Building an Ontology for Cyberterrorism

Namosha Veerasamy [1], Marthie Grobler [1, 2], Basie Von Solms [2]
[1] Council for Scientific and Industrial Research, Pretoria, South Africa
[2] University of Johannesburg
nveerasamy@csir.co.za
mgrobler1@csir.co.za
basievs@uj.ac.za

Abstract:
Cyberterrorism and the use of the Internet for cyberterrorism is an emerging field. Often cyberterrorism activities overlap with traditional hacking and Information and Communication Technology (ICT) Infrastructure exploitation. As a result, the defining and differentiating characteristics of cyberterrorism can easily be misunderstood. The use of an ontology specifically developed for cyberterrorism, will provide a common framework to share conceptual models. By using an ontology, the internal and external environment of a field (in this case, cyberterrorism) can be captured together with the relationships between the environments. This paper proposes an ontology to identify whether a cyber event can be classified as a cyberterrorist attack or a support activity. The role of the cyberterrorism ontological model will be to provide a better structure and depiction of relationships, interactions and influencing factors by capturing the content and boundaries in the field of cyberterrorism.

The ontology will be developed using a cyberterrorism framework covering influencing factors, together with a compiled network attack classification ontology. Classes will be drawn from research carried out on the use of ICT in the support of cyberterrorism. As defined in this research, a cyberterrorism attack consists of a high-level motivation that is religious, social or political. The individual/group can furthermore be classified as having a specific driving force depending of the level of extremism or revolutionary thinking. Thus, the ontology will take into consideration the motivating characteristics that play a significant role in contributing towards the definition of cyberterrorism.

Overall, this paper promotes the understanding of the field of cyberterrorism and its relation to ICT manipulation, together with the use of the Internet to support terrorism in general. Ontologies enable a common view on a specific domain to generate knowledge that can be shared and reused. Ontologies can further be populated with specific dynamic instances of information and therefore can be used to generate real-world scenarios. In this paper, the proposed ontological model will form a knowledge base for the field of cyberterrorism and will provide instances that aim to convey realistic cyberterrorism situations and support examples.

Keywords: anti-forensics, Internet, terrorism, ICT, propaganda, social-networking

1. Introduction

The emergence of the cyberterrorism domain means that a new group of potential attackers on computer and telecommunication technologies may be added to the list of traditional criminals threatening Information and Communication Technology (ICT) Infrastructure (Janczewski, Colarik 2007). In addition, the use of the Internet as both enabler and support mechanism for cyberterrorism can potentially lead to misunderstanding of the field.

A further complication is the overlap between cyberterrorism activities and traditional hacking and ICT Infrastructure exploitation. As a result, the defining and differentiating attributes of cyberterrorism can be misunderstood. In many instances, there are defining characteristics that separate traditional criminal cyber attacks from cyberterrorism. So how does one specify the attributes of a cyberterrorist attack in order to identify the defining concepts? This paper proposes the use of ontologies to define whether a cyber event can be characterised as cyberterror, a support to terrorism or an unclassified other cyber event. This model is build by first looking at the background of ontologies and the motivation for building a cyberterrorism specific ontology. Thereafter, the classes of the ontological model are discussed: actors, effects, motivation, objectives, practices, targets and cyber events. The application of the model is practically demonstrated on examples. Finally, future work in terms of the cyberterrorism ontology is presented. The main contribution of this research is the supplementation of the existing knowledge base of both cyberterrorism and cyber attacks, by enabling the convenient classification of an attack facilitated by ICT through a cyberterrorism specific ontological model.

2. Background to Ontologies

According to Gruber (1993), an ontology is defined as a formal and explicit representation of a shared conceptualization. Frantz and Franco (2005) argue that ontologies provide a shared and common understanding of a domain to be communicated among people and computers to facilitate knowledge sharing and reuse. In addition, Frantz and Franco explain that ontologies provide a formal explicit conceptualization (i.e. meta-information) that describes the semantics of information of the static domain capture of knowledge based systems. Moreover, Noy and McGuiness (2001) provide the following reasons for developing an ontology:

- To share a common understanding of the structure of information among people or software agents.
- To enable reuse of domain knowledge.
- To make domain assumptions explicit.
- To separate domain knowledge from the operational knowledge.
- To analyze domain knowledge.

