Towards a Cyberterrorism Life-Cycle (CLC) Model

N Veerasamy [1, 2], M Grobler [1, 2] S von Solms [2]
[1] CSIR, [2] University of Johannesburg, Pretoria, South Africa
nveerasamy@csir.co.za
mgrobler1@csir.co.za
basievs@uj.ac.za

Abstract: Cyberterrorism has emerged as a new threat in the Information and Communication Technology (ICT) landscape. The ease of use, affordability, remote capabilities and access to critical targets makes cyberterrorism a potential threat to cause wide-scale damage. Cyberterrorism is often incorrectly perceived as encompassing all cybercrimes. However, cyberterrorism differs from cybercrime in various ways including motivation, attack goals, techniques and effects. Motivations for cyberterrorism, which is similar to terrorism in general, stem from religious, social and political views. Cyberterrorists generally would seek to have high impact in order to gain publicity for their cause, whereas cybercriminals often prefer to have their acts undetected in order to hide their financial theft, fraud or espionage. Therefore, there are various factors that drive the development of a cyberterrorist. This paper proposes a model for the development of cyberterrorism in order to show the various influential forces. The Cyberterrorism Life-Cycle (CLC) model presented in this paper is composed of five phases: Prepare, Acquaint, Choose, Execute, and Deter (PACED). In addition the paper looks at various factors, including social, practices, objectives, targets and countermeasures, which are mapped onto the PACED phases in order to show the interaction and dynamic nature during the life-cycle development.

Keywords: cybercrime, cyberterrorism, life-cycle

1. Introduction

Terrorism brings with it a wave of potential devastation and uncertainty. Terrorism has thus entered a new arena in that Information and Communication Technology (ICT) has become both a prime target and weapon to perpetrate and cause onslaughts on innocent victims and high-profile points of interest.

The most cited definition for cyberterrorism comes from Denning which was given before the Special Oversight Panel. It states: “Cyberterrorism is the convergence of terrorism and cyberspace... unlawful attacks and threats of attack against computers, networks, and the information… done to intimidate or coerce a government or its people in furtherance of political or social objectives... to qualify a cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear [15]”.

Desouza and Hensgen define cyberterrorism 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” [8]. Overall cyberterrorism can be seen as the threat or act of causing harm in order to create fear and shock, targeting critical ICT infrastructures based on political, religious or social reasoning.

Janszewski and Colarik have stated that “The emergence of cyberterrorism means that a new group of potential attackers on computer and telecommunication technologies may be added to 'traditional' criminals" [17]. In some cases, when a cyber attack is carried out it is often labeled as cyberterrorism. However, all cybercrimes are not cyberterrorism acts. Cyberterrorists and cybercriminals may use the same underlying security and hacking skills to break into systems but the underlying motivation, objective and effects may differ. Lachow [20] has explained that whilst cyberterror tries to cause a political change and targets innocent victims through computer-based violence or destruction, cybercriminal activities aim to have an economic gain from individuals and companies by carrying out fraud, identity theft, blackmail, and other computer attacks and exploits. In order for a cyber attack to be considered cyberterrorism it should have a terrorist motivation like threatening, disturbing or destroying critical infrastructure based on a political, social or religious background. Terrorists would try to cause fear or the enforcement of demands and not just cause annoyance, carry out fraud or economic espionage.

In addition, terrorists may use very specific practices in order to create a disastrous effect. For example, after the Estonian government chose to move the war memorial in Tallinn honoring Russian-Estonians, the critical government websites were hit by a multitude of requests which caused the systems to fail [28][37]. Due to the large number of requests, the attacks were probably distributed, automated and carried out using a botnet. Furthermore, the conflict between Indian and Pakistan resulted in five megabytes of sensitive nuclear data at the Bahaba Atomic Research Centre being downloaded by unauthorized parties [9, 26, 27, 31]. From events categorized as cyberterrorism, it can be surmised that cyberterrorism would usually take the form of virus, bot or privilege escalation attacks to specifically infiltrate high-profile targets in order to achieve a maximum effect.

Various factors influence the development of a cyberterrorist. These include social factors, practices, objectives, targets, effects and motivation. In some cases, these factors are behaviourally based and in other cases technically based. The following questions therefore arise: How does one encapsulate the development of a cyberterrorist? How can cyberterrorism be deterred? This paper proposes the development of a Cyberterrorism Life-Cycle (CLC) model in order to address the raised questions. The next section looks at the motivation for modelling.

