Formal Ontology in Information Systems
N. Aussenac-Gilles et al. (Eds.)

doi:10.3233/FAIA231138

Boosting D3FEND: Ontological Analysis and Recommendations

Ítalo OLIVEIRA [a,1], Gal ENGELBERG [b], Pedro Paulo F. BARCELOS [a], Tiago Prince SALES [c], Mattia FUMAGALLI [a], Riccardo BARATELLA [a], Dan KLEIN [b], and Giancarlo GUIZZARDI [c],

[a] *Conceptual and Cognitive Modeling Research Group (CORE),*
Free University of Bozen-Bolzano, Bolzano, Italy
[b] *Accenture Israel Cyber R&D Lab, Tel Aviv, Israel*
[c] *Semantics, Cybersecurity & Services (SCS),*
University of Twente, Enschede, The Netherlands

Abstract. Formal Ontology is a discipline whose business is to develop formal theories about general aspects of reality such as identity, dependence, parthood, truthmaking, causality, etc. A foundational ontology is a specific consistent set of these ontological theories that support activities such as domain analysis, conceptual clarification, and meaning negotiation. A (well-founded) core ontology specifies, under a foundational ontology, the central concepts and relations of a given domain. Foundational and core ontologies can be seen as ontology engineering frameworks to systematically address the laborious task of building large (more specific) domain ontologies. However, both in research and industry, it is common that ontologies as computational artifacts are built without the aid of any framework of this kind, often yielding modeling mistakes and representation gaps. In this paper, we analyze a case in the domain of cybersecurity, namely, the case of D3FEND - an OWL knowledge graph of cybersecurity countermeasure techniques proposed by the MITRE Corporation. Based on the *Reference Ontology for Security Engineering* (ROSE), a core ontology of the security domain founded in the *Unified Foundational Ontology* (UFO), our investigation reveals a number of semantic issues and opportunities for improvement in D3FEND, including missing concepts, semantic overload of terms, and lacking constraints that cause an under-specification of the model. As a result of our ontological analysis, we propose several suggestions for the appropriate redesign of D3FEND to overcome those issues.

Keywords. D3FEND, Cybersecurity, (Cyber)Security ontologies, Ontological analysis and engineering, Knowledge Graph

1. Introduction

In any field, as the complexity of the domain grows, there is a need of standardizing the interpretation of domain notions for both human communication and machine inferencing. Taxonomies offer a first step in this direction listing classes of things that are subsumed under certain categories. Ontologies as computational artifacts represent a network of concepts, relations, and constraints pertaining to the domain at hand.

[1] Corresponding Author: Ítalo Oliveira, idasilvaoliveira@unibz.it

In contrast, in philosophy, Formal Ontology is a discipline that aims to develop formal theories about general aspects of reality, including the definition of identity, properties, dependence, part-whole relation, causality, events, etc. A foundational (top-level or upper) ontology is a specific consistent set of these ontological theories, capable of providing support to the tasks of domain analysis, conceptual clarification, and meaning negotiation — that are crucial when one has to build an ontology as a computational artifact [1]. Indeed, top-level ontologies help with the development of high-quality core and domain ontologies, improving their consistency and interoperability [2]. A (well-founded) core ontology specifies, under a foundational ontology, the central concepts and relations of a given domain (e.g., Risk, Value, Trust, Security, etc.). Upper ontologies effectively contribute to detecting and preventing ontology design mistakes [3], enhancing the quality and interoperability of domain and core ontologies [4]. To make an analogy, foundational ontologies, and reference domain ontologies work as *ontology engineering frameworks*, by accelerating and improving the practice of ontology engineering, just like web development frameworks (e.g., React, Angular, Django, etc.) accelerate and improve the practice of web development. Nevertheless, surprisingly, both in research and industry, ontologies as computational artifacts are very often built without the aid of any framework of this kind [5,6], favoring recurrent modeling mistakes and gaps.

In this paper, we dive into the domain of security as a particular case study. In this domain, the need for ontology development was already acknowledged two decades ago by [7], while a recent systematic mapping study of the literature has revealed the limitations of the current security ontologies [5]. In particular, this latter study shows that foundational ontologies are seldom used in the practice of engineering these artifacts. More specifically, in cybersecurity, the situation is not different, as shown by [8,6]. In this domain, an artifact that stands out by its increasing popularity among practitioners and scholars is D3FEND. It is a novel knowledge graph of cybersecurity countermeasure techniques proposed by the MITRE Corporation [9], which aggregates a catalog of defensive cybersecurity techniques and their relationships to offensive techniques. D3FEND's primary goal is to help to standardize the vocabulary used to describe defensive cybersecurity technology functionality. A number of recent cybersecurity studies make use of it for the process of identification and assessment of cyber threats, and response against them [10,11,12,13,14], among other applications, including the design of a game to support security education and risk assessment [15]. D3FEND is also an example of an ontology developed without an explicit tie to an upper ontology, and to the best of our knowledge, there is no systemic ontological analysis of this artifact, whose validity seems to be taken for granted. The combination of these factors makes D3FEND an interesting target for our analysis.

Based on the *Reference Ontology for Security Engineering* (ROSE) [16], a core ontology of the security domain founded in the *Unified Foundational Ontology* (UFO) [17,18], we proceed with an ontological analysis of the conceptual model behind D3FEND, revealing several semantic issues and opportunities for improvement that could be addressed by relying on a foundational ontology as support. In particular, our analysis identifies cases of *semantic overload*, *missing concepts*, and a *systematic lack of constraints*. Under the assumptions of UFO and ROSE, we also suggest how the issues identified can be solved, thus contributing to improving D3FEND accordingly. The implications of our analysis make a case in favor of employing foundational and reference ontologies in ontology engineering practice, as captured by Varzi's dictum "No ontology without Ontology" [19]. Through this work, we expect to contribute to the development of the ontology engineering practice in cybersecurity, in general, and the D3FEND project, in particular.

