Journal of Information Security, 2012, *, **
doi:10.4236/jis.2012.***** Published Online ** 2012 (http://www.scirp.org/journal/jis)

Perception on Cyber Terrorism: A Focus Group Discussion Approach *

Rabiah Ahmad, Zahri Yunos, Shahrin Shahib
Center for Advanced Computing Technology
Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka (UTeM)
Melaka, Malaysia
Email: rabiah@utem.edu.my, zahri@cybersecurity.my, shahrinsahib@utem.edu.my

Mariana Yusoff
Centre for Languages and Human Development
Universiti Teknikal Malaysia Melaka (UTeM)
Melaka, Malaysia
Email: mariana@utem.edu.my

Received **** 2012

Abstract

Focus group discussion is an exploratory research technique used to collect data through group interaction. This technique provides the opportunity to observe interaction among participants on a topic under this study. This paper contributes to an understanding on the cyber terrorism conceptual framework through the analysis of focus group discussion. The proposed cyber terrorism conceptual framework which was obtained during the qualitative study by the authors has been used as a basis for discussion in the focus group discussion. Thirty (30) participants took part in the focus group discussion. The overall results suggest that the proposed cyber terrorism framework is acceptable by the participants. The present study supports our initial research that the cyber terrorism conceptual framework constitutes the following components: target, motivation, tools of attack, domain, methods of attack and impact.

Keywords: Cyber Terrorism Components; Framework; Focus Group

1. Introduction

A more holistic way in describing cyber terrorism is useful in understanding the concept of cyber terrorism. Based on literatures review, it is noted that there is no consensus agreement on the concept of cyber terrorism [1] [2] [3] [4] [5]. However, to have a common understanding on this term is important in order to get a better apprehension on what constitutes cyber terrorism. 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.

Cyber terrorism is about threat perception that makes the concept differ from one to another. This is due to multidimensional structures (or components) of cyber terrorism that made people interprets it differently at different levels. Therefore, understanding similarities and differences in perception of what constitutes cyber terrorism can provide insight to the policy makers and researchers to countering such threats.

2. Method

2.1. Background of this Study

The focus group discussion on cyber terrorism conceptual framework was held in conjunction with the 3-days cyber terrorism workshop organized by the South East Asia Regional Center for Counter Terrorism (SEARCCT), an agency under the Malaysia's Ministry of

Foreign Affairs, in collaboration with the CyberSecurity Malaysia (an agency under the Malaysia's Ministry of Science, Technology and Innovation) and the Universiti Teknikal Malaysia Melaka, Malaysia.

The focus group discussion was held on the last day of the 3-days workshop. The discussion was designed as a platform to address the cyber terrorism framework in a holistic approach. The workshop gave an insight and a basic understanding of terrorism and cyber terrorism, issues and challenges revolving around them and complexity in coming up with one single universal definition before finally embarking to focus group discussion. Speakers from various agencies who are responsible in the area of counter terrorism and counter cyber crimes were invited to provide their thoughts and perspectives on these topics on the first 2-days of the workshop. In addition, detail explanation about the cyber terrorism conceptual framework was presented by the moderator on day 3 of the workshop. The sessions were designed in such a way to trigger the minds of the participants and to channel all relevant issues to the focus group discussion.

2.2. Participants

Focus group discussion is often used as an exploratory technique and is one source of data collection method [6]. Normally, it consists of a group of people, typically between 5 to 10 participants and is led by a moderator.

In this study, 30 participants took part in the focus group discussion. However, they were divided into smaller groups consists of 6 participants for each group. This approach is similar to the focus group discussion conducted by Bray, Johns and Kilburn [7]. The background of the participants varies: management, policy, laws enforcement and prosecution, research and technical and the range of working experiences of the participants is between 10 years to 34 years. All participants were from the government agencies whereby all of them were nominated by the SEARCCT.

2.3. Procedures

The participants were divided into 5 groups and each group consists of 6 participants who are differed in term of age, organizations and working experiences. The rationale to have small number in a group is to give everyone the opportunity to express their views and opinions.

