An Ontology of Cyberspace as a Basis for Decision-Making in Cyberoperations

Alexander Grandin
Finnish Defence Research Agency, Riihimäki, Finland

alexander.grandin@mil.fi

Abstract: In the cyberoperations community there is a commonly accepted starting point for describing cyberspace as comprising of multiple planes through which information flows. However, the model is not a tool that facilitates planning and executing cyberoperations. Tools do exist in the form of technical cybersecurity ontologies. At the moment the link between technical ontologies, that are the tools of experts, and the operational planning process is limited. These technical ontologies provide automated information that would support operational planning. At the moment cybersecurity experts translate the information that military professionals need, which may cause insufficiencies or distortions in communication or cause inconsistencies in the planning process. This paper presents the ongoing work of developing a model of cyberspace in the form of a core ontology. The ontology describes the flow of digital information between persons and the enabling technology as well as geographical data. It is intended as a tool that supports operational planning and decision-making in and through cyberspace, by enabling automation and reasoning. The model is created using the well-established Constructive Research Approach (CRA) methodology, and is developed on earlier research. CRA consists of six phases in which (1) the problem is defined, (2) an understanding of the topic is generated, (3) a solution (model) is constructed which then is (4) demonstrated. Then the models (5) theoretical connections are presented and the (6) scope of applicability is assessed. The challenges of developing an ontology of cyberspace as part of the third phase of the methodology are in focus. The ontology serves as an operational core ontology, aiming to link cybersecurity domain ontologies to the DOLCE+DnS Ultralite (DUL) foundational ontology. The ontology is based on research in Cyberspace Geography and Cyber Terrain. No earlier attempts at creating a core ontology of cyberspace grounded in a foundational ontology, based on these concepts, were found. Overall, the use of reference ontologies in cyberspace research is scarce and few are grounded in a foundational ontology. The starting point for the ontology is a model of cyberspace comprising of six layers, which are the 1) geographic layer, 2) physical network layer, 3) logical network layer, 4) socio-organizational layer, 5) virtual persona layer and finally the 6) persona layer. The model was complemented with levels describing action and information and partially excluded the outer levels 1 and 6, which were directly linked to the DUL foundational ontology.

Keywords: Cyberspace, Cybersecurity, Ontology, Semantic web, Knowledge engineering

1. Introduction to ontologies and cybersecurity

This paper puts in focus the differences between the cybersecurity and operational viewpoints of cyberspace. Cybersecurity has many definitions, and in this paper, it is broadly defined as the technology and measures used to secure networks or information from digital- or cyberattacks. The definition puts focus on the technical measures used. Cyberoperations or cyberspace operations is a term used to describe actions in and through cyberspace, though always utilizing the logical network layer (NATO, 2020). There seems to be a divergence between the operational point of view, highlighting the physical factors of cyberspace, and the cybersecurity aspect, highlighting the technical and virtual aspects (Huntley, 2016). Continuing, cybersecurity ontologies usually lack a grounding to a foundational ontology (Martins, et al., 2020).

Cyberspace is often described using three or more planes or levels. Firstly, these usually portray the physical network, consisting of networked devices and infrastructure. Secondly, the logical network, consisting of software and code that directs the flow of information and the work of the networked devices. And finally, the persona level, consisting of the persons and their virtual representations that use and direct the earlier plane (NATO, 2020) (Grandin, 2023). The flow of information in computer systems is also often described using the International Standardization Organizations seven step Open systems interconnection (ISO/OSI) model[1]. It however only describes the flow of information in the system and not where it moves (geographical information) or to whom (persona).

In medicine the use of ontologies has widely supported scientific development, for instance in research regarding the human genome. However, Smith and Ceusters (2010) have stated that "*it is of obvious advantage if we can find a way to minimize the number of ontologies that are being constructed and at the same time maximize their mutual consistency*". Ontologies are a description of a shared understanding, and are often formed to facilitate information sharing and also to provide a discourse and a shared understanding of the

[1] ISO - 35.100.01 - Open systems interconnection in general

domain (Möller, 2020). An ontology can also be the starting point for visualisations (Sikos, 2023) or useful for different sorts of reasoning (Smith & Ceusters, 2010). van Heerden, et al. (2016) describes the benefits of creating a shared vocabulary and also mention as benefits the clarification of domain assumptions and analysing domain knowledge as well as separating this from operational knowledge. Additionally, the implementation of Knowledge Graphs and automated reasoning requires that concepts are grounded which also elevates the relevance of ontologies (Martins, et al., 2022). An ontology defines, according to Möller (2020), the "*types, properties and interrelationships of entities that really or fundamentally exist for a particular domain of discourse.*" This point of view is in focus in this paper. Thus, an ontology facilitates the creation of a shared understanding, visualization and concretisation of e.g. cyberspace operations, civil as well as military.

In military planning the physical aspects of cyberspace are often highlighted (Grandin, 2023). Cybersecurity ontologies often take a technical viewpoint and often lack a grounding to a foundational ontology. A military commander would gain if presented with a link between persons, organizations, cybersecurity and geography when deciding on how to approach challenges in and thorough cyberspace or physical cyberspace assets. This motivates the development of a core ontology for cyberspace, linking the levels and concepts needed for operational planning. Cyberspace is described as a metaphor and a "*layer on top of our existing reality*" (Kreuzer, 2021). A core ontology should thus present its digital imprint on several planes. This paper presents the ongoing effort of developing a core ontology for cyberspace, incorporating the technical, physical and virtual aspects of cyberspace and the persons using it.

The Core Cyberspace ontology (CoCy) presented here is created *top-down* in pursuit of greater consistency between the existing application ontologies according to the ontological realism methodology described by (Smith & Ceusters, 2010). The chosen methodology for constructing the ontology is the Constructive Research Approach (CRA), presented by Kasanen, et al. (1993). The aim of the produced CoCy ontology, according to the principles set up by Martins, et al. (2022), is a core ontology, which links the foundational ontology (DUL) with cyberspace and cybersecurity domain or application ontologies. The aim is (using the description by Martins, et al., 2022) to produce an operational ontology written in OWL that in formalization and axiomatization is lightweight. It is not based on a reference ontology, and is thus imprecise.

