(IJCSIS) International Journal of Computer Science and Information Security,
Vol. XXX, No. XXX, 2012

A Dynamic Cyber Terrorism Framework

Rabiah Ahmad
Dept of Computer System and Communication
Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka (UTeM)
Melaka, Malaysia
rabiah@utem.edu.my

Zahri Yunos
CyberSecurity Malaysia
Selangor, Malaysia
zahri@cybersecurity.my

***Abstract*—Many nations all over the world have increased their dependency on cyberspace by maximizing the use of Information and Communication Technology (ICT). In this digital age, the concept of cyber terrorism or the use of cyberspace to carry out terrorist activities has emerged. Interestingly, there are many concepts of cyber terrorism provided by researchers, policy makers and individuals. This paper proposes a framework describing the core components of cyber terrorism. The authors have analyzed the data by using a grounded theory approach, in which the framework is drawn. The framework defines cyber terrorism from six perspectives: Target, motivation, method of attack, domain, action by perpetrator, and impact. In addition, the proposed framework provides a dynamic way in defining cyber terrorism as well as describing its influential considerations. Continued research in this area can be further conducted, which may lead to the development of strategic and technological framework to counter cyber terrorism.**

Keywords-component; Cyber Terrorism, Cyberspace, ICT, Terrorism

I. INTRODUCTION

Cyberspace and the Internet are at the center of modern life and have become an important medium for businesses, economics, politics and communities. Many nations all over the world have constantly increased their dependency on cyberspace by maximizing the use of Information and Communication Technology (ICT). ICT offers a double-edged sword. While development in the area of ICT allows for enormous gains in efficiency and productivity, it has also created opportunities for those with devious ambitions to cause harm [1]. At the same time, it can be a powerful tool for perpetrators such as extremists and terrorist groups to promote extremist ideologies and propaganda materials as well as to create public fear by damaging assets that are vital to national interest and security [2] [3]. The same technological advances that are benefiting the public at large are also increasing the arsenal of our adversaries.

Critical National Information Infrastructure (CNII) underlies the nation's economic, political, strategic and socio-economic activities [4]. Many stakeholders are concerned with terrorist attacks against critical infrastructures such as telecommunications, power distributions, transportation, financial services and essential public utility services. Terrorist cyber attacks on CNII is possible, where the motives, resources and willingness to conduct operations of different kinds against specific targets are fundamental [5]. If perpetrators follow the lead of hackers, theoretically they have the capability to use ICT to conduct cyber attacks against specific targets. Due to the fact that cyberspace has no boundaries, there is a possibility that the terrorists or terrorist groups may pursue cyber terrorism in conducting offensive attacks and supporting physical violence in the future [6].

II. CONCEPTS AND TERMS

A. *Cyber Terrorism*

War, crime and terrorism are traditional concepts that occur in the physical domain, the only new aspect is the "cyber" domain. Physical terrorism and cyber terrorism share the same basic elements i.e. sharing a common denominator – terrorism. Several researchers have argued that the underlying principles of terrorism behind the threat remain the same [6], and they have described terrorism activities in the cyber world as cyber terrorism [7].

It is noted that several definitions of terrorism have included targets directed at computer systems and its services that control a nation's energy facilities, water distributions, communication systems, and other critical infrastructures. Malaysia's Penal Code, Chapter VIA, Sections 130B – 130T comprises provisions dealing with terrorism [8]. Section 130B (2) (h) defines terrorism as an act or threat of action designed or intended to disrupt or seriously interfere with, any computer system or the provision of any services directly related to communications infrastructure, banking or financial services, utilities, transportation or other essential infrastructure. Australia's Security Legislation Amendment (Terrorism) Act 2002 defines terrorism, among others, as actions that seriously interfere, disrupt, or destroy, an electronic system including, but not limited to, an information system; a telecommunications system; a financial system; a system used for the delivery of essential government services; a system used for, or by, an essential public utility; or a system used for, or by, a transport system" [9].

The term cyber terrorism was first coined in the 1980s by Barry Collin [10], a senior research fellow at the Institute for Security and Intelligence in California. According to him, the convergence of the "virtual world" and "physical world" form the vehicle of cyber terrorism. Collin further clarifies that the

virtual world is the place in which computer programs function and data moves whereas the physical world is the place in which we live and function. The growing convergence of the physical and virtual worlds is becoming more complex. Nowadays, ICT plays a major role in the convergence of these two worlds.

Denning [11] defines cyber terrorism as unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Denning also clarifies that, "Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt non-essential services, or that are mainly a costly nuisance, would not." Definition by Denning consists of several important components on the concept of cyber terrorism. First, it refers to unlawful attacks. Second, the attacks and threats of attacks against computers, networks and the information stored within them. Third, the purpose of (unlawful attacks) is intimidating or influencing a government or society to further political or social objectives. Fourth, the attack results in violence against persons or property, or at least causes enough harm to generate fear. Lastly, serious attacks against critical infrastructures could be acts of cyber terrorism.

Likewise, Lewis [12] defines cyber terrorism as the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population. Mantel [13] defines cyber terrorism as highly damaging computer attacks by private individuals designed to generate terror and fear to achieve political or social goals. Mshvidobadze [14] defines cyber terrorism as cyber acts designed to foment terror or demoralization among a target population for some purpose of the perpetrator, most likely this will be some kind of attack on critical infrastructure. Cyber terrorism should be involving computer technology and means as a weapon or target by terrorist groups or agents [15]. In the context of cyber terrorism, the above definitions suggest that critical infrastructure's computer system and civilian population would seem become attractive targets and contribute to the uniqueness of cyber terrorism. Here, the direct damage caused by the attack is to the critical infrastructure's computer system and civilian population.

The context of cyber terrorism seems to argue that this term comprises component of motivation such as political, social and belief. For example, Conway [16] describes that, in order to be labeled as cyber terrorism, the attacks must have a terrorist component, which is result in death and/or large scale destruction and politically motivated. Pollitt [17] defines cyber terrorism as the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatants target by sub national groups or clandestine agents. Czerpak [18] argues that cyber terrorism is a politically driven attack perpetrated by the use of computers and telecommunications capabilities, which leads to death, bodily injury, explosions and severe economic loss. Nagpal [19] defines cyber terrorism as the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.

