



A NEW PROFILING FRAMEWORK IN IDENTIFYING CYBER VIOLENT EXTREMISM ATTACK

NURHASHIKIN BINTI MOHD SALLEH

**MASTER OF SCIENCE IN INFORMATION
AND COMMUNICATION TECHNOLOGY**

2018



Faculty of Information and Communication Technology

**A NEW PROFILING FRAMEWORK IN IDENTIFYING CYBER
VIOLENT EXTREMISM ATTACK**

Nurhashikin binti Mohd Salleh

Master of Science in Information and Communication Technology

2018

DECLARATION

I declare that this thesis entitled “A New Profiling Framework in Identifying Cyber Violent Extremism Attack” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in the candidature of any other degree.

Signature :

Name : NURHASHIKIN MOHD SALLEH

Date :

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in term of scope and quality for the award of Master of Science in Information and Communication Technology.

Signature :

Supervisor Name : DR. SITI RAHAYU SELAMAT

Date :

DEDICATION

Dedicated to all my family:

Thank you for all you love

May Allah bless us.

ABSTRACT

Violent extremism has become a serious issue and an area of interest to government as it could leave difficult conditions to the nation. Violent extremism happens when someone chooses to carry out violent method and intent to cause harm to other. These groups of extremists aim to cause as much damage as possible when they intent to create harm to the target. Internet as the medium of communication has led to the formation of cyber communities which attracts violent extremism group. Recently, the violent extremism group uses the Internet as their platform to form online communities and launch their attack, these activities known as Cyber Violent Extremism (Cyber-VE). The ongoing increase in online activities by violent extremist groups along with the lack of mechanisms that can be used to identify violent extremism activity could be considered as a major problem. The threat of Cyber-VE is still on the rise and the existing mechanism do not seem to be reducing this attack. Therefore, the aim of this research is to develop a new profiling framework to help forensic investigators in identifying any activities that related to Cyber-VE attack. This done by integrating the classification of the Cyber-VE traces and the components of criminology theory. Prior to that, an analysis of the exiting profiling process is conducted to identify the process requirements in order to develop the profiling framework. After completing the analysis, an experimental design was setup to generate Cyber-VE traces classification. Traces classification is generated through the process of identifying, extracting and classifying traces. In order to identify the causes that leading to criminal behaviors, two types of criminology theory are used which are social learning theory and space transition theory. A combination of Social Learning Theory and Space Transition Theory was used to explain and identify the criminal behavior in which the criminal behavior will refer to Cyber-VE behavior. Then, both traces classification and criminology theory are integrated in order to develop the profiling framework. The proposed Cyber-VE profiling framework consists of three main processes which are data extraction and classification, Cyber-VE behavior identification, and Cyber-VE profile construction. This profiling framework is evaluated and validated to verify its capabilities in profiling Cyber-VE activities. In the experimental approach, the results from the dataset showed that profiling framework is capable to profile Cyber-VE activities using the proposed profiling framework. In expert view, the results showed that the proposed profiling framework is able to identify the activities that related to Cyber-VE attack.

