The Use of Semantic Technologies in Cyber Defence

Louise Leenen and Thomas Meyer

Abstract: Governments, military forces and other organisations responsible for cybersecurity deal with vast amounts of data that has to be understood in order to lead to intelligent decision making. Semantic technologies is a knowledge representation paradigm where the meaning of data is encoded separately from the data itself. The use of semantic technologies such as logic-based systems to support decision making is becoming increasingly popular. Due the vast amounts of information pertinent to cybersecurity, automation is required for processing and decision making. However, most automated systems are currently based on syntactic rules. These rules are generally not sophisticated enough to deal with the complexity of decisions required to be made. The incorporation of semantic information allows for increased understanding and sophistication in cyber defence systems. An example of an application area is systems that detect and respond to cyber attacks: semantic information enables increased understanding and sophistication in network attack detection systems.
In this paper the authors give an overview of the use of semantic technologies in cyber defence, and identify and discuss emerging trends and the way forward for future research.

Keywords: Cyber defence, Semantic Technologies, Decision Making, Automated Systems