Discovering Cyber Terrorism Using Trace Pattern

Nurhashikin Mohd Salleh, Siti Rahayu Selamat, Robiah Yusof, and Shahrin Sahib
(Corresponding author: Nurhashikin Mohd Salleh)

Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka (UTeM)
(Email: nurhashikinbtmohdsalleh92@gmail.com)
(Received Aug. 13, 2015; revised and accepted Nov. 27, 2015)

Abstract

Nowadays, as the Internet user increased, the number of cyber threats is also increased. Internet has provided a medium for criminal to do the crime and become the target for cyber terrorist to spread their negative propaganda, and promote extreme activities. One of the crimes is cyber terrorism. Cyber terrorism became more sophisticated and it difficult to discover its activities. Hence, this paper proposes tracing technique for discovering cyber terrorism based on trace pattern. Trace pattern will represent the behavior and activities of cyber terrorism. Cyber terrorist's website is used as the datasets. Using tracing technique, cyber terrorist's activities are identified by extraction and classifying the traces to the keyword that is usually used by the terrorist. Then, the traces will be linked with the cyber terrorism components in order to identify the relationship between them. Using trace pattern, the verification process will be conducted to verify the traces in order to identify the cyber terrorism activities and potential terrorist. This trace pattern can be used in facilitating the forensic investigation process in discovering cyber terrorism activities.

Keywords: Critical national information infrastructure (CNII), cyber terrorism, trace pattern, tracing technique

1 Introduction

Cyber terrorism became more sophisticated and it difficult to discover its activities. Since, Internet provides the platform to the user, cyber terrorist could take advantage of the Internet and other IT infrastructure as their target to do terrorist activities. Cyber terrorists may use Internet as the medium for hacking, spreading negative propaganda, and promoting extreme activities. They may also use Internet for the purpose of inter-group communication and inter-networked grouping [15] and create public relations [8] to spread their propaganda and promote their extremist activities. It became more extreme when Critical National Information Infrastructure (CNII) became an attractive target to the cyber terrorist. Cyber terrorism might be attack against information, computer system, computer programs, or data which result in violence [1]. As the result, it could leave the nation with difficult conditions due to the disruption of critical services. It became more difficult to discover its activities.

Therefore, the main objective of this paper is to propose a tracing technique to discover cyber terrorism using trace pattern in facilitating the investigator on identifying cyber terrorist activities and provide the evidence. The traces of the crime are discovered by using tracing technique in order to formulate trace pattern. The potential terrorist website is used.

2 Related Work

2.1 Overview of Cyber Terrorism

Cyber terrorism is the use of internet to launch any terrorist attacks or threats through computer system, computer program, or data which result on damage critical infrastructure or at least cause harm and generate fear to other target. Cyber terrorism continues to rise, and terrorists increase in a cyber space [2]. Terrorists use the Internet as a tool to coordinate action, intra-group communications, fund-raising and public relations [7, 8, 9]. For example, terrorist organize websites for hacking, spreading negative propaganda, and promoting extreme activities. It is very difficult to discover cyber terrorism from carrying out their activities since there is no specific trace pattern [11]. Based on [14], there are at least six components required to describe cyber terrorism activities as shown in Figure 1.

Figure 1 shows the cyber terrorism components consists of actor, motivation, tools, target, method, and impact. Actor can be described as a participant in any action or process. It refers to any person, group, or organization. Motivation refers to any reason of acting or behavior in a particular way. It can be any concept, ideology, or revenge. Tool is a device used to carry out a particular action like weapon or network warfare. Target refers to person, organization, government, society, objects, or