Uschold and King (1995) proposed a four-step methodology for developing ontologies: identify the purpose of the ontology, build the ontology, evaluate and document. The step for building an ontology consists of three iterative sub-steps: ontology capture, ontology coding and integrating existing ontologies. Ontology capture is the identification of the key concepts and relationships in the domain of interest by producing precise unambiguous text definitions for such concepts and relationships. Ontology coding is the explicit representation of the conceptualisation in some formal language. Ontology integration refers to using other ontologies during the capture and coding process (Uschold, King 1995). The next section will explain these steps in more detail in terms of the cyberterrorism ontology.

3. Building a Cyberterrorism Ontology

Ontologies provide a common framework to share conceptual models. By using an ontology, the internal and external environment of a field can be captured in conjunction with the relationships between these environments. This paper proposes that an ontology can be used to identify and capture the content and boundaries in the field of cyberterrorism. The role of the ontology will be to provide a better structure and depiction of relationships, interactions and influencing factors, as suggested by Noy and McGuiness (2001) in Section 2.

The initial step of building an ontology is to determine the purpose thereof. The aim of the proposed ontology is to determine whether a cyber event can be classified as cyberterror or a support to terror. The next step is to build the ontology by capturing key concepts and relationships, coding the explicit representation of the conceptualisation in the ontology language (in this case, Protégé), and integrating it with other ontologies. Ontologies provide the ability to form a knowledge base for a specified field. This step enables the formal capturing of domain knowledge to promote sharing and exchange.

Protégé is ontology specific software that serves as a knowledge base editor and thus facilitates the capturing of an ontology. It was developed at the Stanford University for both the Windows and Linux environments. Protégé provides the ability to define classes, relationships and properties. It is openly available and can be downloaded from http://protégé.stanford.edu. Protégé also comes with visualisation packages such as GraphWiz that allows the asserted and inferred classification hierarchies to be visualised (Horridge et al. 2004). The visualisations help provide succinct images of the deductions drawn from the inserted data and specifications, see Figures 1 to 4.

The next step is the evaluation of the built ontology.The reasoning capabilities within Protégé are used to infer new information from the asserted ontology as part of the evaluation process. Protégé has a number of built-in reasoners or inference engines that can be used to make deductions and queries based on the input specifications (the asserted statements and definitions). In this research project, different reasoners drew the same conclusions and therefore did not influence the evaluation results. An ontology can contain information in an asserted form (stated as a fact) and thus it is valuable to operate on inferred relationships (derived as conclusion from given facts) rather than on the asserted relationships. This process minimizes the loss of information about what has been explicitly asserted by the users (Knublauch et al. 2005). An important consideration is therefore the background logic that is used for reasoning certain arguments.

The final step is the documentation of the ontology. According to Prieto-Diaz (2003), ontologies are built very much ad-hoc with the initial development of a controlled vocabulary for the subject area of interest. This is then organised into a taxonomy whereby key contents are identified and the concepts defined and related to create an ontology. Therefore, to initially develop the cyberterror ontology, a taxonomy was developed to identify the core concepts in the field of cyberterrorism. The process of building a taxonomy and ontology is very much intertwined. The various steps of building an ontology is iterative (Capture, Code and Integrate). The next section looks at the development of the cyberterrorism taxonomy and ontology using Protégé.

4. Classes in the Cyberterrorism Ontology

Previous research by van Heerden, Irwin and Burke (2012) was used as the basis for some of the underlying classes of the proposed cyberterrorism ontology. Van Heerden et al. proposed a Network Attack Ontology to classify computer-based attacks. For the cyberterrorism ontology, the core classes of Actor, Effect and Motivation were adopted and slight modifications were made to address specific requirements within the field of cyberterrorism.

The main classes in the proposed cyberterrorism ontology are the Actor, Cyber Event, Objective, Motivation, Practice, Effect and Target. For example, every Cyber Event would have an Actor entity, Objective, Motivation, Practice, Effect and Target. The goal of the ontology (based on the initial taxonomy whereby the main concepts are defined) was to determine whether a CyberEvent could be classified as a Cyberterror or a SupportTerror, based on its specified attributes in the other classes. Before explaining the functioning of the main class CyberEvent, a discussion on the development of each of the classes follows.