First, a briefing session was conducted in order to ensure that each focus group followed the same structure and had the same understanding on the key objectives as well as the discussion guidelines. Each group was given a flip chart to write their discussion points during the group brainstorming session. Before the group discussion, the proposed cyber terrorism conceptual framework was explained to the participants: target, motivation, tools of attack, domain, methods of attack and impact. Overall, the discussion and presentation sessions took about 3 hours.

Focus group discussion was identified as the appropriate and accessible technique, given the exploratory nature of the research [7]. The objectives of focus group discussion were as follows. Firstly, to discuss factors that make-up the components (or elements) of cyber terrorism and secondly, to evaluate the proposed conceptual framework that describes the components of cyber terrorism. In a nutshell, the focus group discussion was conducted to get consensus on people perception towards the proposed concept of cyber terrorism that was derived from the qualitative study. The proposed cyber terrorism conceptual framework is based on the author's initial study as described in Figure 1.

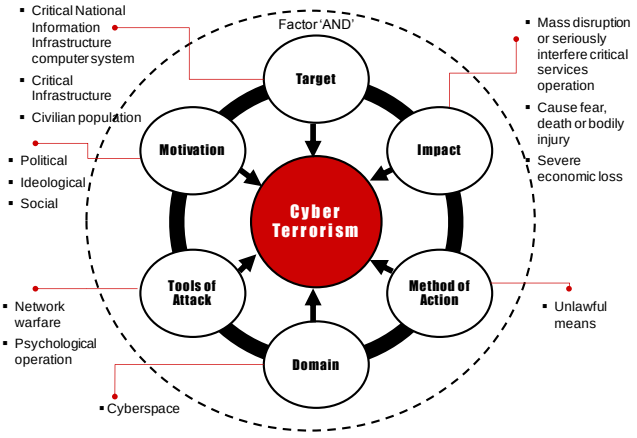

Figure 1: Proposed cyber terrorism conceptual framework

The primary output of this focus group was to gauge the participants view on the proposed cyber terrorism framework. The focus group discussion was facilitated by a moderator to provide guidance to the group and allowing respondents to talk freely and spontaneously in expressing ideas, views and experiences on the given topic. Although the moderator initiated the topic for discussion and thus exercises a certain control over what was to be discussed, he did not offer any viewpoints during the talk-in-process session [6]. As recommended by Bray, Johns and Kilburn [7], a relaxed and conversational method was used during the focus group discussion in order to produce a free flowing discussion with minimum intervention from the moderator.

Kamarulzaman [8] explained that in a focus group, people interacting with each other with the help of a moderator to get more information and to share their own experience. It is noted that the usefulness of focus group

data are affected to the extent that the participants are openly communicating their ideas, views, or opinions during the focus group discussions. This is ascertained by Ho [6] whereby the author explained that, people are gathered together to voice their opinions and perceptions about a study topic in a comfortable environment. During the discussion, participants are encouraged to talk to one another, asked questions and exchanged comment on the group's presentation. The focus group study allows a flexible and in-depth exploration of participants' attitudes and experiences as well as reveals differences in perspective between groups of individuals [9].

For context setting, the participants were asked several questions (Table 1). The questions did not run in any sequential order, rather to provide guidelines and overviews on the topic under discussion. In order to ensure that the objectives of the focus group discussions were met, the questions were focused on the components of cyber terrorism. The questions were selected from the questionnaires which had been used for the in-depth interviews, which were done prior to the focus group discussion.

Q1.	What are the factors that make up the components (or elements) of cyber terrorism?
Q2.	What are the factors that should not be considered as component (or element) of cyber terrorism?
Q3.	From the various literatures, a conceptual framework describing the core components of cyber terrorism can be described as follows (but not limited to): Target, Motivation, Tools of Attack, Domain, Method of Action and Impact. What is your view?
Q4.	The components of cyber terrorism are bound or linked to each other to form the concept of cyber terrorism. We need to combine the components with the conjunction "AND", which means that, each of those components is necessary to constitute cyber terrorism. If one or more components are not provided, the statement would not constitute cyber terrorism. What do you think?

