9-12-2011

A Simple Ontology for the Analysis of Terrorist Attacks

Matthew D. Turner

A Simple Ontology for the Analysis of Terrorist Attacks

Matthew D. Turner
Conjectural Systems, Albuquerque, NM
Mind Research Network, Albuquerque, NM
matthew.turner.phd@gmail.com

David M. Weinberg
Practical Risk, LLC., Rio Rancho, NM
dave@practical-risk.com

Jessica A. Turner
Mind Research Network, Albuquerque, NM
University of New Mexico, Albuquerque, NM
jturner@mrn.org

University of New Mexico
Electrical and Computer Engineering Department
Technical Report **EECE-TR-11-0007**

Abstract

The need for shared understanding in the analysis of terrorist activity has been a clearly defined national priority for over a decade. We present a foundation for an ontology to represent adversary groups and their intentions, classification of their weapons and attack types, and the ability to represent the relationship between the outcomes of an attack and the various recognized intentions of the adversary group. This Adversary-Intent-Target (AIT) model focuses on structuring knowledge to allow reasoning about which groups would be likely to choose what kinds of weapons to perform which kinds of attack. The AIT model is a generalizable and extensible system for organizing the relevant information, serving as an preliminary ontology within a larger computational system.

Contents

1 Introduction

Inter-office and inter-agency coordination of intelligence information is vital to the security of the United States. However current systems in place to perform this coordinating function, when they exist at all, are not sufficiently developed to make light work of the task. The work presented here is part of a larger project to automate, as much as possible, the merger of this information using computational tools.[1] One distinctive feature of the project is the use of the mathematics of Category Theory to preserve the logical structure of the information as it is processed and the upfront recognition of the need for a specialized vocabulary for interoperability.

The software tools being developed require a semantic "grounding," that is, a **controlled vocabulary** of terms (words) with a fixed set of relations on the terms of that vocabulary that enforce a logical structure. Together these features form an **ontology**, in this case an ontology for terrorism research. With such an ontology in place, unthinking machinery can do a wide variety of (seemingly) intelligent reasoning tasks while still preventing the results from becoming semantic gibberish.

The problem addressed by our group is the actual construction of such a core vocabulary. One that is sufficient for the description, discussion, and analysis of terrorist attacks; pre-incident, post-incident, and ongoing; hypothetical and real.

The ultimate goal and product of this research is the development of a system that we refer to as the **Basic Ontology Of Terrorism** or **BOOT**. Such a system represents a significant number of technical and social challenges. To be useful in real intelligence work, it must provide analysts with an environment that is natural for them to use (not asking them to unlearn all their previous training and experience) while simultaneously making more relevant information available. Further, it must not increase the informational load on the analyst user base. It must work across different fixed institutional vocabularies and knowledge bases by allowing different points of view to be represented and keeping the merging of these points of view away from the user base (unless the analyst wants the additional information). Finally, it must be usable for exchanging information among analysts meeting their needs for information sharing while simultaneously maintaining information security.

One issue that is very clear at present is that the construction of a system such as BOOT requires input from a broad range of experts both from knowledge engineering and from the specific domains of use: intelligence analysts, military and operations managers, various governmental systems operators, agency supervisors, etc. As such, our group is particularly concerned with developing the foundational vocabulary that

[1]Contract: DTRA01-03-D-0009-0026, "Pre-incident Analysis using Multigraphs and Faceted Ontologies," T.P. Caudell, principle investigator.

acts as a base to which domain experts can easily add to in order to build a usable system customizable to their own mission, operating environment, and needs. We also seek to establish a foundational system that automated agents can extend to cover new knowledge, in a fashion similar to the connections that exist between **SUMO** (the **Suggested Upper Merged Ontology**) and Princeton's WordNet.[2] Such a natural language acquisition system, based on WordNet but with specialized vocabulary from terrorism research (**Terrornet**), would allow automated agents to incorporate information from both open sources (news reports, etc.) and specialized intelligence reports.

Such complex systems as BOOT and Terrornet are currently beyond the scope of this project, but in the present work we developed clear requirements that such systems must address and determined a number of problems that must be solved in order to develop them. These topics will be discussed at the end of this paper. As the scope of this final project depends on the intellectual input of a large number of people, we focus here on a smaller related problem.

In this paper we develop and analyze a pre-incident subsystem of the larger BOOT system as a test case. We refer to this subsystem as the the **Adversary–Intent–Target** (**AIT**) model. This model reflects the analysis of a single sentence that acts as its organizing principle (detailed below; section 3.1). AIT has been developed sufficiently for software testing purposes and its foundation provides a model useful for further research. This work is related to, but not identical with, previous work on "pre-incident indicator analysis," which addresses prerequisites for terrorist attacks and was developed by some of the present project team.[3]

Ultimately even a small subsystem such as AIT will have to deal with issues of reliability of information, probabilities of events, and varying levels of expert certainty, but in this first phase of the research we develop the basic logical skeleton that a language for terrorism research must have. We will proceed as follows: first, the basic ideas of ontologies and related structures are discussed, as well as the languages/formats for storing them. Next, the development and structure of AIT is explained. Finally, future work on BOOT and AIT is discussed as well as a few of the major challenges faced in the development of such systems. We do not discuss the machine processing of AIT; that presentation will be forthcoming.

[2]SUMO: `http://www.ontologyportal.org/`; WordNet: `http://wordnet.princeton.edu/`. WordNet is the registered trademark of Princeton University. WordNet is released under the WordNet license; Princeton University claims the system is "unencumbered" for commercial use, however the Open Source Initiative (`http://www.opensource.org/`) does not specifically recognize the license as meeting the "open source" definition and requirements.

[3]T. Caudell, F. Gilfeather, M. R. Taha, and D. Weinberg, Pre-Incident Indicator Analysis (PIIA) System, UNM ECE Technical Report, in preparation, August 2011.

2 Knowledge Representation & Ontologies

The problem before us is the same, either in building BOOT or the smaller AIT, and it is one of knowledge engineering. Our approach here is to build an **ontology** (defined in section 2.2 and discussed in 2.3) that provides a collection of basic terms for terrorism research and also encodes the relationships among those terms. The AIT model is based on a "model statement" (section 3.1) that implies a particular organization of knowledge about reality that the ontology must reflect. To build this ontology we must discover the concepts (terms or classes) that are natural to the question, list them, and then make explicit the relationships among these terms.

Before delving into AIT's structure, we discuss some details of ontological modeling and terminology.

2.1 Simple Structures: Taxonomies & Partonomies

One of the simplest representations of concepts, and one that is already known to most people, is a **taxonomy**. A taxonomy is a hierarchical system of classification, in which the only relationship between terms is the **subset** relation. The terms in a taxonomy are always **sets**; taxonomies do not include individual members of the sets. In taxonomic and ontology research the word **class** is usually used as a synonym for set.[4]

The relation is called subset or subclass, but it is sometimes mistranslated as "is-a" (labeled **isA** or ISA in some systems). Whenever is-a is used to discuss set-to-set relations it usually means "is-a-type-of" or "is-a-kind-of," which, for our purposes, is equivalent to the mathematical subset relation that we use. However, is-a can also be used to refer to individuals, not sets or classes, and that relationship is not the same as subset (it is the "element-of" relation). We do not discuss any set elements here, so in this work is-a would always be translated as is-a-kind-of or subset.

Examples of the subset relation abound: a dog is-a kind of animal (that is, the set of dogs is a subset of the set of all animals or a dog is-a-kind-of animal), nuclear weapons are-a subclass of weapons, the Ku Klux Klan (KKK) is-a specific kind of right-wing Christian group, etc.[5] The common feature is that the subset or subclass

[4]Logicians in this field may require the distinction between sets and classes as used, for instance, in Russell's type theory and other systems, but practitioners rarely make these technical distinctions [3].

[5] Referring to the KKK as a set, rather than as an element of a set (a specific group) may seem unnatural, but formally it is not a problem. This is a common approach in foundational mathematics, for example, where elements of sets are never referred to at all in the definition of the concept of "number" [3]. For our purposes it is a formal contrivance.

is more specific than the superset or superclass, and that every member of the subset is also a member of the superset.

This subset relation, denoted $\subseteq$, is a **partial order** which has three defining properties: it is **reflexive**, **anti-symmetric**, and **transitive** (often referred to as RAT).[6] By reflexive, we mean that each class is a subclass of itself ($A \subseteq A$), so, for instance, the set of dogs is a subset of the set of dogs.[7] Anti-symmetric means that if A is a subclass of B then B is *not* a subclass of A ($(A \subseteq B) \Rightarrow (B \nsubseteq A)$), *unless* A and B are the same (unless $A = B$). For example, given that "nuclear weapons" are a subclass of weapon, we have automatically that the more general class of "weapon" is not a subclass of the more specific nuclear weapon. The transitive property means that if A is a subclass of B and B is a subclass of C, then A is automatically also a subclass of C ($A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$). So the KKK is a subclass of right-wing Christian groups, which in turn are a subclass of religious groups, and so the KKK is a subclass of religious groups.