The starting point of the constructed core ontology adheres to the earlier findings by the author (Grandin, 2023). Accordingly, the basis for an ontology of cyberspace was based on the physical network, logical network and persona layers and geographical information. These levels were complemented with two layers. First, the cyber-persona layer, which links virtual persona accounts to physical persons. Secondly, the socio-organizational layer, which describes groups of actors in cyberspace. A possible cognitive layer was identified as an important and often overlooked part of cyberspace (Asquith & Morgan, 2020). The cognitive aspects of cyberspace were however not included in the scope of this paper, but identified as a possible extension. One example of a cyberspace ontology incorporating the cognitive layer is presented by Grant (2014). The levels of cyberspace at the beginning of the work were thus defined as the 1) geographical plane, 2) physical network plane, 3) logical network plane, 4) socio-organizational plane, 5) cyber-persona plane and 6) persona plane.

The importance of time in cyberspace has been highlighted by several researchers, such as Phister (2010), Bromander, et al. (2020), van Heerden, et al. (2016), Morosoff, et al. (2015) and Grandin (2023). This also presents constraints to the ontological engineering of an ontology of cyberspace. The description of time is however not in the scope of this paper.

The paper is organized as follows: section 2 presents related work on ontologies and cyberspace. Section 3 describes the methodology used. Section 4 portrays the created core ontology and section 5 identified challenges. Section 6 presents conclusions and discusses further research directions. In the following sections ontological classes are written with a capital letter.

2. Related Work

Cyberspace can be described as a complex adaptive system (Phister, 2010) where military commanders rely on subject matter experts (SMEs) in their decision-making (Grandin, 2023). Bowman, et al. (2001), Maathuis, et al. (2018) and Mavroeidis & Bromander (2017) have highlighted the need to map the knowledge of SMEs to ontologies, so that information can be shared and to enhance the consistency of produced analytics. Bromander, et al. (2020) and Chan, et al. (2015) also highlight the need to automate and analyse cyberspace information to increase the capability of decision makers and the quality of decisions. Maathuis, et al. (2018) have developed a cyberoperations ontology that aims at bridging the gap between military professionals and cybersecurity experts

so as to enhance cyberspace operations and facilitate the use of machine learning and artificial intelligence. Their work follows the requirements for a cyber warfare ontology presented in (Dipert, 2013).

Several ontologies have been built in the cybersecurity domain. Cybersecurity ontologies and taxonomies are e.g. presented by Burger, et al. (2014), Sikos (2018), Iannacone, et al. (2015) and Mavroeidis & Bromander (2017). Martins, et al. (2020) have discussed and also compared cybersecurity ontologies. They point out that most cybersecurity operational ontologies lack a reference ontology as well as grounding in a foundational ontology. The grounded ontologies they found were all related to the CRATELO project, developed by Oltramari, et al. (2014). Takahashi & Kadobayasi (2015) have in their article presented a reference ontology, which is linked to the information flow in cybersecurity operations centres. Pai, et al. (2017) and Bowman, et al. (2001) have researched on ontologies for cyberspace situational awareness.

There are studies related to combining cybersecurity information sources and standards into complete models of most aspects of cybersecurity, such as the Situation and Threat Understanding by Correlating Contextual Observations (STUCCO) project, developed by Iannacone, et al. (2015). The Unified Cyber Ontology (UCO) project also aims at integrating cyber security and general ontologies (Syed, et al., 2016). The ontology is published on GitHub[2] and has an additional site[3] for material. It is available in the OWL language but lacks academic publications. The UCO version 1.2.0 links several cybersecurity standards and information formats, such as STIX, CVE, CCE, CVSS, CAPEC, CYBOX, KillChain and STUCCO (Syed, et al., 2016). Version 1.2.0 was released in April 2023 and contains 13 486 triples and 420 classes[4]. The top-level classes are shown in figure 1 below. The ontology *"serves as the core for the cyber domain in general"* (Babayeva, et al., 2022). UCO however lacks a link to a reference or foundational ontology and can be described as an operational domain ontology (Martins, et al., 2020). Two attempts at producing an ontology for cybersecurity that provides horizontal depth were found. The first being the ontology of the Cyber Security domain, developed on the Diamond Model of malicious activity by (Obrst, et al., 2012) and the second the earlier mentioned CRATELO ontology with three layers.

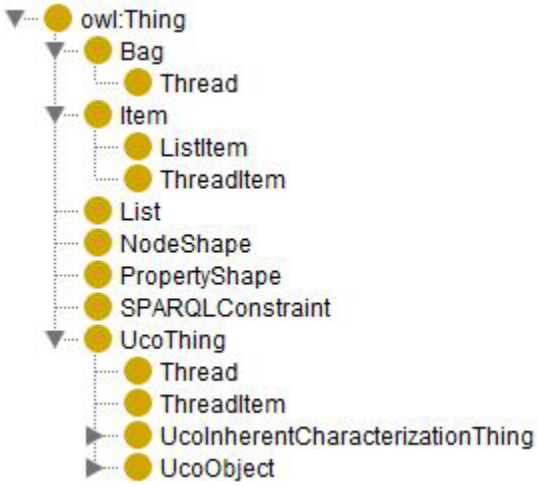

Figure 1: The top classes of UCO 1.2.0. The classes of UCO Thing and UCO Object are the core of the ontology

There are several foundational ontologies that could ground the created ontology. OWL language ontologies were included but licensed ontologies (e.g. CyC) were excluded from the alternatives. The BFO and GFO ontologies, mainly used in biomedical domains, were excluded (Mascardi, et al., 2007). According to Rudnicki, et al. (2016) DOLCE and BFO are described as small, top-level ontologies compared to SUMO and CyC. SUMO expands downwards into different domains of science (Smith & Ceusters, 2010). In the case of cyberspace, the use of a large foundational ontology could however be problematic if concepts and classes overlap. For these reasons SUMO was excluded from the alternatives. DOLCE was subsequently chosen as a fairly compact and flexible ontology. DOLCE is criticized by Smith & Ceusters (2010) because it expands beyond strict ontological realism into "possible worlds", such as mythology or fiction. This however is seen as a justification for the use of

[2] GitHub - ucoProject/UCO: This repository is for development of the Unified Cyber Ontology.