1. Motivation for Modelling

Epstein describes various reasons for modelling. Some of these reasons include [10]:

- Explain
- Illuminate core dynamics
- Suggest dynamical analogies
- Discover new questions
- Bound outcomes to plausible ranges
- Illuminate core uncertainties
- Demonstrate trade-offs/suggest efficiencies
- Educate the general public
- Reveal the apparently simple to be complex.

Thus, models provide a useful manner of explaining, exploring, analyzing, discovering, illuminating, identifying, educating and revealing critical aspects of a subject matter. Models provide the ability to explore a research field, by showing relationships and interactions between concepts. Modelling helps in portraying a concise representation of a field that may have various complex components.

According to Eriksson and Penker, a model is a simplified view of a complex reality and provides a means of creating abstraction that allows one to eliminate irrelevant details and to focus on one or more important aspect at a time [11]. For this reason, as a means of portraying some of the most critical aspects of cyberterrorism, this paper proposes the CLC model. The next section presents the generic CLC model, based on the findings found in literature.

2. Overview Of Cyberterrorism Life-Cycle (ClC) Model

In order to develop a helpful model, it is important to include a number of far-ranging factors that span the field of cyberterrorism. The aim of the model is not to present a set of rigid steps of execution and deterrence, but rather to represent the dynamic nature of the field and demonstrate how the various factors are related in order to identify the best approaches of combating attacks. Literature was used as background to identify the core factors during the phases.

Figure 1 shows the proposed generic CLC model. It is composed of four main phases: Prepare, Acquaint, Choose, Execute, as well as specific countermeasures in the supplementary Deter phase. These phases are loosely based on steps in the Observe-Orient, Decide, Act (OODA) loop proposed by Col John Boyd [1].

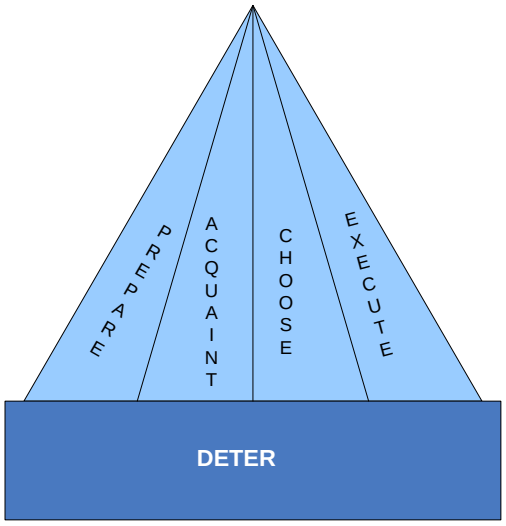

Figure 1: High-level CLC model

To illustrate, a cyberterrorist would identify the affordability and advantages of ICT during the preparation phase, then acquaint himself with the online presence of the targeted organization during the acquaintance phase. Thereafter during the choose phase he would make a selection of targets based on planned effects. During the execute phase, certain practices would be employed. The model can thus be further expanded based on other factors which play an influential role. This is carried out in the next section.

3. Expansion of CLC Model

Figure 2 shows an expansion of the CLC model, with the four main phases shown in the innermost circle. The Deter phase appears on an outer edge as the encompassing countermeasures are applicable across all four main phases. The expanded CLC Model is based on a mapping of cyberterrorism to the OODA loop, shown in Figure 3 [33].

