A High-level Mapping of Cyberterrorism to the OODA Loop

N Veerasamy
Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
nveerasamy@csir.co.za

Abstract: Cyberterrorism relates to the convergance of the two worlds of terrorism and cyberspace. Technically cyberterrorism can be carried out through various information security exploits like targeting Supervisory Control and Data Acquisition (SCADA) systems or Denial of Services attacks on critical governmental web sites. Various factors have an influence on cyberterrorism and include the social factors, capabilities, goals, modes of operation and practices. In order to analyse how these various factors influence the development of a cyberterrorist, a mapping to the Observe- Orient, Decide, Act (OODA) loop is proposed. The OODA loop, previously proposed by Col. John Boyd, provides an apt framework to structure and describe issues that contribute to the development and operation of a cyberterrorist.

The aim of this paper is to describe how various observations made by sections of the world population direct people into making decisions and committing acts of cyberterror. The paper will thus look at issues like the environmental factors, social standing, culture, religion, tribal relations, loyalties, and the drive for power and self-fulfilment. In addition, the mapping will also consider how information is received, transformed and utilised by cyberterrorists, by considering the evolution of information in the Information Hierarchy. The proposed model will thus map various aspects pertinent to the field of cyberterrorism to capture a more dynamic representation of the interacting forces. The mapping will try to show the main relationships between the OODA loop, Information Hierarchy and various factors like characteristics, social factors, terrorist types, capabilities, goals, targets, attack levels, support functions, practices and modes of operation.

Overall, the goal of this paper is to succinctly represent some of the psychological and technical issues relating to cyberterrorism. The OODA loop will be utilised to convey these ideas as well mapping to other relevant fields like the Information Hierarchy. Overall, various components that impact the field of cyberterrorism will be integrated to show a more holistic representation of various operating forces.

Keywords: Cyberterrorism**,** Information Hierarchy, OODA loop

1. Introduction

In various parts of the world, terrorist groups operate and strive to inflict shock and horror on unsuspecting sections of the population. Nuclear, biomedical and chemical weapons have been used to attack innocent bystanders in very public areas in an effort to cause maximum damage. However, now due to the convenience and span of Information and Communications Technology (ICT), terrorists have found another fitting avenue to utilise. Weiman (2004) talks of the growing dependence of society on information technology has created a new form of vulnerability and if terrorists follow the lead of hackers, theoretically they could access and even cripple critical sectors like the military or financial services.

One area that should be clarified is the scope of cyberterrorism. Cyberterrorism has become a buzzword and is often sensationalised in the media whereby reports of cybercrime and attacks are posed as cyberterrorism threats. However, definitions do exist and are presented next.

Pollitt (1998) defines cyberterrorism as "*the premeditated politically motivated attack against information, computer systems and computer programs and data which result in violence against non-combatant targets by sub national groups or clandestine targets*". Furthermore, the most cited definition of cyberterrorism is Denning's testimony before the Special Oversight Panel on Terrorism. It states (Denning 2000):

"*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."*

In addition, according to Desouza (2003) cyberterorism can be 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*."

An argument therefore arises as to whether cyber terrorism is a more apt term versus information terrorism. Webb (2009) describes information terrorism as "*a non-state actor's premeditated and asymmetrical warlike conduct of information activities to fulfil their ethos, foster mass acts of terror and/or affect and disrupt the security and/or well-being of a populace*". Upon closer inspection, the various definitions covering cyber terrorism address the issues of attacking information and information resources which include computers, networks, programs, data, and other electronic devices. Both definitions fundamentally include aspects dealing with the acts of terror to interfere with security and the overall aim of influencing government or a section of the population. Conway (2007) states that cyberterrorism has become a common term when dealing with computers and the Internet to create new words by placing the handle cyber, computer or information before another word, but academic contributions may allow for the broadening of the definition of cyberterrorism. Therefore, the author recognizes that both the terms cyber terrorism and information terrorism have common aspects and whilst nuances might exist, such an argument does not fall within the scope of this paper. Rather, throughout the rest of this paper, the term cyberterrorism will be used.