Method of attack in cyber terrorism seems to use computer technology in carrying out the acts of terrorism. Beggs [20] defines cyber terrorism as the use of ICT to attack and control critical information systems with the intent to cause harm and spread fear to people, or at least with the anticipation of changing domestic, national, or international events. Similarly, Weimann [21] defines cyber terrorism as the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation and government operations). CRS Report for Congress [22] defines cyber terrorism as the use of computer or weapons, or as targets, by politically motivated international, or sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence and audience, or cause a government to change its policies.

As defined by Denning, the action by perpetrator involves to unlawful attacks to the targeted audiences. This notion is supported by Ariely [23] where cyber terrorism is referred as the intentional use or threat of use, without legally recognized authority, of violence, disruption, or interference against cyber systems. The result would be in death or injury of a person or persons, substantially damage to physical property, civil disorder or significant economic harm. This understanding is in line with study conducted by Nelson et al. [24] which defined cyber terrorism as the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological.

Cyber terrorism can have critical impact to the targeted audiences such as to cause fear to anyone in the vicinity or result in violence, death and destruction. Stohl [25] argues that cyber terrorism includes some form of intimidate, coerce, influence as well as violence. He defines cyber terrorism as the purposeful act or the threat of the act of violence to create fear and/or compliant behavior in a victim and/or audience of the act or threat. In a report to the United Nation General Assembly First Committee on Disarmament and International Security, cyber terrorism is mentioned as actions conducted via computer network that may cause violence against or generate fear among people, or lead to serious destruction for political or social problem [26]. Ron Dick, Director of the US's National Infrastructure Protection Center (NIPC) defines cyber terrorism a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies (as cited in [27]). This definition perhaps is taken from the US Government's definition of terrorism with the inclusion of "computer" in the definition.

Kerr [28] believes that cyber terrorism should have three common elements: The use of violence, political objectives, and the purpose of showing fear within a target population.

Ellsmore [29] says that cyber terrorism can be differentiated in terms of intent, outcome and the use of skills. Further analysis suggests that there are at least five elements which must be satisfied to construe cyber terrorism as described in Table I [30].

Table I: Elements of Cyber Terrorism (adapted from Yunos et al. [30])

Elements of Cyber Terrorism	• Politically-motivated cyber attacks that lead to death or bodily injury; • Cyber attacks that cause fear and/or physical harm through cyber attack techniques; • Serious attacks against critical information infrastructures such as financial, energy, transportation and government operations; • Attacks that disrupt non-essential services are not considered cyber terrorism; and • Attacks that are not primarily focused on monetary gain.

Based on the discussion above, there is no common agreement on the concept of cyber terrorism at the international front and among the researchers. While there are many definitions of cyber terrorism, these suggest a trend that further analysis of the phenomena could be further conducted. This is evidence as the study of this concept has been the focus of many policy makers and scholarly studies, but their standpoints and views vary. Due to multidimensional structures (or components) of cyber terrorism, we can say that the concept of cyber terrorism is a contested concept who interpret it differently by a number of parties. The context of cyber terrorism denotes different understandings and interpretations.

B. A Clear Line between Terms

When discussing cyber terrorism, there is always confusion between the term cyber terrorism with "cyber crimes" and "terrorist use of the Internet" [31]. However, these terms should not be mistaken as synonyms for cyber terrorism.

Cyber terrorism has become a buzzword and is often sensationalized in the media whereby reports of cyber crimes are posed as cyber terrorism [31]. Berner [32] argues terms such as "computer crime" or "economic espionage" must not be associated with the term cyber terrorism. In defining cyber terrorist and cyber crime activities, it is necessary to segment the motivation and action [33]. From the motivation perspective, cyber terrorism is clearly different, operating with a specific agenda to support their actions [34]. Cyber crime and cyber terrorism can be differentiated through financial or economic purposes [35] [36].

The United Nations categorized cyber crime as unauthorized access, damage to computer data or programs, sabotage to hinder the functioning of computer system or network, unauthorized interception of data to, from and within a system or network; and computer espionage [37]. From a legal perspective, cyber crimes and cyber terrorism are two different things. In the United States, The Computer Fraud and Abuse Act (18 USC: 1030) defines cyber crimes as unauthorized computer intrusions or misuse as unlawful activity [36]. Malaysia too has enacted the Computer Crimes Act 1997. The purpose of the Act is to provide offenses relating to the misuse of computers. Amongst other things, it also deals with unauthorized access to computer material, unauthorized access with intent to commit other offenses and unauthorized modification of computer contents [38]. From legal perspective, the definition of Malaysia's computer crimes in Computer Crimes Act 1997 and terrorism in Penal Code, Chapter VII A, Section 130B is different. These two concepts cover different areas. In the simplest terms, cyber terrorists' actions may cause prejudice to national security and public safety whereas cyber criminals' actions may cause prejudice to individuals or groups for the purpose of monetary gain.

Many studies have indicated that the Web 2.0 media such as interactive websites and blogs, social networking sites and discussion forums have been rapidly used by extremists as the medium to support their online activities [13]. However, it is important to note that cyber terrorism is different from terrorists' use of the Internet [31]. Taliharm [33] argues that cyber terrorism should not be confused with the use of illicit activities or Internet radicalization in cyberspace by the terrorist groups [33]. Taliharm [33] further argues that terrorists' use of the Internet is just action by certain individual or group to organize illicit activities by using the cyberspace.

Radicalization and extremism in cyberspace, however, can lead to terrorism [39]. Understanding online radicalization is one of the pillars of the fight against terrorism [21]. Perhaps the main concern is the potential for terrorists to use the Internet to inflict damage. The United Nations' report mentioned that the concern is to prevent moderates from becoming extremists, and extremists from becoming terrorists [40]. Threats from terrorism must be analyzed before they evolve into fully-fledged threats. Many of the actors in foiled plots have been discovered to have been radicalized online, on terrorists' and extremists' websites and chat rooms, amongst others, to provide information on weapons and explosives and facilitate large-scale recruitment efforts and propaganda [3].