ABSTRAK

Keganasan melampau telah menjadi satu isu yang serius dan menarik perhatian pihak kerajaan kerana ia boleh meninggalkan keadaan yang sukar kepada negara. Keganasan melampau berlaku apabila seseorang memilih untuk menggunakan kaedah ganas dan berniat untuk membahayakan orang lain. Kumpulan pelampau ini bertujuan menimbulkan banyak kerosakan yang mungkin apabila mereka berniat untuk mencetuskan kemudaratan kepada sasaran. Internet sebagai medium komunikasi telah menyebabkan pembentukan komuniti siber yang menarik kumpulan ini. Baru-baru ini, kumpulan pelampau ini menggunakan Internet sebagai platform mereka untuk membentuk komuniti dalam talian dan melancarkan serangan mereka, aktiviti-aktiviti ini dikenali sebagai siber keganasan melampau (Cyber-VE). Peningkatan aktiviti dalam talian oleh kumpulan pelampau disertakan dengan kekurangan mekanisme yang boleh digunakan untuk mengenal pasti aktiviti ini boleh dianggap sebagai masalah utama. Ancaman Cyber-VE masih terus meningkat dan mekanisme yang ada nampaknya tidak dapat mengurangkan serangan ini. Oleh itu, tujuan penyelidikan ini adalah untuk membangunkan rangka kerja profil baru untuk membantu penyiasat forensik dalam mengenal pasti sebarang aktiviti yang berkaitan dengan serangan Cyber-VE. Ini dilakukan dengan mengintegrasikan klasifikasi jejak Cyber-VE dan komponen teori kriminologi. Sebelum itu, analisis mengenai proses yang terdahulu dijalankan untuk mengenal pasti keperluan proses dalam membangunkan rangka kerja profil. Setelah itu, reka bentuk eksperimen dibentuk untuk menjana klasifikasi jejak Cyber-VE. Klasifikasi jejak dihasilkan melalui proses mengenal pasti, mengekstrak, dan mengklasifikasikan kesan. Untuk mengenal pasti punca yang membawa kepada tingkah laku jenayah, dua jenis teori kriminologi digunakan iaitu teori pembelajaran sosial dan teori peralihan ruang. Gabungan Teori Pembelajaran Sosial dan Teori Peralihan Angkasa digunakan untuk menjelaskan dan mengenal pasti tingkah laku jenayah di mana tingkah laku jenayah merujuk kepada perilaku Cyber-VE. Kemudian, kedua-dua jejak klasifikasi dan teori kriminologi diintegrasikan untuk membangunkan rangka kerja profil. Cadangan kerangka kerja Cyber-VE yang dicadangkan terdiri daripada tiga proses utama yang merupakan pengekstrakan dan klasifikasi data, mengenal pasti perilaku Cyber-VE, dan pembinaan profil Cyber-VE. Rangka kerja profil yang dicadangkan dinilai dan disahkan untuk mengesahkan keupayaannya dalam memprofilkan aktiviti Cyber-VE. Melalui pendekatan eksperimen, hasil dari dataset menunjukkan bahawa kerangka profiling mampu memprofilkan aktiviti Cyber-VE dengan menggunakan rangka kerja profil yang dicadangkan. Dalam pandangan pakar, hasilnya menunjukkan bahawa rangka kerja profil yang dicadangkan dapat mengenal pasti aktiviti yang berkaitan dengan serangan Cyber-VE.

ACKNOWLEDGEMENTS

I would like to extend my sincere appreciation to my supervisor Dr. Siti Rahayu Selamat, who has always been patient and available especially in those times that I felt overwhelmed. Your feedback and suggestions have been so helpful and I sincerely have learnt a lot from you. Thank you for believing in me particularly when I had doubts about this whole project. Also thank to Dr. Zurina Saaya for all her helps, support, and valuable hints.

Many thanks go to the Faculty of Information and Communication Technology for providing me a great environment to study and do research. I have learnt so much from seminars and research presentations that were held in the faculty. In addition, generous helps on study and research are provided by professors and staff in the department. Especially, providing me the facility of hardware during the period of research.

I would like to express my very great appreciation to all my friends for their care, support and encouragement to me. We shared our memorable moments together in the past two years. Finally, special thanks must also go to my parents and my entire family for providing me unconditional support and encouragement throughout my time in graduate school.