4.1 Actor

Van Heerden, Irwin and Burke (2012) formed the Actor Class with the following sub-classes:

- Commercial competitor
- Hacker
  - Script kiddie hacker
  - Skilled hacker
- Insider
  - Admin insider
  - Normal insider
- Organised criminal group
- Protest group

Figure 1 shows the actor classes and sub-classes that were carried over from the Network Attack ontology to the Cyberterror ontology. In ontologies, classes and sub-classes have an “is a” relationship. For example, every class in Protégé is defined as being a Thing and thereafter sub-classes are assigned to classes.

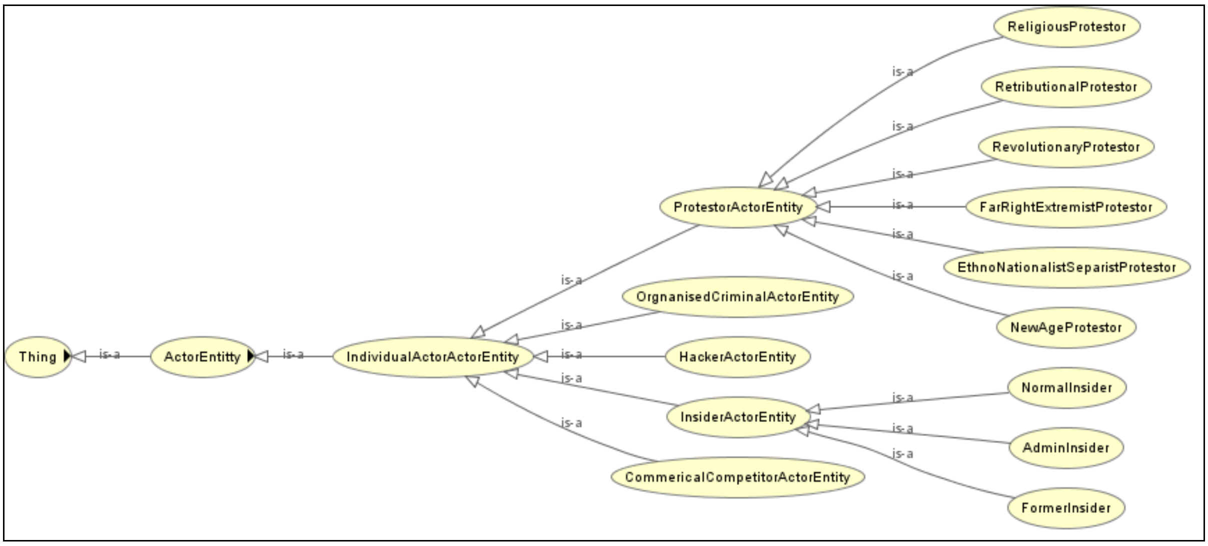

Figure 1: ActorEntity Class

The original class Protest Group was extended to include examples of the type of groups that correspond to terrorist activities and included Religious, Ethno-nationalist separatist, Revolutionary, Far-right extremist, New Age and Retributional (Veerasamy 2009b). The original Actor class was also adapted to cater for individual and group activities by defining the core actor entity as an individual and a group entity as consisting of a number of individuals. In the next section, the possible effects are discussed.

4.2 Effects

Van Heerden, Irwin and Burke (2012) make use of the sub-classes Null, Minor, Major and Catastrophic in their Effects class of their Network Attack Ontology (see Figure 2).

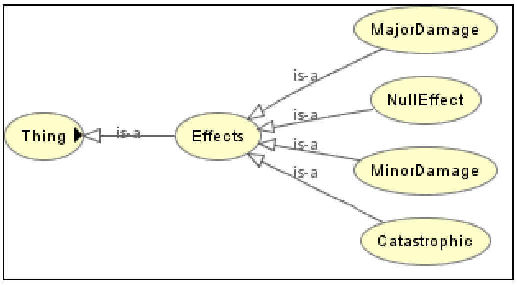

Figure 2: Effects Class

Explanations taken from Mirkovic (2004) define "Null" as being no effect on the target, "Minor" to recoverable damage, "Major" to non-recoverable damage and “Catastrophic” refers to damage of such a nature that the target ceases to operate as an entity, for example declaration of bankruptcy. For this specific cyberterrorism ontology taxonomy, while the sub-classes were carried over, the definitions are adapted slightly:

- Null - no effect on target.
- Minor - recoverable damage to target (minimal financial implications and technical recovery required).
- Major - extensive financial or loss of reputation (more complex technical recovery required).
- Catastrophic - extensive damage such that the target failed to operate (massive damages-financial, technical and possibly life).

