Chapter 15
Using an Ontology for Network Attack Planning

Renier van Heerden
Council for Scientific and Industrial Research (CSIR) and Nelson Mandela Metropolitan University, South Africa

Peter Chan
Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa

Louise Leenen
Council for Scientific and Industrial Research (CSIR), Pretoria and Cape Peninsula University of Technology, Cape Town, South Africa

Jacques Theron
South African National Defence Force (SANDF), Pretoria, South Africa

ABSTRACT

The modern complexity of network attacks and their counter-measures (cyber operations) requires detailed planning. This paper presents a Network Attack Planning ontology which is aimed at providing support for planning such network operations within the cyber domain. The amount of cyber information is increasing constantly and the time that information stays relevant and valuable in decreasing similarly. Thus semantic technologies can contribute towards the intelligent processing of information in this ever-changing environment. An ontology enables the representation of semantic information. In additional, automated reasoning can enrich the representation by inferring unknown relationships. The inferences that can be made with the automated reasoning capabilities of ontologies provide a unique insight into the relationships between network targets and attacks, compared to traditional databases.

DOI: 10.4018/978-1-7998-2466-4.ch015

1. INTRODUCTION

As warfare begins to move away from the physical battlefield and onto the cyber realm, it becomes important to build the necessary capability to keep up with such advances. "*Over the last two decades, the United States has witnessed significant and rapid technological advancements in digital communications (cyber communications) and information technology. Owners and operators of critical infrastructure have capitalised on these innovative technologies to operate their systems more efficiently and provide better service to customers. Despite the many benefits of an increasingly "wired" economy and defence, the nation's exposure to cyber threats have also increased.*" This statement by Dean (2013), the editor of the Hampton Roads International Security Quarterly journal, expresses the fact that nations have to defend themselves against cyber threats; nations are vulnerable in terms of digital attacks with the intention of sabotage, espionage, terrorism and crime by people with ill intent. Symantec highlighted a 91% increase in targeted attacks in the 2014 threat report (Symantic Corporation, 2014). As a consequence, military forces have to include cyber attack counter-measures as part of their military power.

Within military forces there exist Electronic Warfare (EW) threat analysis databases that are populated with all possible electromagnetic threats (such as missile range finding or radar tracing) focusing on fingerprinting the electronic emissions of weapons that use the electromagnetic spectrum. This captured information can be used for analyses. For example, this information is loaded onto an aircraft's early warning and counter-measure system before a mission into enemy territory. This is part of platform protection in an attempt to increase the survivability of the aircraft in combat by automatically countering weapons that use electronic emissions, thus allowing the pilot to focus on the mission itself.

The cyber world can learn from EW by applying the same principles of developing a threat knowledge database for cyber warfare. A Security Information Events Management (SIEM) system is a step in the right direction although mainly focusing on reactive counter-measures. This paper takes this aspect further by presenting the development of a Command and Control (C2) ontology for the subdomain of Cyber Network Attack Planning. This ontology will assist in building a knowledge base for cyber network attack planning and counter measures which will enable proactive cyber counter-measures.

Section 2 contains background information, specifically an overview of ontologies, command and control from a military perspective, and network attack ontologies. Section 3 discusses the presented Cyber Network Attack Planning ontology and the paper is concluded in Section 4.

2. BACKGROUND

This section gives an overview of ontologies, Command and Control and existing Network Attack ontologies. Finally we discuss the defences and advantages of Ontologies compared to databases.

2.1. Overview of Ontologies

An ontology is a technology that provides a way to exchange semantic information between people and machines (Noy and McGuinness 2001). It is a formal encoding of concepts in a chosen domain, and in addition contains properties and instances of these concepts as well as axioms that give information on the concepts and properties. It also has an automated reasoning facility which enables the derivation of