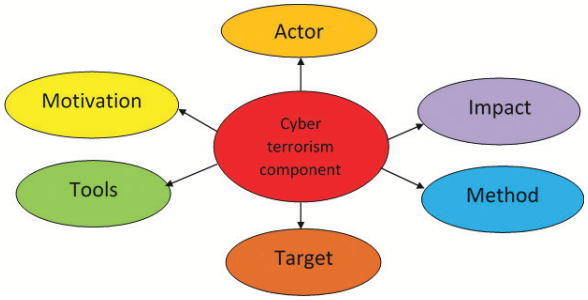

Figure 1: Cyber terrorism components

place that selected as the aim of an attack. Method is a particular procedure for accomplishing or approaching something. Method refers to the any action or operation that relate to the cyber terrorism. Impact defines as a marked effect or influence, and can be classified into four categories namely physical, psychology, social, and economic. Every violence and threats that has been done to the target will be considered as impact [3, 4, 5, 13]. Cyber terrorism components can be represents in terms of "union" statements equation as in Equation (1).

$$CcT = c_1 \cup c_2 \cup c_3 \cup c_4 \cup c_5 \cup c_6 \quad (1)$$

Where, CcT = cyber terrorism components, c_1 = actor components, c_2 = motivation components, c_3 = tools components, c_4 = target components, c_5 = method components, and c_6 = impact components. Equation (1) shows the components of cyber terrorism either actor, motivation, tools, target, method, or impact components.

2.2 Tracing Technique

Tracing technique can be defined as a process of tracing the data based on its attribute [11]. In this research, tracing technique is used to help the forensic investigator to trace any cyber terrorism activities based on its components. By using this technique, behavior of cyber terrorism can be identified.

Two main tracing techniques used namely word searching technique and web address searching techniques. Word searching technique is use to trace the data. This technique can be use by using symbols to search for alternative word endings, combining the concepts in a search statement, searching for phrases, and performing more specific searches. By using this technique, the project can be identified what the keyword and its type. Keyword refer to any word exists in website. The examples of these types are people, organization, group, individual, target place, place, action, mode of action, tools, and motivation [6].

2.3 Trace Pattern

Trace pattern can be defined as the way to discover the origin or starting point of a scenario that has happened [10]. It plays an important role by representing the behavior and activities of cyber terrorism. With trace pattern, it will assist forensic investigators on tracing the traces left at the crime scenes and discovering cyber terrorism activities. Trace pattern will help the forensic investigator to find any evidence about the cyber terrorism because any activities of cyber terrorists or attacker can be identified based on the traces data found in the attack pattern which represent in the form of trace pattern. In this situation, trace pattern will help to determine how cyber terrorism could be happened [12].

In this research, the traces can be any keywords appeared in the terrorist website. Therefore, in order to get a trace pattern, keywords of these traces is identifying based on its meaning and its relation to cyber terrorism components. After that, the traces will be confirming its relation.

3 Methodology

There are three phases involved in the tracing technique for discovering cyber terrorism activities based on the trace pattern. The explanations of these phases are explained below.

Phase I: Traces extraction and classification
The tracing technique namely word searching technique and web searching techniques are used to extract the traces. In order to formulate trace pattern, these technique are used to discover the traces. Traces are referred to any keyword used by the terrorist. The keyword can be word or URL. In this phase, the traces are classified into types of keyword as described as in Table 1.

Table 1 shows the types of keyword which are person, group, organization, concept, ideology, critical infrastructure, action, operation, physical, psychological, emotional, and economic. The process of classifying the keyword traced to the types of keyword based on the meaning of the word. For example, the name of the person is one of the words that referred to an individual and based on Table 1, this trace is classified as person.

Phase II: Traces cross-referencing and linking
The main purpose of this process in this phase is obtaining complete traces of cyber terrorism activities. Therefore, after the traces classified in the Phase I, the traces will be linked in order to identify the relationship between them. The cross-referencing is also carried out to identify the relationship between the traces and the cyber terrorism components.