Technically, cyberterrorism can be carried out through various security exploits targeting critical services like emergency departments, banks, fuel supply or air traffic control. Whilst it is difficult to determine why terrorists pick a target, it would be useful to understand the development, transformation and operation of cyberterrorists.

Studying how insurgent groups arise, can provide insight into environments that incubate and promote the advancement of terrorist conduct. An investigation into the factors that lead to development of cyberterrorists, can reveal why and how this behaviour is taking place. However, due to the large number of factors influencing cyberterrorism ranging from the social circumstances to capabilities and objectives, it would be useful to succinctly represent all these psychological, technical and counter-terrorism issues.

Col John Boyd proposed the theory encapsulated in Observe, Orient, Decide and Act (OODA) loop (shown in Figure 1). Subsequently, this idea has been applied in various ways (such as OODA loops within each phase of the loop). Conceptually, this principle provides an ideal baseline to indicate the transformation of data and information into tacit and explicit knowledge and thus establish further theory relating to the founding processes of cyberterrorism.

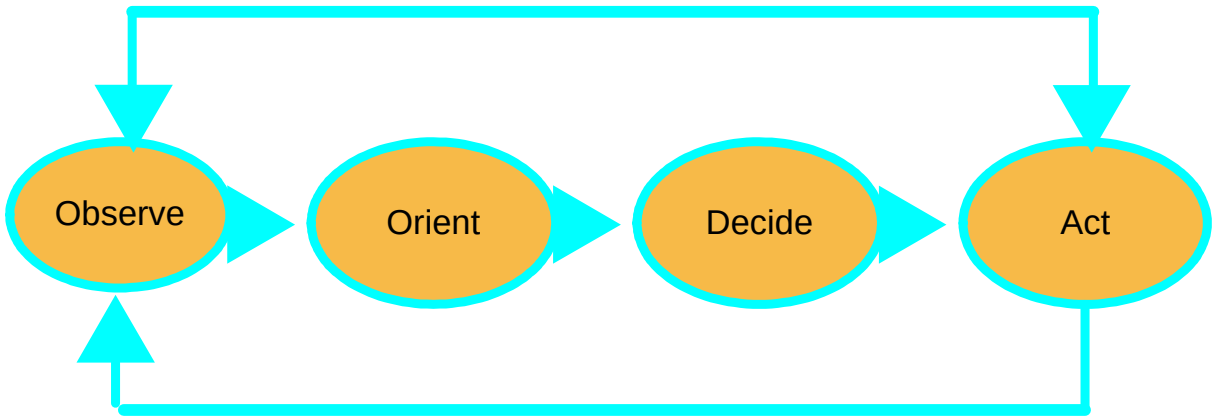

Figure 1: OODA loop

The remainder of this paper is structured as follows: Section 2 provides a description of the hierarchy of information, Section 3 summarises a conceptual framework proposed at ICIW 2008 and Section 4 explains the mapping of the conceptual framework as well as the Information Hierarchy to the OODA loop. The paper is concluded in Section 5.

2. Hierarchy of Information

This Section discusses the Information Hierarchy. The next Section will briefly summarise cyberterrorism with a conceptual framework. Section 4 discusses the mapping of the Information Hierarchy and the conceptual framework to the OODA loop.

To show more detail in the OODA loop, let us consider how information can be classified. This serves to show how information develops hierarchically and thus helps classify the type of information that is being dealt with in the different stages of the OODA loop that lead to the development of the cyberterrorist. Williers (2005/06) explores the hierarchy of information in more detail. A graphical representation is given in Figure 2.

