CONSTRUCTING CYBER TERRORISM TRACE PATTERN

NURHASHIKIN BINTI MOHD SALLEH

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2014

Acknowledgement

Bismillahirrahmanirrahim

Alhamdulillah, Thanks to Allah SWT, whom with His willing give me the opportunity to complete this Final Year Project which is title Constructing Cyber Terrorism Trace Pattern. This final year project report was prepared for Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka (UTeM), basically for student in final year to complete the undergraduate program that leads to the degree of Bachelor of Computer Science.

First of all, I would like to express my very great appreciation to Dr. Siti Rahayu, a lecturer at FTMK, UTeM and also assign as my supervisor who had guide and give useful critiques for this project work. I also would like to thanks to Dr. Siti Rahayu for the advice and assistance in keeping my progress on schedule.

Deepest thanks and appreciation to my parents, family, and friends for their cooperation, encouragement, and full of support for the report completion, from the beginning till the end.

Abstract

Nowadays, cyber terrorism has become serious issue and the number of crime has been increased. Cyber terrorism can be defined as the use of Internet to launch any attacks in terrorist activities such as against computer system, computer program, or data which result on damage cyber space infrastructure itself or some other targets. It can be both internal and external networks. Furthermore, the difficulties to trace the cyber terrorism activities become a very serious problem. In addition, there is no trace pattern is available to describe these activities. Thus, this project is proposed to overcome the problem by identifying about the cyber terrorism and digital forensics, analysing the cyber terrorism activities, and to formulate the cyber terrorism trace pattern. In this project, the cyber terrorism activities are identified based on the analysis of the cyber terrorist websites. Three main websites are analysed based on keyword and URL, and the findings are mapped to the components of the cyber terrorism. This mapping is representing the trace pattern. By generating this trace pattern, it will facilitate forensic investigators to identify the activities or the behaviours of the cyber terrorism and determine the cyber terrorism's origin.

Abstrak

Pada masa kini, keganasan siber telah menjadi isu yang serius dan bilangan jenayah dalam keganasan ini semakin meningkat. Keganasan siber bermaksud penggunaan Internet untuk melancarkan apa-apa jenis serangan dalam akitiviti pengganas seperti terhadap sistem komputer, program komputer atau data yang menyebabkan kerosakan pada infrastruktur siber ruang itu sendiri atau beberapa sasaran yang lain. Kegansan siber boleh melibatkan sama ada rangkaian dalaman dan luaran. Masalah utama adalah kesukaran untuk mengesan aktiviti keganasan siber yang makin serius. Disamping itu, tiada *trace pattern* untuk menggambarkan aktiviti-aktiviti ini. Oleh itu, melalui projek ini, ia dapat mengatasi masalah ini dengan memahami forensik digital dan, mengenal pasti, menganalisis dan menjana corak jejak aktiviti keganasan siber. Tiga laman web telah dianalisis berdasarkan pada kata kunci dan juga URL, hasilnya akan dipetakan dengan komponen keganasan siber. Dengan menghasilkan *trace pattern*, ia akan memudahkan penyiasat forensik dalam mengenal pasti aktiviti-aktiviti atau tingkah laku keganasan siber serta dapat menentukan asal berlakunya keganasan ini.

Dedication

Dedicated to all my family:
Thank you for all you love
May Allah bless us.

TABLE OF CONTENTS

CHAPTER 3 METHODOLOGY

CHAPTER 4 DESIGN AND IMPLEMENTATION

CHAPTER 5 TESTING AND ANALYSIS

CHAPTER 6 CONCLUSION

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Background Study

Cyberspace was first introduced in science fiction and cinema since in the 1980s. It was adopted by computer professionals and became a household term in the 1990s. In terms of definition, cyberspace is the electronic medium of computer networks, in which online communication takes place (American Heritage, 2010). The term is used to refer to objects and identities that exist largely within the communication network it. Cyberspace is which online relationships and alternative forms of online identify were enacted. It does not have a standard or objective definition such other computer terms. It can be clarified as a virtual of computers.