Now that the possible effects have been explored, the discussion moves on to an explanation of possible motivations.

4.3 Motivation

The Motivation class pertains to the high-level motivation or driving force of the actor. Often determining the motivation is subjective. However, a few high-level objectives have been identified from literature. Van Heerden, Irwin and Burke's (2012) sub-classes for Motivation were Criminal, Ethical, Financial, Military and Recreational.

Denning (in (Gordon, Ford 2002)) talks about cyberterrorism being done to intimidate or coerce a government or its people to further political or social objectives. In addition, various terrorist groups are also strongly driven by religious beliefs, for example Al Qaeda prescribes to the principles of Islam. Therefore, while ordinary criminals or attackers may not have political, religious or social motivations, cyberterrorists do have these types of driving forces. Additional sub-classes that were added to the Cyberterrorism ontology included Political, Social and Religious. A summary of the motivation class is given in Figure 3. For example, an actor may have a more specific objection that stems from the high-level motivation. The different types of objectives are discussed next.

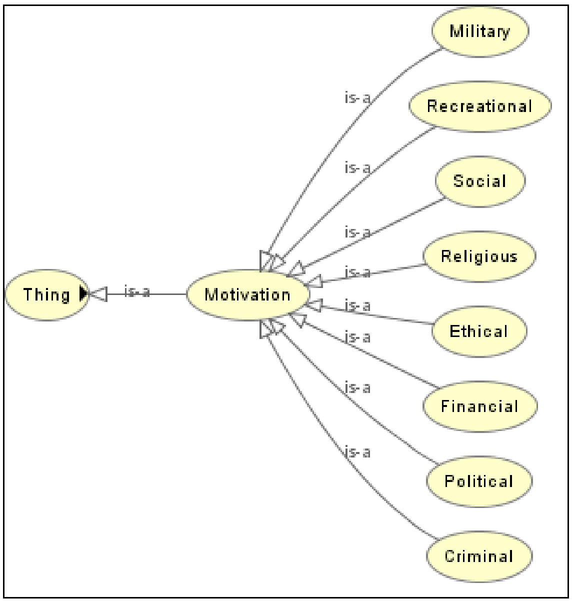

Figure 3: Motivation Class

4.4 Objectives

The Objectives class refers to the low-level purposes of the attack and is sub-divided into Malicious Objectives (correspond to Cyberterror CyberEvents) and SupportTerror CyberEvents (correspond to a support activity). Based on previous research by Veerasamy (2009b) and Jenkins (2006), the Objectives class is divided as follows:

- Malicious or attack objective
  - Destroy
  - Disrupt
  - Force demands
  - Interfere
  - Intimidate
  - Kill or maim
  - Protest
  - Publicity
  - Steal
  - Terrify
- Support Objective
  - Finance
  - Intelligence
  - Logistics
  - Planning
  - Propaganda
  - Recruitment

    - Social services (support for families of suicide attackers)
    - Training

Objectives are not mutually exclusive. For example, a religious terrorist could be trying to interfere in operations, as well as finance the terrorist organisation. Therefore, a terrorist could have multiple objectives. The classification of a Cyberterror Event or SupportTerror Event will be also influenced by the effect, practice and motivation. The defining requirements for a Cyberterror CyberEvent and SupportTerror CyberEvent are given in more detail in Section 4.7. The discussion now moves on to typical practices applicable to the cyberterrorist field.