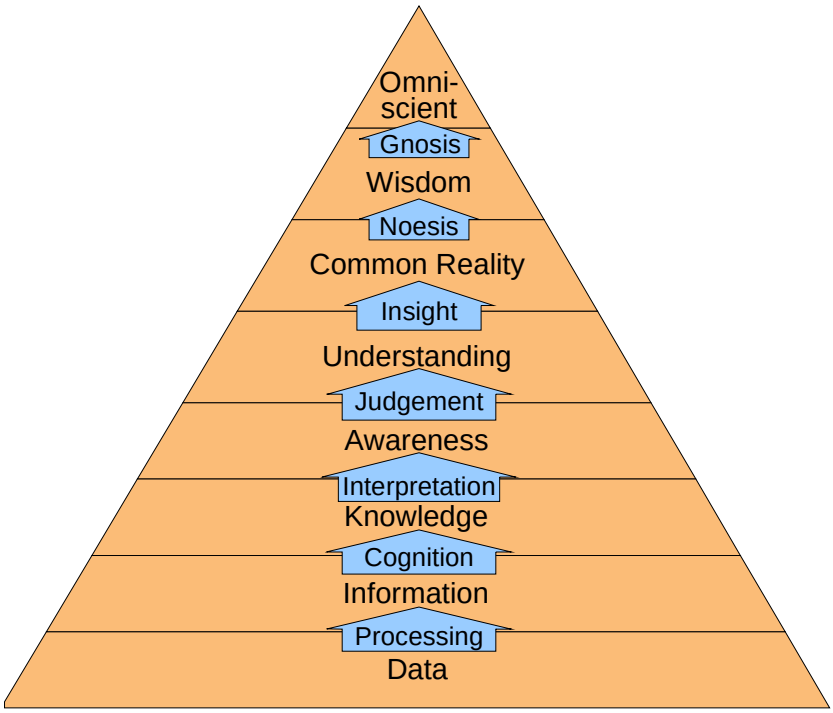

Figure 2: Hierarchy of Information

According to Rowley (1998), data is information that should undergo some processing so that the results of the processing can be communicated for a particular purpose. Data at the most basic level represents information in a raw format that can undergo some processing and can be stored on computer systems.

Definitions of information from the online dictionary Answers.com include (Anonymous)

- A collection of facts or data
- The act of informing or the condition of being informed
- Processed, stored or transmitted data
- Knowledge derived from study, experience or instruction
- Knowledge of specific event or situations that have been gathered or received by communication, intelligence or news.

Data, information and knowledge are intertwined concepts that represent content that is received and thereafter perceived by humans. Knowledge (Anonymous) according to the Oxford dictionary is defined as:

- Information and skills acquired through experience or education
- The sum of what is known
- Awareness or familiarity by experience of a fact or situation

Therefore to summarise data, information and knowledge Hutchinson (2001) states that: data describes attributes of things; information is collated data; and knowledge is information that has been interpreted in the light of experience. Data and information therefore represent the most basic form through which sensory input is received. Data once processed becomes information. When information cognises, knowledge grows.

From knowledge comes awareness. Awareness has a wider scope than knowledge in that awareness involves linking concepts together to make broader conclusions. Knowledge once interpreted can bring about a greater sense of awareness. Awareness leads to understanding through the process of judgement and inference. Understanding involves cognitive and analytic development. Understanding can lead to new knowledge and thus new synthesis of thought can take place.

With insight from a broader sector, understanding can form a common reality. Common reality is representative at a wider level and tries to incorporate more perspectives. From common reality we move on to wisdom, which can be subjective in nature. Established principles and human codes, like morality and ethics, guide behaviour. Wisdom can be philosophical in nature and deals with the judgement between right and wrong or good and bad. Decisions that are considered wise are not easily determined or predicted and require discernment, reflection and contemplation.

At the highest level comes omniscience, which is highly matured wisdom that evolves from gnosis (intuition and knowledge of truths). Acting with omniscience implies infinite knowledge.