C. Empirical Cyber Terrorism Frameworks

Based on literatures, there are several empirical frameworks on cyber terrorism proposed by researchers. Veerasamy proposed a conceptual framework outlining the aspect of cyber terrorism that addresses the operating forces, the techniques and the objectives [41]. The operating forces provide the context in which cyber terrorism is functioning, in which it describes the qualities of a cyber terrorist as well as the properties of cyber terrorism in general. The technique describes practical methods and classification descriptions of carrying out cyber terrorism via invasive or offensive computer and network security practices. The objectives are similar to the motivation, where the intent is to cause direct damage via malicious goals and support functions. The framework provides a high level overview and serves as a basis of considerations in the domain of cyber terrorism. However, the framework's attributes are not interactive and quite complex. The framework signifies that in order to consider cyber terrorism, at least one or more elements must be fulfilled. However, this is not accurate as cyber terrorism should be seen from a holistic perspective.

Another framework on cyber terrorism, proposed by Heickero, illustrates the effects and consequences of cyber terrorism operation from actor-target-effect chain in an asymmetric context [5]. The model illustrates how cyber terrorism in different phases could plan and accomplish a cyber operation as well as the effects and consequences of the digital attack. Figure 1 provides an illustration of how cyber terrorism is conducted.

Figure 1. Actor-target-effect Chain (adapted from Heickero [5])

The framework provided by Heickero is more relevant in understanding the modus operandi of cyber terrorism, which provides an attribute-chain from one attribute to another. The framework consists of the actors which are antagonists; the driving forces behind motives are social, psychological, economical and political; usage of means such as weapons and economy (resources); targets are objects such as infrastructure, organizations and individual; activities in realizing their goals such as planning and disorganization; and effects or consequences such as physical effect and syntax effect.

Gordon and Ford [42] viewed cyber terrorism from the following perspectives; people (or groups), locations (of perpetrators, facilitators, victims), methods/modes of action, tools, targets, affiliations and motivations (Table II). They made an analysis on the attributes of traditional terrorism and integrated computer into the matrix. They concluded that the scope of terrorism changes within each other due to the addition of the computer. However, attributes such as perpetrator and place require further investigation as what important is not the perpetrator or the place, but the action [43]. Perhaps further analysis based on case studies is required.

Table II. Matrix of Terrorism with Inclusion of the Computer (adapted from Gordon and Ford [42])

Attributes	Description	
Perpetrator	Group/ Individual	In the cyber context, virtual interactions can lead to anonymity and desensitization.
Place	Worldwide	The event does not have to occur in a particular location. The Internet has introduced globalization of the environment.
Action	Threats/ Violence/ Recruitment/ Education/ Strategies	Terrorist scenarios typically are violent or involve threats of violence. Violence in the virtual environment includes psychological effects, possible behavior modification and physical trauma.
Tool	Kidnapping/ Harassment/ Propaganda/ Education	Terrorists use the computer as a tool. Facilitating identity theft, computer viruses, hacking are examples that fall under this category.
Target	Government Officials/Corporations	Potential targets are corporations and government computer systems.
Affiliation	Actual/ Claimed	Affiliation refers to recruitment in carrying out given instructions. Affiliation can result in the strengthening of individual organizations as they can immediately acquire access to the information resources of their allies.
Motivation	Social/Political Change	Political, social and economic are the motivations present in real-world terrorism.

III. Analysis of Findings

Should website defacement be considered cyber terrorism? Would the use of the Internet by the terrorists such as fund raising, recruitment and propaganda be considered cyber terrorism? If somebody commits a certain act that meets the criteria of cyber terrorism, under what law will he/she be charged? Such examples highlight the need for a precise definition of cyber terrorism in order to avoid possible ambiguity and misinterpretation. This also will serve as a guide for distinguishing various terms of cyber incidents.

Interestingly, most governments in the world do not agree on one single definition of cyber terrorism [11] [44]. The term cyber terrorism generates different meaning in the minds of different people. However, understanding a common understanding as to what phenomenon contributes to this term is important in order for us to get a better understanding on the root causes of cyber terrorism. Unfortunately, we are in situation where there is still no consensus agreement on a definition on the concept of the phenomenon.

There is no common definition of cyber terrorism that is widely accepted, hence there is a lack of common ground on which policy makers and researchers can agree on what they are fighting against. In general, previous studies have defined cyber terrorism from various points of view. However, the connectivity between each component highlighted in defining this terminology is still unclear. Therefore, there is a strong need to have a specific concept of cyber terrorism, especially for a legal definition. The concept would provide a foundation to the legal fraternity such as prosecutors and judges.

In this study, the analysis is divided into four processes: Plan, data collection, data analysis, and reporting, which are similar with other traditional stages of research [45]. While most of the research methodologies are described in Section III, the reporting is presented in Section IV.

A. Plan

The planning stage started with the identification and investigation of research problems surrounding the identified phenomena. There are many terms of cyber terrorism, and some of them only address a subset of cyber terrorism and not the whole context. Due to the complexity of various interacting attributes or elements in cyber terrorism, to formulate a framework as to describe its influential considerations would be beneficial. Therefore, there is a need for a more structured approach in understanding the various attributes of cyber terrorism. This is crucial to the researchers and policy makers in understanding the context of cyber terrorism.

B. Data Collection

The analysis was conducted by reviewing existing literature on terrorism and cyber terrorism. Our goal was to examine whether particular researchers had developed useful insight into this subject and to learn whether consensus agreement had already been reached on this subject. Based on our observations, we have found that there is limited literature focusing on the cyber terrorism framework. However, most of the literature reviewed is valuable in terms of framing the context rather than directly providing a solution to the issues of this study. The materials reviewed include overseas government reports, articles found in websites, published conference materials and referred publications.

One example of the qualitative research approach is grounded theory. Grounded theory was first presented by Glaser and Strauss in their 1967 book "The Discovery of Grounded Theory", which Goulding [46] describes the book was premised on a strong intellectual justification for using qualitative research to develop theoretical analysis. The phrase grounded theory refers to theory or general concepts that are developed from a corpus of data [47], [48] and the theory emerges through a close and careful analysis of the data [49]. As mentioned by Borgatti [47], the basic idea of the grounded theory approach is to read (and re-read) a textual database (such as a corpus of field note) and discover or label variables (called categories, concept and properties) and their interrelationship.