4.5 Practices

Veerasamy (2009b) introduced some of the typical cyberterrorist practices as part of a framework covering influential factors in the field of cyberterrorism. These include the defacing of web sites, distribution of disinformation, spreading propaganda, denial of services using worms and viruses, disrupting of crucial services, corrupting of essential data, and stealing credit card information for funds. Furthermore, some of the uses of the Internet for cyberterrorism were classified as web literature, social-networking tools, anti-forensics and fundraising (Veerasamy, Grobler 2010). Based on the practices in literature, the Practices sub-class is structured as follows:

- Anti-forensics
    - Draft message folder
    - Encryption
    - IP-based cloaking
    - Proxies and anonymisers
    - Steganography
- Data manipulation
    - Denial of service
    - Infections (worm, trojan or virus)
- Fundraising
    - Auctioneering
    - Casinos
    - Credit card theft
    - Donations
    - Drugs
    - Phishing
- Social networking
    - Applications
    - Blogs
    - Forums
    - Gaming
    - Music
    - Virtual personas
    - Websites
- Web defacement
    - Cross-side scripting
    - SQL injection
- Web literature
    - Biographies
    - Encyclopaedias
    - Essays
    - Manuals
    - Periodicals
    - Poetry
    - Statements
    - Video

The list of practices is an indication of the range of practices that cyberterrorists typically utilise. Due to the growth of technology and digital capabilities, this list is not exhaustive and therefore can be extended as new practices are identified. Cyberterrorists usually have specific targets in mind when an attack is launched or in support of an attack. A discussion of the cyberterrorist targets follows.

4.6 Target

This class refers to the target of the cyber event or the type of system that the event occurs on. In order to distinguish between a criminal activity, a small-scale incident and a high-impact cyberterrorist event, the Target class is divided as follows (see **Error! Reference source not found.**):

- Government or critical
- Individual
- Organisational

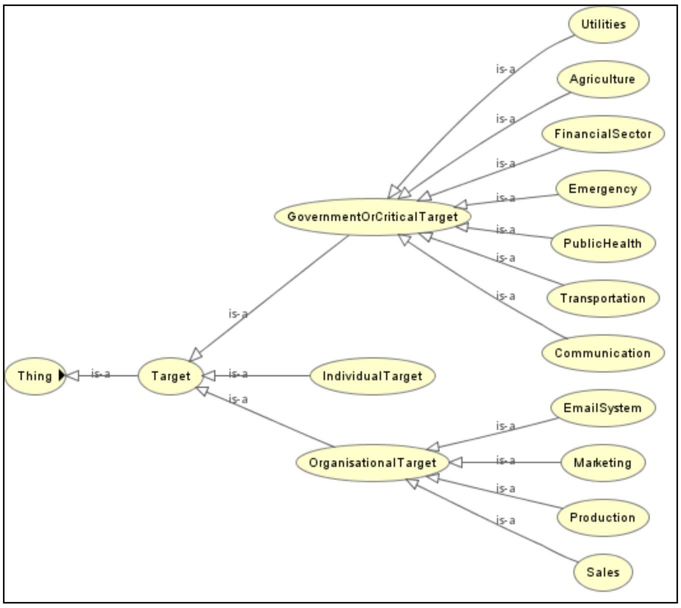

Figure 4: Target Class

For example, terrorists would target high-impact infrastructure which would fall into governmental or organisational facilities. A virus affecting an unsuspecting single user's email address book would not be classified as cyberterrorist and therefore cyberterrorists targets would seek to have a detrimental effect on a critical target. The various industries and services that fall within the government or critical sector are Agriculture, Communication, Emergency, Finance, Public Health, Transportation and Utilities (Veerasamy 2009a). Furthermore, critical systems in an organisation that would be a prime target for a cyberterrorist attack include email systems, marketing, production and sales.

The various classes in the ontology have been discussed. The discussion now moves on to an explanation of the main class CyberEvent which links the previously discussed classes.

4.7 CyberEvent

The CyberEvent class forms a critical aspect as the aim of the overall ontology is to classify a cyber event as Cyberterror, a SupportTerror or as an unclassified OtherCyberEvent.

Cyberterrorism is defined as "A purposeful act, personally or politically motivated, that is intended to disrupt or destroy the stability of organizational or national interests, through the use of electronic devices which are directed at information systems, computer programs, or other electronic means of communications, transfer, and storage" (Desouza, Hensgen 2003). However, ICT infrastructure may not always be the target of an attack but can also serve a supporting role. For example, various techniques, networks and electronic devices may not always be used in a direct attack, it can still provide assistance in terms of communication, guidance, information gathering, preparation and financial backing (Veerasamy 2009a). Thus, it is imperative to differentiate between a cyber event being an actual cyberterrorist attack, and a cyber event that provides technology support to terrorism in general. In order to differentiate between a Cyberterror, SupportTerror and unclassified OtherCyberEvent, assertions were made in the ontology. The assertions relate to the motivation, objective, target, effect and practices.