Table 1: Questions for the focus group discussion

2.4. Data Collection

In exploratory research, the hypotheses that obtained during the in-depth interview (qualitative data) is useful for enriching and comparing the effectiveness of the initial findings [10]. Besides, the ideas and observations are often used for later quantitative testing [10]. Prior to the focus group discussion, separate in-depth interviews were conducted to explore on the concept of cyber terrorism. Meaning to say, the focus group discussion was conducted on top of the in-depth interview to explore the concept of cyber terrorism. The group discussions were tape-recorded and the discussion points that were noted down on the flip chart were collected at the end of the session.

3. Results

3.1. Similarity in Views on the Proposed Conceptual Framework

The overall result of the focus group discussion is presented in Table 2. We included several recommendations from the groups in the findings table. Out of the 5 groups, 3 groups are fully agreed with the proposed framework. The other 2 groups partially agreed with the proposed framework with some recommendations.

Group 1 explained, "Overall, our group found that the proposed cyber terrorism framework is sufficient enough. There are a few things we would like to simplify further just in the terms only, not the content. The content is still important." Group 1 further clarified, "Regarding to the impact, I think the examples of 3 elements: mass disruption or seriously interfere critical services operation; caused fear, death or bodily injury; and severe economic loss, I think that are covered."

Group 3 indicated that, "First of all, I would to extend our appreciation to our speaker today for his very comprehensive presentation. In fact, I think that, the presentation today should be brought back to our first day, to give us a basic understanding on the components of cyber terrorism itself." However, Group 3 stressed that "Domain" and "Motivation" should not be too rigid, as they viewed that the components keep changing and have a wide interpretation.

Group 4 pointed out that, "My group agrees on the proposed framework. However, as for the motivation component, we would like to add an economical factor". One of the respondents from Group 4 stated that, "We agree on the term cyber terrorism. We feel we should stick to that. For a simple reason, it looks like international term now where all countries are using this kind of term. If we deviate, we will be different. And secondly, even if it is cyber terrorism, we only looking at the terrorism, the terrorism act itself. Just because the mean of doing is through cyber, it is known as cyber terrorism. Likewise, why we call human trafficking? Drug trafficking? The offence is trafficking but it involves another way. Likewise, I think cyber terrorism is a better word, stick to it."

With regards to statement that the components of cyber terrorism are bound or linked to each other to form the concept of cyber terrorism, all groups agreed with the statement. For example, Group 4 indicated that, "In our discussion, all of the components must be there. In the absence of any of the components, there will be no cyber terrorism. The inner components must be "AND". If you take out target, that is it, no cyber terrorism."

Further question was posed to Group 1. Question: "In order to consider cyber terrorism, we need to combine all factors such as motivation, target and impact. Do you agree with that?" Answer: "Yes, we agree."

3.2. Difference in Views on the Proposed Conceptual Framework

Group 5 agreed with most of the proposed cyber terrorism framework (Motivation, Target and Impact). However, they suggested that "Tools of Attacks", "Domain" and "Methods of Attack" should be combined as one component, "Medium". Similarly, Group 1 also suggested combining "Tools of Attack" and "Methods of Action" as one component, "Tools & Methods of Action".

Domain here refers to cyberspace, which is defined as an "interactive domain that 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“ [11]. In this particular study, "Domain" is similar to "Medium", but not "Tools of Attacks" or "Methods of Attack".

"Tools of Attacks" means computers and networks that are used as the weapons through which computers are attacked and exploited (via worms, denial-of-service, bots) [12]. While "Methods of Attack" refers to way and mean the attack was conducted, and in this particular case is referred to *unlawful* means. As mentioned by Denning [13] cyber terrorism is generally understood to mean *unlawful 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.