Phase III: Traces verification
In this phase, the traces that are linked in the Phase II will be verified to identify the cyber terrorism activities and indirectly identifying the potential terrorist or the suspect. The verification is used the trace pattern. Trace pattern will describe about the types of keyword and the

Table 1: Types of keyword

Types of keyword	Description
Person	An individual
Group	A number of people or things that are located, gathered, or classed together.
Organization	An organized group of people with a particular purpose, such as a business or government department.
Concept	An idea of something is and how it works.
Ideology	A system of ideas and ideals, especially one which forms the basis of economic or political theory and policy. It also known as the set of beliefs characteristic of a social group or individual
Critical infrastructure	The backbone of nation's economy, security and health. It also known as the assets, systems, and networks, whether physical or virtual.
Action	The fact or process of doing something, typically to achieve an aim.
Operation	It known as any job or tasks consisting of one or more elements or subtasks.
Physical	Involve body contact.
Psychological	Relate to the mental and emotional of a person.

cyber terrorism components involved. For every types of keyword identified in the website are mapped with the cyber terrorism components. The components could be actor, motivation, tools, method, target, and impact. The mapping process is shown in Figure 2.

Figure 2 shows cyber terrorism trace pattern that used in this research as the tracing technique to discover the traces and identify the cyber terrorism. Trace pattern describes the activities of terrorist on how terrorist attack the target and others. This process can be represents in terms of if then statements equation as in Equation (2).

$$IF(a_n == TK_n)THEN(TK_n == CcT_n) \quad (2)$$

Where, a = attributes, TK = types of keyword, CcT = cyber terrorism components, and n = number. Equation (2) is used to verified the traces and discover cyber terrorism activities using trace pattern.

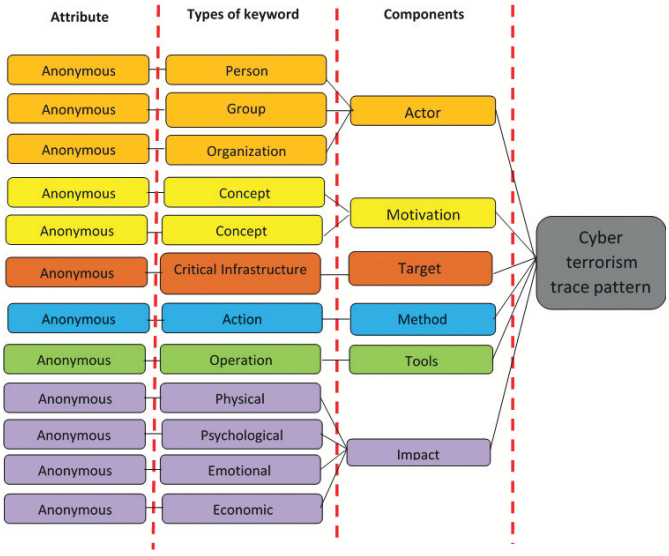

Figure 2: Cyber terrorism trace pattern

4 Proposed Tracing Technique for Discovering Cyber Terrorism Based on Trace Pattern

From analysis and findings, by using trace pattern it able to discover cyber terrorism activities. We proposed tracing technique for discovering cyber terrorism based on the trace pattern as shown in Algorithm 1, Algorithm 2 and Algorithm 3.

4.1 Extraction and Classification

In this process, the traces of the cyber terrorism are extracted and classified into the types of keyword. The algorithm of the extraction and classification process is depicted in Algorithm 1.

Algorithm 1 Extraction and classification data algorithm

```
Start
Read website
Identify traces
if traces == word then
    traces = types of keyword
else if traces == URL then
    traces = types of website
else
    Identify the traces again
end if
End
```

Algorithm 1 shows the pseudo code of extraction and classification data. In this algorithm, the function will read website and identify the traces whether it is word or URL. If the traces equal to word, then traces will be types of keyword. Meanwhile, if traces equal to URL,

then traces will be types of website. If not, the function will be identifying the traces again.

4.2 Cross-referencing and Linking

The traces found in the extraction and classification process are then linked. The process is shown in Algorithm 2.

Algorithm 2 Extraction and classification data algorithm

```
Start
Read website
Identify attribute
if (types of keyword == characteristics) AND characteristics == components) then
    Map the keyword with components
else if (types of website == characteristics) AND (characteristics == components) then
    Map the keyword with components
else
    Identify the attribute again
end if
End
```

Algorithm 2 shows the pseudo code of cross-referencing and linking process. In this algorithm, the function will be read website and identify the attribute whether it is types of keyword or types of website. If the types of keyword is similar to the characteristics and characteristic is equal to components of cyber terrorism, the cross-referencing is then done to the types of keyword and cyber terrorism components. Then, these traces are linked to identify the relationship between them. If the type of website is same to the characteristics and characteristic is equal to components of cyber terrorism, then map the types with its components. If not, the function will be identifying the attribute again.