With ontologies, the core assertions or defining attributes of classes need to be specified. The main class in the ontology is the CyberEvent class. Every CyberEvent could have more than one Actor, Objective, Practice and Target but only one Effect. The reasoning behind the assertion that a CyberEvent needs only one Effect, is that in order for a CyberEvent to be classified as Cyberterror it needs to have a major or catastrophic effect. For example, a cyberterrorist could be carrying out two activities simultaneously, fundraising and web defacement. The fundraising would be classified as a SupportTerror CyberEvent and the web defacement as Cyberterror CyberEvent. The fundraising may have a minor effect but overall the combined practices could have a major or catastrophic effect and the CyberEvent could be classified as Cyberterror CyberEvent.

Furthermore, in this ontology, the Cyberterror CyberEvent and SupportTerror CyberEvent attributes needed to be specified with detailed conditions in order for the cyber event to be correctly classified. To be classified as a CyberterrorEvent the following conditions were specified:

- The effect had to be major or catastrophic - terrorist attacks do not aim to have minor or null effect.
- The motivation had to be political religious or social - terrorists are primarily politically, religiously or socially motivated.
- The practice had to be data manipulation or web defacement - attacks usually constitute malicious behaviour like interfering with a web site of manipulating data using worms, Trojans or viruses.
- The target had to be an organisation, government or critical target - an attack on a minor individual computer or system would not cause terror.

To be classified as a SupportTerror CyberEvent, the event should have:

- A motivation that needed to be political religious or social - terrorists are primarily politically, religiously or socially motivated.
- A practice that had to be anti-forensics, fundraising or web literature - these are mainly practices that support terrorism support activities for recruitment, propaganda and planning.

Now that the various classes in the Cyberterror ontology have been introduced, this section is summarised briefly.

4.8 Overview of Ontology

The classes Actor Entity, CyberEvent, Objectives, Motivation, Practice, Effect and Target were identified to be the main classes in the Cyberterror ontology and form the basis for the development of the ontology. The discussion now moves on to the application of the ontology through the classification of individual cyber events.

5. Ontology Application: Classification of CyberEvent (Individuals)

The description of the development of the ontology is given in the previous section. The main class is CyberEvent, which links all the other classes together. The CyberEvent class provides a means through which an event can be classified by the ontology as a Cyberterror, SupportTerror or OtherCyberEvent. Thereafter, individual examples can be instantiated with data and the reasoner tool in the ontology can be run in order to determine the cyber event's classification.

This section contains examples of individual-based incidents to show whether the reasoner can correctly classify the cyber event. Every cyber event has its own unique attribute specifications that would classify it as a Cyberterrorist CyberEvent, SupportTerror CyberEvent or an unknown OtherCyber Event. The attribute specifications of the individual cyber events are listed next.

5.1 Australian Sewerage Incident

Vitel Boden attacked the Australian Sewerage System in November 2001 (Lemos 2002). He was a former consultant on the project and after being refused a full-time position sought revenge. For this real-life example, the attribute specifications are as follows:

- Actor is a former insider.
- Motivation is social.
- Effect is major damage.
- Objective is a malicious objective of interfere.
- Practice is data manipulation (SCADA manipulation).

- Target is government or critical.

After the reasoner was run, it was inferred that the CyberEvent was of type Cyberterror.

5.2 Pakistan India Example

The political conflict between Pakistan and India is represented in the ontology as follows:

- Actor is a protestor.
- Motivation is political.
- Effect is major damage.
- Objective is a malicious objective of destroy.
- Practice is web defacement.

After running the reasoner, it was inferred that this example could be classified as a Cyberterror CyberEvent.

5.3 Example Religious

Similarly, another example was set up to test for the deduction of Support CyberEvents:

- Actor is a religious actor.
- Effect is minor damage.
- Objective is the support objective of finance.
- Motivations are financial and religious.
- Practice is casinos.

The inference engine in Protégé deduced that this example is a Support CyberEvent.