Group 5 also added one new component, "Perpetrator" which consists of group/individual and country. This is more or less similar with Group 2 where the group identified "Initiator" as one component of cyber terrorism. However, this can be further argued whether "Perpetrator" or "Initiator" is the right component of cyber terrorism. Rollins and Wilson [14] argue that, there are two views in defining cyber terrorism, one of it is the impact (effect-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 doer. Likewise, Tun Dr Mahathir Mohamad [15], a former Malaysia's Prime Minister said, "If we have to determine who a terrorist is and who is not then we have to base it on the act, not on the person, the group, the race or the religion. Once we agree on what constitutes an act of terror, then it would be easy to identify a terrorist."

Although Group 4 agreed with all components of the proposed cyber terrorism framework, they suggested "Attempt" as part of cyber terrorism. One of the participants stated that, "Under the criminal laws, attempt is considered as an offence. What if the terrorist does all this, preparation is done but is unsuccessful in hitting the target? Everything is well prepared but the mission is not achieved. The possibility of causing harm should also be considered as offence in cyber terrorism. Example is murder or manslaughter. The action can cause death, likewise the person conduct whatever action under terrorism, it is possible of causing massive destruction, causing some kind of injury or fear, but the perpetrator did not achieve it. Does is it mean that there is no offence? Does is it mean that he/she is not a terrorist?". One of the objectives of this study is to identify factors that make up the components (or elements) of cyber terrorism. The components then describe the concept and the meaning of cyber terrorism. In this particular case, the authors suggest that an "attempt" should not be considered as factor that make-up the components of cyber terrorism as it is already an offence under the criminal laws. Under the Malaysian law, terrorist means any person who commits, or *attempts* to commit any terrorist act [16]. It means that, if the components are met with supporting evidence, action by the perpetrator can be classified as cyber terrorism and subsequently the person may be charged under the court of laws. In fact, attempt should be part of any criminal action, including cyber terrorism.

3.3. Proposed Future Works in Related to this Study

For future works, the groups have recommended several action plans which can be considered for implementation. The first proposal is amendment to the law. Their argument is that, effective legislation on cyber terrorism is regarded high priority as the countermeasure in counter-cyber terrorism plans. Group 1 recommended that, "We would like to propose amendment to our laws (to counter threats on cyber terrorism)". This is supported by Group 2, "After this, we need to develop further on the counter action of cyber terrorism. If enforcement is not effective enough, cyber terrorism can easily happen". Group 2 further stated that, "From time to time, we need to revise the laws. If such crimes are becoming more

violent and cyber terrorism becoming so developed in times to come, perhaps there is a need specific definition on cyber terrorism."

The second proposal is the preventive measure. One of the participants said, "My views, all of these (the framework) are responsive action. What happen if we want to take preventive measure when it comes to mass disruption or national casualty? We cannot wait the attack to happen and then react. So, we need to think on preventive measure as we don't want to wait until the thing happen, we need to have measure on how to prevent this from happening."

Another participant responded that, "For response, a lot of things need to be considered. For root causes, there is mention the origin of attack. Then, there is non-state issue that gets involve. Also, there are ways and means toward cyber terrorism." In response to this issue, the moderator stated that, "That discussion will be in a different forum. The objective of this research is to provide baseline in understanding the components that make cyber terrorism. After this, we need to come out with response and action plan on how we are going to handle this issue."

The third proposal is the need to have a proper definition on the concept of cyber terrorism. Group 3 stated that, "I think it is crucial for us to have an understanding on the overall definition on the concept of cyber terrorism first before we can approach to the component. There are a few factors that we have to consider in approaching the questions: the perpetrator, the policy of various ministries, the enforcement, and the judicial authority. We think that cyber terrorism is quite similar with other crime. There are starting points and there are ending points. The starting point could be the action itself and the ending points could be the prosecution in court."

Group 3 further explained that, "We would like to admit that there is a need to have a mutual understanding between countries because cyber terrorism is a trans-boundary issue. It is very crucial for each country to have basic understanding or common understanding on what constitute cyber terrorism." Group 3 continued that, "I would like to take example on Convention on Cyber Crimes. In fact in this convention, we do not have any specific definition or understanding what cyber crimes is, but it provides what constitute cyber crimes. Perhaps in one day, we could have convention on cyber terrorism that would provide understanding to each country or at least common understanding on how or what constitute cyber terrorism."