In grounded theory development, the literature review provides theoretical construct, categories and their properties that can be used to organize the data and discover new connections between theory and real-world phenomena [50]. Developing grounded theory should formulate them into a logical, systematic and explanatory scheme [51], [49]. The theory should be based exclusively on data collected whereby the researchers bring a considerable background in professional and disciplinary knowledge to an inquiry. Researchers approach the question with background and some knowledge with the literature in the domain [49]. Levy [51] explains that these positions recognize that a prior understanding of the literature can be therefore be used effectively in developing theory in a number of ways. Based on the review of pertinent literature, prior knowledge and experience of the researcher is useful to formulate of a preliminary conceptual model.

> " .. experience and knowledge are what sensitize the researcher to significant problems and issues in the data and allows him or her to see alternative explanations and to recognize properties and dimensions of emerging concepts" [52].

Haig argues that the grounded theory research begins by focusing on an area of study and gathers data from a variety of sources, including literatures [53]. It is important to note comment made by Levy [51], where the author explains that these positions recognize that a prior understanding of the literature can therefore be used effectively in developing theory in a number of ways. Based on the review of pertinent literature, the prior knowledge and experience of the researcher are useful to formulate a preliminary conceptual model.

Heath and Cowley reveal that a pre-understanding by early reference to the literature can contribute to the researcher's understanding of social processes observed [54]. They argue that prior reading may be required if the researcher wishes to clarify concepts and build an emergent theory. Heath and Cowley [54] cite the work by Jezewski [55] who carried out a literature-based concept before attempting to further develop the concept via grounded theory. Heath and Cowley [54] further cite the comment by Glaser and Strauss [56] that "the researcher will not enter the field from ideas, but differ considerably in the role they see for the literature". Thus, specific understanding from experience and literature may be used to stimulate theoretical sensitivity and generate the hypotheses. This notion is supported by Onion [57] who concludes that the application of the grounded theory method to review literature and derive a meta-theory is novel, whereby literature may be used as the primary data by the grounded theory method. This is ascertained by Esteves et al. [58] whereby they conclude that an analysis of issues related with the use of the grounded theory method is very useful for people starting a research project.

C. Data Analysis

The data analysis was conducted in two steps. In the first step, data analysis proceeded through axial coding (examining conditions, strategies and consequences). This method has been well described by Egan [45] and Borgatti [47]. In the second step, the data was mapped into a matrix format [58], where attributes as well as similarities or patterns between them emerged.

As described by Borgatti [47], axial coding is the process of relating codes (categories and properties) to each other, via a combination of inductive and deductive thinking. Borgatti [47] explains that grounded theorists emphasize causal relationships, and fit things into a basic frame of generic relationships. The author simplifies the process of axial coding framework as per Table III. This framework consists of systematized cause-and-effect schema which the researchers used to explicate relationships between categories (or attributes) and sub-categories.

Egan [45] explains that a general understanding of the phenomenon under investigation is considered sufficient for the initiation of this type of research. Egan [45] further explains, "Having established a problem or topic in general terms and chosen a site where the research questions could be examined more closely, evidence is allowed to accumulate by the

researcher, resulting in an emerging theory". To develop this theory, "early activities by the researcher involve the identification of categories capturing uniformities in the data and then identifying compelling properties and dimensions of the data". This argument is further stressed by Glaser and Strauss [56] where they say, "A discovered, grounded theory, then, will tend to combine mostly concepts and hypothesis that have emerged from the data with some existing ones that are clearly useful".

Levy [51] explains that sampling should be directed by the logic and the types of coding procedures used in analyzing and interpreting data. The result is the revelation of meaningful differences and similarities among and between categories. The possibility for a hypothesis about the relationships between categories is always present. By using the framework provided by Borgatti [47], the relationships of categories are analyzed and observed.

Table III. Axial Coding Framework (adapted from Borgatti [47])

Elements	Description
Phenomenon	This is what in schema theory might be called the name of the schema or frame. It is the concept that holds the bits together. In grounded theory it is sometimes the outcome of interest, or it can be the subject.
Causal conditions	These are the events or variables that lead to the occurrence or development of the phenomenon. It is a set of causes and their properties.
Action strategies	The purposeful, goal-oriented activities that agents perform in response to the phenomenon and intervening conditions.
Consequences	These are the consequences of the action strategies, intended and unintended.

IV. The Proposed Framework

A conceptual framework links various concepts and serves as a motion for the formulation of theory [59]. A complete analysis of the data has revealed six emergent perspectives of cyber terrorism, which became the major findings of the study. In our view, the nature of cyber terrorism framework should have these six perspectives: Target, motivation, method of attack, domain, action by perpetrator, and impact.

With the growing interconnectedness of critical infrastructures on ICT, the selection of a target that allows the maximum level of disruption would significantly influence the terrorists. Motivation is about influencing human beings and the decisions they make. Motivation forces behind cyber terrorism are social, political and belief. Cyber terrorists can exploit vulnerabilities over a targeted system through a vast array of intrusive tools and techniques. The method of attack could be through network warfare and psychological warfare. Cyberspace is the domain in which a terrorist-type attack is conducted. Cyber terrorists employ unlawful use of force or unlawful attacks to conduct the premeditated attack. The impact or consequence is high as the cyber attacks are done to intimidate or coerce a government or people that lead to violence against persons or properties. The framework describing the components of cyber terrorism is proposed in Figure 2.

The framework provides a baseline when establishing and defining cyber terrorism. The aim is to show a more dynamic way in defining cyber terrorism as well as describing its influential considerations. Thus, it can be seen that formulating the framework from various strategic considerations would be beneficial in understanding cyber terrorism in its full context. Summarily, these factors will determine whether someone is involved in cyber terrorism or not.