Nowadays, cyber terrorism has become serious issue and increase sophisticated. It is because the threat of cyber terrorism and the misuse of the Internet for terrorist purposes are particularly alarming because our society is dependent on computer systems and the Internet. It is reported that the number of crimes involving computers and internet has grown up (Selamat, 2011).

Table1.1: The comparison of number of incidents between January-Jun 2012 and January-Jun 2013 (Cyber Security Malaysia, 2013).

Incident	**January – June 2012**	**January – June 2013**	**% increase (decrease)**
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious Codes	353	442	25
Cyber harassment	173	233	35
Content related	10	42	320
Intrusion attempts	55	24	(56)
Denial of service	12	10	(17)
Vulnerability report	45	11	(76)
TOTAL	**5,581**	**5,592**	

Based on the Table 1.1, it shows that from January to June 2013, a total of 5,592 cyber security incidents compared to 5,581 incidents reported in first half of 2012. Fraud is the most-reported incidents followed by intrusion, spam, malicious code, cyber harassment, content related, intrusion attempts, Denial of Service (DoS), and vulnerability reports.

In term of cyber terrorism definition, most government in the world cannot agree on one single definition for terrorism. The part of the problem is in defining cyber terrorism as there are broadly different definitions as to what actually constitutes cyber terrorism (Yunos, 2009). Cyber terrorism is the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses, hacking (Ali Fahad, 2012). It also can be defined as the intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives.

Cyber terrorism is divided into two primary elements which are cyberspace and terrorism. Terrorism in cyberspace can take many different forms which are physical destruction of machinery crucial to an IT infrastructure, remote interference of computer networks, disruption of government networks, or even disturbance of societal networks such as financial networks or mass media (Yunos, 2013). Objectives of cyber terrorism might be political or ideological. The potential targets that involve might be direct or indirect, computer. The terrorist could use the stolen identity to mask their work, carrying out certain operations under their target's name, not their own. Besides, the problem that will some individuals or an organization always face is about the protection of data and cyber terrorists are very easily to pass through into the network. In terms of computer attack and cyber terrorism, it focus on how possible cyber terrorism using computer network attack or cyber attack. Terrorism uses certain tools and methods to unleash this new age terrorism. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, have websites and hate emails, and attack on sensitive computer networks (Alisha, 2010).

By analyse the cyber terrorism behaviour; cyber terrorism can be identified based on data found in trace pattern analysis. Trace pattern is defined as a regular way of process discovering the origin or starting point of a scenario that has happened (Selamat et. al, 2011). It is very difficult to trace the cyber terrorists because there are no specific trace patterns about it. By construct the trace pattern, it will help the investigator in finding evidence about cyber terrorism. By doing the tracing technique, it will able to discover the traces left in digital devices. Trace pattern will provide the clear view on how the cyber terrorism occurs.

1.2 Problem Statement

The number of crime in cyber terrorism has been increase. It is too difficult to trace the cyber terrorism because there is no trace pattern about it. By using the tracing technique, it can help the investigator to discover the cyber terrorism. The trace pattern will provide the evidence how the cyber terrorism occur based on the conceptual framework.

Table 1.2: Problem Statement

No	Project Problem
PP1	Difficult to trace the cyber terrorism because there is no trace pattern to provide the evidence.

1.3 Project Questions

Based on the problem statements, three project questions (PQ) are constructed as shown in Table 1.3.

Table 1.3: Project Question

PP	PQ	Project Question (PQ)
PP1	PQ1	What is the analysis technique can do to overcome the cyber terrorism?
	PQ2	How could we identify the cyber terrorism?
	PQ3	How could we help investigator to trace the cyber terrorism?

1.4 Project Objective

In order to solve the problem identified as in Section 1.2, three project objectives (PO) are derived as shown in Table 1.4.