There is a single term at the top of a taxonomy which, by transitivity, is the superclass of every term in the taxonomy. This term is the most generic object set possible, usually called "thing" or "top" and denoted by the symbol $\top$.[8] Because this is the superset of every other set in the taxonomy, we have that every more specific object defined in the hierarchy is also a "thing," which is consistent with the common use of the word.

It is important to note that taxonomies can be viewed in two ways. The first, and most common way, is to visualize them as a tree or tree-like structure, as in figure 1. However, this picture can be flattened; because the subsets are contained within the supersets, one can visualize the situation as smaller and smaller subsets contained within each other and with the largest set being thing or $\top$ in a format similar to a Venn diagram as in figure 2.

[6] In some works, especially those using descriptive logic, the symbol $\sqsubseteq$ is used for the logical equivalent of $\subseteq$.

[7] If this seems strange, accept it as a vacuous mathematical necessity to make other definitions work correctly. Similar to the formal requirement discussed in footnote 5.

[8] We will not need it for the work presented here, but there is also a corresponding term called "nothing" or "bottom," denoted $\bot$. For lattice/partially ordered structures, this object also exists. While $\top$ can be thought of as the most generic thing, a thing without any distinguishing properties, $\bot$ can be thought of as the thing which (inconsistently) has every possible property. In the current example, for the subset relation, $\bot$ represents the empty set ($\varnothing$) which is—by definition—a subset of every other set.

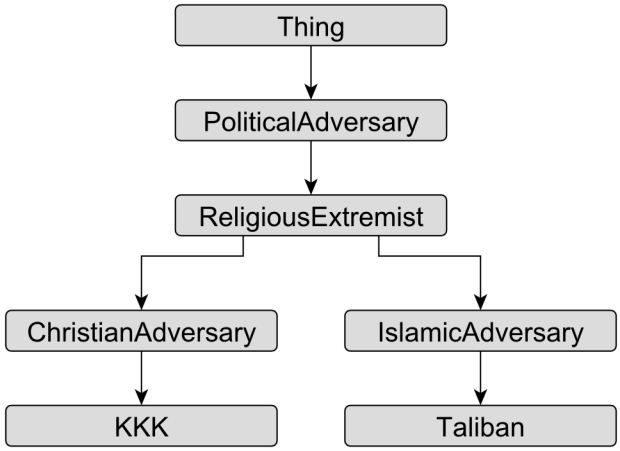

Figure 1: Taxonomy visualized as a tree-like structure. This is the traditional representation.

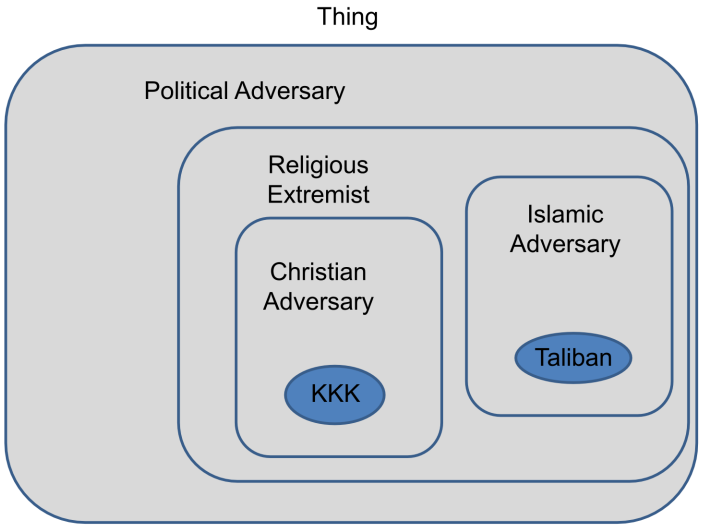

Figure 2: Taxonomy visualized as a Venn diagram. While not usually viewed in this form, it clearly represents the subsets in a more natural way.

The nature of the subset relation defines a subsumptive hierarchy, as each superclass subsumes or contains the elements of all its subclasses. So, a taxonomy is a subsumptive hierarchy. Terminology in the literature is somewhat confusing on this, with taxonomic hierarchies being called "nested hierarchies" and, if the subset relation is strict (that is, never allowing $A = B$ to hold between sets in the anti-symmetric property above), then the taxonomy becomes a "containment hierarchy" which is often viewed as the definitive subsumptive hierarchy. This despite the fact that in some sense all taxonomies "contain" in the sense of the subset relation.

Another single-relationship scheme is a **partonomy**, also called a compositional hierarchy or a compositional containment hierarchy.[9] In a partonomy, the relationship between terms is "part of," for instance: a trigger is part-of a nuclear device, fissile material is part-of a nuclear device, Cook County is part-of Illinois which in turn is part-of the continental United States, etc. The critical difference here is that a partonomy is not based on a relationship of *subsumption* (or containment; as in the taxonomy) but instead is based on a relationship of *composition*: each term in the hierarchy is composed of the terms below it. (It should be noted that the partonomy is still a partial order, if one allows a part to be a part of itself. For instance, Cook County is part of Cook County, the biggest part, while Chicago is clearly only a smaller part of the county.)

The critical difference here is that part-of relations often have to refer to individuals, not sets, and terms at one level (a car, for instance) is made up of various parts (a wheel) but those parts are not subsumed by the higher-level term (a wheel is not a kind of car).

A taxonomy appears only useful for identifying what something is or what it is not, that terrorist organizations are not allies, for example. For humans, there is a lot of taxonomic detail that appears either superfluous or otherwise obvious. For instance, the taxonomy for AIT that we discuss below says explicitly that terrorist organizations are not the same types of thing as are weapons. But such a claim has two critically important aspects: first, it grounds the terms so that unthinking machines can "know" a distinction—one that they otherwise would not know or be able to derive from the terms alone—despite the (human) apparent obviousness of the distinction. Second, this sort of classification identifies what can be said about a term; knowing that terrorist organizations are not the same types of thing as are weapons entails that what we can say about weapons and what we can say about

[9] Also called a mereonomy or (with grammatical apologies) a mereology, with the adjectival form "mereonomic." Mereology is the study of part-whole relations. The literature on this topic has a great deal to offer the more general study of ontologies, but, at present, is not very well integrated into the literature.

terrorist organizations—their characteristics and the relationships we know they have with other concepts—are not the same and must be specified differently.

Taxonomies, unfortunately, cannot represent this latter information. Once we include other relationships besides subclass we are working with an ontology.[10]

2.2 Ontologies & Related Structures: Definitions

The taxonomies discussed above provide a well-known and well-understood way to organize a specific kind of knowledge, such as biological relationships (the set of domestic cats, *Felis catus*, is a subset of the genus *Felis*; *Felis catus* $\subseteq$ *Felis*) or types in mathematics (the set of rational numbers is a subset of the set of real numbers: $\mathbb{Q} \subseteq \mathbb{R}$). The partonomy structure mentioned above is a very obvious extension of the taxonomy replacing the subset relation with the part-of relation. One can imagine a wide variety of similar structures generated by replacing the taxonomy's subset relation with some other relation (be it a partial order or not).

What all of these structures have in common is that they are *single-relationship* structures. In the literature there is some confusion of terminology: some researchers call any single-relationship structure a taxonomy, while others (the present authors included) think that the term should be reserved strictly for subset-relation based structures. Hence, some authors would think of a partonomy as a kind of taxonomy, while others would not. This situation causes some moderate terminological confusion and will likely never sort itself out.

To fix terminology we make the following definitions:

Taxonomy A taxonomy is a tree structure that has *exactly one* relationship expressed in it, specifically the *subset* or *is-a-kind-of* relationship.

Partonomy A partonomy is a tree structure that has *exactly one* relationship, in this case it is the *part-of* relationship.

Ontology An ontology is a tree like structure that has *at least* one relationship, which is *unspecified*, and additionally may have any number of relationships.

Note that by the definitions above both the partonomy and the taxonomy are specialized types of ontologies. Further, we define:

[10] Sadly, the more grammatically and semantically correct ont*onomy*, in parallel with tax*onomy* and part*onomy* has been lost to us.

Singonomy A singonomy is any ontology that has *exactly one* relationship, whatever that relationship may be. The adjectival form of singonomy, **singonomic**, and its complement **multinomic** are both useful descriptions of ontology subtypes.

So taxonomies and partonomies are singonomies.[11]

2.3 Discussion: How Ontologies Are Used

Clearly the real-world cannot be well-described by any singonomy.[12] Therefore to build a structural model for AIT we will require an ontology, with its full multinomic capacity.

So far we've only defined the formal structure of an ontology; intuitively it is a tree or tree-like structure while formally it is a collection of entities and a set of relationships among those entities. But what else can be said about it by way of definition? The most often cited definition is:

> "An ontology is an explicit specification of a conceptualization."
>
> Thomas Gruber [4]

Perhaps a better definition is this: an ontology is a **contract for meaning** [8]. That is, an ontology specifies terms and also rules for using the terms. As long as an agent (a person or a machine) only uses the terms in the way the rules specify, the contract guarantees that the results of these usages will be correct (for some definition of the word "correct"). Usually this means that reasoning over the terms with the fixed relations will not generate logical errors or inconsistencies for the reasoning agent.