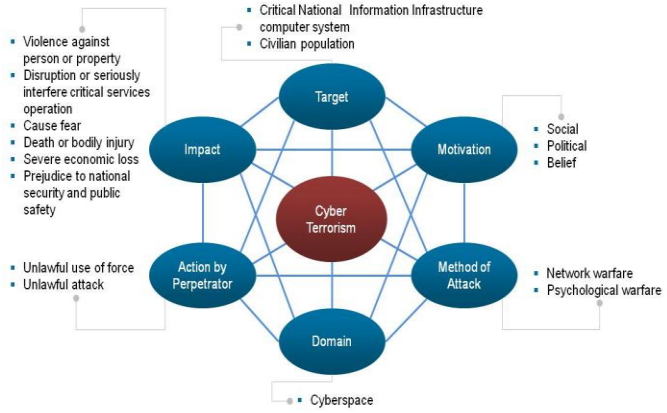

Figure 2. A Dynamic Cyber Terrorism Framework

The framework is dynamic in many aspects since the influential factors on the decision are based on all attributes (or components) within the framework. In other words, the framework suggests that all attributes (or components) contribute in the decision-making process in order to determine whether someone gets involved in cyber terrorism or not. The authors suggest that the framework presented here is an improvement over existing frameworks as it captures the important factors when considering that the perpetrator may combine these factors for conducting cyber terrorism. The components of cyber terrorism in this framework are bind together to form the concept of cyber terrorism. We need to combine the components with conjunction "AND", which means that each of those components is necessary to constitute cyber terrorism. Otherwise, if one or more components are not provided, it would not constitute cyber terrorism.

A. *Target*

The act of cyber terrorism is unique as it combines a specific target with a wider audience [60], which is illustrated in Figure 3. With this argument, the CNII computer system and civilian population contribute to the uniqueness of cyber terrorism [61]. The possibility of disabling the entire CNII communication networks and attacking civilian community at large would seem to provide a variety of attractive targets. At

the same time, targets that are high-profile would probably be among the most influential factors in a terrorist group's decision as the damage and destruction would be extraordinarily significant and costly to society and the country attacked.

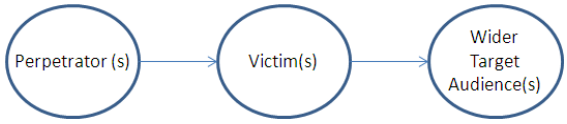

Figure 3. Target Model (adapted from Ackerman et al. [60])

The assumption that attacks against computer systems are less dangerous, such as leading to economic losses rather than human lives is not true. Due to the advancement of technology, many essential computing services are using the Supervisory Control and Data Acquisition (SCADA) systems, and nowadays, they are connected to the Internet and can be controlled remotely. An attack to the SCADA system that controls and manages critical infrastructures may have been unthinkable in the past, but with current technological developments, it is now possible for the SCADA system to become a target for terrorist attacks. Brunst [62] discusses that there are three scenarios that could be taken into consideration; attacks on hydroelectric dams, tampering with railways and air traffic control systems, and taking over control of power plants. Brunst in his literature review provides excellent examples of terrorist attacks in these control systems, which would generate fear within a population. Successful cyber attacks on these control systems certainly have long-term effects, create fear and pose immediate danger to human lives.

Apart from focusing on the ICT infrastructure, cyber terrorism also targets civilian population [5] [25] [60]. Attacks against critical infrastructure that spread fear and harm to innocent people within a community would be classified as cyber terrorism [20]. From an effect perspective, consequences on civilian population are bigger, thus it would get more media attention and be more widely publicized. The selection of a target that allows the maximum level of disruption would significantly influence the terrorists.

B. *Motivation*

Motivation is about influencing human beings and the decisions they make [1]. The motivating forces behind cyber terrorism are social, political and belief [63]. Through these forces, terrorists are psychologically motivated to drive terrorism. From the motivation perspective, cyber terrorism exists if the person or group of people operates with a specific political or ideological agenda to support their activities [20]. For example, the Irish Republican Army engages in terrorist activity for a predetermined political purpose with the objective to maintain and strengthen political control [6].

Cyber terrorism is defined as unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives [11]. Digital technologies thus offer contemporary terrorists and terrorist organizations a wide range of opportunities to support their campaigns of violence and if they are proficient, significantly support their political objectives [25]. Terrorists wish to undermine confidence in the political structure and create difficulty within the body of politics. Cyber terrorists cause harm or damage to people or groups of people with a political agenda [32].

C. *Method of Attack*

Heickero [5] concludes that cyber terrorism comprises different types of methods such as computer network operations and psychological operations. The capability to conduct a cyber attack can be divided into three groups: Simple (unstructured), advanced (structured) and complex (coordinated) [64]. Heickero's [5] description of a computer network operation and O'Hara's [64] model of technical capabilities of a cyber attack fit well with the definition of network warfare. Veerasamy [65] defines network warfare as a modern form of conflict in which computers and networks are used as the weapons with information serving as the leverage control. Modern forms of network warfare include all the computer and network security means through which computers are attacked and exploited (worms, denial-of-service, bots) as well as all the protective mechanism being implemented (intrusion detection tools, anti-virus software and firewalls).

Taliharm [31] suggests that the term cyber terrorism should also involve several other activities carried out by the terrorist via the Internet, including propaganda via terrorist websites. Spreading of propaganda via Web 2.0 media is part of psychological operation [43]. Web 2.0 media enables terrorists or terrorist groups to establish their presence in cyberspace and to spread propaganda, especially for the press and public attention [62]. Coverage of mainstream media is important as news coverage in the media is always repeated, thus increasing the propaganda message's reach.

From a psychological perspective, a disgruntled employee within an organization also poses threats to the organization. One incident took place in Australia where a man had access to the sewerage control systems, which harmed the environment and killed wildlife [66]. It was reported that he had worked for the company and had knowledge of the tools that operated the sewerage control system. The driving forces for his action were revenge and the feeling of unfair treatment from the management. On the other hand, this category of individuals can be bought; and information can be sold to terrorist groups. An insider could also act as a cyber terrorist [5]. The extra advantage is that they have the inside knowledge. An insider can be planted within the organization or through a sympathizer who is working in that organization. The objective is perhaps to provide sensitive information or to perform certain tasks such as putting malware into critical control systems for future attacks. In the US, it was reported that 20 employees were arrested for possession of false identification used to obtain security access to facilities containing restricted and sensitive military technology [43].

