelligence behavior. The Military Cyber-Maturity Model incorporates the concepts of behavioral defense and mission assurance to provide agility and increase the likelihood of success in combat. Information deception provides a behavioral defense, creating uncertainty and doubt in the adversary's mind and reducing the degree of trust they have in the information available. This paper introduces the model, outlines its aims, components and justifications. This work also outlines the need for simulation and testing to validate the model's effectiveness, and introduces a number of potential use-cases.

INTRODUCTION

The broad applicability and influence of digital communications and cyber-enabled systems makes the issue of information security and cyberspace relevant to the entire profession of arms, from the tactical to strategic level. Cyber-systems underpin all facets of modern militaries, from communications through to logistics. The integration of technology into all facets of the military presents both a unique opportunity and a potential source of weakness. The purpose of this paper is to establish a foundation of knowledge and understanding upon which relevant dialogue and debate can be generated, and cyber-doctrine can be built. Doctrine provides "…fundamental principles by which military forces guide their actions in support of national objectives." (Commonwealth of Australia 2012b). Doctrine is developed from concepts, which are the untested ideas about future operations. The relevance of the future to concepts, and subsequent doctrine, arises because of the potentially catastrophic consequences faced by a military that has not kept up with the developments of the environment in which it must operate, or the capabilities of its adversaries.

The United States Department of Defense (US DOD) Joint Publication 3-12 (R) Cyberspace Operations provides the doctrine for US DOD joint cyberspace operations and defines cyberspace as a global domain within the information environment "…consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers…" (US Department of Defense, 2013, pp. I-1). The UK Joint Defense Doctrine Publication 0-01 employs a very similar definition of cyberspace (UK Ministry of Defence, 2014, p. 15). The concept of cyber-warfare presented within these documents is multidimensional, encompassing a diverse array of issues. As a result, the creation of an underlying methodology and unified theory has proven challenging (Robinson, Jones, & Janicke, 2015). "In many ways, we are failing. Partly this is due to attempts to meet the new challenges with approaches, concepts, constructs and institutions inherited before the official recognition of cyberspace as an environment. They are inadequate for the task. They may be necessary, but are altogether insufficient; they are patching over challenges, rather than organically developing with them…" (Maclntosh, Reid, & Tyler, 2011, p. 104).

Military operations require the support of flexible, responsive and resilient cyber-capabilities. Information system security models and information assurance constructs seek to achieve information assurance, a high degree of certainty in the confidentiality, integrity and availability of cyber-systems supporting combat operations. This paper argues that the information assurance approach, whilst a worthy goal, is not reflective of the lessons of history or warfare. Mayfield's paradox mathematically demonstrates the futility of attempting to make any information or Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) system completely assured against every attack (Mayfield, 2001). Reliance on algorithms and technology has consistently been proven to be misplaced