Ontology of Intelligence

Preprint · March 2019

DOI: 10.13140/RG.2.2.25163.54569

1 author:

Nicolae Sfetcu
University of Bucharest

Ontology of Intelligence

Nicolae Sfetcu

March 17, 2019

Sfetcu, Nicolae, "Ontology of Intelligence", SetThings (March 17, 2019), MultiMedia Publishing (ed.), URL = https://www.setthings.com/en/ontology-of-intelligence/

Email: nicolae@sfetcu.com

A partial translation of:
Sfetcu, Nicolae, "Epistemologia serviciilor de informații", SetThings (4 februarie 2019), MultiMedia Publishing (ed.), DOI: 10.13140/RG.2.2.19751.39849, ISBN 978-606-033-160-5, URL = https://www.setthings.com/ro/e-books/epistemologia-serviciilor-de-informatii/

Ontology of Intelligence

In intelligence, the ontological problem is related to the nature and characteristics of entities that threaten and are threatened. According to Eric Little and Galina Rogova, "[t]hreat is a very complex ontological item and, therefore, a proper threat ontology must be constructed in accordance with formal metaphysical principles that can speak to the complexities of the objects, object attributes, processes, events and relations that make up these states of affairs." (Eric G. Little and Rogova 2006)

Björn Müller-Wille's argument on security and threats helps to highlight the interdependence between threatening and threatened entities. In this sense, intelligence analysts must define both what constitutes a threat and what is threatened. Thus, a significant threat ontology must include both threats and threatened entities. (Vandepeer 2011)

Developing a threat ontology requires a taxonomy. A potentially useful taxonomy used in describing the security analysis is provided by Buzan, Waever and Wilde. (Buzan et al. 1998) They argue that the security analysis involves three distinctive actors. From this taxonomy, adapted for the intelligence analysis, the following entities emerge:

- a *referent* is what or who is threatened;
- an *analyst* acts as a "threat determinant"; and
- a *threat actor* who is evaluated by the analyst as threatening the referent.

The threat referent is usually the state, namely the survival of the state and its population. (Singer 1958) *Quadrennial Homeland Security Review* describes security as the requirement to "“[p]rotect the United States and its people, vital interests, and way of life." (Department of Homeland Security 2010, ix) Globalization makes it increasingly difficult to identify the interests of the state, even of the population. Under the Montevideo Convention, the four generally accepted requirements for statehood are: a permanent population; defined territory; a government; and the ability to enter into relations with other states. (Australia Department of Defence 2009) These requirements generally refer to four aspects of a threatened state, namely: population, territory, government, and interests. The nature and characteristics of state and non-state threats consider how these entities can threaten these four factors.

State interests include threatening the political influence of the state, limiting the state's ability to develop favorable or strong relations with other states, regional stability, economic stability, development and financial infrastructure of the state, (Australia Department of Defence 2009) energy resources, communication lines and citizens' ability to travel.

Non-state actors (especially those who threaten) are often undefined. A useful definition for capturing them is "“...any person or group of people who act independently of formal governments." (Australia Department of Defence 2002)

Threat evaluation is defined by Steinberg et al (Omand 2009) as "the process of estimating and anticipating the effects on the situations of planned or expected/anticipated actions by participants, including interactions between the action plans of several actors (e.g., assessing susceptibilities and vulnerabilities to estimated/projected threatened actions, considering their planned actions). " It follows that different functions and elements of threat assessment have to be considered. (Rudd 2008) The ontological complexity of threat elements requires ontological analysis based on metaphysics that can effectively classify different types of complex objects, properties and attributes, events, processes and relationships that are of interest to various decision makers.