The remainder of this paper is structured as follows: section 2 briefly presents the background of our work, namely, D3FEND, UFO, and ROSE. Our exposition of UFO and ROSE is limited to what is necessary to support our analysis; section 3 presents the ontological analysis of D3FEND. In doing that, we identify both general semantic issues of its conceptual model as exposed by UFO, as well as domain-specific issues regarding its conceptualization of security, according to ROSE. In that same section, we indicate a number of concrete opportunities for improving D3FEND according to our frameworks and analysis; section 4 concludes the paper by presenting some final considerations.

2. Background

2.1. The D3FEND knowledge graph of cybersecurity countermeasures

Given the necessity of specifying cybersecurity countermeasures and capabilities, a team at the MITRE Corporation has built D3FEND [9] (which stands for "Detection, Denial, and Disruption Framework Empowering Network Defense")[2]. The motivation is that practitioners should know not only what threats a capability claims to address, but also how exactly these threats are addressed from a security architecture and engineering viewpoint, and under what conditions a solution would work. This is particularly important, for example, to inform acquisitions and investigations in cybersecurity.

D3FEND is an OWL specification representing types and relations that aim to define both the central concepts in the cybersecurity countermeasure domain and the relations necessary to connect those concepts to each other. The process of construction of D3FEND has followed a *bottom-up approach*, by surveying patents from U.S. Patent Office, existing knowledge bases (MITRE Cyber Analytic Repository, ATT&CK knowledge base), and other data sources (academic papers, technical specifications, and publicly available product technical documentation) [9]. The creators of D3FEND have made a deliberate choice to defer alignment to a foundational or reference ontology in a *top-down approach*[3].

A cybersecurity countermeasure is understood as "any process or technology developed to negate or offset offensive cyber activities" [9]. D3FEND is intended to provide not only an understanding of what a countermeasure does but also how it does what it does. D3FEND does not prescribe specific countermeasures, nor does it evaluate their effectiveness and priority. However, by standardizing the vocabulary of cybersecurity countermeasures, D3FEND may support these activities. The primary audience of D3FEND is security systems architecture experts and technical executives who make acquisition or investment decisions.

[2] The D3FEND official website is https://d3fend.mitre.org/. Here is MITRE's announcement of D3FEND: https://www.mitre.org/news-insights/impact-story/mitres-d3fend-connects-cyber-community-counter-threats.

[3] Personal communication with Peter Kaloroumakis and others directly involved in the creation of D3FEND (in the D3FEND Slack channel).

The fundamental idea of the D3FEND model involves relating OFFENSIVE TECHNIQUES, taken from a portion of MITRE's ATT&CK framework[4], and DEFENSIVE TECHNIQUES through DIGITAL ARTIFACTS. By using OWL and SPARQL reasoning services, D3FEND is able to show which DEFENSIVE TECHNIQUES somehow counter which OFFENSIVE TECHNIQUES due to the mediation of DIGITAL ARTIFACTS with which they are both *associated*. This also defines the scope of D3FEND since it does not include administrative and supportive countermeasure functionalities, but only those that directly counter adversary behavior. Moreover, any measure that is not directly related to DIGITAL ARTIFACTS is not under D3FEND's scope. For instance, a strong password policy is in its scope because it directly affects an organization's technology configuration baseline, thus it involves digital artifacts. In contrast, investments in employee cybersecurity awareness through training programs do not directly interact with DIGITAL ARTIFACTS, so this kind of measure is outside D3FEND's scope. [9]

Whereas the ATT&CK framework [20] deals with adversary behavior via OFFENSIVE TECHNIQUES organized by the tactical objectives they support (OFFENSIVE TACTIC), D3FEND deals with DEFENSIVE TECHNIQUES organized by the tactical objectives they support (DEFENSIVE TACTIC). DIGITAL ARTIFACTS are in-between, being affected by both offensive and defensive techniques. TACTICS represent "the what" of an action, a defensive or offensive goal to be achieved by the means of TECHNIQUES ("the how"), which *enable* the TACTICS. OFFENSIVE TACTICS subsume COLLECTION, COMMAND AND CONTROL, CREDENTIAL ACCESS, EXECUTION, among others. DEFENSIVE TACTICS subsume DECEIVE, EVICT, DETECT, HARDEN, among others. None of these lists are intended to be exhaustive. Finally, events are introduced by the concept DIGITAL EVENT, but it is still a work in progress with a minor role in D3FEND's main use cases.

2.2. The Unified Foundational Ontology

UFO is a domain-independent axiomatic theory developed to contribute to the foundations of Conceptual Modeling [17,18]. It is one of the most used foundational ontologies in conceptual modeling [21], and it has been successfully employed in many projects in different countries, by academic, government, and industrial institutions in the development of core and domain ontologies in different domains (e.g., Trust, legal relations and Constitutional Law, Risk and Value, Service, Software Requirements and Anomalies, Discrete Event Simulation, etc.)[17].

UFO makes a distinction between TYPE (Universal) and INDIVIDUAL. One thing is the specific (individual) John's cup of tea; another thing is a cup of tea as a type of object, which may have subtypes, such as an ornamented cup of tea, a metal cup of tea, etc. Types and individuals are disjoint, and whatever exists, according to UFO, is either a type or an individual. Individuals are instances of at least one type, so there is a mirroring of the taxonomy of individuals over the type level (for example, events are instances of types of events). In UFO, individuals are classified as either ABSTRACT INDIVIDUAL (specific numbers, sets, propositions) or CONCRETE INDIVIDUAL (the ones that exist in space-time). The latter branch is divided into EVENTS, SITUATIONS (roughly, individual state of affairs), OBJECTS, and ASPECTS (DISPOSITIONS and QUALITIES). The categories of

[4] MITRE ATT&CK is a knowledge base of adversary tactics and techniques based on real-world observations. Here is its official website: https://attack.mitre.org/.

EVENT and ENDURANT are disjoint (say, a party should not be confused with the people that participate in it). Figure 1 summarizes this taxonomy through a UML Class diagram.