This discussion summarised the transformation of data into wisdom and thus the development of implicit and tacit knowledge that facilitates the execution of activities. This theory will used in the mapping of cyberterrorism to the OODA loop in Section 4. Next, some of the other aspects of cyberterrorism are briefly introduced in a conceptual framework that will also be used in the mapping to the OODA loop.

3. Literature Study

The previous section introduced the Information Hierarchy. This section looks at a conceptual framework of cyberterrorism is which various influential considerations are proposed. The next section maps the Information Hierarchy and the conceptual framework onto the OODA loop.

At the 2008 ICIW conference a conceptual framework for cyberterrorism was established (Veerasamy 2009b).This paper extends this work by showing in more detail how the various aspects of cyberterrorism interact. This aims to show a more dynamic representation of the various factors in cyberterrorism. The conceptual framework previously discussed in (Veerasamy 2009b, Veerasamy 2009a) is shown in Figure 3. In upcoming sections of this paper, the various factors introduced in (Veerasamy 2009b, Veerasamy 2009a) will be considered and included in the mapping to the OODA loop. Thus, the aspects previously proposed will be extended by showing various relationships. The next section, therefore describes the mapping of cyberterrorism to the OODA loop.

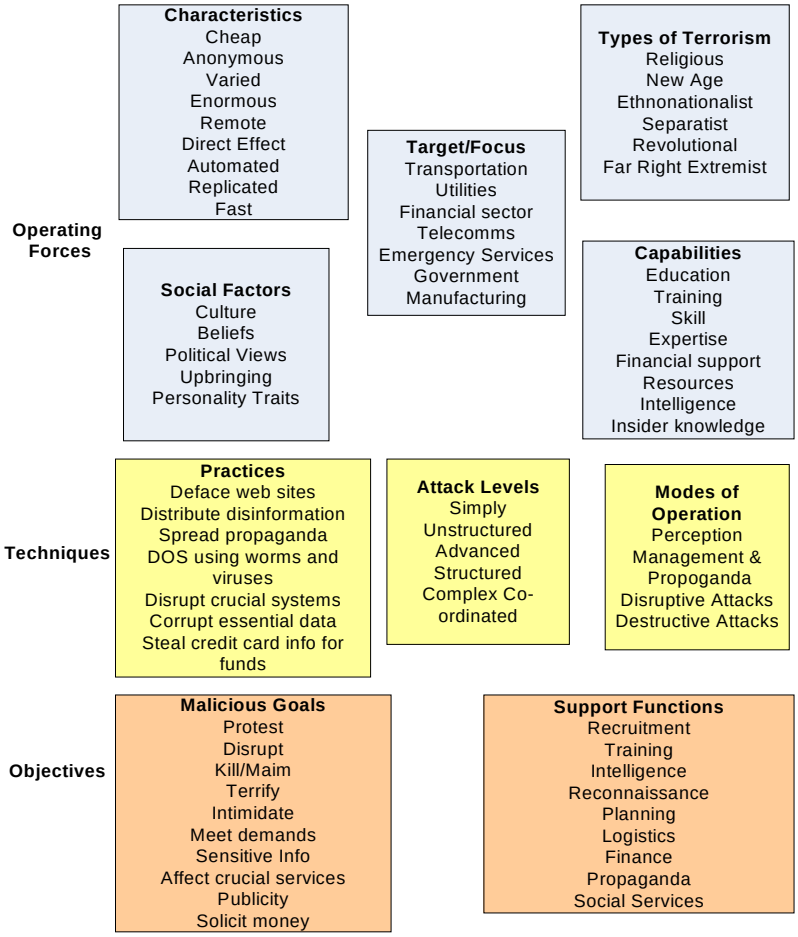

Figure 3. Framework of Cyberterrorism

4. Mapping to OODA Loop

Williers (2007) provides a mapping of the Information Hierarchy, OODA loop and various other factors to describe Integrated Information Warfare. This approach has been applied to show an integrated picture of cyberterrorism. In Figure 4, a high-level mapping is given of the OODA loop to the Information Hierarchy as well as to various aspects in the field of cyberterrorism. This representation serves to show the synergistic effect of all the relevant aspects. The integrated picture thus captures a more holistic representation of all the operating forces. The mapping is not exact in that some overlaps of the elements do occur. However, the map tries to provide an indication of the main relationships and influential considerations in the field of cyberterrorism. A more detailed discussion follows on the various elements in the mapping.