TABLE OF CONTENTS

	PAGE
DECLARATION	
APPROVAL	
DEDICATION	
ABSTRACT	i
ABSTRAK	ii
ACKNOWLEDGEMENTS	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	vii
LIST OF FIGURES	x
LIST OF APPENDICES	xiii
LIST OF ABBREVIATIONS	xiv
LIST OF PUBLICATIONS	xv
CHAPTER	
1. INTRODUCTION	1
1.1 Introduction	1
1.2 Research Problem	5
1.3 Research Questions and Hypothesis	10
1.4 Research Aim and Objectives	11
1.5 Research Scope	13
1.6 Research Contributions	13
1.7 Thesis Organization	14
1.8 Summary	17
2. LITERATURE REVIEW	18
2.1 Introduction	18
2.2 Cyber Violent Extremism (Cyber-VE)	19
2.2.1 Definition of Violent Extremism	19
2.2.2 Root of Violent Extremism	23
2.2.3 Activities of Violent Extremism	25
2.2.4 Analysis of Cyber-VE	46
2.3 Profiling Framework	48
2.3.1 Definition of Profiling	49
2.3.2 Roles of Profiling	50
2.3.3 Method of Profiling	52
2.3.4 Existing of Profiling Framework	54
2.3.5 Analysis of Profiling Framework	62
2.4 Tracing Technique	65
2.4.1 Overview of Tracing Technique	66
2.4.2 Keyword Extraction Technique	67
2.4.3 Analysis of Tracing Technique	77
2.5 Criminology Theory	77
2.5.1 Application of Criminology Theory	79
2.5.2 Analysis of Criminology Theory	86
2.6 Overall Analysis	89

2.6.1	Analysis of Cyber-VE	89
2.6.2	Analysis of Profiling Framework	91
2.6.3	Analysis of Criminology Theory	93
2.7	Proposed Solution on Cyber-VE Profiling Framework	94
2.7.1	Integration of Cyber-VE Traces Classification and Criminology Theory in Developing Profiling Framework	94
2.8	Summary	96
3.	RESEARCH METHODOLOGY	98
3.1	Introduction	98
3.2	Research Approach	99
3.2.1	Quantitative Method	99
3.2.2	Qualitative Method	99
3.3	Research Framework	101
3.3.1	Cyber-VE Traces Classification	101
3.3.2	Criminology Theory	102
3.4	Research Process	102
3.4.1	Theoretical Study	103
3.4.2	Exploratory Study	105
3.5	Experimental Design	110
3.6	Research Tool and Research Equipment	111
3.7	Summary	111
4.	ANALYSIS OF THE CYBER-VE PROFILING FRAMEWORK	113
4.1	Introduction	113
4.2	Analysis Design	113
4.2.1	Traces Identification and Extraction Phase	114
4.2.2	Traces Classification Phase	115
4.3	Analysis and Finding Data	118
4.3.1	Analysis and Finding for DS1	119
4.3.2	Analysis and Finding for DS2	124
4.3.3	Analysis and Finding for DS3	128
4.3.4	Overall Analysis of Findings	132
4.3.5	Proposed Cyber-VE Traces Classification	133
4.4	Summary	136
5.	DISCUSSION OF THE PROPOSED PROFILING FRAMEWORK	137
5.1	Introduction	137
5.2	Proposed Cyber-VE Profiling Framework	138
5.2.1	Traces Classification and Criminology Theory Integration	138
5.2.2	Developing Cyber-VE Profiling Framework	140
5.3	Cyber-VE Profiling Algorithm	146
5.3.1	Design	147
5.3.2	Components and Technologies	147
5.3.3	Limitations	147
5.3.4	Assumptions	148
5.3.5	Traces Identification and Extraction Algorithm	148
5.3.6	Traces Classification Algorithm	149