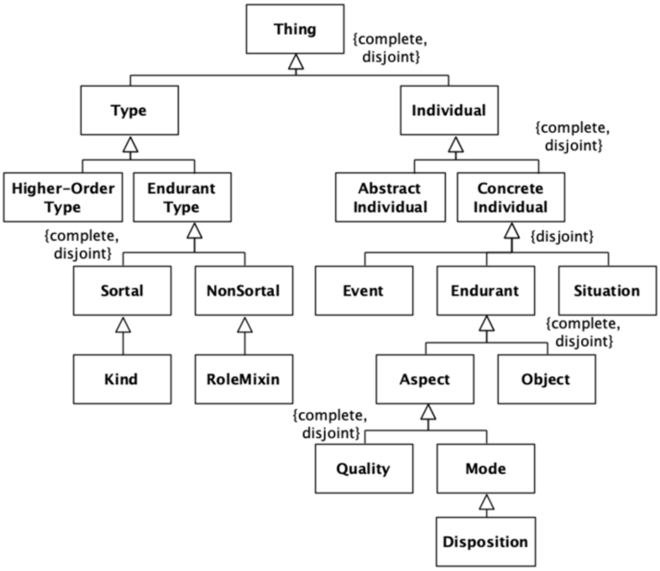

Figure 1. A partial representation of UFO's taxonomy, adapted from [18].

In UFO, events represent changes from one situation to another due to the manifestation of objects' dispositions (e.g., capabilities, liabilities, vulnerabilities, etc.) [22,23]. This creates the following pattern: certain situations activate certain dispositions, which are manifested by events wherein objects (the bearers of those dispositions) participate, leading to new situations. In this case, it is said that a situation triggers an event, which brings about another situation. For example, antivirus software has capabilities to search, detect, and remove viruses. Under the right settings, after detecting a virus, this software removes it from the device. This removal is an event of manifestation of the software's capabilities, and it brings about a new situation where the virus is not present in the device anymore. Figure 2 condenses this modeling pattern[5].

These patterns are useful from an engineering viewpoint because they help the modeler to understand and represent the domain of interest by specializing them into more specific concepts and relations. By doing so, it is possible to build larger ontologies by systematically reusing and combining these micro-theoretical fragments [24]. OntoUML [17] is a UFO-based modeling language defined as a pattern grammar [25], i.e., as a language that supports the creation of models by the iterative instantiation of ontology design patterns, each of which represents a UFO micro-theory. In the remainder of this paper, we use OntoUML for presenting the ROSE core ontology as well as for supporting the analysis of D3FEND.

[5] For a full formalization of UFO-B–the UFO fragment dealing with perdurants–one should refer to [22].

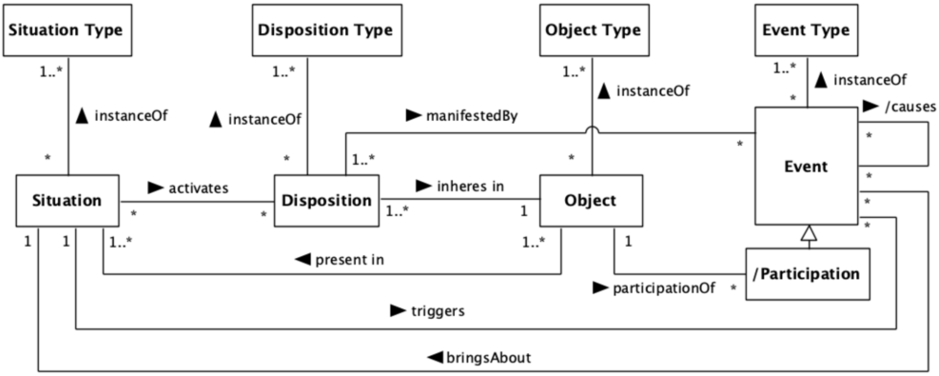

Figure 2. A partial representation of UFO-B modeling pattern [22], expressed by a UML Class diagram

2.3. The Reference Ontology for Security Engineering

ROSE [16] describes the general entities and relations of the security engineering domain, making use of an adapted version of Common Ontology of Value and Risk (COVER) to capture the value and risk-related notions[6]. ROSE understands the domain of security as the *intersection* between the domain of value and risk, understood under the terms of the COVER [26], and the dispositional theory of prevention presented in [23]. The latter extends UFO to explain how certain types of events are prevented or interrupted due to the occurrence of other events of certain types. From this perspective, an SECURITY MECHANISM is an OBJECT (of any kind) that creates value by protecting certain INTENTIONS from RISK EVENTS.

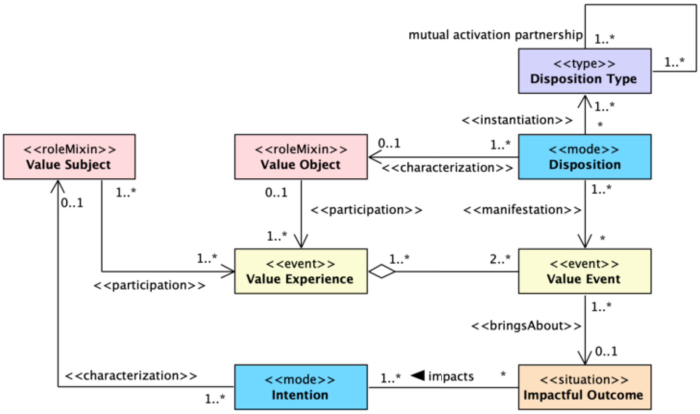

Figure 3. Value Experience, adapted from [26,16].

In COVER[7], whose fragment is depicted in Figure 3, value is a relational mode that emerges from the relations between the capacities (DISPOSITIONS) of certain objects

[6] Files related to ROSE can be found in the following public repository: https://github.com/unibz-core/security-ontology.

