Chapter 10. An Ontological Framework for Understanding the Terror-Crime Nexus

Colonel Bill Mandrick, Ph.D.

Introduction

Transnational terrorists and criminals may collaborate, appropriate shared tactics, and otherwise benefit from interaction, resulting in bolstered capabilities, enhanced organizational infrastructure, improved access to resources, and expanded geographic reach. Historical examples also indicate that terrorist and transnational criminal groups may evolve, converge, transform, or otherwise alter their ideological motivations and organizational composition to appear similar.¹

In an increasingly interconnected world, people within one complex network can seek out and merge with people in other complex networks, thereby creating a network of networks. The merging of complex social networks (i.e., globalization) can contribute to the betterment of society by increasing capabilities to solve difficult problems. However, the merging of complex networks also results in deviant globalization where illicit “cross-border economic networks produce, move, and consume things as various as narcotics and rare wildlife, looted antiquities and counterfeit goods, dirty money and toxic waste, as well as human beings in search of undocumented work and unorthodox sexual activities.”² Terrorist and insurgent networks benefit from deviant globalization by connecting with TCOs in order to employ their capabilities and generate funds to continue operations. The National Security Council’s SCTOC states that:

Colonel Bill Mandrick, U.S. Army Reserve, Ph.D., is a civil affairs officer who has planned and led civil-military operations in austere environments. He is a Senior Fellow at the Center for Special Operations Studies and Research within the Joint Special Operations University. His current research pertains to the use of property information for joint intelligence processes.
Terrorists and insurgents increasingly are turning to TOC to generate funding and acquire logistical support to carry out their violent acts. The Department of Justice reports that 29 of the 63 organizations on its FY 2010 Consolidated Priority Organization Targets list, which includes the most significant international drug trafficking organizations (DTOs) threatening the United States, were associated with terrorist groups. Involvement in the drug trade by the Taliban and the Revolutionary Armed Forces of Colombia (FARC) is critical to the ability of these groups to fund terrorist activity. We are concerned about Hizballah’s drug and criminal activities, as well as indications of links between al-Qa’ida in the Lands of the Islamic Maghreb and the drug trade. Further, the terrorist organization al-Shabaab has engaged in criminal activities such as kidnapping for ransom and extortion, and may derive limited fees from extortion or protection of pirates to generate funding for its operations.3

The purpose of this chapter is to provide a semantic framework (i.e. ontology) that will enhance the counterterrorism analyst’s ability to understand and describe the nexus between transnational terrorist organizations and criminal organizations. This framework will enhance the management of disparate data as it becomes available to the analyst, planner, or decision maker in CT operations.4 For this chapter, consider a case where a CT analyst has access to already existing data sets on terrorist activities and related events. These disparate data sets are structured, meaning that they are created in compliance with a predefined data model, for use in some specific information system. The result is that each data set is ‘stove-piped’ or incompatible with the other data sets. The analyst also has access to near-real-time tactical level reports from various sources, ranging from maneuver unit situation reports to site exploitation team forensics reports. Much of this data is unstructured—i.e., it is in report format consisting of text strings, descriptive sentences, paragraphs, and images. With some effort, this data can be ‘tagged’ with category terms taken directly from the ontological framework, making it interoperable with any other data that is similarly aligned.

The enhancement of data in this way, (a) generates alignment because it adds consistent descriptions to the inconsistent sets of codes, and (b) does this in a way that allows software tools to reason over the result. Enhanced data can be ingested into an IT system that facilitates analysis based upon
a powerful set of algorithms. With properly collated data, the system can graphically depict correlations between physical objects, realizable attributes, locations, and events. The ultimate purpose of the system is predictive analytics, based upon large amounts of aligned data. The CT analyst can use the following ontological framework to organize the disparate data so that it can be analyzed to identify these hidden correlations, and then disseminated (shared) across the larger CT enterprise.

Ontology is the disciplined study of what is, of the kinds and structures of objects, properties, events, processes, and relations in every area of reality. From this philosophical perspective, ontology seeks to provide a definitive and exhaustive classification of entities in all spheres or domains of being. As a theoretical discipline concerned with accurately describing the taxonomy of all things that exist, philosophical ontology is synonymous with classical metaphysics. High quality ontologies define, disambiguate, and relate the objects, attributes, and processes that make up any domain of interest.