D. Domain

Cyber terrorism is the convergence of cyberspace and terrorism. Cyberspace, whether accessed by computer systems or other devices, is the domain (medium) through which a cyber attack would be delivered. The National Security Presidential Directive 54/Homeland Security Presidential Directive 23 of the US Government defines cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers [67]. The UK Government defines cyberspace as an "interactive domain that is made up of digital networks that is used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure and services" [68].

Cyber terrorism thus can be seen as a relevant threat due to its strong relation to ICT and cyberspace. Apart from land, sea, air and space, cyberspace is another dimension of warfare. Weimann [21] writes that cyberspace is in many ways an ideal arena for activity of extremist of terrorist organizations. Among others, it offers easy and fast flow of information. By its very nature, cyberspace is also capable of reaching out to a wide audience throughout the world and disseminates information in a multimedia environment via the combined use of text, graphics, audio and video.

E. Action by Perpetrator

Flemming and Stohl [6] argue that, terrorism is a process that involves acts or threats, emotional reactions and the social effects of the acts or threats and the resultant action. Terrorism in the cyber environment involves all of the above components. The advancement of ICT and rapid changes in the technological environment influence terrorist resources and opportunities. The convergence of physical terrorism and new advancements of ICT have spawned a new term called cyber terrorism.

Rollins and William [43] argue that, there are two views in defining cyber terrorism, which are based on impact (effect-based) and intention (intent-based). They clarify that, effect-based cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals. This implies that, cyber terrorism should focus on the act rather than the perpetrator. While, intent-based cyber terrorism exists when "unlawful or politically-motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage".

The cyber terrorist can have the same motives as the traditional terrorist, but they use computer and network media to attack [69]. Cyber terrorists conduct unlawful use of force or unlawful attack to conduct the premeditated attack to intimidate or coerce a government or people to further political, social or belief objectives, or to cause severe economic damage. The impact or consequence is high as the attacks are done to intimidate or coerce a government or people that lead to violence against persons or properties.

F. Impact

The act of cyber terrorism is unique as it combines a specific target with a wider audience [6]. In this argument, the components of a purposeful violence against persons or properties, disruption or serious interference of critical services operation, causing fear, death or bodily injury, severe economic loss, and prejudice to national security and public safety contribute to the uniqueness of cyber terrorism.

Cyber terrorism exists when there is an attack on a computer system that leads to violence against a person or property; and the disruption is enough to generate fear, death or bodily injury [11] [12]. Cyber terrorism is done to cause grave harm or severe economic damage or extreme financial harm [6] [22]. As reported by Rollins and Wilson [43], if terrorists were to launch a widespread cyber attack, the economy would be the intended target for disruption, while death and destruction might be considered collateral damage. Terrorist-type cyber attacks may target chemical, biological, radiological or nuclear (CBRN) computer network installations [18] [43]. A successful attack to these installations would cause enough severe economic disruption and harm to civilian population (death and bodily injury).

With the growing interconnectedness and interdependencies of critical infrastructure sectors, the target selection of cyber terrorism is likely to be significantly influenced by those targets that allow for a maximum level of disruption [6] [20]. Terrorists' cyber attacks probably aim at critical infrastructure as their target. Successful cyber attacks in one sector will have cascading effects on other sectors. Due to this nature, a large-scale terrorist-type cyber attack could bring unpredictable and perhaps catastrophic impact to other sectors, and possibly long-lasting impact to the country's economy.

V. CONCLUSION

The term cyber terrorism generates different meanings in the minds of different people. Cyber terrorism is about threat perception that makes the concept differ from one to another. The concept of this term is an essentially-contested concept where it is interpreted differently at different levels such as researcher, professional and policy maker. Understanding similarities and differences in perception of what constitutes cyber terrorism can provide insight on the concept of cyber terrorism.

In this work, the data collected from the extensive literatures was analyzed using the grounded theory approach, in which the framework was drawn. The analysis was conducted to determine how the components of the concept of cyber terrorism come together to form the concept. From the finding, the authors have concluded that the concept of cyber terrorism can be described from six perspectives: Target, motivation, method of attack, domain, action by perpetrator, and impact.

This work provides a baseline when establishing and defining the concept of cyber terrorism. The perspectives are useful in determining whether someone is involved in cyber terrorism or not. In addition, the proposed framework shows an overall framework of cyber terrorism in a simplistic and dynamic manner. For future works, this framework can be

validated and assessed by encompassing both qualitative and quantitative techniques. Continued research in this area can be further conducted, which may lead to the development of strategic and technological framework to counter cyber terrorism.

ACKNOWLEDGMENT

The authors would like to thank the following individuals who provided valuable input to this paper: Professor Dato' Husin Jazri, CEO of CyberSecurity Malaysia; Sazali Sukardi, Head of Strategic Policy Research, CyberSecurity Malaysia and Nor'azuwa Muhamad Pahri, Specialist of Research Division, CyberSecurity Malaysia. We also would like to thank the Universiti Teknikal Malaysia Melaka (UTeM) that provided research grant for this project.

REFERENCES

[1] N. Veerasamy and J. H. P. Eloff, "Towards a Framework for a Network Warfare Capability," in *Council of Scientific and Industrial Research, Pretoria, South Africa*, 2008.

[2] D. E. Denning, "Activism, Hactivism and Cyberterorism: The Internet as a Tool for Influencing Foreign Policy," in *Conference on The Internet and International System: Information Technology and American Policy Decision Making*, 1999.

[3] The Lipman Report Editors, "Cyberterrorism: The Invisible Threat Stealth Cyber Predators in a Climate of Escalating Risk," *Guardsmark, LLC, Memphis, Tennessee, USA*. 2010.

[4] Ministry of Science Technology and Innovation of Malaysia, "National Cyber Security Policy." 2006.

[5] R. Heickero, "Terrorism Online and the Change of Modus Operandi," *Swedish Defence Research Agency, Stockholm, Sweden*, pp. 1-13, 2007.

[6] P. Flemming and M. Stohl, "Myths and Realities of Cyberterrorism," *Proceeding on Countering Terrorism through Enhanced International Cooperation*, pp. 70-105, 2000.