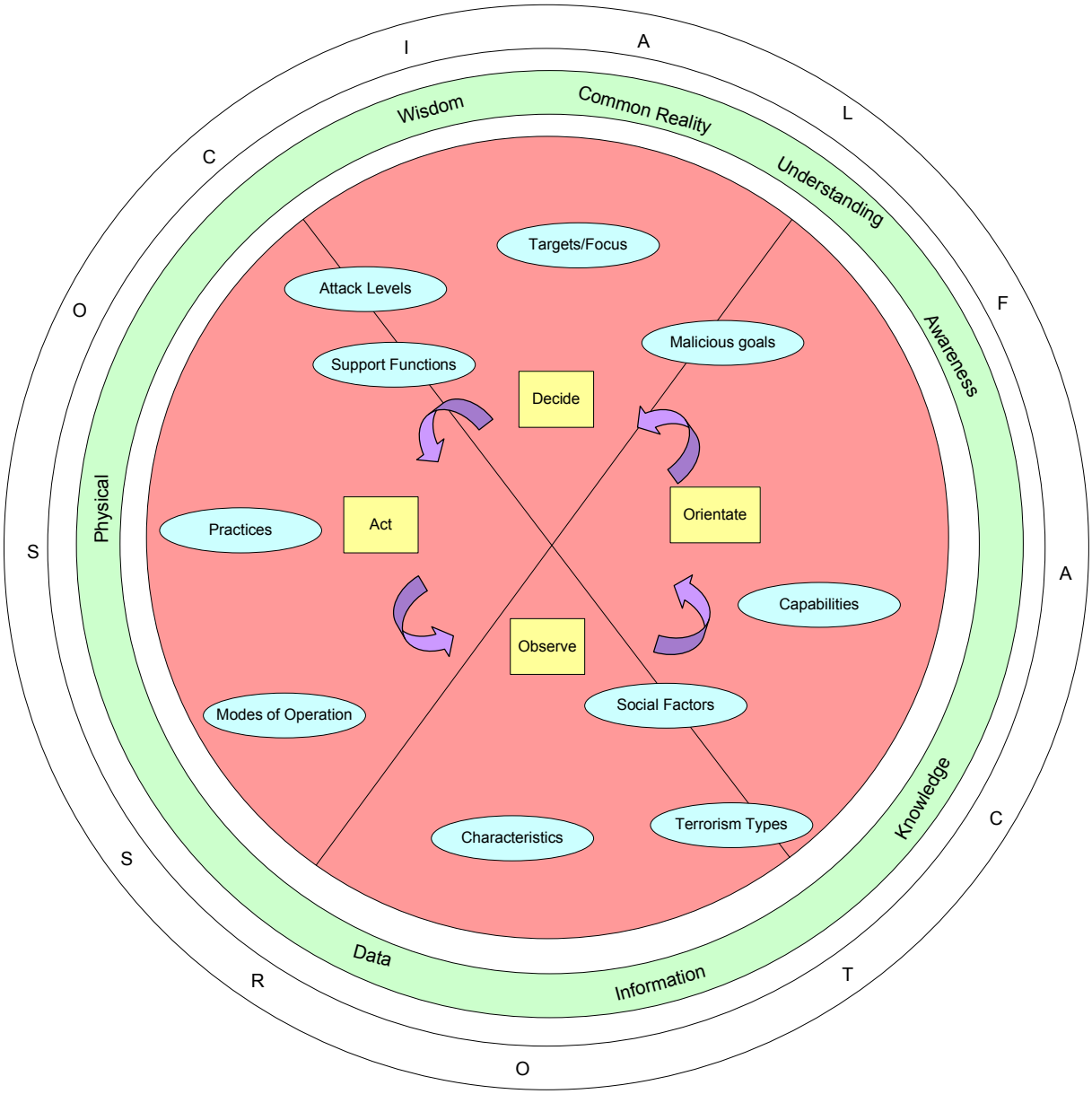

Figure 4: Mapping of Data Hierarchy to OODA Loop

At the centre of the mapping (Fig 4) is the OODA loop. As we move outwards, the various aspects described in the conceptual model (in Section 3) are shown. The outermost ring represents the various levels in the Information Hierarchy (as discussed in Section 2).

The Observe and Orient aspect of the OODA loop looks at the various forms of data and information that are communicated. At a cyberterrorism perspective this can deal with the observations that cyberspace has several advantages such as anonymity, variation, replication, enormity, remoteness, directness, automation and speed (Weimann 2004, Denning 2000). Furthermore Webb (2009) mentions that low entry costs, difficulties in identifying an attack and its origins and the potential for extreme chaos are all selling points for this form of terrorism.

In addition, various social factors and different terrorist types of information mainly influence the observations that can be made. Jenkins (2006) states that terrorism is generally derived out of the concepts of morality, law and the rules of war, whereas actual terrorists are shaped by culture, ideology and politics. Furthermore, Wilson (2005) shows that culture, genetics, experience and new information is fundamental to orientation. To further elaborate on these social factors that influence the development of a cyberterrorist, the findings of Daly and Gerwehr (Kamien 2006) are given. Daly and Gerwehr (Kamien 2006) author a chapter in the McGraw Hill Security Handbook and mention a few variables that are conducive for extremist recruitment. In summary these include: distress or dissatisfaction, cultural bombardment (disillusion), family dis-functionality and dependant personality tendencies. Thus, these conditions that affect a person's upbringing, can also impact the way in which data and information is perceived and thus the development of certain viewpoints. It was mentioned earlier that overlaps do occur and the various aspects do not strictly map to a single aspect of the OODA loop or the Information Hierarchy only. When considering social factors, we may find that that aspects, like culture, beliefs, political views, upbringing and personality traits will play a supportive role throughout all phases of a cyberterrorist life. In this way, social factors are also shown in a central ring encompassing the entire model to indicate its influence throughout all stages. The discussion returns to how various aspects of cyberterrorism is mapped onto the OODA loop and Information Hierarchy.