The ontology to be described here is intended to enhance intelligence processes, and assist analysts, planners, and decision makers in analyzing, defining, and representing the elements (nodes and links) that make up any dynamic human network, such as an insurgent network, terrorist network, or TOC network. The intelligence products produced by using this framework will inform the find, fix, finish, exploit, analyze, and disseminate process as prescribed in Joint Publication 3-26, Counterterrorism.

The proposed semantic framework provides an extendable vocabulary to which any data source (information element) that describes some aspect of the complex operational environment (OE) could be translated. In order to provide coverage of any aspect of an OE, the chosen strategy was to build a framework sufficient to express general-level facts but which were easily extended in a consistent and uniform way to ontologies having finer grained content as needed. Ultimately, the framework is designed to assist analysts and planners in understanding the form of these networks, as well as their capabilities and functions, and the types of activities they participate in. These elements form nodes and links (relationships) in a graph-like structure, which can be used for enhanced reasoning by both humans and machines.

Information that is managed in accordance with this semantic framework will be in a format that will assist operations planners in their reasoning and decision making about clandestine human networks within the complex OE. The proposed framework consists of a small set of ontologies, which are more
effective for organizing information because they consist of more specific categories than those that make up overly general acronyms or mnemonic memory devices. For example, the civil information management process contributes to understanding the OE through civil considerations analysis, which focuses upon areas, structures, capabilities, organizations, people—the ASCOPE mnemonic. Systems analysis identifies centers of gravity (e.g., some highly connected individual) and enhances situational understanding by focusing upon political, military, economic, social, information, infrastructure (PMESII), systems within the OE, as well as the physical environment and time. These two mnemonic devices can be combined into the following crosswalk matrix, which helps analysts and operators to organize information about the OE.

Nodal analysis reveals the interrelationship between people, organizations, entities, and locations. The individual nodes represent complex relationships between a person, place, or physical thing that are a fundamental component of a system and link the behavioral, physical, or functional relationships between the nodes. Critical nodes are those identified as being essential and whose disruption or removal becomes a single trend analysis point failure. Link analysis is the process of identifying and analyzing relationships between personnel, contacts, associations, events, activities, organizations, and networks to determine key or significant links. Analysts

![Table 1. The PMESII—ASCOPE crosswalk matrix assists in the identification of types of data needed for civil considerations and systems analysis. This same data will become inputs for nodal and link (relationship) analysis. Source: Author](image-url)
use link analysis to determine who is involved with whom and how they are involved.

The ontological framework described here is for the enhancement of civil information management, especially where it is concerned with nodal and link analysis for complex social systems. Applied ontology offers a strategy for the organization of scientific information in computer-tractable form, drawing on concepts not only from computer and information science but also from linguistics, logic, and philosophy. Data sets that are aligned with this ontological framework can be integrated with each other so that they become one larger enhanced data set. Enhanced data sets facilitate analytics intended to show hidden correlations between system variables. As will be described later in the chapter, data that is aligned in this way (i.e. enhanced data) contributes to JIPOE.

**Definitions for Terrorism and Transnational Crime**

Terrorism is defined in Joint Publication (JP) 3-07.2, *Antiterrorism*, as:

> the unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political.

The ontology of terrorism starts by decomposing this definition into discrete elements such as an act of violence, the belief that is a motive for that action, the government or group of people that are the target of the action, and the goal of the action. What is implied in this definition is that there are relationships between individual persons, and that these relationships make up a terrorist organization that is a participant in the act of terrorism. Furthermore, the terrorist organization is the bearer of certain dispositions and capabilities—see Figure 1.

TOC is defined as “those self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms. There is no single structure under which transnational
organized criminals operate; they vary from hierarchies to clans, networks, and cells, and may evolve to other structures. The crimes they commit also vary …” 10 This definition includes social relationships between individual persons in an organization or structure, such as: associate of, subordinate of, relative of, commander of, et cetera. The definition also describes the actions, motivations, and locations of these organizations. TOC organizations will also have certain realizable attributes such as dispositions to act and enabling capabilities. Dispositions and capabilities are realized by certain activities.

