Modelling the Cybersecurity Environment using Morphological Ontology Design Engineering

JC Jansen van Vuuren, L Leenen, MM Grobler, KFP Chan and ZC Khan

Keywords: cybersecurity, design science, general morphological analysis, Morphological Ontology Design Engineering (MODE), ontology, research methodologies

Abstract:
Acquiring, representing, and managing knowledge effectively has a considerable impact on constructing accurate and intelligent systems. A challenge faced by domain experts is the manner in which information about the cybersecurity environment can be extracted and represented, seeing that it is messy problem with great uncertainty within the environment. To address this problem, this article presents a new methodology to model the cybersecurity environment: Morphological Ontology Design Engineering (MODE). This methodology is based on the combination of three different research methods, i.e. design science, general morphological analysis, and ontology based representation. General morphological analysis offers a solution for extracting meaningful information from domain experts, while ontology based representation is used to logically and accurately represent such information. On a high level, the design science methodology guides the entire process. When applied to the cybersecurity environment, the results reveal that the approach of using mixed methods is beneficial. The new hybrid methodology allows domain experts to solve a messy problem that has quantitative and qualitative information, long term and short term goals, as well as logical and empirical evidence. The main benefit of the general morphological analysis aspect of the methodology is the acquisition of meaningful information, and the main benefit of the ontological aspect of the methodology is the semantic representation of the information. This article demonstrates the new methodology by applying it to the cybersecurity domain, resulting in a cybersecurity ontology which can be used in support of implementing a South African cybersecurity policy.