Situation and Threat Assessment (STA) processing refers to context-dependent information about the dynamic facets of reality (Eric G. Little and Rogova 2006) so that STA ontologies must be able to capture the reality structure by providing capabilities to describe the multitude of types of relationships (e.g., space-time, intentional, and dependency relationships) that exist between different situational entities (and their aggregations) at different levels of granularity. (Bittner and Smith 2003) For this reason, the ontologies to be used to assess the situation and threats require a wider understanding of the types of relations and relational entities found initially in Aristotle's writings (Aristotle 1991) and later formalized by Edmund Husserl. (Husserl 1900) It is important for STA ontologies to be structured in a superior general metaphysical framework in order to break down the most abstract elements of the field of interest and the relationships between them.

In *An Ontological Analysis of Threat and Vulnerability*, Eric G. Little and Galina L. Rogova developed a "threat ontology" (ThrO), (Eric G. Little and Rogova 2006) a modified version of the basic formal ontology (Grenon and Smith 2004) composed of two orthogonal sub-levels, SNAP and SPAN, which are designed to capture the spatial and temporal features of ontology. Based on the distinction between the *continuants* and the *occurents*, they have ontologically modeled complex spatio-temporal objects with a formal bifurcation between objects as elements that can exist entirely at some point in space and time versus processual events whose parts and partial relationships are constantly evolving over time, and therefore there are never entirely in a certain place or time. The distinction helped to avoid certain traditional philosophical problems of identity. The basic formal ontology is designed in accordance with the theory of mereotopology, (Smith 1996) a theory that combines a logic of parts and partial relationships (e.g., mereology) with a logic of spatial expansion and connection (i.e., topology) language capable of treating the multitude of ontological objects required for higher-level fusion processing, e.g. objects, properties/attributes, spaces, times, and the many simple and complex relationships between them. The information used to assess the threats is extremely uncertain, contradictory, redundant, of varying importance and low fidelity. This makes it necessary to ”incorporate uncertainty, reliability, and imprecision into the characterization of qualitative mereotopological relations.” (Eric G. Little and Rogova 2006)

At a higher level, as a whole, people exist as relational entities, not just as collections of independent elements. The problem here is of ontological significance, where the modeling of the element collections is not the same as the modeling of the whole, because the same complex element can be understood differently depending on whether it is understood as a collection or as a whole. (Smith 1996) The theory of mereotopology provides a way to describe formally the types of complex partial relations between them that contain elements such as threats, in which the three elements of intent, capacity and opportunity are in a formal relationship fundamental dependence. The capture of metaphysical relationships, such as fundamental dependence, is necessary for the design of threats ontologies. Given the complexity of the threats, it is essential to design an ontological framework that can include many types of relationships necessary for the correct breakdown of complex elements. (Eric G. Little and Rogova 2006)

The ontological definition of certain essential features of the parts and their relationships, together with proximity and constraint metrics, will then allow better definition and identification of dispersed groups. (E. G. Little and Rogova 2005)

An ontology for threat analysis and action must be able to shape ontological distinctions between potential and viable threats. This provides a better understanding of how threats (ie intentions, capabilities, and opportunities) can exist and can be changed over time. Escalating threats from a state of potency to a state of viability could be avoided by using appropriate threat mitigation techniques. (E. G. Little and Rogova 2005)

On the other hand, for Barry Smith in *Ontology for the intelligence analyst*, (Smith 2012) the Strategy of Semantic Enhancement (SE) (Salmen et al. 2011) is based on the use of simple ontologies whose terms are used to mark (or annotate) source data artifacts in a coherent way. Terms in a SE ontology are linked together in a simple hierarchy through the relationship "is_a" (or subtype). Each term appears once in this hierarchy and is paired in a stable way with parent and child hierarchy terms, even if new terms are added to ontology over time. This stability is important because the success of the strategy requires ontologies that can be repeatedly reused to annotate many different types of data in ways that serve multiple different community of analysts, thus contributing to creating an increasingly common operational picture. SE is designed to be at the same time more stable and more flexible than traditional approaches to harmonization and integration, which are usually based on ad hoc mapping between data models, their effectiveness over time often degrades. (Smith 2012)