5.3.7	Profile Construction Algorithm	151
5.4	Summary	152
6.	EVALUATION AND VALIDATION OF THE PROPOSED CYBER-VE PROFILING FRAMEWORK	153
6.1	Introduction	153
6.2	Experiment for Evaluation and Validation	154
6.2.1	Result for DS4	156
6.2.2	Result for DS5	163
6.2.3	Result for DS6	170
6.3	Evaluation and Validation Processes	177
6.4	Result Evaluation and Validation	178
6.4.1	Identify Category	179
6.5	Validation by Expert View	179
6.5.1	Expert Information	180
6.5.2	Cybercrime Profiling Framework	180
6.5.3	Cyber Violent Extremism (Cyber-VE) Attack	181
6.5.4	Data Profiling	182
6.5.5	Improvement of Cybercrime Profiling Framework	182
6.5.6	Current Cyber-VE Profiling Framework	185
6.5.7	Summary of Expert Validation	185
6.6	Analysis of Result Validation	187
6.6.1	Analysis of Experimental Result Validation	187
6.6.2	Analysis of Expert Validation	188
6.7	Discussion on Result Validation	189
6.8	Summary	190
7.	DISCUSSION AND FUTURE WORKS	191
7.1	Introduction	191
7.2	Summary of the Completed Work	192
7.3	Research Contributions	192
7.4	Research Constraints and Limitations	194
7.5	Further Research	194
7.6	Summary	195
	REFERENCES	197
	APPENDICES	215

LIST OF TABLES

TABLE	TITLE	PAGE
1.1	Ten Worst Attacks in OECD Countries Since 2015	2
1.2	Summary of research problem	10
1.3	Summary of research question	11
1.4	Summary of research objective	12
1.5	Summary of research contributions	13
2.1	Definition of violent extremism	22
2.2	Analysis and synthesis of violent extremism activities	36
2.3	Description of Cyber-VE components	40
2.4	Description of Cyber-VE attributes	42
2.5	Relationship between Cyber-VE components and Cyber-VE attributes	46
2.6	List of components and attributes for Cyber-VE	47
2.7	Existing process of profiling	60
2.8	Definition and roles of keyword	70
2.9	Technique of extraction	75
2.10	Summarization of criminology theory	87
2.11	Components of Cyber-VE	90
2.12	Process in developing profiling	92
2.13	Integration of Cyber-VE traces classification and criminology theory	95

3.1	Summarization of the research framework	102
3.2	Sources of information	105
3.3	Software description	111
3.4	Hardware description	111
4.1	Description of dataset (DS)	119
4.2	Traces extracted and its frequency for DS1	121
4.3	List of attributes and traces for DS1	121
4.4	List of components, attributes, and traces for DS1	122
4.5	Traces extracted and its frequency for DS2	125
4.6	List of attributes and traces for DS2	126
4.7	List of components, attributes, and traces for DS2	127
4.8	Traces extracted and its frequency for DS3	129
4.9	List of attributes and traces for DS3	130
4.10	List of components, attributes, and traces for DS3	130
4.11	Summarization of Cyber-VE attributes	132
4.12	Summarization of Cyber-VE components	133
5.1	Summarization of the proposed profiling framework	145
6.1	Description of dataset (DS)	154
6.2	Traces identification for each DS	155
6.3	Traces extracted and its frequency for DS4	156
6.4	List of attributes and traces for DS4	157
6.5	List of components, attributes, and traces for DS4	158
6.6	Traces extracted and its frequency for DS5	164
6.7	List of attributes and traces for DS5	165

6.8	List of components, attributes, and traces for DS5	166
6.9	Traces extracted and its frequency for DS6	171
6.10	List of attributes and components for DS6	172
6.11	List of components, attributes, and traces for DS6	173
6.12	Result of <i>Category Identification</i> for DS4-DS13	179
6.13	Summarization of validation on cybercrime profiling framework	181
6.14	Summarization of validation on improvement of cybercrime profiling framework	184
6.15	Result of <i>Profile Identification</i> for DS4-DS13	187
6.16	Characterization of validation experimental result	188
6.17	Summary of result validation of the proposed Cyber-VE profiling framework	188
6.18	Summarization of result validation of existing profiling framework	189
6.19	Summarization of result validation	189