[7] C. Lim, K. I. Eng, and A. S. Nugroho, "Implementation of Intelligent Searching Using Self-Organizing Map for Webmining Used in Document Containing Information in Relation to Cyber Terrorism," in *2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies*, 2010, pp. 195-197.

[8] ACT 574 Penal Code, "Chapter VIA – Offences Relating To Terrorism. Section 130B (1) & (3) (h)." Zul Rafique & Partner Report, 1997.

[9] "Australia's Security Legislation Amendment (Terrorism) Act," no. 2005. 2002.

[10] B. L. Collin, "The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge," in *11th Annual International Symposium Criminal Justice Issues*, 1996, vol. 93, no. 4.

[11] D. E. Denning, "Cyberterrorism," *Testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism*, 2000.

[12] J. A. Lewis, "Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats," *Center for Strategic and International Studies*, 2002.

[13] B. Mantel, "Terrorism and the Internet. Should Web Sites That Promote Terrorism Be Shut Down?," *CQ Researcher*, pp. 129-152, 2009.

[14] K. Mshvidobadze, "State-sponsored Cyber Terrorism : Georgia's Experience," *Presentation to the Georgian Foundation for Strategic and International Studies*, pp. 1-7, 2011.

[15] S. Krasavin, "What is Cyber-terrorism," *Computer Crime Research Center (CCRC)*, 2001. [Online]. Available: www.crime-research.org/library/cyber-terrorism.htm. [Accessed: 09-Jun-2008].

[16] M. Conway, "Reality Bytes : Cyberterrorism and Terrorist ' Use ' of the Internet," *FIRST MONDAY, Journal on the Internet*, 2002. [Online]. Available: www.firstmonday.org/ISSUES/issue7_11/conway. [Accessed: 09-Jun-2008].

[17] M. M. Pollitt, "Cyberterrorism — Fact or Fancy?," *Computer Fraud & Security*, no. 2, pp. 8-10, 1998.

[18] P. Czerpak, "The European Dimension of the Flight against Cyber-terrorism – A Theoretical Approach," 2005.

[19] R. Nagpal, "Cyber Terrorism in the Context of Globalization," in *II World Congress on Informatics and Law*, 2002, no. September, pp. 1-23.

[20] C. Beggs, "Cyber-Terrorism in Australia," *IGI Global*, pp. 108-113, 2008.

[21] G. Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," *United States Institute of Peace*, no. 116, pp. 1-11, 2004.

[22] C. Wilson, "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," 2005.

[23] G. Ariely, "Knowledge Management, Terrorism and Cyber Terrorism," in *Cyber Warfare and Cyber Terrorism*, L. J. Janczewski and A. M. Corarik, Eds. Hersey, New York: Information Science Reference, 2008.

[24] B. Nelson, R. Choi, M. Iacobucci, M. Mitchell, and G. Gagnon, "Cyberterror: Prospects and Implications." Center for the Study of Terrorism and Irregular Warfare, Montery, CA, 1999.

[25] M. Stohl, "Cyber Terrorism : A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Game?," *Springer Science + Business Media B.V*, 2007.

[26] S. T. Dang, "The Prevention of Cyberterrorism and Cyberwar," in *Old Dominion University Model United Nations Conference (ODUMUNC)*, 2011, pp. 1-6.

[27] S. Berinato, "Cybersecurity - The Truth About Cyberterrorism," 2002. [Online]. Available: http://www.cio.com/article/30933/CYBERSECURITY_The_Truth_About_Cyberterrorism?page=2&taxonomyId=3089. [Accessed: 26-Jan-2012].

[28] K. Kerr, "Putting Cyberterrorism into Context," *The Journal of The System Administrators Guild of Australia*, vol. 9, no. 3, pp. 5-10, 2003.

[29] N. Ellsmore, "Cyber-terrorism in Australia: The Risk to Business and a Plan to Prepare." SIFT Pty Ltd, 2002.

[30] Z. Yunos, S. H. Suid, R. Ahmad, and Z. Ismail, "Safeguarding Malaysia's Critical National Information Infrastructure (CNII) Against Cyber Terrorism: Towards Development of a Policy Framework," *IEEE Sixth International Conference on Information Assurance & Security*, pp. 21-27, 2010.

[31] A. M. Taliharm, "Digital Development Debates: Emerging Security Challenges and Cyber Terrorism," no. 5, 2011.

[32] S. Berner, "Cyber-Terrorism : Reality or Paranoia ?," *South African Journal of Information Management*, vol. 5, no. 1, pp. 1-4, 2003.

[33] E. Noor, "The Problem with Cyber Terrorism," *Proceeding of Southeast Asia Regional Center for Counter Terrorism's (SEARCCT) Selection of Articles, Ministry of Foreign Affairs Malaysia*, vol. Volume 2/2, pp. 51-64, 2011.

[34] Y. Li, "National Information Infrastructure Security and Cyber Terrorism in the Process of Industrializations," in *Proceeding of the IEEE Computer Society*, 2009, pp. 532-535.

[35] N. Veerasamy and M. Grobler, "Countermeasures to Consider in the Combat Against Cyberterrorism," *Proceedings of the Workshop on ICT Uses in Warfare and the Safeguarding of Peace*, pp. 56-85, 2010.

[36] C. Wilson, "Holding Management Accountable : A New Policy for Protection Against Computer Crime," *IEEE Explore*, pp. 272-281, 2000.

[37] N. B. Sukhai, "Hacking And Cybercrime," *Proceeding of InfoSecCD Conference*, pp. 128-132, 2004.

[38] "Malaysia's Computer Crime Act 1997," 1997. [Online]. Available: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025630.pdf. [Accessed: 20-Oct-2011].

[39] A. Bergin, S. Osman, C. Ungerer, and N. A. Mohamed Yasin, "Countering Internet Radicalisation in Southeast Asia." An RSIS–ASPI Joint Report by S. Rajaratnam School of International Studies and Australian Strategic Policy Institute, 2009.

[40] United Nations General Assembly, "Uniting Against Terrorism: Recommendations for a Global Counter-terrorism Strategy." 2006.