[7] The OntoUML stereotype connects types and relations in these models to ontological categories of monadic and relational universals in UFO, respectively. For their ontological justification and semantics, one should

and the Intentions of an Agent. The manifestations of these capacities are Events that *bring about* a Situation that *impacts* or satisfies the Intention of a given Agent (a Value Subject)–in UFC-C, a goal is understood as the propositional content of an Intention [27], which is an internal commitment that inheres in an Agent, which specializes Object. Risk is the anti-value: Risk Events are the manifestations of certain Dispositions (namely, Threat Capabilities and Vulnerabilities), and, sometimes, Intentions that inhere in an Agent; these Events *bring about* a Situation that *hurts* the Intention of a given Agent (a Risk Subject), as shown by Figure 4. Analogous to value, security (Figure 5) is also a relational mode that emerges from the relations between the (control) capabilities of Objects and the Intentions of an Agent, particularly a Protected Subject; however, manifestations of these capabilities *bring about* a Situation that *impacts* the Intention of an Agent in a very specific way: *preventing* Risk events [16].

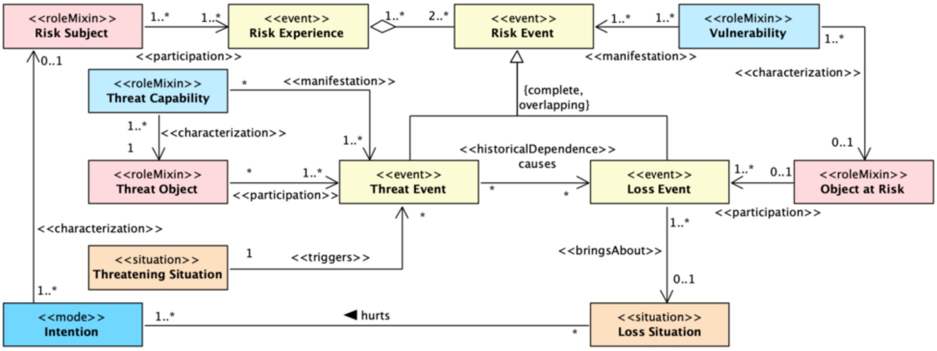

Figure 4. Risk Experience, adapted from [26,16]

Using the prevention theory described in [23], ROSE understands that Threat Capability, Vulnerability, and, sometimes, Intention are dispositions associated with types whose instances maintain a *mutual activation partnership* [28] to each other[8]. This means that a Threat Object can only manifest its Threat Capability if a Vulnerability can be exploited; if the Threat Object participates in an Attack (an Action, an intentional Event), then the Intention is also required. Analogously, a Vulnerability is only manifested in the presence of a Threat Capability. From a security point of view, the importance of this *generic dependence* relation among these entities is that it determines multiple ways by which security measures can work: the removal of any of them from the situation that could activate them all together implies the prevention of the associated Risk Event. In general, mutual activation partners compose the conditions of activation of any Disposition, as shown by Figure 3.

A Security Mechanism is always designed by an Agent called the Security Designer to be a *countermeasure to* events of a certain type (Risk Event Type)

refer to [18]. Moreover, the colors in these diagrams represent a color convention used by the OntoUML community: object types are represented in pink, intrinsic aspect types in blue, situation types in orange, event types in yellow, and higher-order types in darker blue.

[8] For simplicity, the diagram of Figure 4 omits the mutual activation partnership relations between Threat Capability Type, Vulnerability Type, and Intention Type but Figure 3 clearly states that types of dispositions hold that relationship with each other.

[23,16]. When an OBJECT is made to be a countermeasure to certain types of events, it aggregates capabilities whose manifestations ultimately prevent these EVENT TYPES in a systematic fashion. The AGENT creating a SECURITY MECHANISM is not necessarily the one protected by its proper functioning, i.e., the PROTECTED SUBJECT. However, both agents have INTENTIONS that are positively impacted by this proper functioning. For example, the government designs policies for public safety, and the functioning of such policies satisfies some goals the government had when designing them but also satisfies the goal of people who want to be safe. Sometimes, the PROTECTED SUBJECT is the same AGENT as the SECURITY DESIGNER, such as when a person places an electric fence surrounding their own house.

As shown in Figure 5, a SECURITY MECHANISM is an OBJECT, which may be a simple physical object like a wall, a high-tech air defense system like the Israeli Iron Dome, an AGENT like a policeman, a social entity like a security standard or anti-COVID-19 rules, that bears capabilities called CONTROL CAPABILITIES. The manifestation of this kind of capability is a CONTROL EVENT, which may come in a form of a chain of events that ultimately causes the CONTROL EVENT. The CONTROL EVENT is of a type (CONTROL EVENT TYPE) that prevents, directly or indirectly, events of a certain type (RISK EVENT TYPE). This is so because the CONTROL EVENTS bring about a CONTROLLED SITUATION, which is of a type that is *incompatible with* the types of SITUATIONS (RISK TRIGGER TYPE) that trigger RISK EVENTS of certain types.

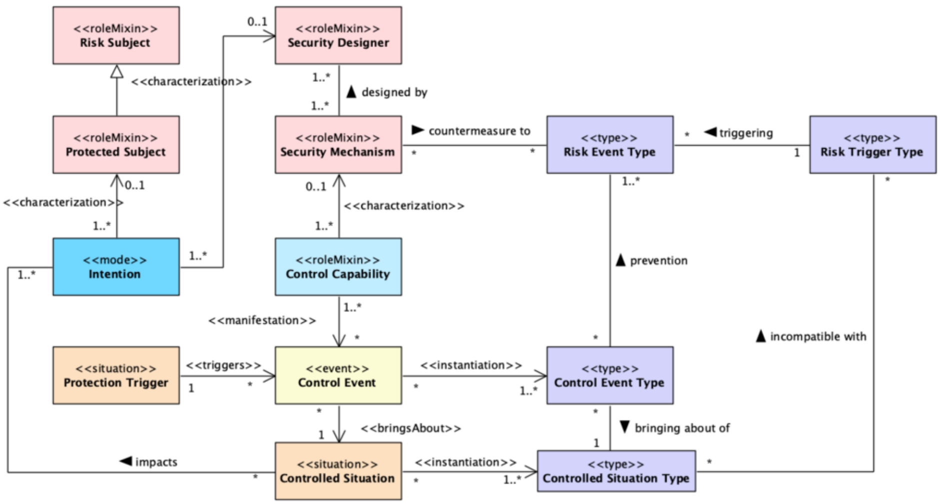

Figure 5. Security Mechanism, adapted from [16]