The basic ontological structure of any organization has similar elements—see figure 1. The organization will be the bearer of certain realizable attributes. Any realizable attribute is realized by the organization being a participant in some action (or set of actions), which has location in some geopolitical territory. The relationships depicted in italics, are a nexus, bond, link, or junction; a means of connection between things or parts. 11

An Ontological Framework for Understanding the Transnational Terrorism-Crime Nexus

At issue is how to make sense of this complex crime-terrorism phenomenon and oversee the implementation of cross-cutting activities that span geographic regions, functional disciplines, and a multitude of policy tools that are largely dependent on effective interagency coordination and international cooperation. 12
The wrong ontology and epistemology, largely based on mirror-imaging information-age network theories onto clandestine cellular networks, have led many network and counter-network theorists astray. Most theorists and practitioners cognitively mirror information-age networks to clandestine cellular networks, which is largely incorrect. Failure to understand the aspects of clandestine cellular networks has huge implications to both the way network theorists study and model networks, as well as how network attack theorists recommend defeating clandestine cellular networks.\textsuperscript{13}

CT analysts, operations planners, and command staff members are charged with making sense of the complex OE, which is doctrinally defined as a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.\textsuperscript{14} In order to analyze and define the elements of an OE, analysts adopt a systems perspective that is intended to provide an understanding of significant relationships within interrelated PMESII, and other systems relevant to a specific joint operation.\textsuperscript{15} The systems perspective facilitates the identification of nodes and links within and between systems. These nodes and links (relationships) are the subjects of planning and decision making processes—e.g., observing, targeting, engaging, and influencing.

For the purposes of analyzing the nexus between TCOs and terrorist organizations, the analyst must adopt the same systems perspective toward those types of systems, and then identify the nodes and links that connect them to other PMESII systems—e.g., some person involved in TOC may be associated with some political organization. This section describes a semantic framework (i.e., ontology) that is intended to assist analysts, planners, and decision makers in analyzing, defining, and representing the elements (nodes and links) that make up an OE, where TCOs and terrorist organizations sometimes collaborate in order to advance their interests through criminal activities.

The proposed framework consists of a small set of ontologies for organizing information in conjunction with the PMESII and ASCOPE crosswalk matrix. It provides an extendable vocabulary to which any data source (information element) that describes some aspect of the OE could be translated. In order to provide coverage of any aspect of an OE, the chosen strategy was to build a framework sufficient to express general-level facts but which were
Figure 2. 34 Categories of the basic formal ontology. Source: permission of authors Robert Arp, Barry Smith, and Andrew Spear, Building Ontologies with Basic Formal Ontology, MIT Press, August 2015.
easily extended in a consistent and uniform way to ontologies having finer
grained content as needed.16

The proposed framework extends from the basic formal ontology (BFO),
which is a small, upper level ontology that is designed for use in suppor-
ting information retrieval, analysis, and integration in scientific and other
domains. BFO is a genuine upper ontology designed to serve data integration
in scientific and other domains.17 It consists of only 34 classes, from which
13 will be employed in this framework—see Figure 2 for a full rendering
of the BFO taxonomy. BFO adopts a view of reality as comprising: (1) con-
tinuants, entities that continue or persist through time, such as physical
objects, qualities, and functions; and (2) occurrents, the events or happenings
in which continuants participate. The continuant category is then further
subdivided into those entities that exist independently, such as a person,
and those entities that are ontologically dependent upon some other entity
for their existence, such as some person’s engineering or forgery capability.
The subtypes of continuant and occurrent entities are represented in BFO
as independent (material entity) and dependent (generally and specifically),
continuant and occurrent.

The BFO provides the categories needed to decompose and analyze the
complex OE. Analysis starts with decomposition, which is the process of
separating some composite entity into constituent parts or elements. Decomp-
osition exposes individual elements (nodes in a graph), and the relation-
ships between them. The result is a semantic framework (i.e., ontology) that
facilitates the organization of data about the OE. The semantic framework is
populated with instance-level data that refers to the actual objects, realizable
attributes, events, and relationships within the OE. Its purpose is to assist in
the organization of data in such a way that it becomes useful for reasoning
and decision making. The semantic framework will also help to identify gaps
in the analyst’s knowledge of the OE.