[41] N. Veerasamy, "A Conceptual High-level Framework of Cyberterrorism," *International Journal of Information Warfare*, vol. 8, no. 1, pp. 1-14, 2009.

[42] S. Gordon and R. Ford, "Cyberterrorism?," *Symantec White Paper*, 2002.

[43] J. Rollins and C. Wilson, "Terrorist Capabilities for Cyberattack: Overview and Policy Issues," CRS Report for Congress, 2007.

[44] J. J. Prichard and L. E. MacDonald, "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks," *Journal of Information Technology Education*, vol. 3, 2004.

[45] T. M. Egan, "Grounded Theory Research and Theory Building," in *Advances in Developing Human Resources*, vol. 4, no. 3, Sage Publications, 2002, pp. 277-295.
[46] C. Goulding, "Grounded Theory: Some Reflections on Paradigm, Procedures and Misconceptions," pp. 1-29, 1999.
[47] S. Borgatti, "Intro to Grounded Theory," 1996. [Online]. Available: trp.jlu.edu.cn:8000/yuhongyan_jpk/.../2006120116524l756.doc.
[48] D. R. Cooper and P. S. Schindler, *Business Research Method*. NY: McGraw-Hill Companies, Inc, 2008.
[49] L. Lingard, M. Albert, and W. Levinson, "Grounded Theory, Mixed Methods, and Action Research," *British Medical Journal*, vol. 337, pp. 459-461, Aug. 2008.
[50] C. Marshall and G. B. Rossman, "The 'What' of the Study - Building the Conceptual Framework," in *Designing Qualitative Research 3rd Edition*, Sage Publications, 1999, pp. 21-54.
[51] D. Levy, "Qualitative Methodology and Grounded Theory in Property Research," *Pacific Rim Property Research Journal*, vol. 12, no. 4, pp. 369-388, 2006.
[52] A. Strauss and J. Corbin, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Newbury Park, CA: Sage Publications, 1990.
[53] B. D. Haig, "Grounded Theory as Scientific Method," in *In Philosophy of Education 1995 : Current Issues*, no. 1, University of Illinois Press, 1996, pp. 281-290.
[54] H. Heath and S. Cowley, "Developing a Grounded Theory Approach: A Comparison of Glaser and Strauss," *International Journal of Nursing Studies*, vol. 41, no. 2, pp. 141-150, Feb. 2004.
[55] M. A. Jezewski, "Evolution of a Grounded Theory. Conflict Resolution through Cultural Brokering," *Advances in Nursing Science*, vol. 17, no. 3, pp. 14-30, 1995.
[56] B. Glasser and A. Strauss, "The Discovery of Grounded Theory," in *Strategies for Qualitative Research*, New York: Aldine, 1967.
[57] P. E. W. Onions, "Grounded Theory Applications in Reviewing Knowledge Management Literature," *Leeds Metropolitan University Innovation North Research Conference*, pp. 1-20, 2006.
[58] J. Esteves, U. Politécnica, and J. Carvalho, "Use of Grounded Theory in Information Systems Area : An Exploratory Analysis," *European Conference on Research Methodology for Business and Management*, pp. 129-136, 2000.
[59] G. A. Bowen, "Grounded Theory and Sensitizing Concepts," *International Journal of Qualitative Methods*, pp. 12-22, 2006.
[60] G. Ackerman et al., "Assessing Terrorist Motivations for Attacking Critical Infrastructure," *Center for Nonproliferation Studies, Monterey Institute of International Studies, California*, Jul. 2007.
[61] T. G. Lewis, T. J. Mackin, and R. Darken, "Critical Infrastructure as Complex Emergent Systems," *International Journal of Cyber Warfare & Terrorism*, vol. 1, no. 1, pp. 1-12, 2011.
[62] P. W. Brunst, "Terrorism and the Internet: New Threats Posed by Counterterrorism and Terrorist Use of the Internet," pp. 51-79, 2010.
[63] M. D. Cavelty, "Critical Information Infrastructure: Vulnerabilities, Threats and Responses," 2007.
[64] T. F. O'Hara, "Cyber Warfare/Cyber Terrorism," *USAWC Strategy Research Project*, 2004.
[65] N. Veerasamy and J. H. P. Eloff, "Application Of Non-Quantitative Modelling In The Analysis Of A Network Warfare Environment," in *World Academy of Science, Engineering and Technology Conference, Paris, France*, 2008.
[66] D. E. Denning, "Is Cyberterrorism Coming?," 2002. [Online]. Available: www.marshall.org/pdf/materials/58.pdf . [Accessed: 17-Oct-2010].
[67] United States of America, "Cyberspace Policy Review : Assuring a Trusted and Resilient Information and Communication Infrastructure." 2009.
[68] UK Cabinet Office, "The UK Cyber Security Strategy - Protecting and Promoting the UK in a Digital World," 2011.
[69] N. Veerasamy, "Motivation for Cyberterrorism," *9th Annual Information Security South Africa (ISSA) - Towards New Security Paradigms*, p. 6, 2010.

AUTHORS PROFILE

Rabiah Ahmad is an Associate Professor at the Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka, Malaysia. She received her PhD in Information Studies (health informatics) from the University of Sheffield, UK, and M.Sc. (information security) from the Royal Holloway University of London, UK. Her research interests include healthcare system security and information security architecture. She has delivered papers at various health informatics and information security conferences at national as well as international levels. She has also published papers in accredited national/international journals. Besides that, she also serves as a reviewer for various conferences and journals.

Zahri Yunos is currently working with CyberSecurity Malaysia. Zahri holds a Master's degree in Electrical Engineering from the Universiti Teknologi Malaysia, Malaysia and a Bachelor's degree in Computer Science from the Fairleigh Dickinson University, New Jersey, USA. He is a certified Associate Business Continuity Professional by the Disaster Recovery Institute International, USA. Zahri has been awarded Senior Information Security Professional Honouree in July 2010 by the $(IS2)^2$, USA. He has contributed various articles and presented papers on topics related to cyber security and Business Continuity Management. He is currently pursuing his PhD at the Universiti Teknikal Malaysia Melaka, Malaysia.