SE ontologies are organized on three levels with successive degrees of flexibility: 1) a unique, small, domain-neutral Upper-level Ontology (ULO), for which our selected candidate is the official ontology; (Volkswagen Foundation 2002) 2) Mid-level ontologies (MLO), formed by grouping terms that refer to specific areas of action or specific tasks such as inter-agency information exchange; (Smith, Vizenor, and Schoening 2009) 3) low-level ontologies (LLO) that focuses on specific areas. The SE approach is designed to be of maximum use to intelligence analyst users. Ontological content is created only as a response to analysts' situational needs, and architectural requirements are designed to ensure a consistent evolution of SE resources without sacrificing the flexibility and expressivity required in real-world deployment. (Smith 2012) The SE Strategy can determine collaborative ontological development and re-use for multiple internal and external data collection purposes.

Bibliography

Aristotle. 1991. "The Metaphysics." 1991. https://www.amazon.com/Metaphysics-Great-Books-Philosophy/dp/0879756713.

Australia Department of Defence. 2002. "Future Warfighting Concept." http://www.defence.gov.au/publications/fwc.pdf.

Australia Department of Defence, Canberra. 2009. "Defending Australia in the Asia Pacific Century: Force 2030 (2009 Defence White Paper)." Text. 2009. https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1516/DefendAust/2009.

Bittner, Thomas, and Barry Smith. 2003. "A Theory of Granular Partitions." In *Foundations of Geographic Information Science*, edited by M. Duckham, M. F. Goodchild, and M. F. Worboys, 117–151. London: Taylor & Francis.

Buzan, Barry, Ole Wæver, Ole Waever, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Department of Homeland Security. 2010. "Quadrennial Homeland Security Review Report: A Strategic Frameworkfor a Secure Homeland." https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

Grenon, Pierre, and Barry Smith. 2004. “SNAP and SPAN: Towards Dynamic Spatial Ontology.” http://ontology.buffalo.edu/smith/articles/SNAP_SPAN.pdf.

Husserl, Edmund. 1900. “Logische Untersuchungen.” 1900. https://philpapers.org/rec/HUSLU.

Little, E. G., and G. L. Rogova. 2005. “Ontology Meta-Model for Building a Situational Picture of Catastrophic Events.” *2005 7th International Conference on Information Fusion* 1: 8-NaN.

Little, Eric G., and Galina L. Rogova. 2006. “An Ontological Analysis of Threat and Vulnerability.” *2006 9th International Conference on Information Fusion*, 1–8. https://doi.org/10.1109/ICIF.2006.301716.

Omand, David. 2009. “TheNationalSecurityStrategy: Implications for the UK Intelligence Community.” https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/national_security_strategy1.pdf.

Rudd, Kevin. 2008. “The First National Security Statement to the Australian Parliament, Address by the Prime Minister of Australia.” https://dfat.gov.au/people-to-people/public-diplomacy/programs-activities/Pages/speech-by-prime-minister-kevin-rudd-to-the-parliament.aspx.

Salmen, David, Tatiana Malyuta, Alan Hansen, Shaun Cronen, and Barry Smith. 2011. “Integration of Intelligence Data through Semantic Enhancement.” In *STIDS*.

Singer, J. David. 1958. “Threat-Perception and the Armament-Tension Dilemma.” *The Journal of Conflict Resolution* 2 (1): 90–105. https://www.jstor.org/stable/172848.

Smith, Barry. 1996. “Mereotopology: A Theory of Parts and Boundaries - ScienceDirect.” 1996. https://www.sciencedirect.com/science/article/pii/S0169023X96000158.

———. 2012. “Ontology for the Intelligence Analyst.” 2012. https://philarchive.org.

Smith, Barry, Lowell Vizenor, and James Schoening. 2009. “Universal Core Semantic Layer.” In .

Vandepeer, Charles. 2011. “Rethinking Threat: Intelligence Analysis, Intentions, Capabilities, and the Challenge of Non-State Actors.” Thesis. https://digital.library.adelaide.edu.au/dspace/handle/2440/70732.

Volkswagen Foundation. 2002. “Basic Formal Ontology.” http://basic-formal-ontology.org/.