[11] In developing the work presented here we have found the concept of a singonomy to be useful. Any ontology can be thought of as a collection of singonomies, where each singonomy represents the tree (or forest) generated by a single relation taken from the ontology. Any one-relation **projection** from an ontology is a singonomy.

[12] Notable early failures in an attempt to do this date to the beginnings of Western philosophy: Thales (624–546 BCE), taking an ambiguous is-a relation and starting with water as his "thing" or $\top$; followed later by Anaximenes (585–528 BCE) conducting a similar analysis using air as the first principle or thing. Anaximander (610–546 BCE) recognized an *undifferentiated stuff* or generic thing as the root of existence, and had a scheme requiring the use of oppositions—or recognizable binary opposites—as the principle of ontology, requiring more than a simple *is-a* relation. As such, he might be viewed as the earliest ancestor to modern information science/computational ontologies. See [1, 2].

So while it gives a controlled vocabulary, it does not depend on human understanding of the terms in the vocabulary: these words no longer have more than one meaning, there is no dependence on connotation or simile, or on other human aspects of natural language processing. The terms have sharp, singular definitions, and interact with the other terms in the vocabulary in precisely defined—or perhaps better, precisely *restricted*—ways. The relationships in the ontology govern the usage of the terms completely.

This eliminates much of the so-called grounding problem, specifically what we will call the **local grounding problem**: terms are defined precisely and therefore all their relevant semantic properties are accessible to any agent interacting with the vocabulary (or to any programmer developing a new agent) without any need for appeal to a higher-order intelligence to resolve the meaning of the term. (We call this problem "local" to recognize that for very limited problem domains we often only need a small quantity of built-in semantics to do useful work.) Another way to describe it is to say that the necessary semantics are built into the terms, when operating within the context of the ontology. (We call these built-in semantics meanings interior to the ontology.)

Note, however, that the other meanings and connotations of the terms are not necessarily irrelevant. An ontology supplies a minimum of explicit meaning required to do useful automatic work within the controlled vocabulary. Well chosen terms, with connotative, idiomatic, or metaphorical meanings consistent with the built-in semantics, will be especially useful at the human-machine interface. Such terms allow the full vagaries of human information processing while allowing machine intelligence to extend this in useful ways. While automated agents will not and can not extend or process these other implicit (or exterior) meanings, there in no reason to assume that these other usages will be damaged by machine processing. Ultimately this is an empirical question.

Essentially any version grounding problem invokes the same sort of question: "how do you attach the semantic meaning to purely symbolic expressions?" The sentence (symbolic expression):

I moved the horse out into the middle of the floor.

is ambiguous. If we look around and see a large animal of the species *Equus ferus caballus* standing in the middle of the floor, we might be satisfied. But we might also see a large bar shaped object, covered with leather or plastic and with two large handles all supported on a metal stand that has been set up for a gymnastics competition. Or instead we might see a wooden beam with four legs supporting a carpenter's work. The point is that the sentence is symbolically a constant, but its

meaning (semantic value) changes depending on the context. The grounding problem is the problem of determining this semantic value from the sentence and additional information.

Once again this appears tedious or superfluous to humans; we are constantly aware of our changing environmental context and adjust our vocabularies automatically. We also understand connotation and simile; most people faced with a gymnast's (pommel) "horse," or a carpenter's (saw-)"horse," understand implicitly that it does bear a physical or historical relationship with the animal we call a horse. But these similarities and additional meanings need to be specified to a computer, if they are to be used, or sacrificed as meanings lost at the human-machine interface.

The main method of dealing with grounding in ontology research is through **domain restriction**. By giving words singular definitions, precisely defined rules for use, and limiting systems to dealing with just one domain at a time, the grounding problem can be solved, at least partially.

A more general approach, one that attempts to extend the grounding beyond a single domain, is the use of so-called "upper" or "foundational" ontologies. A number of these exist, and they provide a very high level basis for smaller, domain-specific, ontologies [9].[13] When specialized domain ontologies can be made consistent (compatible) with a given upper ontology, this implies that the logical structure that inheres in the domain ontology does not violate the relations in the upper ontology. If multiple domain ontologies are all consistent with the same upper ontology, this implies that the domain ontologies—at least in principle—ought to be harmonizable with each other.

The present work is consistent with the **Basic Formal Ontology** (**BFO**).[14] We discuss some of the problems of harmonization of ontologies in the conclusions below, but for the most part this matter and its related problems are not addressed in detail here.

2.4 Machine Representations of Ontologies

In order to make use of an ontology, it must be represented in some formal language that is capable of serialization. Specifically, we must be able to store, transmit, and process the ontologies by machine.

In recent years, a number of languages for this **representation problem** in on-

[13]Examples include SUMO, mentioned above (`http://www.ontologyportal.org/`); GFO, the General Formal Ontology (`http://www.onto-med.de/ontologies/gfo/`); DOLCE (`http://www.loa-cnr.it/DOLCE.html`); and Cyc (`http://www.opencyc.org/`); among others.

[14]More on BFO can be found at: `http://www.ifomis.org/bfo/`.

tologies have been proposed and used. If one goes further back into the AI literature there are other formats and languages—not explicitly tied to ontologies—that are adequate for representing them, such as KIF, the Knowledge Interchange Format.[15] Most of these languages implement some restriction on first-order logic. Restricting first-order logic in these languages is necessary to make the languages either computable generally or to guarantee certain convergence or speed of processing requirements.

For our purposes, **serialization** is the process of converting a complex data structure into a form that can be stored in a file which can then be moved from place to place on the internet or on a given intranet.[16] The most common bottom-level format for serialization in ontology research is XML (the eXtensible Markup Language) and various extensions built on top of this, especially RDF (the Resource Description Framework) and its schema language, RDFS.[17]

The current standard for representing ontology terms and their relationships on the semantic web is the **Web Ontology Language** or **OWL**.[18] Specifically we use OWL2 for development of AIT. OWL is a family of languages with differing levels of logical expressiveness. We make use of OWL2 Full, in principle, but the bulk of our work is at the level of OWL2 DL (Description Logic), a restricted sublanguage of OWL2 Full with better computational properties.

[15]KIF is important for this research, forming the core representation for PowerLoom (`http://www.isi.edu/isd/LOOM/PowerLoom/`) and providing a formal language for first-order logic. See: `http://logic.stanford.edu/kif/` and `http://www.cs.umbc.edu/csee/research/kif/` for more details.

[16]See `http://www.parashift.com/c++-faq-lite/serialization.html` for more on serialization generally.

[17]XML: `http://www.w3.org/XML/`; RDF: `http://www.w3.org/RDF/`; RDFS: `http://www.w3.org/TR/rdf-schema/`.

[18]See: `http://www.w3.org/TR/owl2-overview/` for details. See `http://www.w3.org/TR/owl2-xml-serialization/` for specific details of OWL serialization.

3 The Adversary–Intent–Target (AIT) Model

3.1 Development of the AIT Model

The AIT model begins with a **model statement** regarding a terrorist attack. This statement is a simple sentence in natural language:

> **The AIT Model Statement:** A terrorist attack occurs when an adversary, with intent and capability, uses a weapon against a target.

This statement expresses a particular point of view (POV) toward terrorist attacks, and any POV implies a corresponding ontology. What we do in the AIT modeling process is develop the appropriate ontology for breaking up the world-at-large into parts and relations that reflect the assumptions embedded in this model statement. Part of the larger project for BOOT—and also the associated computing research this AIT model was developed to support—is to allow multiple, overlapping ontologies to coexist and exchange data despite their differences in POV.

This particular model statement, for instance, clearly requires definitions for words such as "attack," "adversary," "intent," "weapon," "target," etc. Analysis of the word "adversary" leads almost immediately to concepts such as "organization" (as in a "terrorist organization") and that leads to the requirement that we also specify the complementary concept of a non-terrorist organizations (called "lawful organizations" in AIT). All of these words must be analyzed by subject matter experts, with guidance by the ontology curator(s).

This analysis proceeds in a mixture of formal and informal analysis of *words*, until certain critical words keep appearing; these critical words become the basic *terms* of the ontology. Once the controlled vocabulary of terms is fixed, the relations among the terms must be determined. This is not a simple or linear process; as the relations are set, some terms stop making sense as they have been used, which in turn changes the term's definitions, which then changes other relations, and so on. As this developmental process iterates, eventually a core of terms and relations begin to form which makes sense to the team of subject-matter experts.[19]

[19] We discuss this further in the conclusions, but it makes sense to use graphical tools to produce draft ontology pictures. While a picture of a tree-like structure does not contain the complete ontology information, it does capture enough detail to be useful for workgroup discussions. In our development we used CMAP (`http://cmap.ihmc.us/`) and yED (`http://www.yworks.com/en/products_yed_about.html`). The CMAP tools come from an older community which has a very idiosyncratic way of conducting conceptual analysis; we found the yED editor more useful, especially for pictures made for publication. Unfortunately, neither tool is open source software,

AIT has a number of terms, such as **LawfulOrganization**, **AdversaryOrganization**, **Organization**, **Weapon**, **Place**, and **Intent**, among many others. (The labeling system and other details will be discussed in section 3.2.) Additionally, other auxiliary terms appear to fill out these concepts, seeming proper nouns such as **KKK** (the Ku Klux Klan) as a specific **AdversaryOrganization**, and generic nouns like **NuclearWeapon** as a kind of weapon.[20]

In the analysis of the model statement, certain relations among terms become apparent. For example, each **AdversaryOrganization** has an **Intent** (or more than one); so one of the relations in AIT is **hasIntent**. Answering the following sorts of questions leads to a rich vocabulary of terms and relations: *What are adversaries? Which intents do they have? Which adversaries are likely to prefer bombs over economic attacks? A particular adversary group has access to which types of weapons? What kinds of targets are vulnerable to which kinds of attacks?* Etc.