LIST OF FIGURES

FIGURE	TITLE	PAGE
1.1	Terror attacks are on the rise around the world	2
1.2	Thesis Organization	14
2.1	Framework of literature review	18
2.2	Types of extremists	23
2.3	Terrorism pyramid	26
2.4	Method of profiling	53
2.5	Components in explaining and understanding the criminal behavior	93
2.6	Proposed solution on Cyber-VE profiling framework	95
3.1	Research framework	101
3.2	Research process	103
3.3	Process of data collection	107
3.4	Process of data analysis	108
3.5	Design of experiment	110
4.1	Analysis design of acquiring Cyber-VE traces	114
4.2	Process flow of identifying and extracting traces	115
4.3	Process flow of classifying traces	116
4.4	Process flow of classifying attributes	117
4.5	Process flow of classifying components	118

4.6	The potential extremist's website for DS1	120
4.7	Cyber-VE traces classification for DS1	123
4.8	The potential extremist's website for DS2	125
4.9	Cyber-VE traces classification for DS2	127
4.10	The potential extremist's website for DS3	128
4.11	Cyber-VE traces classification for DS3	131
4.12	Overall Cyber-VE traces classification	134
4.13	Cyber-VE component	135
5.1	Integration between Cyber-VE traces classification and criminology theory	139
5.2	Proposed Cyber-VE profiling framework	140
5.3	Sub-processes in the data extraction and classification process	141
5.4	Sub-processes in Cyber-VE behavior identification process	142
5.5	Sub-processes in Cyber-VE profile construction process	143
5.6	Cyber-VE profile	144
5.7	Cyber-VE profiling prototype	146
5.8	Algorithm of identifying and extracting traces	149
5.9	Algorithm of classifying traces into attribute	150
5.10	Algorithm of classifying attributes into component	151
5.11	Algorithm of constructing Cyber-VE profile	152
6.1	The potential extremist's website for DS4	156
6.2	Cyber-VE traces classification for DS4	159
6.3	Integration between Cyber-VE traces classification and criminology theory for DS4	161

6.4	Cyber-VE profile for DS4	162
6.5	The potential extremist's website for DS5	163
6.6	Cyber-VE traces classification for DS5	167
6.7	Integration between Cyber-VE traces classification and criminology theory for DS5	169
6.8	Cyber-VE profile for DS5	168
6.9	The potential extremist's website for DS6	170
6.10	Cyber-VE traces classification for DS6	174
6.11	Integration between Cyber-VE traces classification and criminology theory for DS6	176
6.12	Cyber-VE profile for DS6	175
6.13	Evaluation and Validation Processes	177

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Source Code	215
B	Sample of Dataset	218
C	Traces Classification of Each Dataset	222
D	Cyber-VE Profile of DS7-DS13	229
E	Expert's Biography and Acceptance Letter	233
F	Expert's Interview Questions and Answers	236

LIST OF ABBREVIATIONS

AI	-	Artificial Intelligence
Cyber-VE	-	Cyber Violent Extremism
DS	-	Dataset
IR	-	Information Retrieval
TF	-	Term Frequency

LIST OF PUBLICATIONS

Saleh, N.M., Selamat, S.R., Saaya, Z., 2018, August. Profiling Framework in Identifying Cyber Violent Extremism (Cyber-VE) Attack. *Journal of Theoretical and Applied Information Technology*, 96(16), pp. 5615-5624.

Salleh, N.M., Selamat, S. R., Yusof, R. and Sahib, S., 2016. Discovering Cyber Terrorism using Trace Pattern. *International Journal of Network Security*, 18(6), pp. 1034-1040.

Salleh, N.M., Selamat, S.R., Saaya, Z., Ahmad, R. and Masúd, Z., 2016. Identifying Cyber Violent Extremism (Cyber-VE) Components by Exploring Dark Web. *International Journal of Computer Science and Information Security*, 14(9), p.52.