An independent continuant entity is a continuant entity that is the bearer
of qualities (and realizable entities), and is a participant in occurrent pro-
cesses. This category of entities includes physical objects that are the bearers
of qualities, functions, roles, and dispositions—e.g., a person is an indepen-
dent continuant entity that is the bearer of certain physical properties, and
realizable attributes such as capabilities, functions, or roles. The independent
continuant is represented as either a physical object (agent—person or orga-
nization) or object aggregate, such as a network.
Another type of independent continuant entity includes geographic features, which are further subdivided into natural and human-constructed geographic features. They are important for this framework because they are where clandestine networked cells operate. The data and information about geographic features will be addressed later in the chapter (see the section below on generically independent continuant—information artifacts). Independent continuant geographic features are represented as natural (hill, mountain, canyon, valley), or humanly-constructed (crops, industry, marketplace, city) geographic features.

The next major category in BFO is the dependent continuant entity. This category includes entities that are ontologically dependent upon independent continuant entities (i.e. their bearers) for their existence—i.e., they inhere in, or are borne by, other entities. Dependent continuant entities are further subdivided into generically dependent continuants (GDC) and specifically dependent continuants (SDC), and will be described later in the chapter.

Generically dependent continuant entities can migrate from one independent continuant entity to another—e.g., a PDF file can be transferred or copied to several hard drives simultaneously. The physical byte array may be different, but the generic content or meaning migrates with each instance of the PDF. For example, your jpeg image of Bill Clinton may be physically distinct from my exact copy, but the identical image migrates with each copy. We will return to GDC (information artifacts) later in the chapter.

SDC entity is defined as a continuant entity that depends upon precisely one independent continuant entity for its existence. The former is dependent on the latter in the sense that, if the latter ceases to exist, then the former will, as a matter of necessity, cease to exist also. SDC entities exist as an attribute of an independent continuant, and cannot migrate to another independent continuant—i.e., an independent continuant is the bearer of some SDC. SDC entities include qualities and realizable entities such as capabilities, emotions, functions, and motivations. Qualities are exhibited, manifested, or realized in some independent continuant entity. They are represented in BFO as physical characteristics (color, height, mass, weight).

A realizable entity is defined as a SDC entity that has at least one independent continuant as its bearer, and whose instances can be realized (manifested, actualized, executed) in associated processes. Examples of SDC entities include the roles of people in an organization or the dispositions of people that are realized by their actions and interactions. A disposition
is defined as a realizable entity (a power, potential, or tendency) that exists because of certain features of the physical makeup of the independent continuant (e.g., a person) that is its bearer.\textsuperscript{20} Examples include the capabilities, emotions, functions, and motivations that inhere in people and organizations. Examples of SDC realizable include: capability, emotional disposition, functions, and roles.

Emotional dispositions (action tendencies) and behavioral motives are properly treated in affective science, which is the study of emotions and of affective phenomena such as moods, affects, and bodily feelings. It combines the perspectives of many disciplines, such as neuroscience, psychology, and philosophy.\textsuperscript{21} The BFO treats emotional dispositions (action tendencies) and behavioral motivations as BFO: realizable dispositions, which inhere in some person. These dispositions are realized in (BFO: occurrent) mental processes such as emotion occurrences and appraisals, which are addressed next.\textsuperscript{22}

The next BFO category pertains to events, processes, happenings, or activities. An occurrent process is something that happens, or unfolds, through time and space, and always depends on some material entity. Recall that dependent continuant entities, such as roles, functions, or capabilities, are realized through occurrent processes. Naturally occurring processes include such things as geologic processes, weather events, biological processes, and planetary orbits. However, this chapter is concerned with another type of occurrent process, wherein agents (persons or organizations) are the participants. Actions are events that people perform with intentions and for reasons. One and the same action can be specified as intentional under some description and as purely physical under another description. But in order to be an action an event must have at least one description under which it is specified as intentional.\textsuperscript{23}