Table 1.4: Project Objective

PP	PQ	PO	Project Objective (PO)
PP1	PQ1	PO1	To study and identify cyber terrorism activities.
	PQ2	PO2	To analyze the cyber terrorism behavior.
	PQ3	PO3	To formulate the cyber terrorism trace pattern.

1.5 Project Scope

The scope for this project are:

1. This project analyse the cyber terrorism behavior based on the components of cyber terrorism that consists of actors, motivation, tools, method, target, and impact.
2. By knowing the cyber terrorism behavior, create a tracing technique to discover the trace pattern of the cyber terrorism.
3. The data used in this project is limited to the potential cyber terrorist websites.

1.6 Expected Output

The expectation by the end of this project is to contribute and provide a better trace pattern of cyber terrorism, which may lead to the effective strategy to counter cyber terrorists and gain more theoretical knowledge practical of cyber terrorism.

1.7 Report Organization

This project consist of six chapter which are introduction, literature review, methodology, design and implementation, testing and analysis, and conclusion. The report organization will be organize as the Figure 1.1.

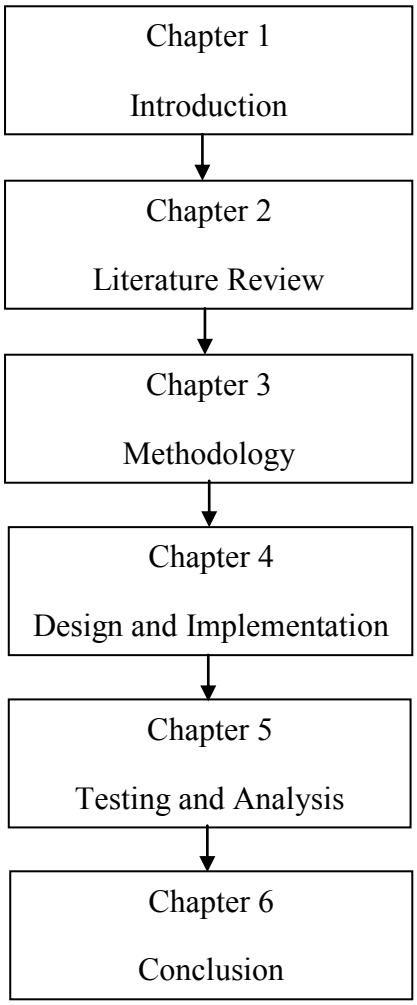

Figure 1.1: Flow of report organization.

Figure 1.1 shows the flow of report organization for this project. The explanation for each chapter will be elaborate below.

Chapter One: Introduction

This chapter explained about the definition, background, problem statement, objective, scope and expected output related to the cyber terrorism.

Chapter Two: Literature review

This chapter explained about cyber terrorism, tracing technique, and trace pattern. It will help to more understanding about what is the constructing cyber terrorism trace pattern.

Chapter Three: Methodology

This chapter provide a decision of the method or what analysis techniques to be used for experimental part. With the certain analysis technique, it helps to know about the cyber terrorism behaviour. It also will involve about the trace pattern of cyber terrorism based on the framework.

Chapter Four: Design and Implementation

The design of tracing technique is describe in details on how it works carried out. The sample of result and output will be providing.

Chapter Five: Testing and analysis

On the testing and analysis part, it explains about the method use and procedure on how to test and analyse the experiment. After the tracing technique was obtained, we compare the result with the trace pattern of cyber terrorism.

Chapter Six: Conclusion

This chapter compile the entire chapter in a final documentation and state the contribution that able to provide for future works.

1.8 Summary

Cyber terrorism is a serious matter at the national and international level. There is a broad range of differing opinions as to what actually constitutes cyber terrorism. As long as the term continues to be used without a proper understanding of the nature of cyber terrorism threats, the misinformation and hype associated with it will remain. There are reported that cyber terrorist use the Internet as a medium for hostile activities. It is imperative that an explanatory study of cyber terrorism activities on the Internet be conducted. In the next chapter, it will explain the details about the related work of constructing cyber terrorism trace pattern.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

The previous chapter has been discussed the problem statement, objectives and the scope of this project. In this chapter, it will explain about the related topics as shown in Figure 2.1. The literature is based on the several resources such as journal articles, proceeding, technical reports and white paper.