Terrorist types correlate to the causes being promoted. It is linked to the religious, philosophical, social or ideological issue/s being fought for and is thus linked to various observations. For example, terrorist types can include religious, New Age, ethnonationalist separatist, revolutionary and far-right extremist (Weimann 2004). A cyberterrorist will proceed to act in support of a particular viewpoint or favourable cause. The type of information that people can be exposed to includes:

- Religious: strong religious ideas which can include the justification for the taking of lives
- New Age thinking: manipulation tactics and impact of unconventional attacks
- Ethnonationalist separatist: promotion of the establishment of a new political order based on ethnicity
- Revolutionary: inadequacy of the government or state and need to overthrow social order
- Far–right extremist: justification for seizing power due to superiority belief system

Information due to social circumstances, psychological development and exposure to the environment all form part of the baseline observations that are made. During observation and orientation, identification with family, tribes, religion and social loyalties plays a huge role. The social environment that a youngster is exposed to impacts later decisions and activities in life. For example, in impoverished war-torn African countries, young children are forced to join guerrilla groups and fight indiscriminately. Arabic scholars are taught in madresses whereby the pillars of Islam are instilled at a very young age. This type of exposure promotes loyalty to a cause for the purposes of survival, acceptance and social norms. In cultural groups, there is the tendency for a common set of principles to be established and followed. Behaviour that is compliant with this common set of principles is often encouraged. Whilst personality and relationships are immense driving forces, culture, customs and society does affect an individual's development. Culture is the cornerstone for encouraging new members and provides an avenue to direct and influence existing members. Values, impressions and loyalties are developed through culture as well as provide the sense of belonging.