4.3 Cyber Terrorism Identification

After all relevance traces extracted, classified and linked, there is a need to verify the traces in order to identify the cyber terrorism activities by comparing to the cyber terrorism pattern as described in previous section. The algorithm of identification process is depicted in Algorithm 3.

Algorithm 3 depicts the pseudo code of cyber terrorism identification process. If the type of website is same to the characteristics and characteristic is equal to components of cyber terrorism, then map the types with its components. If not, the function will be identifying the attribute again. Then, after finished tracing the traces, the traces are then compared with the trace pattern in order to verified the cyber terrorism activities and identifying the potential terrorist.

Algorithm 3 Identification algorithm

```
Start
Read Traces
Traces = keyword OR Traces = website
if (types of keyword == characteristics) AND characteristics == components) then
    Map the keyword with components
else if (types of website == characteristics) AND (characteristics == components) then
    Map the keyword with components
else
    Identify traces again EOF
end if
Compare traces
End
```

5 Analysis and Findings

In this section, the ability of tracing technique for discovering cyber terrorism activities based on the trace pattern is identified. The capabilities of tracing technique need to be measured to identify its effectiveness to discover the traces based on the total percentage of relevant traces discovered in the website. Thus, the metric used in this research is known as Tracing Percentage (TC_p) used to measure the effectiveness of tracing process. Tracing Percentage for each component (TC_n) is the ratio of related traces discovered ($N_{related\_traces}$) and the total traces (N_{total_traces}) expressed in percentage value. These metric is represented as Equations (3) and (4).

$$TC_n = \frac{N_{related\_traces}}{N_{total\_traces}} \times 100 \quad (3)$$

$$TC_p = TC_n + TC_{n+1} + TC_{n+2} + ... + TC_{n+i}. \quad (4)$$

Equation (3) shows the equation to calculate traces percentage for each component while Equation (4) is the equation to calculate total percentage of the components discovered. In this research, three dataset are analyzed to identify the ability of tracing technique to discover cyber terrorism activities based on the trace pattern. These dataset (DS) are describes in Table 2.

Table 2: Dataset description

Dataset (DS)	Description
DS1	Website name: Anonymous W1, Website type: Blog, URL: Anonymous U1
DS2	Website name: Anonymous W2, Website type: Blog, URL: Anonymous U2
DS3	Website name: Anonymous W3, Website type: Blog, URL: Anonymous U3

Table 3: Total percentage of related traces

DS	Components	N_{total_traces}	$N_{related\_traces}$	TC_n %
DS1	Actor	153	57	37.25
	Motivation	153	55	35.95
	Tools	153	5	3.27
	Method	153	17	11.11
	Target	153	5	3.27
	Impact	153	6	3.92
			TCp = 94.77 %	
DS2	Actor	309	186	60.19
	Motivation	309	36	11.65
	Tools	309	7	2.27
	Method	309	24	7.77
	Target	309	48	15.53
			TCp = 97.41 %	
DS3	Actor	272	127	46.69
	Motivation	272	41	15.07
	Tools	272	12	4.41
	Method	272	31	11.40
	Target	272	40	14.71
			TCp = 92.28 %	

Table 2 shows the information of dataset using namely DS1, DS2, DS3. The names of all websites are hidden due to the sensitive issues. The scripting is use to trace and identify the frequent of the keyword which contribute to the cyber terrorism activities. By using Equations (2) and (3), the tracing percentage for three DS is shown in Table 3.