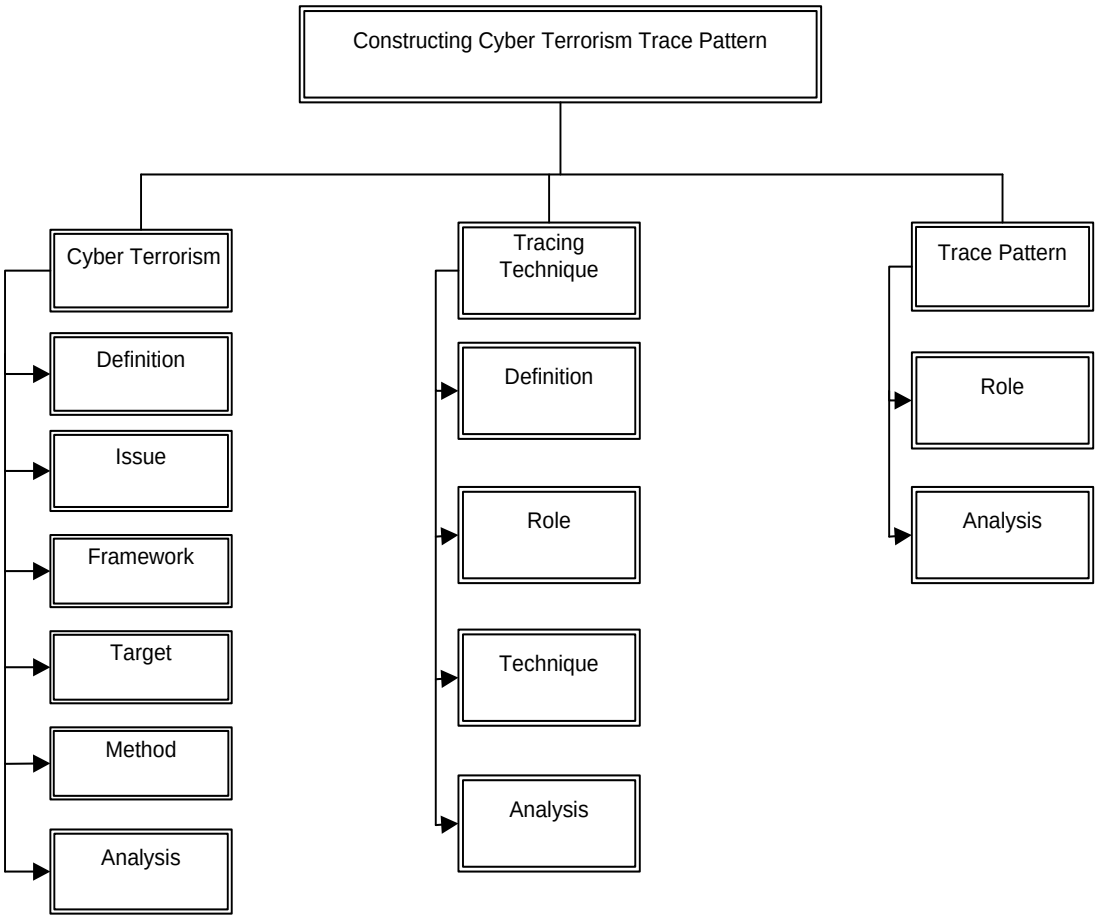

Figure 2.1: Framework of literature review

Figure 2.1 shows the topics that will elaborate and analyse in this chapter. Three main topics are selected namely cyber terrorism, tracing technique and trace pattern.

2.2 Cyber Terrorism

In this section, the definition, problem related, framework, targets, methods, tools, and trace of cyber terrorism are elaborated and analysed.