It is important to note that the AIT model is just one way of structuring knowledge; specifically, it organizes information about terrorism in a way that emphasizes the enabling resources, knowledge, and motivations that terrorist groups have at their disposal. A system such as BOOT would have to have a number of ways of structuring knowledge that would allow different analysts to organize the world according to the problems they address and structures that are relevant to their work. The modeling here develops only one point of view, albeit a realistic and important one.

Following the type of analysis described above suggested several taxonomies and specific relationships among these taxonomies as a starting point. In addition, several singonomies also appeared naturally in the analysis. The complete assembly of these separate trees yielded the AIT ontology.

As mentioned above (section 2.3), we work within the metaphysics of the Basic Foundational Ontology (BFO), which for our purposes divides things in the world into material entities and their parts, the qualities which material entities can have, and processes in which material entities participate. So in discussing AIT's details we will need to introduce some metaphysical terminology near the top of our ontology.

---

which precludes using either as a basis for building an ontology development tool with a graphic orientation (something that the field needs).

[20] As mentioned above, we treat all terms in the ontology as sets, so seeming proper nouns are still sets, with the subset relation, and not individual elements, which would require the element-of relation. See section 2.1 and footnote 5 (on page 4).

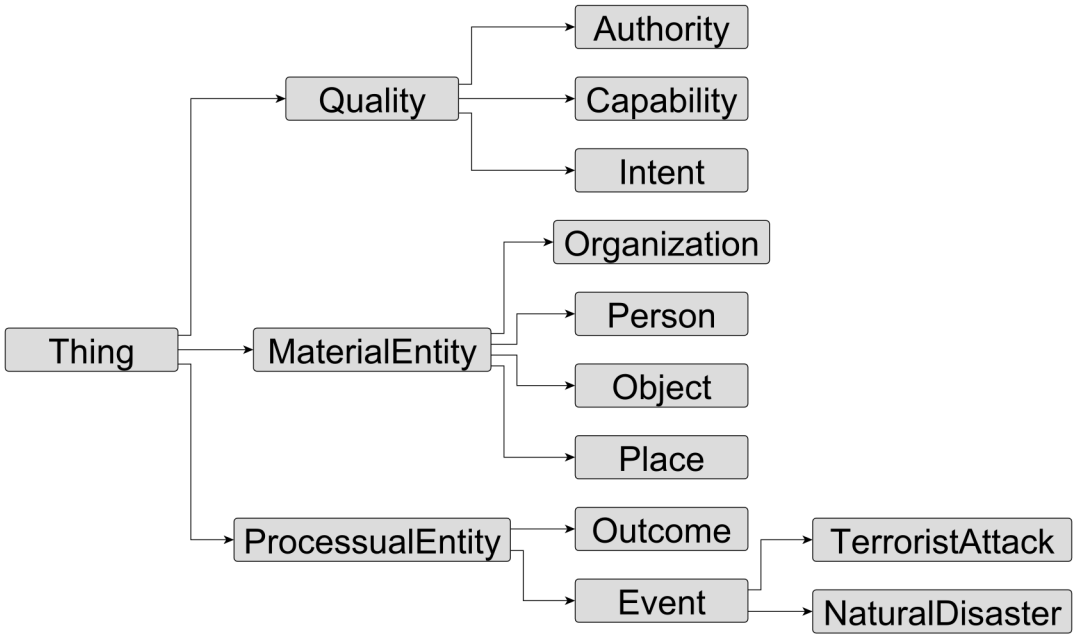

Figure 3: The backbone taxonomy of AIT, with the top three levels and the path to **TerroristAttack**. Arrows indicate subclass relationships.

3.2 Structure of AIT

In the discussion of the AIT ontology, we use the following notation. Terms, such as "adversary organization" are labeled in capital camelCase (also called CamelCase) and set in boldface font, as in **AdversaryOrganization**. (On occasion, a label will be pluralized, as in **AdversaryOrganization**s.) Relations between terms are labeled in boldface (lower) camelCase, as in the relation "results in" which is labeled **resultsIn**. The label for a term (relation), and the term (relation) itself, will be used interchangeably as grammatical necessity demands. Generally this will cause no confusion. This notation and the rules of use follow common practices in ontology research.

3.2.1 High-Level Classes

The high level classes within AIT are shown in figure 3, and will be referred to more fully as we proceed.

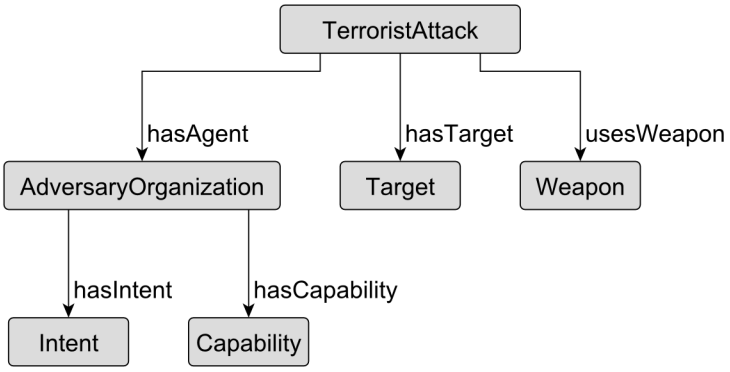

Figure 4: A **TerroristAttack** requires targets, weapons, and adversaries. Adversaries require capabilities and intents. Arrows indicate various relationships as labeled.

The top two tiers, **Thing** and the three concepts directly below it (**Quality**, **MaterialEntity**, and **ProcessualEntity**) are from BFO and are used according to the definitions given there.[21] The complete set of relationships used in AIT, and their logical restrictions, are shown in the table in the appendix. (See page 31.)

Our basic modeling statement (section 3.1 on page 13) is translated into the OWL framework as follows: A **TerroristAttack** is an **Event** with a minimum of one **Target**, using a minimum of one **Weapon**, and involving a minimum of one **AdversaryOrganization** as an agent that has both the **Capability** and **Intent**. See figure 4. Events, whether they are terrorist events or natural disasters, are kinds of **ProcessualEntity** (processes) which occur in some **Place** (which is a kind of **MaterialEntity**), as shown in figure 3.

3.2.2 Adversary Organizations

AdversaryOrganization in figures 4 and 5 is an **Organization**, which is a **MaterialEntity** within the BFO terminology. We distinguish a **LawfulOrganization** such as a police force from an **AdversaryOrganization**, while maintaining that both classes have the characteristics of an **Organization**, such as that any **Organi-**

[21] General information at `http://www.ifomis.org/bfo`. The manual and definitions are located at: `http://www.ifomis.org/bfo/documents/manual.pdf`.

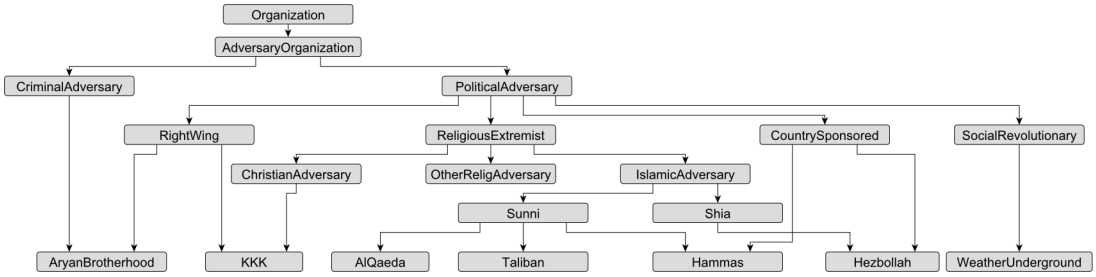

Figure 5: The Adversary Taxonomy. Solid arrows indicate the subclass relationship. The **Organization** concept is the same as in figure 3. Disjointness constraints are not represented in this figure, only subclass relationships. Note **Hezbollah** and **Hamas** are both subclasses of **ReligiousExtremist** (indirectly) and **CountrySponsored** (directly).

zation has members who are **Persons** (also material entities, for simplicity). In the current version of AIT, an **AdversaryOrganization** also can have an **Intent**, and a **Capability**, often more than one of both. Organizational intents are those such as stated in charters, on organizational websites, or presented by the spokespeople of a given group. Capabilities are reflected in the knowledge, training, or experience of its members or equipment in the organizations possession, for instance.