Salleh, N.M., Selamat, S.R., Saaya, Z., Ahmad, R. and Masúd, Z., 2016, November. A New Taxonomy of Cyber Violent Extremism (Cyber-VE) Attack. *6th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*, pp. 234-239.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Violent extremism has become an area of interest to government as it could leave to the nation with difficult conditions. This group aims to cause as much damage as possible as they intent to create harm to the target (Nasser et al., 2011). Violent extremism threats come from a range of groups and individuals (Neumann, 2013). Most forms of violent extremism are undertaken by one individual known as lone wolf attacks (Nasser et al., 2011). The threat of violent extremism immediately topped the international agenda (Guilain and Lynn, 2009) and this remains significant and concern for many governments in Southeast Asia and beyond (Ramakrishna, 2015). Violent extremism continues to spread (Haynes and Mangas, 2015) as it shows more than six-fold increase in the number of global terror attacks, from 2,750 attacks in 2006 to more than 16,000 in 2014 as reported by Global Terrorism Index(2015) shown in Figure 1.1.

Figure 1.1 shows the terror attacks around the world reported by (Global Terrorism Index, 2015). In their research, the number of terror attacks is divided based on the region such Asia and Pacific, Middle East and North Africa, Sub-Saharan Africa, Europe and Eurasia, and Americas, and it shows that the annual count by region are increasing year by year. Asia and Pacific, and Middle East and North Africa region recorded the highest number of terror attacks compared to another region. From the attacks reported, it indicates that the number of violent extremism has grown over the nine years. In 2016, Global

Terrorism Index released reports ten worst attacks in Organization for Economic Co-operation and Development (OECD) countries since 2015 as shown in Table 1.1.

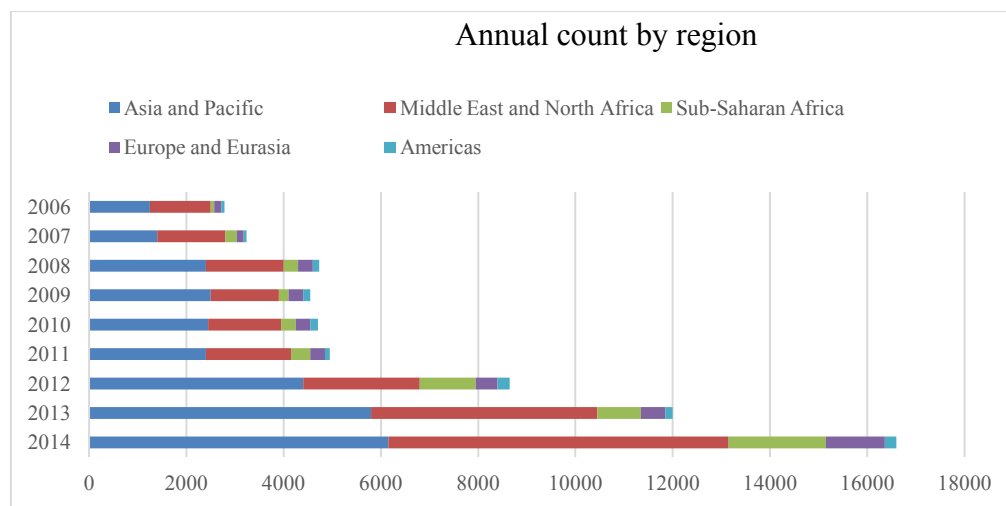


Figure 1.1: Terror attacks are on the rise around the world (Sources: *Global Terrorism Index, 2015*)

Table 1.1: Ten Worst Attacks in OECD Countries Since 2015

Country	Year	Attack	Deaths	Injuries	Responsible
France	2015	Paris attacks	137	368	ISIL
Turkey	2015	Ankara bombings	105	400	ISIL
Turkey	2015	Suruc bombing	33	104	Lone actor (ISIL inspired)
France	2015	Ile-de-France attacks	20	22	Local group (al-Qa'ida/ ISIL inspired)
France	2016	Nice truck attack	85	300	Lone actor (ISIL inspired)
Turkey	2016	Ataturk Airport attack	50	230	ISIL
United States	2016	Orlando nightclub shooting	50	53	Lone actor (ISIL inspired)
Belgium	2016	Brussels attacks	35	330	ISIL
Turkey	2016	March Ankara bombing	34	125	Kurdistan Freedom Falcons (TAK)
Turkey	2016	February Ankara bombing	30	60	Kurdistan Freedom Falcons (TAK)