2.2.1 Definition of Cyber Terrorism

The term cyber terrorism is becoming increasingly common nowadays, yet a solid definition for it and what it constitutes is subjective and covers a wide area. There are several definitions by different authors on what is actually means by cyber terrorism as shown in Table 2.1.

Table 2.1: Definition of Cyber terrorism.

Definition	Author
Cyber terrorism is the convergence of terrorism and cyberspace. It is generally known 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, 2000
The unlawful use of force or violence, committed by a groups of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.	FBI, 2002.
Cyber terrorism can be defined as electronic attacks from cyber space from both the internal and external networks, particularly from the Internet that emanate from various terrorist sources with different set motivations and are directed at particular targets.	Jalil, 2003
A cyber attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal.	NATO, 2008
Cyber terrorism refers to attacking computers, networks, and other electronic technologies capabilities to either damage the cyberspace infrastructure itself or to damage some other target, motivated by terrorism.	ISC, 2009
An act or threat of action within or beyond Malaysia, among others, “designed or intended to disrupt or seriously interfere with any computer systems or the provision of any services directly related to communications infrastructure, banking or financial services, utilities, transportation, or other essential infrastructure.	Yunos, 2009
Cyber terrorism is sometimes referred to as electronic terrorism or information war.	Rouse, 2010
Cyber terrorism is the premeditated, politically motivated attacks against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents.	Curran, 2011
The premeditated, politically-motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.	W.Singer, 2012
“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”.	A.Lewis, 2013
“Exploitation of electronic vulnerabilities by terrorist groups in pursuit of their political aims”.	Cruz, 2013

Table 2.1 shows the several definitions by different authors; we can conclude that there are differing opinions as to what actually is cyber terrorism. This project defines cyber terrorism as the use of Internet to launch any attacks in terrorist activities such as against computer system, computer program, or data which result on damage cyber space infrastructure itself or some other target. It can be both internal and external networks.

2.2.2 Issue on Cyber Terrorism

Nowadays, the issue on the cyber terrorism has become serious due to the increase of number cases on cyber crime. As we know that with Internet, it can provide connection between computers, sharing any information or news, and be able to communicate with people even do it far away from us. Internet has become one of the most important tools because cyber terrorists will use Internet or cyber space as a medium to launch any attack on their target.

Cyber terrorists usually attacks by distributed denial of service attacks, hate websites and hate emails, and attacks on sensitive computer networks (Alisha, 2010). Cyber terrorists may also use Internet as the medium for hacking, spreading negative propaganda, and promoting extreme activities. They also includes warfare attacks against a nation's state and forcing ICT infrastructure and assets to be fail or destroy. Cyber terrorists use to obtain inside access to networks and systems. These types of attack actually are more dangerous because it is extremely difficult to detect or trace them.

It is very irrelevant in terms of preventing cyber terrorism from carrying out any attacks. The cyber terrorism has been raised and the world has still not had any specific trace pattern to detect the cyber terrorism. With the trace pattern, we are able to trace cyber terrorism because it will give and let us to get an evidence of who are actually involves in cyber terrorism. But since this is happen, cyber terrorism continues to rise, and terrorists increase in a cyber space (Noor, 2011) and also reported by Cyber Security Malaysia (2013) as shown in Table 2.2.

Table 2.2: 10 riskiest countries (CyberSecurity Malaysia, 2013).

No.	Country	Percentage of cyber crime reported (%)
1.	Indonesia	23.54
2.	China	21.26
3.	Thailand	20.78
4.	Philippines	19.81
5.	Malaysia	17.44
6.	India	15.88
7.	Mexico	15.66
8.	UAE	13.67
9.	Taiwan	12.66
10.	Hong Kong	11.47

Figure 2.2 shows Malaysia is the sixth most vulnerable country in the world to cyber crime, in the form of malware attacks through the computer or smart phone. From the table, Malaysia have highest riskiest compared to India, Mexico, UAE, Taiwan, and Hong Kong.