3.4. Research Limitation

This study has several limitations. Therefore, some of the imperfections may lead to the unreliability of the data collected [10]. First, the constraint of this study is that majority of the participants were representatives from the defense & security and the government sectors of the Critical National Information Infrastructure (CNII). In Malaysia, there are 10 CNII sectors: water, banking & finance, defense & security, transportation, information & communication, government, emergency services, food & agriculture, energy and health. Therefore, the participants of the focus group discussion did not represent the CNII sectors as a whole. The second constraint is that from observation, not all participants were participating in the discussion. As a result, not all the participants' viewpoints were heard and well noted.

4. Conclusion

Cyber terrorism is a serious matter at the national and international level, and this is demonstrated through the conduct of this workshop. The present study supports our initial research [17] that the cyber terrorism conceptual framework constitutes the following components: target, motivation, tools of attack, domain, methods of attack and impact. This is evident from the overall result whereby 3 out of 5 groups are fully agreed with the proposed framework, while the other 2 groups agreed with the proposed framework with some recommendations. Although there are differences in opinions on some of the components, but their views are not that critical and can be further justified. These results suggest that the proposed cyber terrorism framework is acceptable.

Further research can be conducted to test or verify the conceptual framework. The outcome can be achieved by using quantitative method to quantify them and then applied statistical method to test the dynamic relationship of components of the cyber terrorism framework. Additionally, future research from this study could be used to help better in defining and adopting the concept of cyber terrorism in a holistic manner.

5. Acknowledgements

The authors would like to thank Sazali Sukardi and Zaleha Abd Rahim of CyberSecurity Malaysia who provided valuable input to this paper. The authors also would like to thank the Center for Advanced Computing Technology, Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka (UTeM) that provided research grant for this project.

REFERENCES

[1] J. Matusitz, "Social Network Theory: A Comparative Analysis of the Jewish Revolt in Antiquity and the Cyber Terrorism Incident over Kosovo," *Information Security Journal: A Global Perspective*, vol. 20, no. 1, pp. 34-44, Feb. 2011.

[2] M. Dogrul, A. Aslan, and E. Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," in *2011 3rd International Conference on Cyber Conflict, Tallinn, Estonia, 7-10 June*, 2011, pp. 1-15.

[3] M. Conway, "Against Cyberterrorism," *Communications of the ACM*, vol. 54, no. 2, p. 26, Feb. 2011. doi:10.1145/1897816.1897829

[4] 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," in *IEEE Sixth International Conference on Information Assurance & Security, Atlanta, GA, 23-25 Aug*, 2010, pp. 21-27.

[5] P. A. H. Williams, "Information Warfare: Time for a Redefinition," in *Proceedings of the 11th Australian Information Warfare & Security Conference, Perth Western, Australia, 30 Nov - 2 Dec*, 2010, pp. 37-44.

[6] D. Ho, "The Focus Group Interview: Rising to the Challenge in Qualitative Research," *Australian Review of Applied Linguistics*, vol. 29, no. 1, pp. 1-19, 2006.

[7] J. Bray, N. Johns, and D. Kilburn, "An Exploratory Study into the Factors Impeding Ethical Consumption," *Journal of Business Ethics*, vol. 98, no. 4, pp. 597-608, 2011. doi:10.1007/s10551-010-0640-9

[8] Y. Kamarulzaman, "A Focus Group Study of Consumer Motivations for e- Shopping : UK versus Malaysia," *African Journal of Business Management*, vol. 5, no. 16, pp. 6778-6784, 2011.