[3] Ontospy > uco-1.2.0-docs (unifiedcyberontology.org)

[4] Ontospy > uco-1.2.0-docs (unifiedcyberontology.org)

it when describing a manmade and partially metaphorical domain. The conclusion is supported by Semy, et al. (2004).

The used CRA methodology bears close resemblance to the Design Science Research (DSR) methodology, which is widely used in Information Systems Research (Piirainen & Gonzalez, 2014). The authors also present an analysis of the differences in their article (Piirainen & Gonzalez, 2014). According to the analysis, DSR and CRA have many similarities, but DSR puts more weight on supporting the design on an earlier kernel theory than CRA, which is explicitly based on a pragmatist research philosophy. Continuing, the evaluation is more extensive in DSR. The methodology of CRA as described by Lehtiranta, et al. (2015) is based on six phases. In these, (1) the problem is defined, (2) an understanding of the topic is generated, (3) a solution (model) is constructed which then is (4) demonstrated. Then the models (5) theoretical connections are presented and the (6) scope of applicability is assessed.

3. The Constructive Research Approach

The Constructive Research Approach (CRA), presented by Kasanen, et al. (1993) was refined for project management by Lehtiranta, et al. (2015). The first and the second phase of the methodology were in part concluded in an earlier paper (Grandin, 2023). The paper was also the first step in obtaining an understanding of the subject through a systematic literature review. The understanding is here further developed towards ontologies of cyberspace and cybersecurity, as well as ontology engineering. The WebProtégé tool was chosen to construct the ontology. It is a lightweight ontology editor that supports collaboration and has a user-friendly interface (Tudorache, et al., 2013).

The third step of the CRA is designing the constructs. The extensive literature review of cyberspace related ontologies was carried out using Google Scholar. In a recent systematic literature review, almost all references in this area of research were found using it (Martins, et al., 2020). The extensive literature review used the search terms “Cyberspace Ontology” and “Cybersecurity Ontology” and was extended based on the results. Results after the year 2000 were included and resulted in 53 articles that were chosen after analysis of the abstract. In the literature review no core or reference ontology of cyberspace, as defined here, was found. Instead, multiple domain ontologies incorporating either different aspects of cybersecurity or a combination of cybersecurity and decision-making or situational awareness were discovered.

Since cyberspace is metaphorical and contextual, the Descriptive Ontology for Linguistic and Cognitive Engineering (DOLCE) foundational ontology was selected as a starting point for the work. The DOLCE ontology is descriptive and has a clear cognitive bias (Masolo, et al., 2003). DOLCE is available in multiple versions. According to the homepage of the laboratory maintaining DOLCE, the OWL versions “*do not cover modality, nor temporal indexing, and include the representation of entities such as descriptions and situations which are not covered in DOLCE* “[5]. The Dolce+DnS Ultralite version (DUL)[6] was chosen for the work, as it is a simplification that also include a descriptions and situation ontology (DnS). A simplified picture of the main classes of DUL is shown in figure 2 below.

[5] Descriptive Ontology for Linguistic and Cognitive Engineering (DOLCE) – Laboratory for Applied Ontology (LOA) (cnr.it)

[6] Ontology:DOLCE+DnS Ultralite - Odp (ontologydesignpatterns.org)

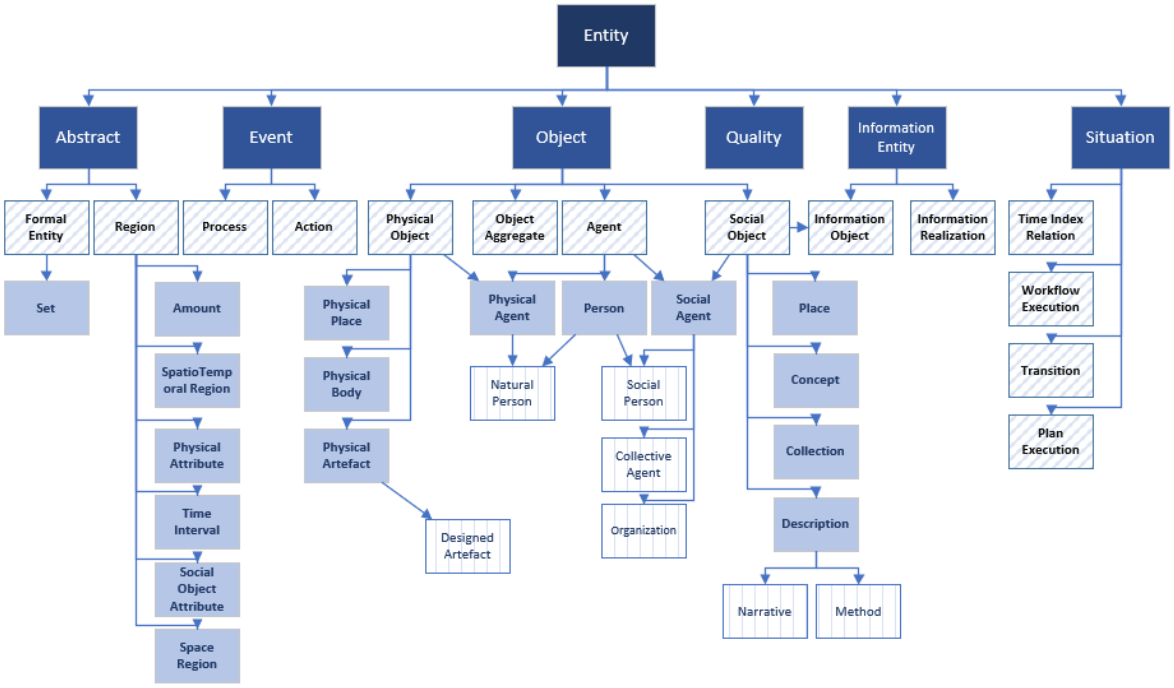

Figure 2: A simplification of the uppermost DUL classes are shown in shades of blue