An **AdversaryOrganization** does not necessarily have a relationship to **Place**; those relations will need to be added to describe the place(s) where members of the organization are likely to be found, and the places that are their theaters of operations. The representation of capabilities and places, and any associated details, will be modeled at a later date.

The primary divisions of adversary organizations (**AdversaryOrganization**) are shown in Figure 5, and include **CriminalAdversary** and **PoliticalAdversary**, which are not disjoint sets—a group such as the Aryan Brotherhood could be both a criminal and a political adversary. Within our model, the **PoliticalAdversary** class includes the following subclasses: **NationalSeparatist**, **ReligiousExtremist**, **RightWing**, **SocialRevolutionary**, and **CountrySponsored**. The **ReligiousExtremist** includes the following disjoint subclasses: **ChristianAdversary** (e.g., the **KKK**), **IslamicAdversary** (further subdivided into **Sunni** and Shi'a (**Shia**), which are disjoint), and **OtherReligiousAdversary** (e.g., **AumShinrikyo**). A group may fall into several of these categories, such as **Hamas** which is both **CountrySponsored** and **ReligiousExtremist**, specifically **Sunni**; or **Hezbollah** which

is also **CountrySponsored** and **ReligiousExtremist**, but is **Shia**. By making terms such as **Sunni** and **Shia** disjoint or, at a higher level, making **ChristianAdversary** and **IslamicAdversary** disjoint, we enforce that no organization fall under both terms in these pairs of terms.[22] The fact that the subclasses are disjoint must be taken into account, as two groups could have very different expressed intents and capabilities, and thus the forms that their attacks take on would likely be different as well.

3.2.3 Intents of Adversary Organizations

The intentions of each subclass of **AdversaryOrganization** can be denoted at various levels; for instance, if **ReligiousExtremist** was defined by having the intention of converting people to their religion through their attacks, then each subclass of **ReligiousExtremist** would inherit that as an intention. However, the **AumShinrikyo** may have the **Intent** of **Anarchy** without **FinancialGain**, while **Hamas** wants to change US foreign policy (**ChangingGovPolicy**)as well as having **FinancialGain**; thus we would denote that multiplicity of intents specifically for those subclasses.[23]

This can be seen in part in figure 6, which shows the **hasIntent** relationships between the various of the **AdversaryOrganization** and **Intent** subclasses. For example, **AlQaeda** is represented as having four intents: **ReligiousConversion**, **ChangingGovPolicy**, **EconomicDistress**, and **HarmingHumans**. They do not have the intent of **Anarchy**, for example, or the specific intent of **FinancialGain**, except in so far as they require financial support for their operations.

3.2.4 Weapons & Targets

The **Object** class (from figure 3) includes the subclasses of **Weapon**, **Target**, and **WeaponizableComponent**, as shown in figure 7 (on page 20). All objects exist in some **Place** (though that place can change with time, and time is not yet modeled in AIT).

[22]The authors appreciate that in reality disjoint subclasses may, from time to time, cooperate for some operational or common goal, but for the purposes of keeping this model simple, we have not addresses such subtleties. We also realize that for every disjoint distinction in any given ontology there is almost always an exception that can not be expressed within the ontology's controlled language.

[23]For the present, **ChangingGovPolicy** refers to changing US government policy; modeling the intent of changing policies of other governments is being planned for the AIT ontology.

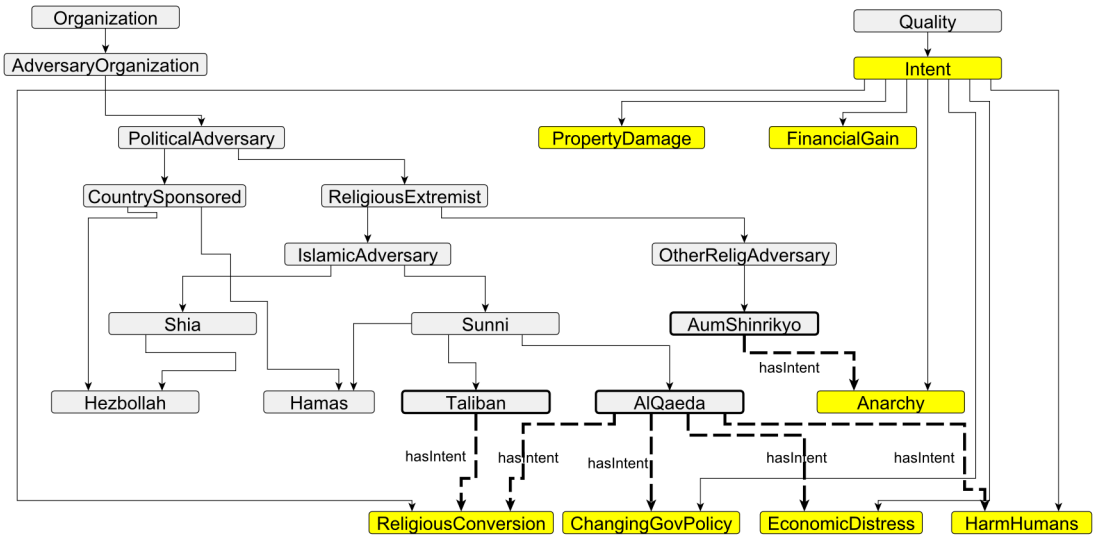

Figure 6: A portion of the adversary organizations and intents represented in AIT. (The full collection is hard to visualize clearly.) The **Intent** taxonomy is indicated in yellow. Solid unlabeled arrows indicate subclass relations, as in previous figures. The dashed labeled arrows between subsets of **AdversaryOrganization** shown here and the various **Intents** indicate the **hasIntent** relationship.

The **Weapon** class is broadly classified by subtypes: **ChemicalWeapon**, **CyberWeapon**, **BiologicalWeapon**, **RadiologicalWeapon**, **NuclearWeapon**, and **ExplosiveWeapon** (commonly referred to as CBRNE). There are other taxonomies of weapon types and components which could be incorporated into AIT to make it more complete, so that the individual components of a biological weapon, for example, could be classified as such. The key point for AIT is that the subclasses of weapon define the subclasses of **TerroristAttack**: A **BiologicalAttack** requires a **BiologicalWeapon**, while a **CyberAttack** requires a **CyberWeapon**, a **NuclearAttack** requires a **NuclearWeapon**, and so on. This does not rule out multiple heredity—an attack could be both Explosive and Chemical, for example.

The **Target** taxonomy, only partially refined within the AIT representation at present, is shown in figure 8. The **Target** class is subdivided into **PublicSector** and **PrivateSector**, with the **PublicSector** class including NGO targets (**NGOTarget**) and **GovernmentTarget**. The **PrivateSector** is broken into sec-

tors by industry, which can be expanded as needed in two ways, first by adding more high-level industries and second by working down the subclasses to individual instances, such as a particular military base or a specific cruise ship.

There are other taxonomies of types of targets that could be incorporated to make it more complete (power plants, military bases, schools, the White House,

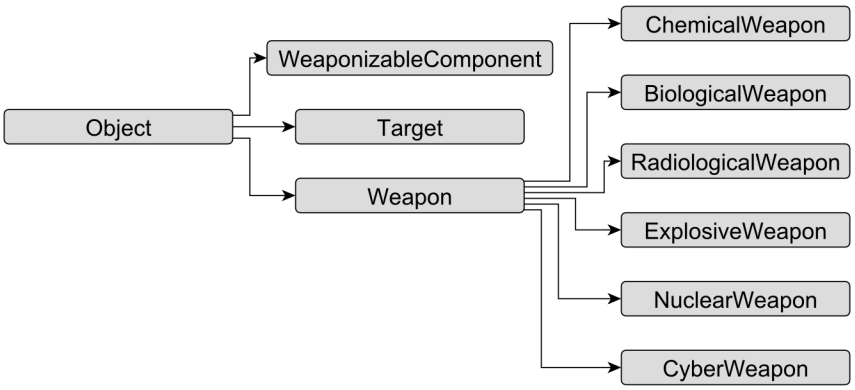

Figure 7: The **Object** taxonomy. The top concept here, **Object**, is the same as in figure 3. Arrows indicate subclass relations.

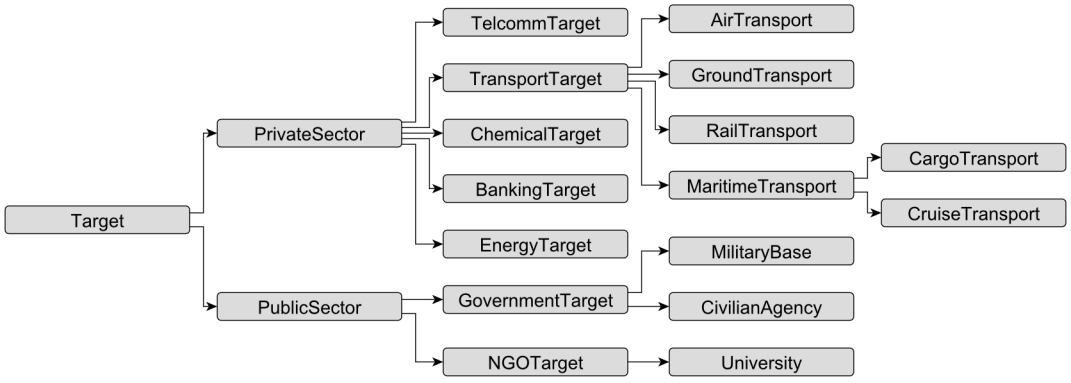

Figure 8: A portion of the **Target** taxonomy. Arrows indicate subclass relations.