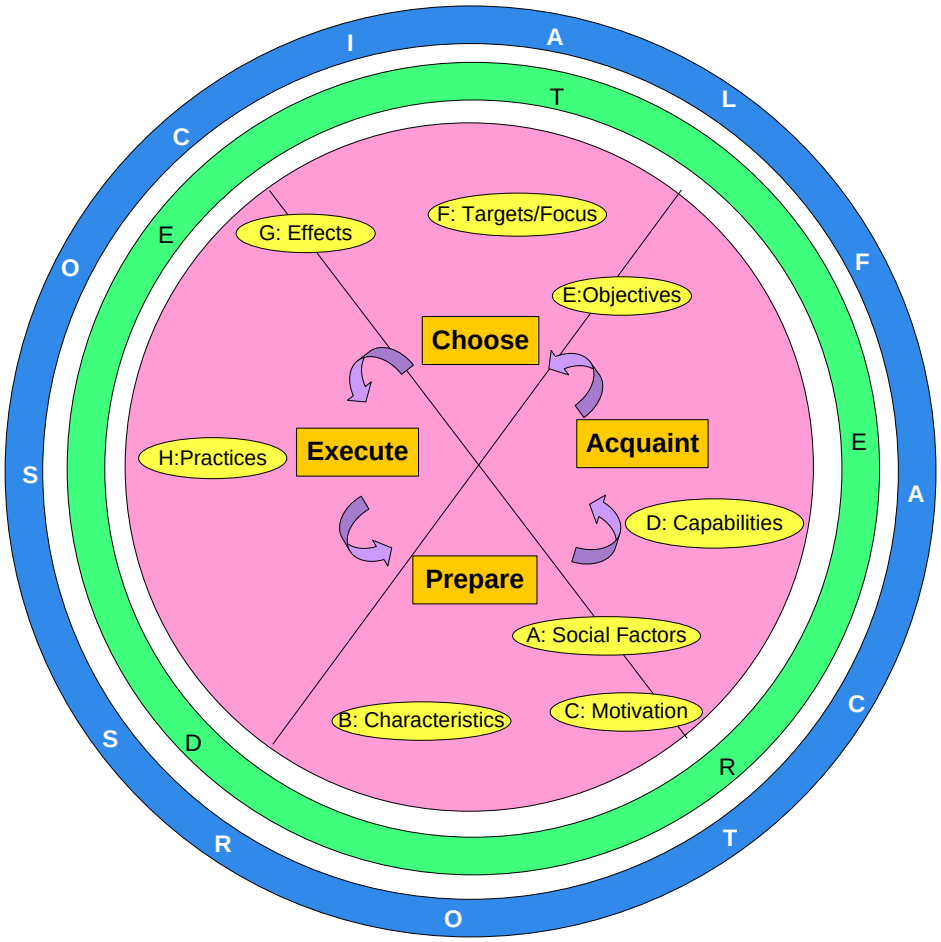

Figure 2: Expansion of CLC Model

Figure 3. Mapping of Cyberterrrorism to OODA loop [33]

The original OODA loop phases (see Figure 3) are adapted to the PACED phases, Prepare, Acquaint, Choose and Execute (see Figure 2). The Deter phase is also added and consists of countermeasures specific to cyberterrorism. Within each of the four main phases factors are displayed that applies to that specific phase. These factors are labeled A-H in Figure 2, and include: Social Factors (A), Characteristics (B), Motivation (C), Capabilities (D), Objectives (E), Targets/Focus (F), Effects (G) and Practices (H). Some factors do not map strictly to one phase only. For example, social factors like culture, beliefs, political views, and personality traits will affect all the phases (indicated by the overarching outer circle of Figure 2). However a social factor like upbringing is influential in the initial phases of prepare and acquaint (indicated by the A in the innermost circle). Thus, social factors are represented as a ring covering all phases, as well as a specific factor overlapping during the Prepare and Acquaint phases (in Figure 2).

Some of the factors captured in the model were slightly adapted from the original OODA loop mapping. For example, Malicious Goals and Support Functions (in Figure 3) have been encapsulated into a single factor entitled Objectives (E) in the CLC model (in Figure 2). Similarly Attack levels and Modes of Operation (in Figure 3) have been removed and Effects (G) has been added (in Figure 2). These changes are based on the analysis from an ontological study by Veerasamy Grobler and Von Solms [34] [36] which closely examined the core concepts related to the field of cyberterrorism. The cyberterrorist effects were identified to be a core factor in the life-cycle development during an ontological study of the field [36] and were thus included in the CLC model.

4. Development of CLC Model

The CLC model was derived based on the identification of critical points from literature and various existing models. The critical points were identified from findings taken from a framework summarizing the core aspects of cyberterrorism [32], a study of terrorists' use of terrorism [34], an ontological compilation to identify the core aspects relevant to the field of cyberterrorism [36] as well as an investigation of countermeasures [35]. These critical points are matched against identified factors in the CLC model to which the main contribution is made (labelled A-H in Figure 2). This section describes these various points.

5.1 Social Factors

- Various social factors can influence the development of a cyberterrorist. These include: culture, beliefs, political views, upbringing and personality traits [32] [18]. These social factors are a significant influential force in the CLC model during the Prepare and Acquaint phases.
- Social factors are an influential factor throughout the life-cycle of a cyberterrorism [33]. This critical concept will be reflected in the CLC model.