A transnational terror-crime nexus can be represented as part of the complex operational environment. The ontological framework assists the analyst’s understanding of the terror-crime nexus, and its place in the complex OE, by facilitating the creation of nodes and links (relationships) in a graph-like structure—a prerequisite for decomposition and analysis. This results in enhanced reasoning and information management. Figure 3 represents the basic ontology of a networked cell as the bearer of some realizable attributes, and is a participant in some occurrent processes (actions), which has location some geopolitical territory.
The final BFO category to be considered in this chapter pertains to the data and information that is about the terror-crime nexus and the complex OE. GDCs, or information artifacts, can exist in (i.e., migrate between) more than one object at the same time—e.g., a certain pdf that exists in several different hard drives at the same time. The story of War and Peace migrates to every physical instantiation to include paper copies or digital versions in someone’s reader. Information artifacts (e.g., descriptions, plans, grid coordinates, or images) are the subject of their own information artifact ontology, which is currently being developed.

**Joint Intelligence Preparation of the Operational Environment**

Data that is created, organized, or aligned with the above described ontological framework will be in a better format for JIPOE, which is the analytical process used by joint intelligence organizations to produce intelligence
assessments, estimates, and other intelligence products in support of the joint force commander’s decision-making process. As previously described, JIPOE analysts adopt a systems perspective that is intended to provide an understanding of significant relationships within interrelated PMESII, and other systems relevant to a specific joint operation.

The systems perspective, that is representable with nodes and links in a graph, facilitates understanding of the continuous and complex interaction of friendly, adversary, and neutral systems. Products developed during this step include network nodal and link analysis diagrams associated with adversary and neutral PMESII and other systems—see Figure 4 below. Some of the nodes will inevitably be linked to nodes in other PMESII systems, which may indicate a center of gravity—e.g., an influential political figure who controls access to land with valuable resources. Though there may be a wide variety of interactions between networks, dependency focuses on the scenario in which the nodes in one network require support from nodes in another network.

Figure 4. The Systems Perspective of the Operational Environment. Source: Joint Publication 2-01.3.
This data will enhance intelligence analysis at both the operational and strategic levels, as analysts study the nodes and links related to criminals, crime suspects, incidents, issues, and trends. By collecting and assessing this data, they can identify relationships or connections between different crimes in different places—e.g., suspect names, organization names, event locations, activity types, or even capabilities can show connections hiding within the available data. The analysis can then be used to provide insights that can drive or support CT operations and strategy, provide timely warning of threats, and influence government policy and decisions.

Conclusions: Applying the BFO Framework to Information Management Processes

The ontological framework described is intended to; (a) facilitate the CT analyst’s ability to understand and describe the nexus between transnational terrorist organizations and criminal organizations, and (b) enhance the management of disparate data as it becomes available to the analyst, planner, or decision maker in CT operations. This framework is applicable to situations where CT analysts have access to already existing structured data sets on terrorist activities and related events—this data will most likely be stovepiped in an IT system. It also applies to unstructured data from near-real-time tactical level reports, such as unit situation reports, or site exploitation team forensics reports, which contain detailed information from technical and forensic examination of documents, cell phones, computers, biometric information, weapons, bomb making, and other materials. Unstructured data consists of text strings, descriptive sentences, paragraphs, technical terms, and images. With some effort, this data can be ‘tagged’ with category terms taken directly from the ontological framework, making it interoperable with any other data that is similarly aligned—i.e., any data that is enhanced by the ontological framework becomes part of one large data set.

Endnotes


5. In a series of e-mail exchanges to the author on 18 March 2015, Ron Rudnicki described an overview of the Common Core Ontologies being developed for the Intelligence Information Warfare Directorate (I2WD).


7. Ibid., 6-7.


16. In a series of e-mail exchanges to the author on 18 March, 2015, Ron Rudnicki described an overview of the Common Core Ontologies being developed for the Intelligence Information Warfare Directorate (I2WD).


19. Ibid., 98.

20. Ibid., 101.


25. Ibid., xii.


27. For more information on enhanced intelligence data see: http://ncorwiki.buffalo.edu/index.php/Distributed_Development_of_a_Shared_Semantic_Resource.