3. Ontological analysis and recommendations for the D3FEND knowledge graph

In [29], an ontological analysis framework is described. The general idea is to compare two ontologies (as descriptions of a domain), assuming one is the reference to assess the other. Notice, however, that as shown by [30], this sort of analysis is more than a matter of direct comparison between the actual structures of these models; it is a matter of reconstructing the underlying intended conceptualizations of these models, i.e., about making their ontological assumptions explicit. Here, UFO and ROSE are our references to analyze D3FEND. Specifically, three recurrent semantic deficiencies of D3FEND will be demonstrated in the sequel, namely: (a) *ontological incompleteness*, when there is an element in the reference ontology that finds no representation in the evaluated ontology; (b) *construct overload*, when two disjoint notions in the reference ontology are represented by the very same element in the evaluated ontology; (c) *under-specification*, when missing domain constraints allow for unintended models of the ontology.

Before we delve into ontological issues, we should highlight that D3FEND is a work in progress. When we made the analysis reported in this paper, the latest version of D3FEND at the time (named '0.11.0-BETA-1') was *logically inconsistent*, which can be shown by the reasoners (Pellet or FaCT++ 1.6.5, for example) available on the Protégé ontology editor[9]. For this reason, in our analysis, we work with a previous (beta) version of D3FEND (named '0.10.1-BETA-1'), released in June 2022[10]. The goal of this analysis is not to cover all semantic issues within D3FEND, but primarily to highlight a few of them that could have been prevented (and which can be fixed) by relying on the support of a foundational ontology. These problems if not properly addressed can impact the reusability, interoperability, and *domain appropriateness* of that artefact [30]. An ontology should not only capture intended instances (scenarios that satisfy the ontology specification) but also exclude unintended ones [31]. Our analysis intends to show the analyzed version of D3FEND falls short both in capturing intended instances and excluding unintended ones. For the purposes of transparency and reproducibility of this research, all the related files are publicly available at https://purl.org/d3fend-analysis.

3.1. General semantic issues within D3FEND

The analyzed version of D3FEND is clearly under-specified thus missing many important constraints. In particular, it systematically lacks many constraints that should establish *disjointness* between classes. In other words, several classes that, even *intuitively*, are expected to be disjoint are not disjoint, including DIGITAL ARTIFACT and PHYSICAL ARTIFACT (for example, HARDWARE DEVICE), PHYSICAL OBJECT and DIGITAL OBJECT, DIGITAL ARTIFACT and DIGITAL EVENT, PHYSICAL LOCATION and PHYSICAL OBJECT, among others. Actually, similar issues have been found in other large ontologies, such as Schema.org[11], where, for example, LOCALBUSINESS is both a PLACE and an ORGANIZATION[12]. In this case specifically, under UFO assumptions, ORGANIZATION and PLACE can be seen as different OBJECTS with different unique principles of identity, so they cannot be a subtype of one another [32,2]. The case of D3FEND is often simpler than that because it involves confusion between, for instance, an EVENT, an ASPECT, and an OBJECT, represented by Figure 1, as we will see — a case of construct overload. *We conjecture that, without the aid of the systematic taxonomy of a foun-*

[9] Protégé is available at https://protege.stanford.edu/.

[10] While this paper was being reviewed, another version of D3FEND was released in January 2023, named '0.12.0-BETA-2', which fixed some of the issues that we identified in our analysis, including the logical inconsistency found by the reasoners. Nonetheless, our main argument about the importance of ontological foundations in the ontology engineering practice still holds.

[11] See: https://schema.org/.

[12] LOCALBUSINESS in Schema.org: https://schema.org/LocalBusiness.

dational ontology, ontology engineers usually drop constraints to avoid inconsistencies as the ontology gets bigger, consequently admitting unintended instances.

In Figure 6, we represent a fragment of D3FEND, as an UML class diagram, in order to show several semantic issues revealed as unintended subsumption relations. Figure 6 displays the general idea that (offensive or defensive) TECHNIQUES are *associated with* DIGITAL ARTIFACTS and can *enable* OFFENSIVE or DEFENSIVE TACTICS.

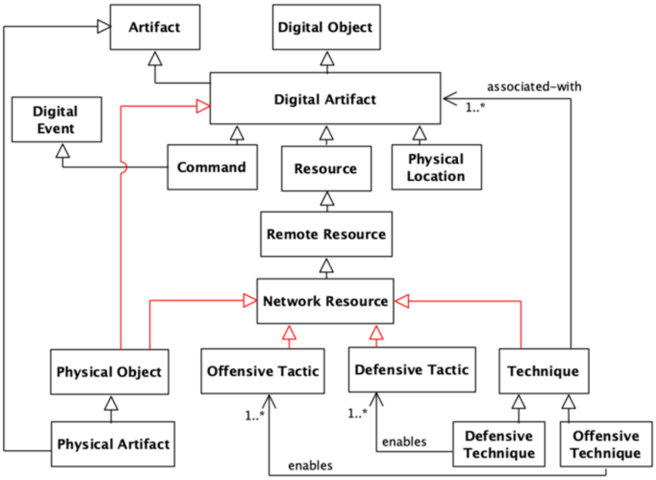

Figure 6. A fragment of D3FEND 0.10.1-BETA-1 expressed as a UML class diagram. Black elements are asserted in the ontology. Red elements are inferred.