5.4 Overview of Ontology

The ontology was set up to classify a cyber event as Cyberterror, SupportTerror or OtherCyberEvent depending on the details specified for its Actor, Motivation, Objective, Practice and Target attributes. Various examples can be instantiated in the ontology and therefore classified.

6. Future Work and Conclusion

This paper proposed the use of ontologies to clarify the field of cyberterrorism. It is relevant as it aims to classify a cyber event as a being cyberterrorism or a support to terrorism. The other attributes in the ontology also show the dynamic use of ICT by terrorist groups in manipulating systems to their advantage.

The attributes shown in the proposed ontology do not solely represent the only characteristics of a cyberterror attack but rather represent an abstraction of the most important considerations. By combining the ontology with other classification and development models, a better understanding of cyberterrorism can be gained. Later on, it is envisaged that the ontology proposed in this paper will open the dialogue for further discussion on the development of cyberterrorism by classifying attacks and identifying new practices, targets, motivations and objectives. In addition, the ontology captures important information about cyberterrorist motivations, objectives, practices, effects, targets and actors. The paper also provides practical insight into the communication and intimidation methods used by terrorists over cyberspace.

References

Desouza, K.C. & Hensgen, T. (2003), "Semiotic Emergent Framework to Address the Reality of Cyberterrorism", *Technological Forecasting and Social Change,* vol. 70, no. 4, pp. 385-396.

Frantz, A. 2005, "A semantic web application for the air tasking order", *10th International Command And Control Research And Technology Symposium Experimentation Track* .

Gordon, S. & Ford, R. (2002), "Cyberterrorism?", *Computers & Security,* vol. 21, no. 7, pp. 636-647.

Horridge, M., Knublauch, H., Rector, A., Stevens, R. & Wroe, C. 2004, "A Practical Guide To Building OWL Ontologies Using The Protégé-OWL Plugin and CO-ODE Tools Edition 1.0", *The University Of Manchester* .

Gruber, T.R. (1993), "A translation approach to portable ontology specifications", *Knowledge acquisition,* vol. 5, no. 2, pp. 199-220.

Janczewski, L. & Colarik, A.M. (2007), *Cyber warfare and cyber terrorism,* Information Science Reference.

Jenkins, B.M. (2006), "The New Age of Terrorism" in McGraw-Hill, New York, pp. 118–119.

Knublauch, H., Horridge, M., Musen, M., Rector, A., Stevens, R., Drummond, N., Lord, P., Noy, N.F., Seidenberg, J. & Wang, H.(2005), "The Protégé OWL Experience", *Proc. OWL: Experiences and Directions Workshop*.

Lemos, R. (2002), "What are the real risks of cyberterrorism", *ZDNet, August,* vol. 26.

Mirkovic, J. & Reiher, P. (2004), "A taxonomy of DDoS attack and DDoS defense mechanisms", *ACM SIGCOMM Computer Communication Review,* vol. 34, no. 2, pp. 39-53.

Noy, N.F. & McGuinness, D.L. (2001), *Ontology Development 101: A Guide to Creating Your First Ontology*, Stanford Knowledge Systems Laboratory Technical Report.

Prieto-Díaz, R. (2003), "A faceted approach to building ontologies", *Information Reuse and Integration, 2003. IRI 2003. IEEE International Conference on*IEEE, , pp. 458.

Uschold, M. & King, M. (1995), "Towards a methodology for building ontologies", *Workshop on Basic Ontological Issues in Knowledge Sharing*.

Van Heerden, R.P., Irwin, B. & Burke, I.D. (2012), "Classifying network attack scenarios using an Ontology", *Proceedings of the 7th International Conference on Information Warfare and Security.* Academic Conferences.

Veerasamy, N. (2009a), "A high-level conceptual framework of cyberterrorism", *Journal of Information Warfare,* vol. 8, no. 1, pp. 42-54.

Veerasamy, N. (2009b), "Towards a conceptual framework for cyberterrorism", *Proceedings of the 4th International Conference on Information Warfare and Security*, ed. L. Armistead, Academic Conferences International, 26-27 March, pp. 129.

Veerasamy, N. & Grobler, M. (2010), "Terrorist use of the Internet: Exploitation and Support Through ICT Infrastructure", *Proceedings of the 6th International Conference on Information Warfare and Security.* Academic Conferences, pp. 260.