The design of CoCy begun by linking the earlier mentioned six levels of cyberspace with DUL. Then the core ontology would be linked to a cybersecurity domain ontology, as proof of concept. For this, the earlier mentioned UCO ontology was chosen as a comprehensive attempt to link cybersecurity application ontologies and standards. UCOThing is the core class of the top classes presented in figure 1. The main subclasses of UCOThing are UCOInherentCharacterizationThing and UCOObject. According to the ontology documentation, the first mentioned is "*a grouping of characteristics unique to a particular inherent aspect of a UCO domain object.*". Continuing, UCOObject contains fundamental concepts of the cyber domain and functions as a base class for all content objects. The top classes of UCOThing is shown in figure 3 below.

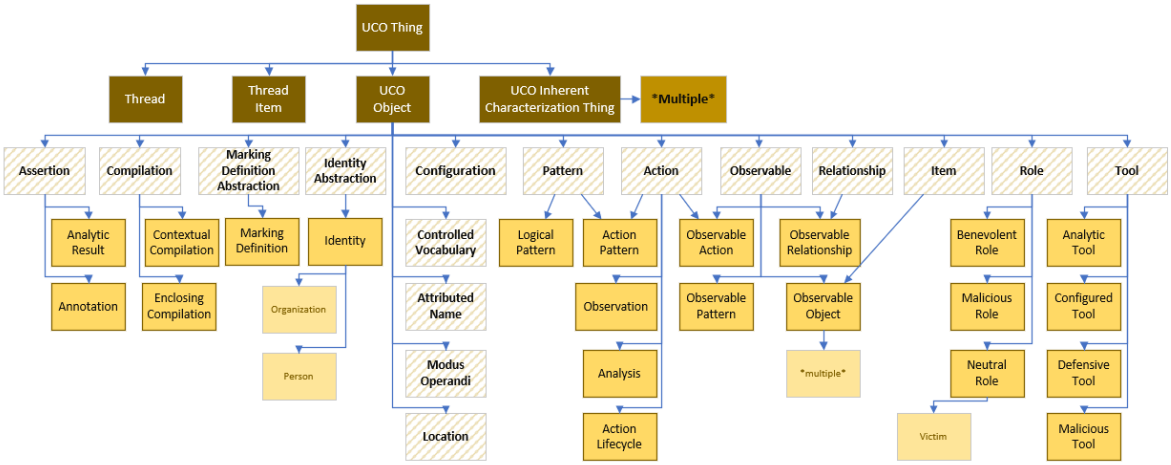

Figure 3: The subclasses of the UCOThing class, focusing on UCOObject

Since the work was identified as laborious, some restrictions were defined. Firstly, only the classes of the ontologies were to be linked and properties and relations only later. Secondly, only the UCOObject class and its subclasses was chosen as sufficient proof of concept. The work was carried out by creating the classes and the links between them in Office Visio.

4. An Ontology of Cyberspace

The six-level starting point of this paper linked DUL and partially the UCO ontologies. Cyberspace is herein seen as a digital extension of the world, and linked to DUL through the Concept class. The levels persona and

geographical information were left unlinked to Cyberspace, since the concepts were sufficiently described in DUL and would not directly benefit from a link to the Cyberspace class. CoCy was also extended in the process. Mainly, there was a need to describe information entities and action in cyberspace. This resulted in three new classes under Cyberspace, linked directly to corresponding classes in DUL. These are Action, InformationRealization and InformationObject. The following two classes from UCO were directly linked to DUL. ModusOperandi was linked to the class Method and Role to the class Narrative. These could be defined as double-linked to the class Cyberspace, but the subject needs further examination. The subclasses of the levels are still under construction but includes at the moment the most basic entities of the classes. The resulting core ontology is shown in figure 4.

