International Journal of Cyber Warfare and Terrorism, vol. 6(3), 65-78

Using an Ontology for Network Attack Planning

Renier van Heerden1,2, Peter Chan2 , Louise Leenen2,3 Jacques Theron4

1 Nelson Mandela Metropolitan University, South Africa

2 Council for Scientific and Industrial Research (CSIR), South Africa

3 Cape Peninsula University of Technology

4 South African National Defence Force (SANDF) rvheerden@csir.co.za kchan@csir.co.za

lleenen@csir.co.za jacques.theron@sita.co.za

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.