2.2.3 Framework of Cyber Terrorism

There are several of frameworks of cyber terrorism proposed since today. However, the most familiar are the frameworks proposed by Heickero (2007), Gordon and Ford (2002), and Yunus (2012).

a-Heickero (Actor-target-effect Chain)

Heickero introduced his framework known as Actor-target-effect Chain in order to know about the cyber terrorism behaviour as shown in Figure 2.2.

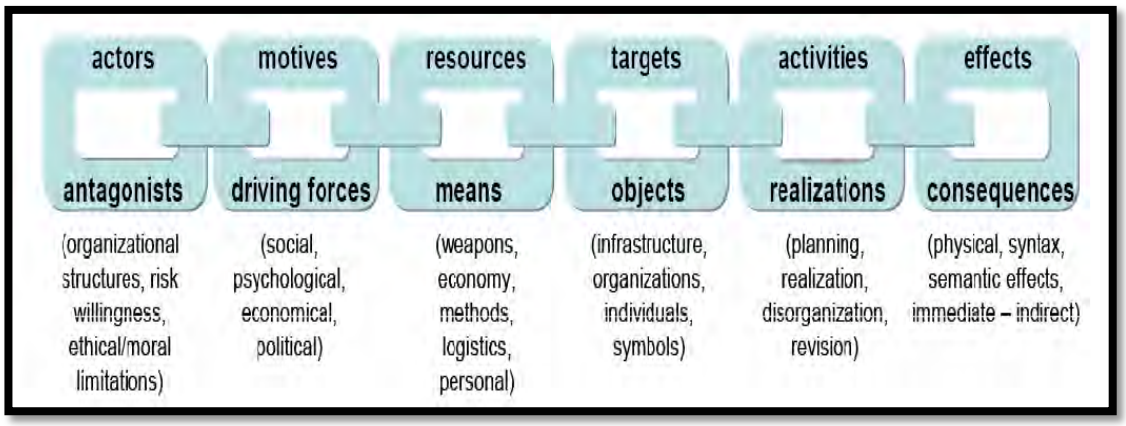

Figure 2.2: Cyber terrorism framework (Heickero, 2007).

Figure 2.2 shows the details about the cyber terrorism framework which are consist of actors, motives, resources, targets, activities, and effects. Actor might be organizational structures, risk willingness, and ethical or moral limitations. The motives of cyber terrorism can be social, psychological, economical, and political. The cyber terrorist resources are weapon, economy, methods, logistics, or personal. The cyber terrorism targets might be infrastructure, realization, disorganization, or revision. The effects of cyber terrorism might be in terms of physical, syntax, or sematic attacks. It could be immediate or indirect effects.

b-Gordon and Ford

Gordon introduced his framework in order to know the cyber terrorism behaviour as shown in Figure 2.3.

Components	LTTE (Example)	Description
Perpetrator	Group/Individual	In cyber context, virtual interactions can lead to anonymity.
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 virtual environment includes psychological effects, possible behavior modification and physical trauma.
Tool	Kidnapping/ Harassment/ Propaganda/Education	Terrorist use the computer as tool. Facilitating identity theft, computer viruses, hacking are examples 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 strengthening of the 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 the real-world terrorism.

LTTE = Liberation Tigers of Tamil Eelam (Sri Langka)

Figure 2.3: Cyber terrorism framework (Gordon, 2002).

Figure 2.3 shows the details about the cyber terrorism framework which consists of perpetrator, place, action, tool, target, affiliation, and motivation. Gordon was state that perpetrator might be group or individual. Worldwide is a place for the cyber terrorism activities. This activity does not have to occur in a particular location. The Internet has introduced globalization of the environment. Action can be any threats, violence, recruitment, education, and strategies. Tool refers to kidnapping, harassment, propaganda, and education. The computer is use as terrorist's tools to launch any attack such as computer viruses and hacking. Cyber