- **Physical Objects and Locations and Digital Artifacts:** By inference, PHYSICAL OBJECT $\sqsubseteq$ DIGITAL ARTIFACT. Consider that an ARTIFACT, in D3FEND, according to Wordnet[13], is "a man-made object taken as a whole". Clearly, not all PHYSICAL OBJECTS are artifacts, let alone DIGITAL ARTIFACTS. Moreover, PHYSICAL OBJECTS (i.e., things that exist in the world having spatial extension) are necessarily not digital objects and, hence, not DIGITAL ARTIFACTS. Furthermore, we have that PHYSICAL LOCATION $\sqsubseteq$ DIGITAL ARTIFACT, which can be criticized on the same grounds.
- **Tactic and Technique:** TECHNIQUE are specialized into offensive and defensive, although *incompletely* and with *type overlapping*. This means that an instance of DEFENSIVE TECHNIQUE can also be an instance of OFFENSIVE TECHNIQUE, and that individuals that are neither of these can be an instance of TECHNIQUE. Likewise, there are OFFENSIVE TACTIC and DEFENSIVE TACTIC, although there is no explicit generalization set called TACTIC within D3FEND. The meanings of these categories are unclear. We believe that (offensive or defensive) TACTIC can be interpreted as an INTENTION (to perform certain actions), which in UFO is an ASPECT (more specifically, an INTRINSIC MODE). TECHNIQUE seems to either refer to a NORMATIVE DESCRIPTION [27] describing an EVENT TYPE or that EVENT TYPE itself. MODES, NORMATIVE DESCRIPTIONS or, more generally, OBJECT (of which NORMA-

[13] See: http://wordnet-rdf.princeton.edu/id/00022119-n.

tive Description is a subtype) and Event Types are mutually disjoint categories. By inference, Technique is a Digital Object, but it is commonly annotated with definitions that use action verbs (which suggests its strong connection to Event types). Moreover, D3FEND also contains the following constraints: Technique $\sqsubseteq$ Remote Resource and Offensive Tactic $\sqcup$ Defensive Tactic $\sqsubseteq$ Network Resource. These are clearly unintended constraints, particularly when we notice that Network Resource $\sqsubseteq$ Digital Artifact, which means that a Tactic can be a Digital Artifact, mixing up Intentions with Objects, and, allowing that a Tactic could be also a Technique. It seems that the notion of Technique collapses ontologically different entities (construct overload) while at the same type suffering from the systematic lack of proper constraints.

- **Types and Instances:** in UFO, individuals are instances of at least one type. D3FEND, actually, makes use of types explicitly: Reference Type and Reference. However, they bear no relation to each other. The Reference Types include, e.g., the individuals Patent and Internet Article, which seem to be better categorized as types rather than individuals. At the same time, there are classes called Patent and Internet Article, which, however, do not include those individuals as their instances.
- **Digital Artifacts and Digital Events:** Numerous classes are *explicitly* asserted (i.e., not inferred) to be simultaneously a Digital Artifact and a Digital Event, such as Command, DNS Lookup, User Action, System Call. Once again, an unintended fusion between an Event and an Object, which should have been defined as disjoint ontological categories (Figure 1).

As a final example of missing constraints, we made an experiment by creating an individual that is, *concomitantly*, a Defensive Tactic, a Defensive Technique, a Digital Event, a Digital Object, an Offensive Tactic, an Offensive Technique, an Agent, a Proposition, a Sensor, an Assessment, a Physical Location, a Physical Object, a Reference, and a Reference Type. In contrast with what one would expect from an ontology capturing the real-world semantics of these notions, no inconsistency results from that.

3.2. Domain-specific ontological issues within D3FEND

ROSE is not an ontology of cybersecurity *per se*. However, it is an ontology of security engineering that can be specialized to capture subdomains of security, including cybersecurity. We here show that D3FEND does not address a number of questions and patterns of security, which negatively impacts its expressivity/domain appropriateness. Particularly, D3FEND core conceptual model contains three interconnected main ontologies: digital artifact, attack, and defense ontologies. From a ROSE perspective, they can be seen as, respectively, the ontologies of value, risk, and security. With these notions in mind, we can directly identify domain appropriateness issues in D3FEND.

The first issue refers to the lack of subjects within D3FEND. Although it includes the concept of Agent, which subsumes Organization and Person[14], it does not

[14] Notice that, in D3FEND, Person and Organization are not disjoint classes, and the former is oddly a subclass of $\exists$*has-member*.Person.

seem to play a role in D3FEND's core conceptual model. As ROSE and COVER show, the phenomena of value, risk, and security depend on the subjects' INTENTIONS that are affected by the manifestations of dispositions. As an ASPECT, an INTENTION is existentially dependent on their bearers, the subjects. In other words, D3FEND currently lacks the subjects that would bear OFFENSIVE or DEFENSIVE TACTICS. The practical implication of this deficit is that it is not possible to recognize which PERSONS and ORGANIZATIONS are being affected by the TECHNIQUES that are associated with TACTICS. In summary, this is a case of ontological incompleteness regarding VALUE SUBJECT, RISK SUBJECT, PROTECTED SUBJECT, and SECURITY DESIGNER.

Analogously, the concepts of THREAT OBJECT and ATTACKER are currently missing in D3FEND, so it is not possible to identify the OBJECTS that are sources of a RISK EVENT or a ATTACK. Furthermore, the conditions that favor the appearance of a RISK EVENT (THREATENING SITUATION) or the conditions that favor the occurrence of a CONTROL EVENT (PROTECTION TRIGGER) are absent. As a result, we cannot properly describe and assess the situations associated with risk or security.

Then, considering that a cybersecurity countermeasure is defined as "any process or technology developed to negate or offset offensive cyber activities" [9], there is a blending of different entities that compose the UFO-B pattern shown by Figure 2, which appears within the ontologies of value (Figure 3), risk (Figure 4), and security (Figure 5): the notion of TECHNIQUE obfuscates the distinction between an OBJECT (say, a SECURITY MECHANISM, its capability (say, a CONTROL CAPABILITY), the event or process that is the manifestation of this capability (CONTROL EVENT), and the resulting state of the world (CONTROLLED SITUATION) that impacts (positively or negatively) an INTENTION of a subject. This is a clear case of construct overload. D3FEND, actually, includes a notion of CAPABILITY, but which, ontologically speaking, must be interpreted either as an INTENTION or a PROPOSITION, given that it is subsumed by CAPABILITY FEATURE CLAIM. In any case, neither INTENTIONS nor PROPOSITIONS are capabilities, in fact, all these types are (again) mutually disjoint. Curiously, D3FEND does not include the notion of VULNERABILITY, which is one of the most common concepts among security [5] and cybersecurity [8] ontologies.

