

Ontologies and other types of semanticware - assets to protect, or instruments to use in Cyber Warfare?

Martin Luts, ELIKO Competence Centre in Electronics-, Info- and Communication Technologies
martin.luts@eesti.ee

Abstract In the dawn of Web3, the Semantic Web, the paradigm and techniques of Cyber Warfare will alter. How one can protect web3 specific assets and services in Cyber Warfare and/or can make use of web3 features to attack/defend, is terra incognita, largely unexplored.

The Semantic Web is an evolving extension of the World Wide Web in which the semantics of information and services on the web is defined, making it possible for the web to understand and satisfy the requests of people and machines to use the web content. At its core, the semantic web comprises a set of design principles, collaborative working groups, and a variety of enabling technologies. Some elements of the semantic web are expressed as prospective future possibilities that are yet to be implemented or realized. Other elements of the semantic web are expressed in formal specifications. Some of these include Resource Description Framework (RDF), a variety of data interchange formats (e.g. RDF/XML, N3, Turtle, N-Triples), and notations such as RDF Schema (RDFS) and the Web Ontology Language (OWL), all of which are intended to provide a formal description of concepts, terms, and relationships within a given knowledge domain.

The military has numerous problem domains at the tactical, operational, and strategic levels of war where knowledge-based systems, including ontologies, have been and can be deployed. The intersection of OWL and ontologies in general, on one hand, and Cyber Warfare, on the other, is the topic of this paper. We consider two different scenarios here:

1. A passive scenario - ontologies as assets to protect in Cyber Warfare.

We'll outline the architecture of web3 and pinpoint the critical services which make use of ontologies in web3 infrastructure, how these could be attacked and defended, estimate the consequence of paralyzed/collapsed ontology-based infrastructure services. We'll give examples using Finnish national ontology infrastructure FinnONTO.

2. An active scenario - ontologies as instruments to use in Cyber Warfare.

In order for ontologies to become truly useful in high-level military applications it is necessary to identify, document, and integrate into automated systems the human knowledge that military professionals use to solve problems.

We consider two types of interrelated ontologies: a. Cyber Warfare Attacks Ontology b. Cyber Warfare Defence Mechanisms Ontology

These ontologies contain human readable and machine "understandable" definitions of classes (for example, DDoS attack and its subtypes - like NULL flood - with its properties), typed relationships between these classes (for example - between attack types and counter mechanisms), rules and axioms (for example, to generate/critique courses of action at tactical or at operational level). Based on these ontologies a simulation of cyber attacks could be run and the quality of competing/alternative ontologies/knowledge bases estimated. Also, these ontologies serve as shared, controlled vocabulary between several parties, and more unambiguous Cyber Warfare defence handbooks could be created and maintained. With the respect to Natural Controlled Languages we give some ideas how to use them do define the classes/concepts of Attacks and Defence Mechanisms Ontologies using Attempt Controlled English (ACE) with ACE parser.

We will draw a parallel with the ontology development done for the Defence Advanced Research Project Agency (DARPA) High Performance Knowledge Bases (HPKB) a.o programs.

Keywords: Cyber Warfare, ontologies, OWL, course of action automatic generation, knowledge-bases