5.2 Characteristics

- ICT has characteristics that assist in carrying out wide-scale high-impact attacks. This stems from the identification of the various advantages including affordability, anonymity, variation, enormity, remote control, direct effect, automation, replication and speed. The identification of these characteristics will be used in the CLC model during the preparation phase [32][7][39][29].
- During the initial OODA loop's Observation phase, the important influential factors are the characteristics of ICT that make it a viable target or weapon, together with initial motivations forces that stems from the classification of terrorism types [33]. This idea will be represented in the CLC model during the Prepare Phase.

5.3 Motivation

- The differentiation between cybercrime and cyber-terrorism is an important aspect that is often confused. For a cybercrime or attack to be considered as cyberterrorism, there needs to be elements of terror through threats, disturbances or the infliction of violence [32]. The CLC model will take into consideration an ordinary cybercrime and those that take the form of cyberterrorism.
- Cyberterrorism is mainly motivated by political, social or religions reasons. The CLC model will incorporate the different motivating reasons [15][8][25].
- In a framework summarising cyberterrorism, [32] an explanation is given on the different types of terrorism based on motivations. These include: Religious, New-Age, Ethno-National Separist, Revolutionary Thinking and Far-Right Extremism. The different motivations will be captured in the CLC model [39].
- Motivation is a key aspect in separating traditional cybercrimes from cyberterrorism. The ontology shows motivations that correspond to cybercrime in general (criminal, ethical, financial, military and recreational) [30] and those that relate to cyberterrorism (political, social and religious) [15]. The CLC model will specifically capture the motivations relating to cyberterrorism.

5.4 Capabilities

- The capabilities that an individual/group has will determine the scope of the cyberterrorism attack. Some of the capabilities that an individual/group could possess include: education, training, skills, expertise, financial support, resources, intelligence and insider knowledge. These capabilities will be reflected in the CLC model [32].
- Critical to the orientation of a potential cyberterrorist is the capabilities that they possess. In addition, key to driving the development of a cyberterrorist is the social factors and motivation forces that stems from terrorism types, together with the formulation of initial malicious goals [33]. This will be shown during the CLC model's Acquaint Phase.
- An actor is needed to initiate and execute an action [36]. The following types of actors were identified: commercial competitor, hacker, insiders, criminal and protestor [30]. This classification is based on certain capabilities that the actor possesses. In order to capture this idea, the actor concept would be reflected in the capabilities element of the CLC model.

5.5 Objectives

- The scope of terrorism has now spread to the world of ICT. ICT infrastructure can serve as both a weapon to support an attack or as the target. This idea is important in differentiating between support and attack goals and will be covered in the CLC model [32].
- Some of the support functions that can be carried out include training, recruitment, networking and funding. The support functions will be covered in greater detail in the CLC model [32][6].

- The driving forces behind cyberterror stems from different objectives. Cybercrime can be related to causing annoyance, economic loss, fraud and espionage whereas cyberterrorism is linked to causing fear [32]. The CLC model will cover the different objectives behind cyberterrorism that will demonstrate its distinction from cybercrime in general.
- Cyberterrorism differs from cybercrime due to its distinct malicious goals. These include goals like: protest, disrupt, kill or maim, terrify, intimidate, demands, access sensitive information, affect crucial services, publicity and soliciting money [32][39][13]. The CLC model will describe the specific malicious goals that differentiate cyberterrorism from other forms of cyber crime.
- ICT can also play a support role to cyberterrorism. The supporting functions that ICT can play include: recruitment, training, intelligence, reconnaissance, planning, logistics, finance, propaganda and social services [32][18][29]. The CLC model will show how ICT can also be used as a support function.
- Due to the unique nature of the Internet, many traditional and innovative Internet activities can be carried out in either a uni-directional or bi-directional fashion, depending on the nature of the communication required [34]. The traditional and innovative uses of the Internet will be represented as malicious objectives and support functions in the CLC model respectively.
- These support functions include all the processes from recruitment and training of new members, communicating with existing members, planning and executing operations, distributing propaganda, fund raising and carrying out psychological warfare [34]. These support functions will be captured in the CLC model.
- During the OODA loop's Decision phase, the malicious goals or support function features with the target [33]. This will contribute to the development of the CLC model to show the formulation of objectives and targets which will be represented in the Choose Phase.