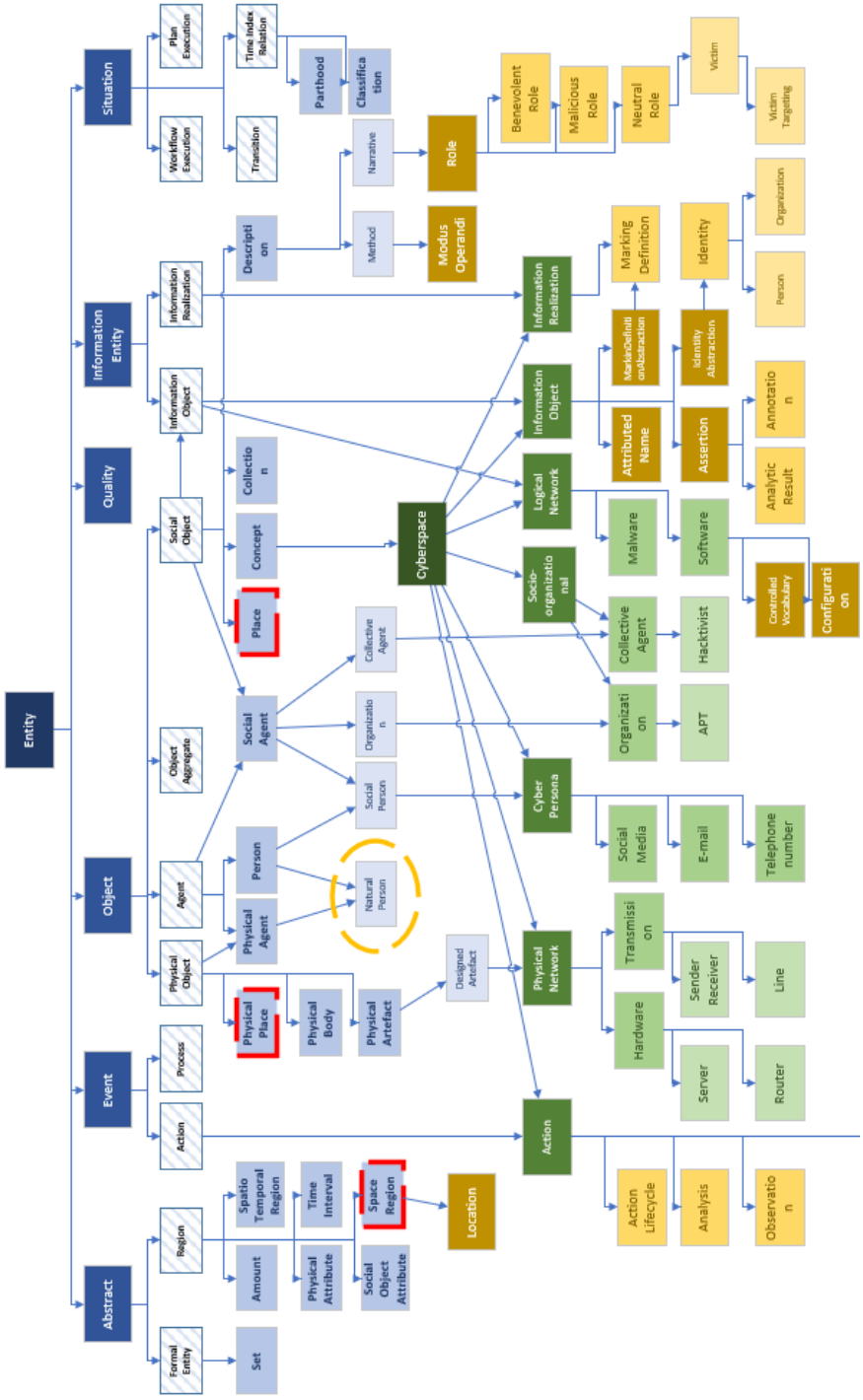

Figure 4: The ontology classes of DUL shown in blue, cyberspace in green and UCO in brown. The classes highlighted with a dashed line are the planes not directly linked to CoCy but essential to cyberspace planning

5. Challenges in Creating a Core Ontology Linking UCO to DUL

5.1 Challenges Linking CoCy to DUL

The connection between DUL and the defined levels of cyberspace encountered some challenges. Primarily the difficulties reside in the concept of cyberspace as a digital imprint of the physical world. A reference ontology (here also seen as a requirement for core ontologies) should according to Rudnicki, et al. (2016) provide all necessary nodes to support the development of lower-level ontologies. Cyberspace consist of parts that could form domain ontologies of their own, e.g. the physical network, cyber persona and the logical network. The guidelines they present are thus challenging to adhere to. E.g. in CoCy the PhysicalNetwork ends in a root node that is linked to the DUL class DesignedArtifact, CyberPersona to the DUL class SocialPerson and the LogicalNetwork to the DUL class InformationObject. To keep these linked to the core ontology, the class Cyberspace was constructed, which is a subclass of the DUL class Concept. The mentioned levels thus have two links – to the common world through the DUL class and through cyberspace relevance to the Cyberspace class. This is depicted in figure 5 below.

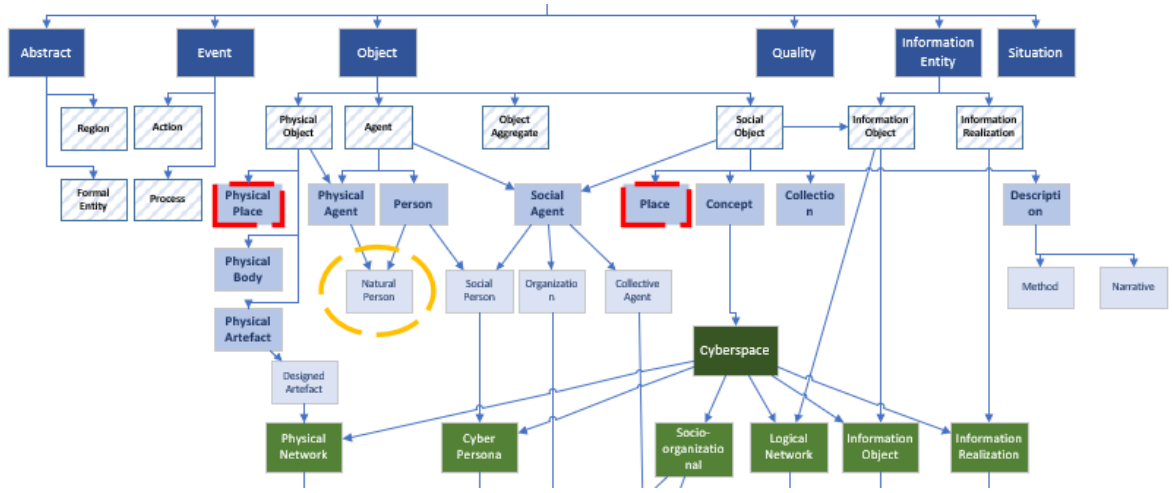

Figure 5: DUL classes are shown in shades of blue and CoCy classes in green. Geographical information and natural persons are directly linked to DUL classes marked with a dashed line. In the middle the DUL Concept subclass Cyberspace which acts as a unifying class

The created Cyberspace class denotes entities that are relevant to cyberspace. The union of the constructed subclasses and the class Cyberspace thus discards the entities that are irrelevant for the core ontology, but could otherwise be included in the description of the class (e.g. cyberspace irrelevant organizations).