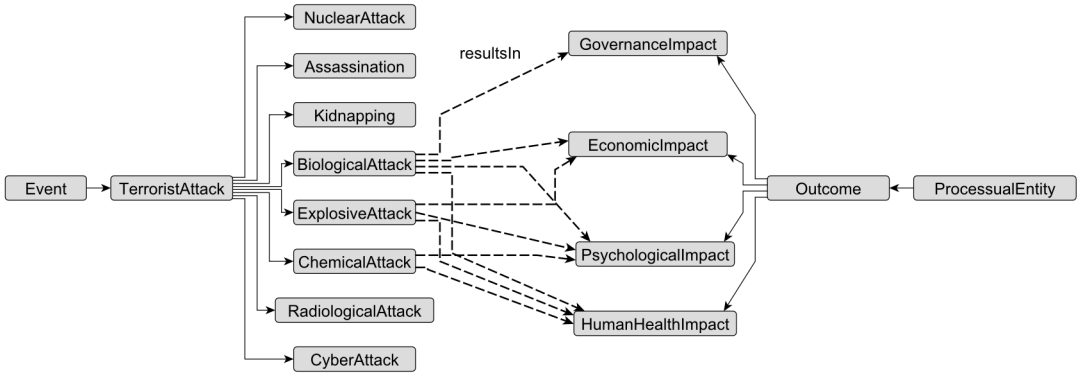

Figure 9: Different types of attacks result in different impacts (outcomes). From the left is the **TerroristAttack** taxonomy; from the right, the **Impact** taxonomy. Plain arrows indicate subclass relationships; dotted arrows indicate the **resultsIn** relationship between attack types and their impacts. For clarity, the **resultsIn** relation is only shown for biological, explosive, and chemical attacks. The complete AIT ontology contains this relation for all of the attack types.

etc.). Some targets exist in a **Place**, which are divided into the Continental United States (CONUS) or outside it (OCONUS), and can of course be subdivided into regions, states, cities, townships and eventually exact latitude and longitude. Other targets may also be temporally defined, such as the event/target called the "Super Bowl," or a Presidential Inauguration; we have excluded the temporal aspects of this ontology at present for simplicity, although we recognize its critical importance.

3.2.5 Outcomes & Impacts

The **Outcome** or impact of a **TerroristAttack** is a **ProcessualEntity** (see figure 3), and can be broadly classified by its **HumanHealthImpact**, psychological impact (**PsychologicalImpact**), **EconomicImpact**, and **GovernanceImpact**. Different kinds of terrorist attacks have different impacts, as shown in figure 9.

The different impacts (or types of **Outcome**) have a relationship to the original intents of an **AdversaryOrganization** as shown in figure 10 with the **supportsIntentTo** relation.

A key question in AIT is the link between the intentions of an **AdversaryOrganization** and the types of attacks they are likely to choose as a result of those intentions. The adversary chooses the attack type based, at least in part, on the **Outcome**

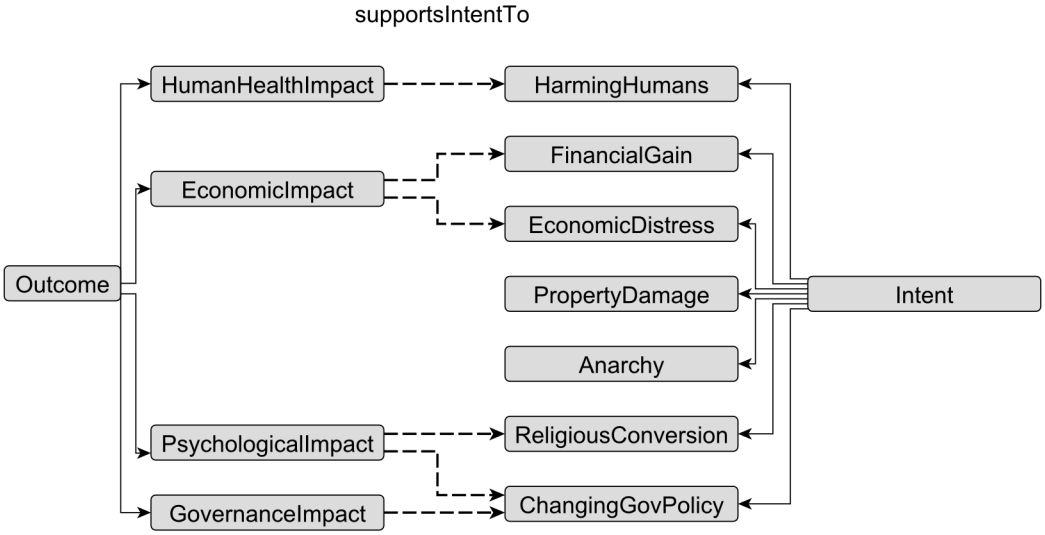

Figure 10: Examples of the **supportsIntentTo** relation between the **Outcome** of an attack and the **Intent** of the original **AdversaryOrganization**. Plain arrows indicate the subclass relationship; dashed arrows indicate the **supportsIntentTo** relationship.

they expect it to have, and whether that expected outcome supports their original intent. In figure 10, we show the relationship between types of **Outcome** and types of **Intent**. A **HumanHealthImpact** supports the intent of **HarmingHumans**, for example, while a **GovernanceImpact** can support the intent of changing government policy (**ChangingGovPolicy**), and an **EconomicImpact** supports the intent of creating **EconomicDistress**. This is clearly an oversimplification; it is an initial model of the very complicated factors that affect the likelihood of a particular kind of attack based on what the adversary is trying to achieve. With these relationships in place, we can reason that the groups most likely to be interested in a biological weapon are those with the intent of harming humans and causing economic and psychological distress, and those with the sole intent of religious conversion are not high priority ones to consider as likely planning or executing a biological attack.

In figure 11, we show a portion of the ontology that relates **TerroristAttack** types, the kinds of **Intent** held by various **AdversaryOrganization** types, and various types of **Outcome**. In this figure we can see that the intent to **ChangeGov-**

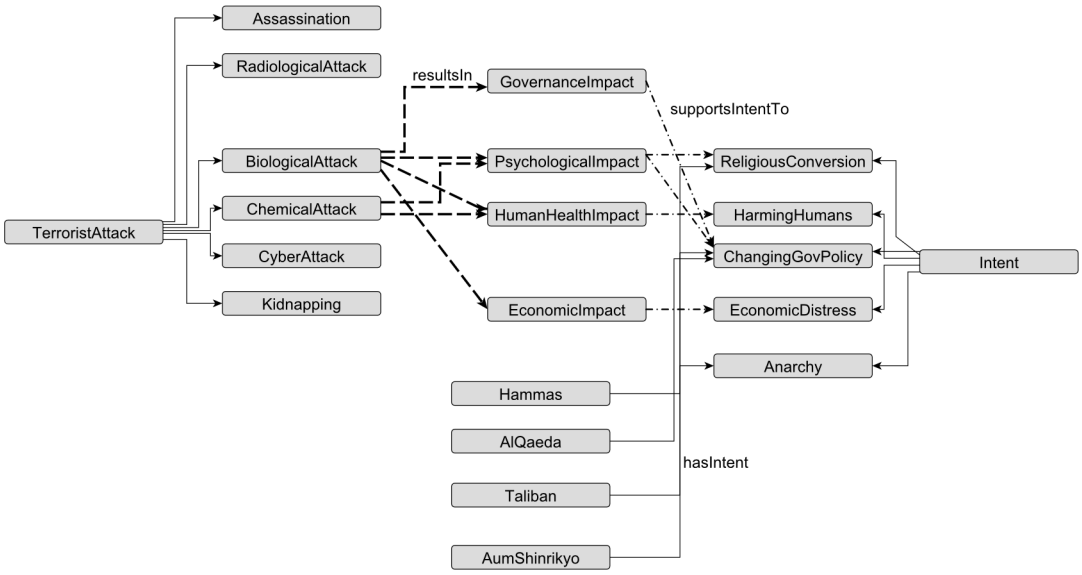

Figure 11: A portion of the ontology relating how attack types and outcomes implicate an adversary's intents. Solid arrows indicate subclass relationships *unless otherwise labeled*; dashed and labeled arrows indicate the **resultsIn** relationship; dashed/dotted labeled arrows indicate the **supportsIntentTo** relationship between outcomes and intents. Solid labeled arrows indicate the **hasIntent** relationship between an **AdversaryOrganization** and their **Intent**s. Thus, **ChangeGovPolicy** is held as an **Intent** by **AumShinrikyo**, and **Hamas**; and it **isSupportedBy GovernanceImpact** and **PsychologicalImpact**, which come from **BiologicalAttack**s (among others).