5.6 Targets

- Targets of cyberterrorist attacks include governmental and critical systems [37][32]. The CLC model will include the identification of prime targets of attack and facilitation.
- Cyberterrorism attacks will most likely be carried out against high-profile targets in order to maximize the damage and coverage of the attack. Typical targets include the following industries and areas: transportation, utilities, finance, communication, emergency, public health and agriculture [8][32] [4][12]. The CLC model will cover the different types of targets.
- The types of cyberterrorist targets were classified in the ontology in order to distinguish between low-profile individual attacks and wider-spread government or organization targets. The various targets identified in a framework by Veerasamy and Grobler [32] were placed into the governmental and critical targets category. Examples in the organizational targets group are email, production sales and marketing systems [36]. The range of targets would be specified in the CLC model.

5.7 Effects

- A cyber event can have different targeted effects which are null, minor, major or catastrophic damage [36] [30][22]. The CLC model will show the effects that cyberterrorist are trying to achieve depending on a malicious objective or support function.

5.8 Practices

- Crashing critical systems demonstrate the types of practices that are used to carry out cyberterrorist attacks [37][32]. The CLC model will describe the different practices.
- Cyberterrorism has been compared to cybercrime and cyber attacks. Cyberattacks can be performed by ordinary recreational hackers testing out their skills or trying to commit some fraudulent activity, and hacking skills and security violations can also be used as part of cyberterror attacks [32]. The CLC model will take into consideration the various technical practices that can be used to carry out cyberterrorism but will also expand on the high-level objectives and motivations to show its defining characteristics.
- Cyberterrorists will employ specific technical and hacking methods to carry out their attacks. Practices include: web defacement, disinformation distribution, propaganda, worms and viruses, affecting critical data and systems, credit card theft. The CLC model will indicate the different types of practices that are carried out [32].

- The use of the Internet for cyberterrorism can also be grouped under the following classifications: web literature, social-networking tools, anti-forensics and fundraising [34]. These classifications and detailed uses will form part of the practices in the CLC model.
- Propaganda and knowledge creation is carried out using web literature. Examples of web literature include periodicals, essays, manuals, encyclopedias, poetry, videos, statements and biographies [19][3][16][38]. These concepts will form part of the explanation of practices in the CLC model.
- Social-networking tools include forums, blogs, websites, gaming, virtual personas, music and applications [40]. The effect that social-networking tools can have in recruitment, training and communications will be shown as part of the practices in the CLC model. These topics offer opportunities for significant further research in studying the recruitment, training and communication practices in order to develop ways of interception and prevention.
- Terrorists are constantly trying to utilize ICT to their advantage without leaving a trace of their actions. Some of the identified anti-forensics methods that are being used include: steganography, draft message folders, encryption, IP-based cloaking, proxies and anonymizers [21][23][2]. The CLC model will indicate these anti-forensic techniques in order to show the ingenious practices that are being carried out in order to hide cyber activity and highlight that new and innovative methods will most likely be developed.
- Fund-raising is carried out using various scams including auctioneering, casinos, fake drugs, donations, credit card theft and phishing [40][24][14]. The CLC model will incorporate these fund-raising schemes.
- When carrying out a cyberterrorism act, certain practices will be employed [33]. The CLC model will show the various practices that can be utilized as part of a cyberterror attack or support function.
- Further practices that were identified and classified are web defacement and data manipulation [36]. A broader range of cyberterrorism practices will be covered in the CLC model.

5. Additional Input to CLC Model

Further input to the model was based on general observations of the cyberterrorism field as well as a study of possible countermeasures. These findings are discussed in this section.

6.1 Countermeasures

Countermeasures form part of the Deter phase of the CLC model. The development of the countermeasures is discussed next.

- Countermeasures need be devised from a strategic and technical point of view. . Examples of countermeasures cannot strictly be classified as belonging to a single category. For example, the establishment of cultural centers which promotes the understanding of religion and culture while exposing visitors to outside opinions can be considered as both a social and religious countermeasure [35]. The CLC model will show the overlapping classification of countermeasures.
- Strategic countermeasures can be grouped as legal, political, economic, social and religious categories [35]. Other examples of strategic countermeasures include: media, charities, cultural centers, analysis, education, humanitarian aid, military response, peace-keeping, policies, treaties, protocols, laws, fusion centers and perception management [35][5][41]. The range of countermeasures will be captured in the CLC model.
- Technical countermeasures include: CSIRTs, intrusion prevention, network monitoring, interception and blockage, disaster recovery and forensics [35]. These technical countermeasures will form part of the CLC model.