Table 3 shows the total percentage of related traces for DS. It consists of actor, motivation, tools, method, target, and impact components. The result obtained in Table 3 demonstrates the Tracing Percentage (TC_p) is able to discover the cyber terrorism activities by identifying the components and the types of keyword. These abilities are demonstrated through the result obtained using three DS; DS1, DS2, and DS3. For each DS, the total traces found for each types of keyword and components are shown in Tables 4, 5, and 6 respectively. Due to the sensitive data, the keyword traced in this paper is represented as K_1 to K_n.

Tables 4, 5, and 6 shows the traces found in DS1, DS2, and DS3 respectively. Scripting is used in the analysis and design process to trace the frequent keyword appears that identified. Based on these tables, the components of cyber terrorism have appeared in all DS except one of cyber terrorism components known as impact is not found in DS2 and DS3. However, this component is found in DS1 with the keyword identified is Threat. From the traces found as shown in all tables, this research identified that Actor can be person, group, organization, or place. While, by having any concepts that make a person become motivated or fanatic, it can contribute to cyber terrorism activities which classified as the Motivation component. This was proved that most of the traces found is belong to this component. This can be proved when the traces found in the three DS are majority below to motivation components. For example, there are 55 traces found on keyword concept in DS1, 36 traces in DS2, and 41 traces in DS3. The findings also shown that, in all attacks, target become the important component in cyber terrorism activities in which it was found in all DS analyzed.

6 Conclusion and Future work

This paper introduces the tracing technique for discovering cyber terrorism activities based on the trace pattern. Two main tracing techniques used namely word searching technique and web address searching techniques. Word searching technique is use to extract the traces. Tracing technique consists of traces extraction and classification, traces cross-referencing and linking, and traces verification. Tracing Percentage (TC_P) used to measure the effectiveness and the capabilities of tracing technique to discover the traces based on the total percentage of relevant traces discovered in the website. The abilities of tracing technique are demonstrated through the result obtained using DS. From the research findings, we are able to derive the equation to represent the components of the cyber terrorism.

Acknowledgments

The authors would like to thank INSFORNET Research Group of Universiti Teknikal Malaysia Melaka

Table 4: Traces found in DS1

Keyword	Count	Types of keyword	Components
K_1	27	Concept	Motivation
K_2	21	Concept	Motivation
K_3	18	Person	Actor
K_4	10	Group	Actor
K_5	9	Organization	Actor
K_6	8	Mode of action	Method
K_7	7	Concept	Motivation
K_8	6	Person	Actor
K_9	6	Threat	Impact
K_{10}	5	Tools	Tools
K_{11}	5	Target place	Target
K_{12}	5	Mode of action	Method
K_{13}	4	Person	Actor
K_{14}	4	Person	Actor
K_{15}	4	Mode of action	Method

Table 5: Traces found in DS2

Keyword	Count	Types of keyword	Components
K_1	48	Target Place	Target
K_2	43	Group	Actor
K_3	35	Group	Actor
K_4	30	Concept	Motivation
K_5	27	Organization	Actor
K_6	20	Group	Actor
K_7	18	Mode of action	Method
K_8	17	Place	Actor
K_9	17	Group	Actor
K_{10}	11	Person	Actor
K_{11}	10	Place	Actor
K_{12}	7	Tools	Tools
K_{13}	6	Concept	Motivation
K_{14}	6	Person	Actor
K_{15}	6	Action	Method

Table 6: Traces found in DS3

Keyword	Count	Types of keyword	Components
K_1	40	Target place	Target
K_2	35	Concept	Motivation
K_3	31	Group	Actor
K_4	31	Group	Actor
K_5	25	Organization	Actor
K_6	23	Mode of action	Method
K_7	12	Person	Actor
K_8	12	Tools	Tools
K_9	11	Place	Actor
K_{10}	10	Place	Actor
K_{11}	8	Action	Method
K_{12}	7	Person	Actor
K_{13}	6	Concept	Motivation

(UTeM) for the financial support under the Fundamental Research Grant Scheme with Project No. FRGS/1/2015/ICT04/UTeM/02/5.

References

[1] M. Dawson and M. Omar, *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, Information Science Reference, 2015.