Most DUL classes have a digital coupling which make them relevant for CoCy. For instance, the geographical plane (1) and the persona plane (6), are essential for operational planning regarding cyberspace. It is worth noting that these, as defined here, lack a link to the Cyberspace class. These levels present information that exist independently of cyberspace and are thus directly defined by DUL classes. Human persons are thus linked to the class NaturalPerson in DUL and geographical information to classes AbstractRegion, PhysicalPlace and Place in DUL. These can also be regarded as extensions of the "core" of cyberspace, defined in planes (2) to (5). In for instance a wartime situation a military commander needs the information how an attack through cyberspace is linked to physical assets and persons to determine the best course of action. As such, the information presented to a decision maker should include the options to engage either the geographical or persona planes if assessed efficient. The importance of this information is for instance exemplified in Michel & King (2019). Another use case is identifying and apprehending cybercriminals or to prevent cybercrime. The link between the geographical plane and DUL and also physical persons is depicted in figure 6 below. As seen, the core ontology would be difficult to link to a single root node and still be grounded in the DUL foundational ontology. Hence, CoCy is a conceptual extension of DUL and will contain all of DUL and also the extensions of cyberspace classes.

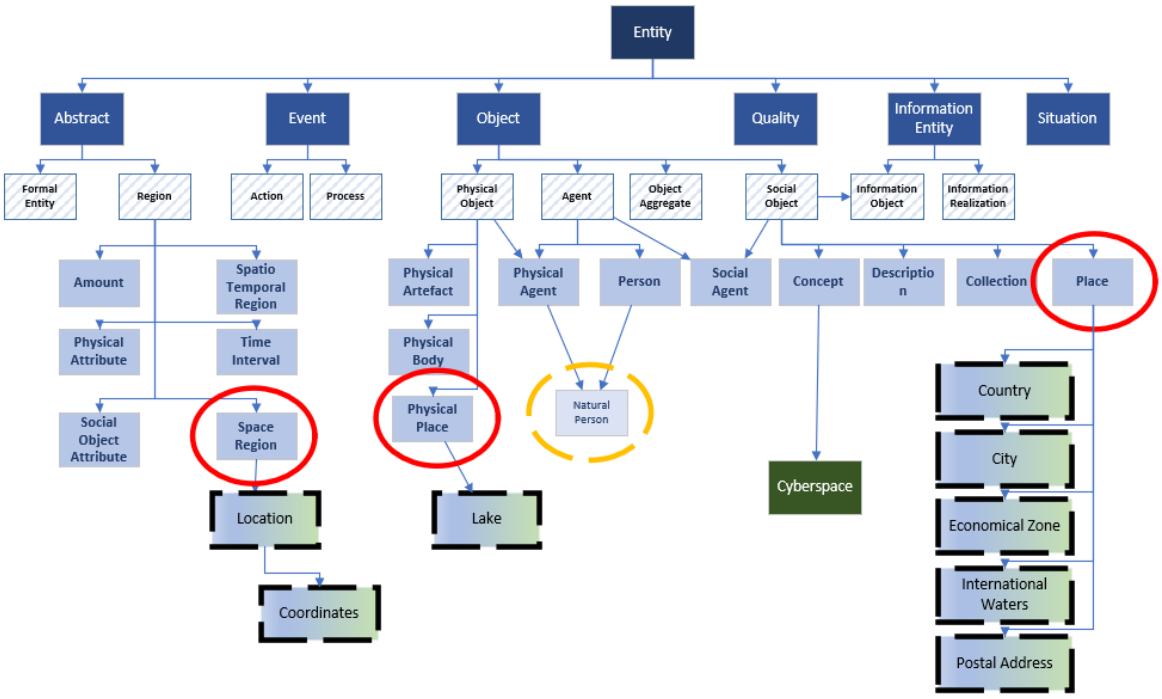

Figure 6: A simplified picture of the classes that are relevant, but not linked to the created Cyberspace class. Geographical information exists in the DUL classes highlighted with a red ellipse. Preliminary sub-classes are highlighted with a dashed black line. Natural persons are grouped under the DUL class Natural person, highlighted with a yellow dashed ellipse

5.2 Challenges Linking CoCY to UCO

Early on, it became clear how the construction of CoCy and UCO differed. DUL and CoCy are created top-down as where the UCO is a compilation of several existing taxonomies, information exchange and categorization standards, and constructed bottom-up. UCO also showed to be constructed mainly according to the concept of combining similar entities into classes with a (cybersecurity) technical point of view and not according to the ontological realism of a foundational ontology. For instance, the UCOObject subclass ObservableObject includes a large variety of cybersecurity related characteristics, such as software, information, devices etc. as shown in figure 7 below. The class is in the documentation described as "*a grouping of characteristics unique to a distinct article or unit within the digital domain*.".

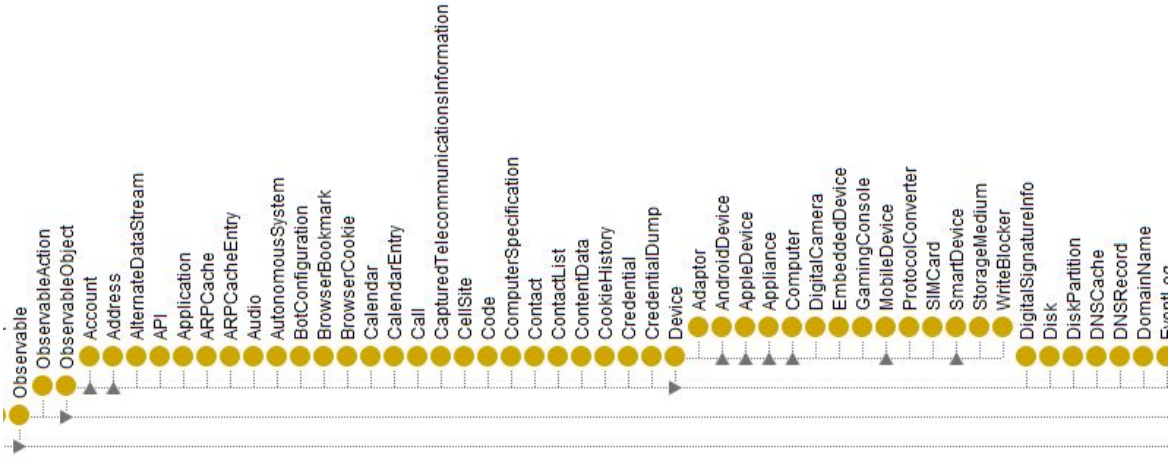

Figure 7: A part of the subclasses of the UCO ObservableObject class, showing information, devices and accounts etc.