Once, inherent tendencies are stimulated or loyalty to a cause is established, the potential to become a cyberterrorist exists. Thereafter, during the orientation stage capabilities and malicious goals can be formed which will aid with the decision making and execution of cyberterror activities in the future. Capabilities include education, training, skills, expertise, financial support, resources, intelligence or insider knowledge (see Figure 2). Some of the capabilities like education, intelligence and training lead to the establishment of higher knowledge. Knowledge contributes to the skill set, expertise and experience. Thus, the various forms of data and information that are received and interpreted into knowledge, are interrelated. Whilst familiarising oneself with systems, networks, techniques and learning the appropriate skills, awareness is created. Awareness requires some analytical development which is facilitated through the interaction on ICT systems as well as interfacing with support members who are providing intelligence or funding. Thus, the capabilities of a cyberterrorist are developed.

At the decision phase of the OODA loop, the cyberterrorist operates at Common Reality as the impact of the broader environment is the focus. The Common Reality may seem skewed due to the malicious goals which objectively do not promote greater good. However, at the subjective level the cyberterrorism characteristics, social factors, capabilities and terrorist type thinking is the driving force behind subsequent decisions and will continue to influence future actions. During the decision phase, targets can be selected based on underlying goals that are trying to be achieved. Cyberterorist targets include (Lewis 2002) (Desouza, Hensgen 2003) (Collin 1997) (Foltz 2004):

- Transportation: air, rail, road
- Utilities: water, energy
- Financial Sector: banks, foreign exchange agencies
- Telecoms: telephone,
- Emergency Services: health, fire, police
- Government : agencies, municipalities
- Manufacturing : pharmaceutical, farming

Overall, the cyberterrorist seeks to: protest, disrupt, kill, maim, terrify, intimidate, demand, affect sensitive information or crucial services, gain publicity or solicit money (see Figure 2).ICT can also play a supportive role to terrorism in general. This will have an impact across the OODA loop. Examples in which ICT plays a supportive role include: recruitment, training, intelligence, reconnaissance, planning, logistics, finance, propaganda, and social services. Such activities utilise the capability provided by ICT to enable communication, marketing and funding. Thus, computers and networks also enable terrorism by providing supporting functionality.

Furthermore, decisions concerning the levels of attack will be made. This relates to whether simple exploits will be executed or complex co-ordination over a number of years will take place. At a high level, cyberterrorism can have different modes of operation to carry out a number of practices. Arquilla (2001) talks of the three broad offensive categories which include perception management and propaganda; disruptive attacks to temporarily immobolize a site/service/system and; destructive attacks that ruin physical of virtual systems/networks. This correlates to the modes of operation which determines the type of action that will be unleashed. Typical examples of practices used to carry out cyberterrorism are web defacement, disinformation, propaganda, denial of service with malware, crucial service disruption, data corruption and credit card information theft. Whilst operating in the virtual world of cyberspace and networks, execution of cyberterrorism practices will require physical interaction with ICT equipment. Thus, whilst cyberterrorsim does mainly involve virtual connections, there are some associated physical connotations.

Overall, the mapping in Figure 4 captures the transformation of information that influences the mindset of an individual into a cyberterrorist. Thus, it shows how information at a certain level is received and used. The mapping also captures the development of a cyberterrorist by showing how various components affect observation, orientation and decision-making to eventually lead to the execution of cyberterrorist acts.