6.2 General Points

A formal definition of cyberterrorism establishes the foundation knowledge. The definition also contributes to the CLC model by providing a basic explanation of the field. The definition given in Section I states that overall cyberterrorism can be seen as the threat or act of causing harm in order to create fear and shock, targeting critical ICT infrastructures based on political, religious or social reasoning [15][8] .

Cyberterrorism is often mistaken as any cybercrime event. Ontologies helped identify the defining concepts of cyberterrorism as it allows for a structuring of a field by showing relationships, interactions and definitions. In the ontological study of cyberterrorism, the following concepts are introduced based on the motivation, objective, effect, target and practice: a cyberterror attack, support function and an unknown cyber event [36]. The CLC model caters for the different types of objectives and practices.

In order for a cyber event to be classified as cyberterrorist the effect has to major or catastrophic, the motivation has to be political, religious or social, the practice has to data manipulation or web defacement and the target should be an organization, government or critical target [36]. The requirements for a cyberterror attack will be shown in the CLC model. A support event needs a motivation of politics, religion or social issue and the practice can fall into the group of anti-forensics, fundraising, web literature and social networking [36].

Overall, the CLC model was compiled based on the identification of the various factors, as well as the adaptation of the OODA loop. The model encapsulates the critical aspects pertinent to the field of cyberterrorism.

6. Conclusion

Since various factors can either directly or indirectly influence the development of a cyberterrorist, there is a lot of uncertainty in terms of classifying cyber events as either a terrorist attack or a cybercrime. This paper set out to propose the development of the CLC model to address this classification.

The CLC model allows for adaptation, while still providing clarification of the groundwork definitions, concepts and ideas relating to the field of cyberterrorism. The model also allows for the identification of future areas of research and development by looking at emerging methods of attack and deterrence. In addition, the model can be useful for introducing and explaining the field to an audience who have no prior background or knowledge. This is especially important in reducing the confusion about cyber attacks being perceived as regular cybercrime or cyberterrorism.

References

[1] J. Boyd, "A discourse on winning and losing," Maxwell Air Force Base, 1987.

[2] J. Carr, "Anti-Forensic Methods Used by Jihadist Web Sites," ESecurity Planet, 1608. 2007.

[3] S. Coll and S.B. Glasser, "Terrorists turn to the Web as base of operations", *The Washington Post,* vol. 7, pp. 77–87, 2005.

[4] B.C. Collin, "The Future of Cyberterrorism: The Physical and Virtual Worlds Converge", *Crime and Justice International,* vol. 13, pp. 14-18, 1997.

[5] A.K. Cronin, "The diplomacy of counterterrorism lessons learned, ignored and disputed," International Research Group on Political Violence (IRGPV), pp. 1-8, 2002.

[6] A. de Borchgrave, T. Sanderson and J. Harned, "Force multiplier for intelligence," Centre for Strategic and International Studies, 2007.

[7] D. Denning, "Cyberterrorism," Global Dialogue, vol. 18, 23 May. 2000.

[8] K.C. Desouza and T. Hensgen, "Semiotic Emergent Framework to Address the Reality of Cyberterrorism", *Technological Forecasting and Social Change,* vol. 70, pp. 385-396, 5 2003.

[9] M. M. Elmusharaf , "Cyber Terrorism:The new kind of terrorism", Computer Crime Research Center, Accessed 20086 October, Available online at http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism.

[10] J.M. Epstein, "Why Model?", *Journal of Artificial Societies and Social Simulation,* vol. 11, pp. 12, 2008.

[11] H.E. Eriksson and M. Penker, Business modeling with UML, New York: John Wiley & Sons, 2000.

[12] C. Foltz Bryan., "Cyberterrorism, Computer Crime, and Reality", *Information Management & Computer Security,* vol. 12, pp. 154-166, 2004.

[13] G. Giacomello, "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism", *Studies in Conflict and Terrorism,* vol. 27, pp. 387-408, 2004.

[14] S.E. Goodman, J.C. Kirk and M.H. Kirk, "Cyberspace as a medium for terrorists", *Technological Forecasting and Social Change,* vol. 74, pp. 193-210, 2007.