These would in DUL be subclasses of InformationRealization, InformationObject, DesignedArtefact or SocialPerson (accounts) etc. While many of the classes of UCO are possible to link either directly to DUL or CoCy classes, the above-mentioned class presents a challenge. In essence, it would be practical if the

ObservableObject class of UCO would be divided into multiple classes that differentiated between the different physical aspects of the sub-classes. Another problematic example are classes including hardware and software components, such as the subclass Tool, which include instances of as well InformationRealization, InformationObject and DesignedArtefact. The upper level classes from UCO that were unsuccessfully linked are shown in figure 8 below.

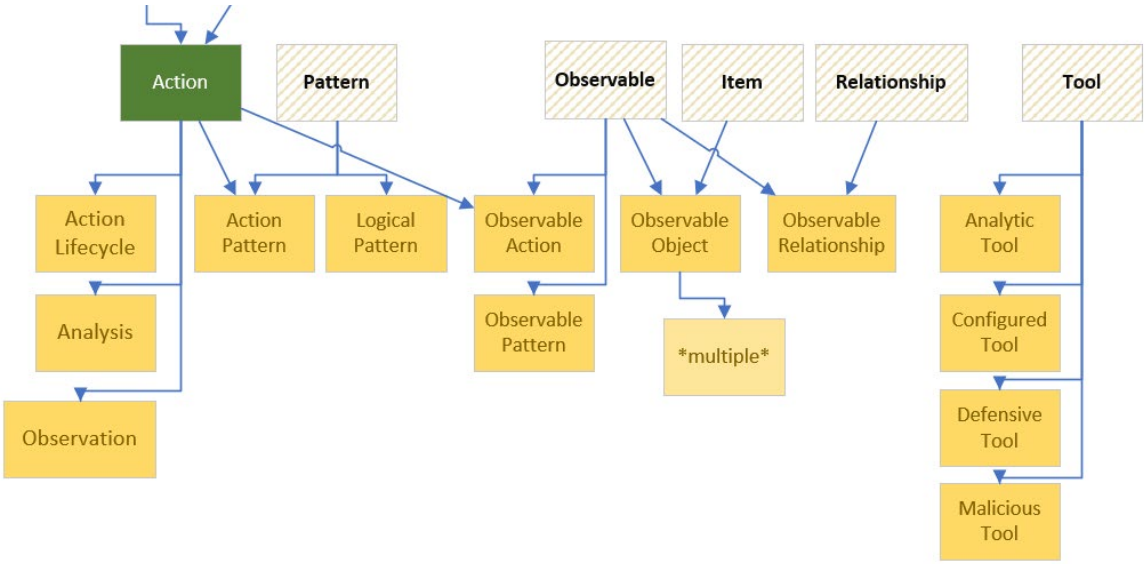

Figure 8: The classes of UCO that were unsuccessfully linked to either DUL or CoCy are shown in brown. The CoCy class Action is included to depict interconnections

The linking of CoCy to UCO also revealed important aspects of cyberspace undefined by the original six planes of cyberspace, namely information (entities) and actions. These were included in CoCy. Cyberspace-related information is linked to the class Cyberspace and either to the general DUL InformationObject and InformationRealization classes.

6. Conclusions

This paper presents the ongoing work of constructing a core ontology for cyberspace called CoCy. The domain lacks a unifying core ontology, and this paper has demonstrated that such an ontology can be constructed, grounded to a foundational ontology. Since cyberspace is a domain that imbues the world we live in, and as such consists of multiple sub-domains, the core ontology was created as an extension of the DUL foundational ontology. The starting point of the work, which was a model of cyberspace consisting of six different planes, evolved by excluding the periphery levels persona and geographical information. The exclusion was done by linking this information directly to DUL. The model was extended by including classes of action and information. Due to the fundamental differences of the foundational ontology and the chosen proof of concept (the Unified Cyber Ontology UCO), some classes were unsuccessfully mapped to the core ontology. These difficulties are however manageable, but requires further research.

The proposed solution in form of an extension of DUL needs further research on its feasibility. Also, the introduction of the class Cyberspace should be further investigated. The work on writing the proposed core ontology in OWL using WebProtégé, continues. As such, research adhering to the chosen methodology still needs to 1) be demonstrated, 2) present theoretical connections and finally, 3) continue by assessing the scope of applicability. The work with linking CoCy to UCO however validated the need for a flexible core ontology for cyberspace, grounded in a foundational ontology.

References

Asquith, P. & Morgan, P., 2020. Representing a Human-Centric Cyberspace. In: I. Corradini, E. Nardelli & T. Ahram, eds. *Advances in Human Factors in Cybersecurity, Advances in Intelligent Systems and Computing, vol 1219.* Cham: Springer, pp. 122-128.

Babayeva, G., Maennel, K. & Maennel, O. M., 2022. *Building an Ontology for Cyber Defence Exercises.* Genoa, IEEE, pp. 423-432.

Bowman, M., Lopez, A. & Tecuci, G., 2001. *Ontology Development for Military Applications.* New York, ACM Press.

Bromander, S. et al., 2020. Modeling Cyber Threat Intelligence. *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020),* pp. 273-280.

Burger, E. W., Goodman, M. D., Kampanakis, P. & Zhu, K. A., 2014. *Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies.* New York, Association for Computing Machinery, pp. 51-60.

Chan, P., Theron, J., van Heerden, R. & Leenen, L., 2015. *An ontological knowledge base for cyber network attack planning.* Kruger National Park, South Africa, Academic Conferences Limited, pp. 69-77.

Dipert, R. R., 2013. The essential features of an ontology for cyberwarfare. In: *Conflict and Cooperation in Cyberspace : The Challenge to National Security.* Boca Raton: CRC Press, pp. 35-48.

Grandin, A., 2023. *Cyber Geography and Cyber Terrain: Challenges producing a universal map of Cyberspace.* Reading, UK, Academic Conferences International Limited, pp. 207-213.