3.3. Concrete proposals for improving D3FEND

Proposing a complete analysis and improvement of D3FEND is out of the scope of this paper. However, we can indicate benefits that can be incorporated to D3FEND according to the ROSE/UFO ontological framework and the analysis conducted here. Based on ROSE, the strategy we suggest is the following: (1) specializing the value ontology with cybersecurity domain-specific entities to capture D3FEND's digital artifact ontology; (2) specializing the risk ontology into the cybersecurity domain to capture the ATT&CK framework — D3FEND's attack ontology (the entities under the class named 'ATTACK Thing' defined in the OWL file); (3) specializing the security ontology into the cybersecurity domain to capture the defensive dimension of D3FEND.

In general, the taxonomic parts of D3FEND can be, systematically, added to its improved version, including the lists of OFFENSIVE TACTIC, OFFENSIVE TECHNIQUE, DEFENSIVE TACTIC, DEFENSIVE TECHNIQUE, and DIGITAL ARTIFACT, but now introducing the right constraints inherited from UFO and ROSE, thus, removing inconsistencies. Moreover, interestingly, MITRE's ATT&CK framework maintains a list of threat groups cataloged by security community[15], but D3FEND does not make use of it. This catalog would be suitable to populate/instantiate the THREAT OBJECT category.

Information security practitioners and scholars often refer to the notions of *Confidentiality*, *Integrity*, and *Availability* as the "CIA triad", the fundamental elements of security controls in information systems [33]. They can be used not only to specialize the subjects' INTENTIONS (security goals [34]) but also to specialize LOSS EVENT and LOSS SITUATION. The latter would result in an incomplete generalization set with the derived types LOSS OF CONFIDENTIALITY, LOSS OF INTEGRITY, and LOSS OF INTEGRITY. Currently, D3FEND lacks these domain-specific distinctions.

We advocate that following the suggestions and underlying principles discused in this paper would produce an ontologically improved version of D3FEND. However, the resulting artifact would also have the additional benefit of facilitated interoperability with other UFO-based ontologies in related domains including, naturally, those in the domain of risk [26] and risk progagation [35] but also Trust [36] and Law.

4. Final considerations

Ontology engineering is not an easy task. One of its main challenges involves the appropriate conceptualization of the domain of interest because the ontology is supposed to not only correctly represent the domain but also excluded unintended interpretations. To address this problem there are foundational and reference ontologies, exemplified by the Unified Foundational Ontology's (UFO) ecosystem. Still, ontologies, as computational artifacts, are often built without the assistance of this sort of ontology engineering framework.

D3FEND is a novel OWL knowledge graph of cybersecurity countermeasures that is gaining popularity among practitioners and academics alike. Exactly because it is practically relevant as well as a work in progress, we believe it can substantially benefit from processes of detailed ontological analyses and systematic improvement recommendations in line with what we put forth in this paper.

In this paper, with the support of UFO and the Reference Ontology for Security Engineering (ROSE), we systematically identify a number of semantic issues and opportunities for improvement within D3FEND. These issues include cases of semantic overload, ontological incompleteness (both at a general and domain level), and recurrent lack of constraints (underspecification). They dent D3FEND's reusability, interoperability, and correctness with regard to the cybersecurity domain. More to the point, they could have been avoided (and can be addressed) with the support of a foundational ontology. So, this case adds to the growing evidence supporting the thesis that ontological foundations really matter in the ontology engineering practice.

As previously mentioned, [5] and [8], respectively, systematically analyzed a multitude of ontologies in the security and, more specifically, cybersecurity domains. As shown there, very few of these ontologies have been developed with the support of foundational ontologies - despite the criticality of the domain. However, to the best of our knowledge, there is no similar work providing an ontological analysis of, and improvement recommendation proposal for, the D3FEND knowledge graph - again, despite the

[15] List of threat groups, registered by MITRE: https://attack.mitre.org/groups/.

wide practical impact and diffusion of that ontology among practitioners. So, we believe this paper brings contributions to the development of the ontology engineering practice in cybersecurity, in general, and the D3FEND project, in particular.

The natural next step of our research is to: (1) propose a complete ontological analysis of D3FEND with the support of ROSE/UFO, aiming at exhaustively identifying semantic issues and opportunities for improvement; (2) generate the OWL version of the improved D3FEND knowledge graph with the support of gUFO[16]; (3) demonstrate the implications of these improvement interventions in real-world use cases, such as cybersecurity risk assessment. In addition to that, as a complementary work, we shall conduct an analogous ontological analysis of the complementary ATT&CK framework.

Acknowledgement

Work supported by Accenture Israel Cybersecurity Labs. We sincerely thank Peter Kaloroumakis, Michael J. Smith and the D3FEND community at large for the helpful discussions on the issues addressed in this paper.

References

[1] Guizzardi G. Ontology, ontologies and the ”I” of FAIR. Data Intelligence. 2020;2(1-2):181-91.

[2] Guizzardi G. The role of foundational ontologies for conceptual modeling and domain ontology representation. In: 7th Intl. Baltic Conf. on Databases and Information Systems. IEEE; 2006. p. 17-25.

[3] Schulz S. The Role of Foundational Ontologies for Preventing Bad Ontology Design. In: 4th Joint Ontology Workshops (JOWO). vol. 2205. CEUR-WS; 2018. .

[4] Keet CM. The use of foundational ontologies in ontology development: an empirical assessment. In: ESWC. Springer; 2011. p. 321-35.

[5] Oliveira Í, et al. How FAIR are Security Core Ontologies? A Systematic Mapping Study. In: Research Challenges in Information Science.; 2021. p. 107-23.

[6] Martins BF, et al. A framework for conceptual characterization of ontologies and its application in the cybersecurity domain. Software and Systems Modeling. 2022;21(4):1437-64.