Policy is supported by any attack which results in either **PsychologicalImpact** or **GovernanceImpact**, for instance. As a **BiologicalAttack resultsIn** both of these outcomes, we can deduce that the groups which have the Intent of changing government policy might choose a **BiologicalAttack**. So adversaries such as **AumShinrikyo** and **Hamas** are reasonable suspects for such attacks. Other groups, such as the **Taliban** which are modeled here as focusing on **ReligiousConversion**, are therefore not likely agents of a **BiologicalAttack**.

3.2.6 Instances

Within the OWL framework, **instances** are the final (terminal) nodes in the graph, the specific entities in the real world which we are talking about. A particular gun in someone's hands is an instance of **Gun**; a particular vial of weaponized anthrax is an instance of **WeaponizedAnthrax**; thus what we know about the class **Gun**, in general, applies to that particular gun, and what we know about the class **WeaponizedAnthrax** applies to that specific vial. Instances inherit all of the properties of their class. (Hence, instance-of has a strong similarity to element-of as used in mathematics, see section 2.1.)

The human **members** of an organization, however, do not as individuals carry all of the properties of their organizations; what we know to be true about Al Qaeda—as a whole group—is not necessarily true of a given individual who is a member of Al Qaeda. Thus, a member of the group Al Qaeda is not an instance of the set (term) **AlQaeda**. Individual human beings have a "member of" relationship to their organizations which is clearly a different relationship from "instance of" above. "Member of" is called **memberIn** in AIT notation.[24]

However, the converse is not completely identical in the analysis; there is an asymmetry present. If a **memberIn** an organization is known to personally (as an individual) have some capacity or expertise, then the organization—simply by the fact of that member's presence in the group—has that capacity or expertise. For instance, if there is a particular person who is a nuclear engineer, and this member joins a particular group, then that group now has a nuclear engineering expertise.

Various terrorist attacks are instances of the class of terrorist attack. Knowing all the details about the assassination of JFK is not particularly helpful at the present time, though that can be modeled as an example within this framework. However, knowing the details of the recent (2011) attack in Norway: *Who was the adversary? What weapons did he use? Which targets did he select, and why?* allows us to infer some capacities and intents, which in the context of an ongoing incident, provides relevant support for intelligence reasoning.

[24]There is no explicitly defined "instance of" relation in AIT, as OWL ontologies automatically have such a relation.

4 Discussion

We have presented a preliminary model of a knowledge structure that could be useful for intelligence analysis. Starting with a model statement regarding what constitutes a terrorist attack, and developing from that statement a framework of concepts and relationships which can be used to answer questions regarding *who?* (which terrorist organizations exist and what are their characteristics); *what?* (what kind of weapons are used for what kind of attack, and what kind of attack leads to what kind of outcome); *where?* (geographical location as well as classes of targets); and *why?* (the intentions or motivations that lead to different choices of attacks, weapons, and targets). This model serves as a foundation for the more complex semantics within pre-incident analysis. Several choices were made in the development of AIT which require more discussion.

4.1 Ontological Commitments & Consistency

We discovered a number of upper-ontology related problems for a general ontology for terrorism research such as BOOT. The approach of using a single upper ontology to enforce consistency in smaller specialized domain ontologies, while appealing in its simplicity, suffers from a number of technical problems. These problems are very similar to problems in the foundations of mathematics. For instance, while set theory provides a common framework that can express almost all of mathematical structure, the set-theoretic expressions of these structures are so complex as to be unusable for practical work. In a similar way, enforcing the strictures of a single upper ontology onto multiple domain ontologies for terrorism research makes some things easy to express and other things too complex.

For instance, consider analyses that are political, social network based, economic, technological, and logistic. While there might be an upper ontology that can, in principle, express domain-specific languages for all of these, it is likely that the initial choices in how to structure language about the world that are made by a biologist thinking about biological weapons manufacture are quite different from an economist looking at terrorist funding flows, or an analyst concerned with terrorist social networks. If a single upper ontology makes it easy to talk about one domain at the expense of making another very hard to talk about, that is not a practical solution. Two approaches are currently being followed in this line.

The first approach uses very abstract upper ontologies as bases for larger, more detailed ontologies. BFO, for example, plays a central role in biomedical ontologies, with a goal of representing medical results, biological experimental processes,

and related biological and biomedical knowledge; all the ontologies within the Open Biomedical and Biological Ontology (OBO) Foundry are committed to working within the BFO framework. DOLCE, in contrast, is the exemplar for all the Wonderweb ontologies, with a focus on semantic web applications (though the Wonderweb project ended its funding some years ago, the ontological work has continued in business and education applications).[25] Other upper-level ontologies have also been developed over time.[26]

The AIT division of things into **MaterialEntity**, **ProcessualEntity**, and **Quality** classes is driven by the metaphysics of the Basic Formal Ontology. BFO divides the world into things which occur or unfold over time, known as occurrents (processes and temporal durations, for example), and things which exist in time as a whole, continuing in time as themselves, known as continuants. These two divisions exist at the topmost level of BFO, and there are no other concepts at this level. Within the occurrent branch of BFO is the **ProcessualEntity** that AIT models at its top level; within the continuant branch of BFO is found the **MaterialEntity** and the **Quality** classes that make up the rest of the AIT upper level. BFO has other subdivisions within continuants and occurrents, but the AIT model does not use them, so we defer discussion of these BFO terms.

BFO is a realist (revisionary) ontology, with the goal of modeling what *actually* exists in the world. This is not the only way to proceed; other foundational ontologies such as DOLCE have a cognitive bias (also referred to as a descriptive ontology), modeling how humans talk and think about the world, rather than strictly modeling what exists.[27] DOLCE includes in its top-level divisions both continuants and occurrents, as BFO does, but distinguishes "qualities" as a branch that is distinct from either of these. It also includes at this highest level a fourth term, "abstract" which is used to cover things that lack spatial or temporal qualities, such as "facts" (which BFO does not include explicitly at all). Thus, temporal intervals such as "the two months that it will take to grow a particular antibiotic" are considered a subclass of abstract in DOLCE, but would be under occurrents in BFO.

This distinction might seem trivial, and one might argue that as long as both ways of thinking about the world allow us to represent the information we have about those "two months," it doesn't matter which foundational ontology we use. This is a valid

[25]DOLCE and WonderWeb: `http://wonderweb.man.ac.uk/`; business and education applications of WonderWeb: `http://stlab.istc.cnr.it/stlab/The_Semantic_Technology_Laboratory_%28STLab%29`.

[26]See `http://en.wikipedia.org/wiki/Upper_ontology_(information_science)` for a list of upper ontologies. (Retrieved on 2011-08-24.)

[27]See: `http://wonderweb.semanticweb.org/deliverables/documents/D18.pdf`. For more on terminology used to describe upper ontologies, see [9].

argument, up to a point. However, by choosing a particular upper-level ontology, the ontology builders make an "ontological commitment," committing to dividing the world according to the metaphysics of that particular ontology, and therefore constraining or limiting what can be said within the ontological representation. For instance, classes in any foundational ontology inherit certain characteristics and can participate in certain kinds of relationships but not in others. The fact that we model those "two months" as a **ProcessualEntity** constrains what we can say about them. It allows us to infer that asking whether those "two months" are "blue," for example, is not a meaningful question, as processes in BFO and abstracts in DOLCE can't have qualities like color.

BFO in its original instantiation, however, could not model intentions or desires or the fact that a particular assertion was incorrect. DOLCE, in contrast, was built to include the ability to represent what someone is thinking about. We have worked around this limitation in AIT by modeling **Intent** as a subclass of **Quality**, which is consistent with the BFO usage of a quality as being a property of other things. This choice introduces no logical inconsistencies in AIT. However, we may find that on expanding the AIT vocabulary that what are cognitively simple concepts (e.g., "we thought person A was in Lebanon at time T, but that was wrong") are very complex to represent in the BFO framework, and more straightforward in the DOLCE or another framework. While using the BFO approach has been sufficient for AIT to this point, it may need to be reconsidered as modeling becomes more complex.

This top-down approach hides much of the consistency problem behind a wall of more usable ontologies, each of which models a non-overlapping set of topics within the framework of the upper-level ontology. So far this approach has not resolved the largest problems.

The second approach is to acknowledge that complete logical consistency may be impossible, and instead to modify logical analysis and reasoning procedures that operate on this (necessarily) inconsistent knowledge. In other words, we build reasoning agents that are tolerant to inconsistencies in their ontologies. Approaches of this sort go by names such as paraconsistent ontologies, paraconsistent logics, nonmonotonic reasoning, default reasoning, defeasible reasoning, etc. We are currently investigating these ideas in our ongoing research.

4.2 Future directions

Even within the foundational ontological framework we have chosen, key terms and relations within the AIT model are still missing. For instance: there is currently no rigorous connection between certain subclasses of expertise or **Capability** (and

the corresponding inferred ability to carry out a particular attack); the differing levels of granularity desired by different users has not been addressed; there is no representation of social factors, such as perceived authority; and (fundamental to ontologies in general) the problems of time, probability, and conditional statements have not been addressed. We consider each of these below.