In general, the model can be practically applied when studying certain insurgent/clandestine groups and documenting how the terrorist tendencies and behaviour developed. It is often difficult to infiltrate a ethnic/religious/cultural group as a limiting factor will lie in the physical appearance of the operative. Members who are part of the cultural or belief system can be convinced to provide information and thus contribute to intelligence gathering. In this way, insight can be gained into the different personality differences, inherent tendencies, values and morals that contribute to the initial psychological seeds that are planted which then promote the struggle for a certain political or social cause. This model is helpful in profiling a terrorist group and understanding how the capabilities are developed, how targets are selected, the supportive functionality that ICT plays in the organisation and how they operate. In this way the life-cycle of a cyberterrorist can be established as a person moves from the initiation stages through to immersed operation in a terrorist organisation.

5. Conclusion

Various facets ranging from the technological to the psychological, drive cyberterrorism. This paper shows a mapping of these various components to the OODA loop in an attempt to capture a more dynamic representation of these influential considerations. This paper provides insight into the growth and execution of cyberterrorsim activities by capturing various interacting aspects in the field. Aspects in the mapping include the Information hierarchy (to show the transformation of information) as well as factors like characteristics, social factors, terrorist types, capabilities, goals, targets, attack levels, support functions, practices and modes of operation. The OODA loop provides an ideal baseline to show the synergistic effect of all these aspects. Overall, this paper aims to place the field of cyberterrorism in context against various developmental and technical issues.

References

Information, [Homepage of Answers.com], [Online]. Available: http://www.answers.com/topic/information [2008].

*Knowledg*e, [Homepage of Compact Oxford English Dictionary], [Online]. Available: http://www.askoxford.com/concise_oed/knowledge?view=uk [2008].

Arquilla, J. & Ronfeldt, D.F. 2001, *Networks and Netwars: The future of terror, crime, and militancy,* Rand Corporation, Santa Monica, California, USA.

Collin, B.C. 1997, "The Future of Cyberterrorism: The Physical and Virtual Worlds Converge", *Crime and Justice International,* vol. 13, no. 2, pp. 14-18.

Conway, M. 2007, "Cyberterrorism: hype and reality" in *Information Warfare separating hype from reality*, ed. L. Armistead, Potomac Books, Inc., Washington, USA, pp. 73-93.

Denning, D. 2000, *Cyberterroris*m, Georgetown University.

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.

Foltz, C.,Bryan. 2004, "Cyberterrorism, Computer Crime, and Reality", *Information Management & Computer Security,* vol. 12, no. 2, pp. 154-166.

Hutchinson, W. 2001, *Information Warfare: Corporate attack and defence in a digital world,* Butterworth-Heinemann.

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

Kamien, D.G. 2006, *The McGraw-Hill homeland security handbook,* McGraw-Hill, New York.

Lewis, J.A. 2002, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", *Center for Strategic and International Studies,* pp. 1-12.

Pollitt, M.M. 1998, "Cyberterrorism - fact or fancy?", *Computer Fraud & Security,* vol. 1998, no. 2, pp. 8-10.

Rowley, J. 1998, "What is information?", *Information Services and Use,* , no. 18, pp. 243-254.

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 Securit*y, ed. L. Armistead, Academic Conferences International, , pp. 129.
Webb, K. 2009, "Considerations for management from the onset of Information Terrorism", *Proceedings of the 4th International Conference on Information Warfare and Securit*y, ed. L. Armistead, Academic Publication Limited, , pp. 138.
Weimann, G. 2004, *Cyberterrorism: How real is the threat*?, United States Institute of Peace, Washington, United States.
Williers, C.J. 2007, *Agent Based Modelling Repor*t, CSIR, Pretoria, South Africa.
Williers, C.J., Voster, C.J., van 't Wout, A., Venter, J.P., Naude, S.J. & van Buuren, R. 2005/06, *IW Basic Cours*e, Council for Scientific and Industrial Research, Pretoria, South Africa.
Wilson, G.I., Wilcox, G. & Richards, C. 2005, "Fourth Generation Warfare & OODA Loop Implications of The Iraqi Insurgency", *16th Annual AWC Strategy Conferenc*e.