[7] Donner M. Toward a security ontology. IEEE Security & Privacy. 2003;1(03).

[8] Martins BF, et al. Conceptual characterization of cybersecurity ontologies. In: IFIP Working Conference on The Practice of Enterprise Modeling. Springer; 2020. p. 323-38.

[9] Kaloroumakis PE, Smith MJ. Toward a knowledge graph of cybersecurity countermeasures. The MITRE Corporation. 2021. Available from: https://d3fend.mitre.org/resources/D3FEND.pdf.

[10] Kaiser FK, Andris LJ, Tennig TF, Iser JM, Wiens M, Schultmann F. Cyber threat intelligence enabled automated attack incident response. In: 2022 3rd International Conference on Next Generation Computing Applications (NextComp). IEEE; 2022. p. 1-6.

[11] Sadlek L, Čeleda P, Tovarňák D. Identification of Attack Paths Using Kill Chain and Attack Graphs. In: NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. IEEE; 2022. p. 1-6.

[12] Shin Y, Kim K, Lee JJ, Lee K. Focusing on the Weakest Link: A Similarity Analysis on Phishing Campaigns Based on the ATT&CK Matrix. Security and Communication Networks. 2022;2022.

[13] Akbar KA, et al. Knowledge Mining in Cybersecurity: From Attack to Defense. In: Data and Applications Security and Privacy XXXVI. DBSec 2022. vol. 13383. Springer; 2022. p. 110-22.

[14] Aghamohammadpour A, Mahdipour E, Attarzadeh I. Architecting threat hunting system based on the DODAF framework. The Journal of Supercomputing. 2022:1-28.

[15] Luh R, Eresheim S, Größbacher S, Petelin T, Mayr F, Tavolato P, et al. PenQuest reloaded: A digital cyber defense game for technical education. In: 2022 IEEE Global Engineering Education Conference (EDUCON). IEEE; 2022. p. 906-14.

[16] gUFO - standing for gentle UFO - is a lightweight OWL implementation of the UFO ontology [37].

[16] Oliveira Í, et al. An Ontology of Security from a Risk Treatment Perspective. In: Chakravarthy U, Mohania M, Ralyté J, editors. Conceptual Modeling. ER 2022. Springer; 2022. .

[17] Guizzardi G, et al. Towards ontological foundations for conceptual modeling: The Unified Foundational Ontology (UFO) story. Applied ontology. 2015;10(3-4):259-71.

[18] Guizzardi G, Botti Benevides A, Fonseca CM, Porello D, Almeida JPA, Sales TP. UFO: Unified foundational ontology. Applied ontology. 2022;17(1):1-44.

[19] Varzi A. Carnapian Engineering. In: Ontology Makes Sense; 2019. p. 3-23.

[20] Strom BE, Applebaum A, Miller DP, Nickels KC, Pennington AG, Thomas CB. MITRE ATT&CK®: Design and Philosophy. The MITRE Corporation. 2020. Available from: https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy.

[21] Verdonck M, Gailly F. Insights on the use and application of ontology and conceptual modeling languages in ontology-driven conceptual modeling. In: Intl. Conf. on Conceptual Modeling. Springer; 2016. p. 83-97.

[22] Benevides AB, et al. Representing a reference foundational ontology of events in SROIQ. Applied Ontology. 2019;14(3):293-334.

[23] Baratella R, et al. Understanding and Modeling Prevention. In: Research Challenges in Information Science. RCIS 2022. vol. 389–405. Springer; 2022. p. 389-405.

[24] Ruy F, et al. From reference ontologies to ontology patterns and back. Data & Knowledge Engineering. 2017;109:41-69.

[25] Guizzardi G. Ontological patterns, anti-patterns and pattern languages for next-generation conceptual modeling. In: Conceptual Modeling: 33rd International Conference, ER 2014, Atlanta, GA, USA, October 27-29, 2014. Proceedings 33. Springer; 2014. p. 13-27.

[26] Sales TP, Baião F, Guizzardi G, Almeida JPA, Guarino N, Mylopoulos J. The common ontology of value and risk. In: Conceptual Modeling. ER 2018. vol. 11157. Springer; 2018. p. 121-35.

[27] Guizzardi G, et al. Grounding Software Domain Ontologies in the Unified Foundational Ontology (UFO): The case of the ODE Software Process Ontology. In: Ibero-American Conference on Software Engineering; 2008. p. 127-40.

[28] Mumford S. Dispositions. Clarendon Press; 2003.

[29] Rosemann M, Green P, Indulska M. A reference methodology for conducting ontological analyses. In: Conceptual Modeling. ER 2004. vol. 3288. Springer; 2004. p. 110-21.

[30] Guizzardi G. On ontology, ontologies, conceptualizations, modeling languages. and (Meta) Models, Frontiers in Artificial Intelligence and Applications, Databases and Information Systems IV, IOS. 2007.

[31] Guarino N, Oberle D, Staab S. What is an ontology? In: Handbook on Ontologies. Springer; 2009. .

[32] Guarino N, Welty CA. An overview of OntoClean. Handbook on ontologies. 2004:151-71.

[33] Samonas S, Coss D. The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security. 2014;10(3).

[34] Sumra IA, Hasbullah HB, AbManan JlB. Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey. In: Vehicular Ad-hoc Networks for Smart Cities: First International Workshop, 2014. Springer; 2014. p. 51-61.

[35] Fumagalli M, Engelberg G, Sales TP, Ítalo Oliveira, Klein D, Soffer P, et al. On the Semantics of Risk Propagation. In: Research Challenges in Information Science. RCIS 2023. Springer; 2023. Forthcoming.

[36] Amaral G, Sales TP, Porello D, Guizzardi G. Towards a reference ontology of trust. In: On the Move to Meaningful Internet Systems: OTM 2019 Conferences. vol. 11877. Springer; 2019. p. 3-21.

[37] Almeida J, Guizzardi G, Falbo R, Sales TP. gUFO: a lightweight implementation of the Unified Foundational Ontology (UFO). URL http://purl org/nemo/doc/gufo. 2020.