An Ontological Knowledge Base for Cyber Network Attack Planning

Peter Chan, Jacques Theron, Renier van Heerden and Louise Leenen

Abstract:
In modern warfare it is no longer sufficient to only focus on physical attacks and counter-measures; the threat against cyber networks is becoming increasingly significant. Modern military forces have to provide counter measures against these growing threats in the cyberspace. These forces thus find themselves in the position where they need the capability to perform cyber operations. This paper presents a Network Attack Planning ontology which is aimed at providing support for military cyber operations. The cyber network operation domain is growing at a rapid rate and involves an ever increasing volume of associated information. Semantic technologies can contribute towards the intelligent processing of information in this complex problem area. An ontology enables the representation of semantic information and automated reasoning that can support the complexity of planning cyber operations. It also contributes towards the sharing of information and the creation and maintenance of a common vocabulary. 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 that could be launched against them.

Keywords: ontology, network attack planning, command and control, cyber warfare