Grant, T. J., 2014. Formalized Ontology for Representing C2 Systems as Layered Networks. In: T. J. Grant, R. H. P. Janssen & H. Monsuur, eds. *Network Topology in Command and Control: Organization, Operation, and Evolution.* s.l.:IGI Global, pp. 85-124.

Huntley, W. L., 2016. *Cyber Key Terrain: A Conceptual Assessment,* s.l.: U.S. Naval Postgraduate School.

Iannacone, M. et al., 2015. *Developing an Ontology for Cyber Security Knowledge Graphs.* New York, Association for Computing Machinery, pp. 1-4.

Joint Chiefs of Staff, 2018. *Joint publication 3-12, Cyberspace Operations,* Washington DC: Joint Chiefs of Staff.

Kasanen, E., Lukka, K. & Siitonen, A., 1993. The constructive approach in management accounting research. *Journal of Management Accounting Research,* pp. 243-264.

Kreuzer, M. P., 2021. *Cyberspace is an analogy, not a domain: Rethinking domains and layers of warfare for the information age.,* s.l.: The Strategy Bridge.

Lehtiranta, L., Junnonen, J.-M., Kärnä, S. & Pekuri, L., 2015. The Constructive Approach: Problem Solving for Complex Projects. In: *Designs, Methods and Practices for Research of Project Management.* s.l.:Gower Applied Business Research, pp. 95-106.

Maathuis, C., Pieters, W. & van den Berg, J., 2018. Developing a Cyber Operations Computational Ontology. *Journal of Information Warfare , Vol. 17, No. 3,* pp. 32-49.

Martins, B. F. et al., 2022. A framework for conceptual characterization of ontologies and its application in the cybersecurity domain. *Software and Systems Modeling volume 21,* pp. 1437-1464.

Martins, B. et al., 2020. *Conceptual Characterization of Cybersecurity Ontologies.* s.l., Springer, pp. 323-338.

Mascardi, V., Cordì, V. & Rosso, P., 2007. *A Comparison of Upper Ontologies,* s.l.: Workshop From Objects to Agents.

Masolo, C. et al., 2003. *Wonderweb deliverable d18: Ontology library,* s.l.: Laboratory for Applied Ontology, ISTC-CNR.

Matheus, C. J. & Ulicny, B., 2007. *On the Automated Generation of an OWL Ontology based on the Joint C3 Information Exchange Data Model.* s.l., s.n., pp. 1-19.

Mavroeidis, V. & Bromander, S., 2017. *Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies.* s.l., IEEE, pp. 91-98.

Michel, M. C. K. & King, M. C., 2019. *The Future of Cyber Analytics: Identity Classification for Systematic and Predictive Insight.* Oxford, UK, IEEE, pp. 1-4.

Morosoff, P. et al., 2015. *Joint Doctrine Ontology: A Benchmark for Military Information Systems Interoperability..* s.l., CEUR-WS, pp. 2-9.

Möller, D. P. F., 2020. Cybersecurity Ontology. In: *Cybersecurity in Digital Transformation : Scope and Applications.* Cham, Switzerland: Springer, pp. 99-109.

NATO, 2020. *Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations,* s.l.: NATO STANDARDIZATION OFFICE (NSO) .

Obrst, L., Chase, P. & Markeloff, R., 2012. *Developing an Ontology of the Cyber Security Domain..* s.l., CEUR-WS, pp. 49-56.

Oltramari, A., Cranor, L. F., Walls, R. J. & McDaniel, P. D., 2014. Building an Ontology of Cyber Security. *Semantic Technologies for Intelligence, Defense, and Security,* pp. 54-61.

Pai, F.-P., Yang, L.-J. & Chung, Y.-C., 2017. Multi-layer ontology based information fusion for situation awareness. *Applied Intelligence 46,* pp. 285-307.

Phister, P. W., 2010. Cyberspace: The Ultimate Complex Adaptive System. *The International C2 Journal | Vol 4, No 2,* pp. 1-25.

Piirainen, K. A. & Gonzalez, R. A., 2014. Constructive Synergy in Design Science Research: A Comparative Analysis of Design Science Research and the Constructive Research Approach. In: *Liiketaloudellinen aikakauskirja LTA - Finnish Journal of Business Economics.* s.l.:Liiketaloustieteellinen Yhdistys ry, pp. 206-234.

Rudnicki, R., Smith, B., Malyuta, T. & Mandrick, W., 2016. *Best Practices of Ontology Development,* s.l.: NIST.

Semy, S. K., Pulvermacher, M. K. & Obrst, L. J., 2004. *Toward the Use of an Upper Ontology for U.S. Government and U.S. Military Domains: An Evaluation,* Bedfod, Massachusetts: MITRE.

Sikos, L. F., 2018. OWL Ontologies in Cybersecurity: Conceptual Modelling of Cyber-Knowledge. In: *AI in Cybersecurity.* Cham, Switzerland: Springer, pp. 1-17.

Sikos, L. F., 2023. Cybersecurity knowledge graphs. *Knowledge and Information Systems 65,* p. 3511–3531.

Smith, B. & Ceusters, W., 2010. Ontological realism: A methodology for coordinated evolution of scientific ontologies. *Applied Ontology, vol. 5, no. 3-4,* pp. 139-188.

Syed, Z. et al., 2016. *UCO: A Unified Cybersecurity Ontology.* Baltimore, University of Maryland, Baltimore County.

Takahashi, T. & Kadobayasi, Y., 2015. Reference ontology for cybersecurity operational information. *The Computer Journal vol. 58 no.10,* pp. 2297-2312.

Tudorache, T., Nyulas, C., Noy, N. F. & Musen, M. A., 2013. WebProtégé: A collaborative ontology editor and knowledge acquisition tool for the web. *Semantic web, 4(1),* pp. 89-99.

van Heerden, R. C. P., Leenen, L. & Theron, J., 2016. *Using an Ontology for Network Attack Planning.* s.l., IGI Global, pp. 65-78.