[2] S. Gilmour, "Policing crime and terrorism in cyberspace: An overview," *The European Review of Organised Crime*, vol. 1, no. 1, pp. 143–159, 2014.

[3] S. Gordon and R. Ford, "Cyberterrorism?," *Computers & Security*, vol. 21, no. 7, pp. 636–647, 2002.

[4] S. Gordon and R. Ford, "On the definition and classification of cybercrime," *Journal in Computer Virology*, vol. 2, no. 1, pp. 13–20, 2006.

[5] R. Heickerö, "Cyber terrorism: Electronic jihad," *Strategic Analysis*, vol. 38, no. 4, pp. 554–565, 2014.

[6] L. Jarvis and S. Macdonald, "What is cyberterrorism findings from a survey of researchers," *Terrorism and Political Violence*, vol. 27, no. 4, pp. 657–678, 2015.

[7] M. Kenney, "Cyber-terrorism in a post-stuxnet world," *Orbis*, vol. 1, no. 59, pp. 111–128, 2015.

[8] J. A. Lewis, "Assessing the risks of cyber terrorism, cyber war, and other cyber threats," Center for Strategic and International Studies, Nov. 2002.

[9] O. Oluwafemi, F. A. Adesuyi, and S. M. Abdulhamid, "Combating terrorism with cybersecurity: The nigerian perspective," *World Journal of Computer Application and Technology*, vol. 1, no. 4, pp. 103–109, 2013.

[10] S. R. Selamat, R. Yusof, S. Sahib, M. Z. Masu'd, M. F. Abdollah, and Z. Z. Abidin, "Advanced trace pattern for computer intrusion discovery," *Journal of Computing*, vol. 2, no. 6, pp. 200–207, 2010.

[11] S. R. Selamat, N. M. Salleh, R. Yusof, and S. Sahib, "Constructing cyber terrorism trace pattern for forensic investigation process," in *Proceedings of the 14th International Conference on Applied Computer and Applied Computational Science*, Recent Advances in Computer Science, pp. 240–245, 2015.

[12] S. R. Selamat, R. Yusof, S. Sahib, N. F. Hassan, M. F. Abdollah, and Z. Z. Abidin, "Traceability in digital forensic investigation process," in *IEEE Conference on Open Systems*, pp. 101–106, Sept. 2011.

[13] R. Smith, "The cyber terrorism threat to critical infrastructure," Master thesis, Utica College, 2014.

[14] Z. Yunos, "Cyber terrorism conceptual framework," in *Proceeding in OIC-Certificate Annual Conference*, pp. 1–8, 2012.

[15] Z. Yunos and R. Ahmad, "Evaluating cyber terrorism components in malaysia," in *The 5th International Conference on Information and Communication Technology for The Muslim World*, pp. 1–6, Nov. 2014.

Nurhashikin Mohd Salleh is currently a Master student at the Universiti Teknikal Malaysia Melaka, Malaysia. She holds Bachelor of Computer Science (Hons) in Computer Networking. Her research interests include network forensic, cyber terrorism and cyber violent.

Siti Rahayu Selamat is currently a lecturer at the Universiti Teknikal Malaysia Melaka, Malaysia. She received her Doctor of Philosophy in Computer Science. Her research interests include network forensic, cyber terrorism, intrusion detection, network security and penetration testing.

Robiah Yusof is currently a lecturer at the Universiti Teknikal Malaysia Melaka, Malaysia. She received her Doctor of Philosophy in Computer Science. Her research interests include network management, network forensic, intrusion detection, network security and malware.

Shahrin Sahib received the Bachelor of Science in Engineering, Computer Systems and Master of Science in Engineering, System Software in Purdue University in 1989 and 1991 respectively. He received the Doctor of Philosophy, Parallel Processing from University of Sheffield in 1995. He is a professor and the Vice Chancellor of Universiti Teknikal Malaysia Melaka. His research interests include network security, computer system security, network administration and network design. He is a member panel of Experts National ICT Security and Emergency Response Center and also Member of Technical Working Group: Policy and Implementation Plan, National Open Source Policy.