A terrorist organization may have an **Intent** which is compatible with their likelihood of choosing to carry out a nuclear attack, but if they do not have the appropriate knowledge to acquire and deliver the appropriate weapon to their chosen target, any intent that they may have is not actionable. Intent simply suggests what kind of attacks a group would be interested in trying to obtain the expertise and weaponry for; it is a model of desire, rather than ability. Modeling the information required to determine whether a group has the ability—the expertise and capacity—to carry out a specific attack, is currently outside the AIT model.

This leads to the related problem of granularity, and the ability to expand upon the current framework to include the levels of fine detail that are required for specific questions. How much detail do we specify for the processes of building weapons for attacks? Knowing that X is needed for building weapons of types Y and Z may be more important for identifying what kind of attack is imminent, and thus more important to represent, than knowing in detail how X is used in constructing the weapon. However, if we want to be able to infer that chemical P could be used to build weapon Q, so that we can add P to a list of materials with restricted access, say, then we may need to include more detail about the processes of weapon construction.

Social relationships are not modeled in the AIT system; the idea that some specific person has the authority to carry out some specific action, or that a given organization believes that they have the authority to carry out an attack, is not represented. For instance, the role that *fatwas* play in authorizing attacks is not included. Nor are collaborations, or other tribal relationships that might lead to either obstructions or advantages for some given group carrying out a given attack.

This leads directly into a problematic area for ontologies and descriptive logic structures generally: anything that is modeled in an ontology is always considered to be a true statement. That is, statements are always either true or false, false statements are not supposed to be included, and false conclusions are a sign that something went wrong with either the knowledge base or the reasoning software.[28] However, in many domains statements are neither true nor false, but may have a probability of being true, depending on the evidence to date or the reliability of the

[28]The paraconsistent approaches mentioned above can approach this problem by allowing additional truth values, such as the set of values {true, false, neither, both}, or sets of truth values including the idea of "unknown."

source of the statement. In this particular domain, we may strongly believe that some given person was in, say, London last year and met with members of terrorist Group X, but we don't know this with absolute certainty. A vial of anthrax that went missing from a military facility could be used by Groups X, Y, or Z; but we can not be completely sure if Group Y has the expertise to turn it into a weapon and deliver it to a target. Or perhaps we were informed that Group Z had available personnel near the military facility at the time, and therefore may be in possession of the vial, but we do not completely trust the source of this intelligence.

The AIT system can not, at this point, take these sorts of partial, conditional, or probable truth into account. There are many interesting options available to add this capacity to AIT, including such tools as probabilistic logics and reasoning, fuzzy logic, possibility theory, and evidence theory [10].[29]

Another challenge is the representation of time. For instance, AIT cannot represent the concept that some piece of information was true at a time in the past (and was necessary for reasoning at that time) but is no longer true and should not be used in current reasoning. Much of the content of AIT are facts considered to be always true: Hamas can not suddenly become a right wing Christian organization, for example, and a biological attack must involve a biological weapon, by any reasonable definition. These sorts of facts do not change. But it may be, for example, that some terrorist group did not have the expertise or intent to use a nuclear weapon in 1995, but they do have that expertise now; or they did have it last year, but with the death of their expert they no longer have the needed expertise. That is, if we have built a reasoning system that can infer that Group X has a given expertise because person Y (who is a member of Group X) has the expertise, and we remove person Y from the knowledge base, then we will correctly infer that Group X does not currently have the expertise. However, deleting all of the information about person Y may lead to other problems; we would probably need to include more complex constraints, such as the concept that individuals are alive at certain times—person Y was alive from 1950 to 2010, it is now 2011—and the concept that only the expertise of living individuals is used in inferring the expertise of an organization. This is an issue that has helped shape ontological development for situational awareness [7], which needs to represent rapid changes in a situation over time, and an OWL ontology to allow changes over time exists [6]. This kind of time-dependency greatly increases the complexity of the system by including a time stamp on all statements, so that some statements are always true, and some are true only for various limited intervals of time. The inclusion of time both in the representation and in the reasoning will

[29]T. Caudell, F. Gilfeather, M. R. Taha, and D. Weinberg, Pre-Incident Indicator Analysis (PIIA) System, UNM ECE Technical Report, in preparation, August 2011.

be a future development.

4.3 The larger framework

The current AIT model is not the full implementation of BOOT required for pragmatic, real-world, use. Besides the actual modeling work described above that is needed to represent more of the concepts and relationships used in intelligence analysis, the actual ontology (or ontologies, across different domains of expertise) requires connections to other systems; connections to knowledgebases and databases, to methods for adding or updating specific information and instances, and to mechanisms for updating the core model itself.

The approach to linking ontologies and repositories, to update views based on new information and link different ontologies, is the topic of other parts of this project [5]. Systems for new information to be accounted for within the model need to be included, so that the most current information is retrieved and used in reasoning. The cultural blocks to sharing information collected by different governmental agencies across those agencies will not be solved by any knowledge engineering system; however, a shared vocabulary and knowledge structure that could be agreed to is a significant first step toward facilitating such data sharing for information fusion.

5 Supplemental Materials

This report, along with supplements, will also be available from Conjectural Systems beginning in November 2011. These supplements include the OWL file for the AIT ontology, as well as any future revisions of the ontology or errata for this paper. Please go to `www.conjecturalsystems.com` to obtain the files.

6 Acknowledgments

The authors would like to thank the members of the "Facets" group at UNM: Tom Caudell, George Luger, Frank Gilfeather, Steve Smith, Michael Healy, Chayan Chakrabarti, Renzo Sanchez-Silva, and Nate Gauntt for many fruitful discussions.

A AIT Relationship Table

The following table includes all of the relationships in AIT.

Relation	Domain	Range	Usage
hasAgent	Thing	Adversary Organization	This is the relationship between a terrorist attack and the adversary organization(s) which orchestrated it.
hasTarget	Thing	Target	This is the relationship between the target of an attack and either the adversary organization or the attack itself.
usesWeapon	Thing	Weapons	This is the relationship between the weapon used in the attack and either the attack or the adversary organization who is the agent of the attack.
hasLocation	Thing	Place	The relationship of occurring or existing in some place.
occursIn	Event	Place	The relationship between the event and the place it occurs in. It is a subtype of **hasLocation**.
existsIn	Material Entity	Place	The relationship between a material entity and where it happens to be at a given time. It is a subtype of **hasLocation**.
resultsIn	Terrorist Attack	Outcome	The relationship between a terrorist attack and the predefined categories of outcomes of interest.
supportsIntentTo	Outcome	Intent	The relationship between the outcome of an attack and the original intent of the adversary organization.
hasIntent	Adversary Organization	Intent	The relation between an adversary organization and any of its intents.
hasCapability	Organization or Person	Capability	The relationship between an organization and its capabilities, or between a person and their capabilities.
hasMember	Organization	Person	The relationship between an organization and its members (persons).
memberIn	Person	Organization	The inverse of **hasMember**.
targetOf	Target	Thing	Inverse of **hasTarget**.
resultOf	Outcome	Terrorist Attack	Inverse of **resultsIn**.
isSupportedBy	Intent	Outcome	Inverse of **supportsIntentTo**.

References

[1] Charles M. Bakewell. *Source Book in Ancient Philosophy.* Charles Scribner's Sons, 1939.

[2] John Burnet. *Early Greek Philosophy.* Wolrd Publishing Company, 1961.

[3] Herbert B. Enderton. *Elements of Set Theory.* Academic Press, 1977.

[4] Thomas R. Gruber. A translation approach to portable ontology specifications. *Knowledge Acquisition*, 5:199–220, 1993.

[5] Michael J. Healy, Renzo C. Sanchez-Silva, and Thomas P. Caudell. A categorical model for faceted ontologies with data repositories. Technical Report EECE-TR-11-0002, University of New Mexico, 2011.

[6] M. Kokar, C. Matheus, and K. Baclawski. Ontology-based situation awareness. *Information Fusion*, 10(1):83–98, 2009.

[7] C. Matheus, M. Kokar, and K. Baclawski. A core ontology for situation awareness. In *Proceedings of FUSION 03*, pages 545–552, 2003.

[8] Toby Segaran, Colin Evans, and Jamie Taylor. *Programming the Semantic Web.* O'Reilly, 2009.

[9] Salim K. Semy, Mary K. Pulvermacher, Leo J. Obrst, and Mary K. Pulvermacher. Toward the use of an upper ontology for u.s. government and u.s. military domains: An evaluation. Technical report, Submission to Workshop on Information Integration on the Web (IIWeb-04/VLDB-2004), 2004. MITRE Technical Report 04B0000063.

[10] B. Ulicny, G. M. Powell, C. F. Brown, M. M. Kokar, C. J. Matheus, and J. Letkowski. Augmenting the analyst via situation-dependent reasoning with trust-annotated facts. In *Proceedings of the 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA 2011)*, 2011.