[9] F. Saleem, M. Hassali, A. Shafie, S. Bashir, and M. Atif, "Perceptions of Disease State Management Among Pakistani Hypertensive Patients : Findings from a Focus Group Discussion," *Tropical Journal of Pharmaceutical Research*, vol. 10, no. 6, pp. 833-840, 2011. doi: 10.4314/tjpr.v10i6.18

[10] D. R. Cooper and P. S. Schindler, *Business Research Method*. NY: McGraw-Hill Companies, Inc, 2008.

[11] UK Cabinet Office, "The UK Cyber Security Strategy - Protecting and Promoting the UK in a Digital World," 2011. [Online]. Available: http://www.cabinetoffice.gov.uk/sites/default/files/resources/The UK Cyber Security Strategy- web ver.pdf. [Accessed: 19-Mar-2012].

[12] 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.

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

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

[15] M. Mohammad, "The Need to Identify Terrorists and Remove the Causes of Terrorism," in *Terrorism and the Real Issues*, H. Makaruddin, Ed. Subang Jaya, Selangor: Pelanduk Publications (M) Sdn Bhd, 2003, pp. 29-40.

[16] ACT 574 Penal Code, "Chapter VIA – Offences Relating to Terrorism. Section 130B (1) - (5)." Zul Rafique & Partner Report, 1997.

[17] R. Ahmad and Z. Yunos, "A Dynamic Cyber Terrorism Framework," *International Journal of Computer Science and Information Security*, vol. 10, no. 2, pp. 149-158, 2012.

Proposed Components	Group 1		Group 2		Group 3		Group 4		Group 5	
Target	Target	Critical National Information Infrastructure computer system Critical Infrastructure	Target	CNII Civil population Critical Infrastructure	Target	Critical National Information Infrastructure computer system Critical Infrastructure Civil population	Target	Critical National Information Infrastructure computer system Critical Infrastructure Civil population	Target	Government Country Corporation CNII
Motivation	Motivation	Political Ideological Social Economic	Initiator 100% personal or group with motivation	The person or group must have the intention to commit the act of cyber terrorism (Refer to Note 3)	Motivation	Political Ideological Social Economic	Motivation	Political Ideological Social Economic	Motivation	Political Ideological Social Economic
Tools of Attack	Tools & Methods of Action	Network warfare Psychological operation The method of action is through unlawful means	Medium	Computer network	Tools of Attack	Network warfare Psychological operation	Tools of Attack	Network warfare Psychological operation	Medium (Tools & Methods) (Refer to Note 5)	Techniques (e.g. recruitment) Domain (e.g. cyberspace)
Domain	Refer to Note 1		Domain	Cyberspace Physical world	Domain	Cyberspace	Domain	Cyberspace		
Methods of Attack	Refer to Note 2		Method	Unlawful means	Methods of Attack	Unlawful means	Methods of Attack	Unlawful means		

Impact	Impact	The target must be impactful	Impact	Mass disruption lead to • destruction • cause-fear, death, instability of country • Severe economic loss • Doctrinazation	Impact	• Mass disruption or seriously interfere critical services operation • Cause fear, death or bodily injury • Severe economic loss	Impact	• Mass disruption or seriously interfere critical services operation • Cause fear, death or bodily injury • Severe economic loss	Impact	Physical Non Physical National • Security • Economic • Image • Government to function • Health and safety
							Attempt	(Refer to Note 4)	Perpetrator	Group/ Individual Country

Table 2: Results of the Focus Group Discussion

Note:

1. Group 1 excludes "Domain" as the factor which is by default is part of cyber terrorism.

2. Group 1 combines "Tools of Attack" and "Methods of Action" as one component, "Tools & Methods of Action".

3. Group 2 starts the concept of cyber terrorism with initiator, where the person or group has the intention to commit the act of cyber terrorism. The person or group also must have the motivation to do the act of cyber terrorism.

4. Group 4 suggests "Attempt" should be considered as part of cyber terrorism.

5. Group 5 combines "Tools of Attack", "Domain" and "Methods of Action" as one component, "Medium".

Journal of Information Security, **2012, *, ****
doi:10.4236/jis.2012.***** Published Online ** 2012 (http://www.scirp.org/journal/jis)