[15] S. Gordon and R. Ford, "Cyberterrorism?", *Computers & Security,* vol. 21, pp. 636-647, 2002.

[16] Jamestown Foundation, "Next Stage in Counter-Terrorism: Jihadi Radicalization on the Web," 2310. 2006.

[17] L. Janczewski and A.M. Colarik, Cyber warfare and cyber terrorism, Information Science Reference, 2007.

[18] B.M. Jenkins, "The New Age of Terrorism," New York: McGraw-Hill, 2006, .

[19] D. Kimmage and K. Ridolfo, "Iraqi Insurgent Media. The War of Images and Ideas. How Sunni Insurgents in Iraq and Their Supporters Worldwide are Using the Media", *Washington, Radio Free Europe/Radio Liberty,* 2007.

[20] I. Lachow, "Cyber security: A few observations," 2008.

[21] S. Lau, " An analysis of terrorist groups' potential use of electronic steganography ", *Bethesda, Md.: SANS Institute, February,* pp. 1-13, 2003/02/18 2003.

[22] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms", *ACM SIGCOMM Computer Communication Review,* vol. 34, pp. 39-53, 2004.

[23] Y. Noguchi and S. Goo, "Terrorists' Web Chatter Shows Concern About Internet Privacy," The Washington Post, 0413. 2006.

[24] P. Piper, "Nets of terror: Terrorist activity on the internet," Searcher, vol. 16, November/December 2008. 2008.

[25] M.M. Pollitt, "Cyberterrorism - fact or fancy?", *Computer Fraud & Security,* vol. 1998, pp. 8-10, 1998.

[26] R.C. Puran, "Beyond Conventional Terrorism… The Cyber Assault," SANS, Tech. Rep. GIAC Security Essentials Certification (GSEC) v1.4b, 2003.

[27] Supercourse lectures, "Cyber Terrorism (When the Hackers Grow Up)," 2008.

[28] I. Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," Guardian, vol. World News, 2007.

[29] US Army Training and Doctrine Command, Critical infrastructure threats and terrorism, Fort Leavenworth, Kansas: US Army Training and Doctrine Command, 2006.

[30] R.P. Van Heerden, B. Irwin and I.D. Burke, "Classifying network attack scenarios using an Ontology", *in Proceedings of the 7th International Conference on Information Warfare and Security,* 2012.

[31] M.A. Vatis, "Cyber Attacks During the War on Terrorism: A Predictive Analysis", 2001.

[32] N. Veerasamy, "A high-level conceptual framework of cyberterrorism", *Journal of Information Warfare,* vol. 8, pp. 42-54, 2009.

[33] N. Veerasamy, "High-level Mapping of Cyberterrorism to the OODA Loop", *in Proceedings of the 5th International Conference on Information Warfare and Security,* pp. 352-360, 2010.

[34] N. Veerasamy and M. Grobler, "Terrorist use of the Internet: Exploitation and Support Through ICT Infrastructure", *in Proceedings of the 6th International Conference on Information Warfare and Security,* pp. 260, 2010.

[35] N. Veerasamy and M. Grobler, "Countermeasures to consider in the combat against cyberterrorism", *in Proceedings of the Workshop on ICT Uses in Warfare and the Safeguarding of Peace 2010,* pp. 58, 2010.

[36] N. Veerasamy, M. Grobler and B. Von Solms, "Building an Ontology for Cyberterrorism", *in Proceedings of the 11th European Conference on Information Ware and Security,* 2012.

[37] B. Von Solms, "Critical Information Infrastructure Protection- Essential During War Times, or Peace Times or both?", *in IFIP TC9 Proceedings on ICT uses in Warfare and the Safeguarding of Peace,* pp. 36-40, 2008.

[38] G. Weimann, "How modern terrorism uses the internet", *The Journal of International Security Affairs,* vol. Spring 2005, Spring 2005 2005.

[39] G. Weimann, "Cyberterrorism: How real is the threat?" United States Institute of Peace, Tech. Rep. 119, pp. 1-12, 2004.

[40] J. Whelpton, "Psychology of Cyber Terrorism," in Cyberterrorism 2009 Seminar, South Africa: Ekwinox, 2009, .

[41] C.J. Williers, C.J. Voster, A. van 't Wout, J.P. Venter, S.J. Naude and R. van Buuren, "IW Basic Course," Council for Scientific and Industrial Research, Tech. Rep. DEFT-IW-00200, 2005/06.