Table 1.1 shows the ten worst attacks in OECD countries since 2015 which the highest deaths are recorded about 137 people and 368 people injuries. Even though Table 1.1 indicates the most responsible groups were conducted by a certain religion, however (United States Institute of Peace, 2018) stated the spread of violent extremism is not controlled by the religion of the person. However with the poor governance, injustices, and the radicalization of people, this attack can be happens. These groups use religious ideas

whether from Christianity, Islam, Buddhism, or other beliefs as their tools in order to encourage violent acts. It has been supported by (Salleh et al., 2018) stated anyone can become extremist as long as they have motive to carry out and intent to cause harm to the target using violent method. With this statistic, it shows the attack still happen year by year and the mechanism needs to be developed in order to counter this attack.

Nowadays, the use of the Internet as the main medium of communication has led to the formation of cyber communities which become attractive for violent extremist groups (Scanlon and Gerber, 2015). Looking at the current situation reported in many countries, the utilization of Web Technology to support extremism activities increased dramatically (Zhang, 2009). Violent extremism used cyber communities as their platform to do illegal activities. There are some research shows that cyber communities are most influence ways at the onset of a future member's extremist activity (Robyn, 2010). For example, terrorist group use Internet to form online communities which they can form online communities and disseminate materials without having to rely on traditional media which might censor or change their message (Robyn, 2010). Cyber communities enable violent extremists to increase recruitment by allowing them to build personal relationships with the worldwide users capable for accessing their activities. It has been reported that some extremist group uses social media like Facebook, Twitter, YouTube, Second Life, and web forums to engage direct communication or advertisement, spread the materials, recruit and training members, exchange ideology, fundraising and even plan an attack (Robyn, 2010). As it plays a critical role in the success of the revolution, it brings a challenge for government, law enforcement, and intelligence agencies (Scanlon, 2014) (Quintero, 2014). The causes of violent extremism are complex and multidimensional and strategy is needed to deal with them.

Therefore, the aim of this research is to develop a new profiling framework in identifying any activities that related to Cyber-VE attack. Profiling is known as an educated attempt to provide specific information as to the type of individual who committed a certain crime. It' based on characteristics patterns or factors of uniqueness that distinguishes certain individuals from the general population (Douglas et al., 1986). Profiling is the method of categorizing people and predicts their behavior based on the characteristics (Warikoo, 2014). It is also known as the process of learning information about someone based on what is already known (Merriam-Webster, 2015). Profiling also describe about the person characteristics without knowing the identity of that person. It's also known as psychological assessment of defining characteristics that are common in a particular of person (Saroaha, 2014). Criminal profiling is one of the examples that have been implemented the criminology theory as their approach in order to develop a profile. Profiling does not provide the specific about the criminal but it rather indicates what kind of person likely. It is an important tool employed by law enforcement agencies in their investigations (Warikoo, 2014). Besides, Alazab (2015) define profiling as an investigative tool that consists of analyzing the crime scene and likely behavior of the offender and using all this information to determine the possible identity of the cybercriminal.

Criminology theory is a theory used to study about crime (Gennaro et al., 2005) in understanding and identifying why people tend to commit crime. It refers to the origins of criminal behaviors either individual or groups of people (Lilly et al., 2007). Generally, criminology theories assist to understand about why criminal commit crimes (Tania, 2014). It attempts to explore and understand the causes that leading to criminal behavior and the factors that contribute to the crime (Ronald and Christine, 2013), (Lyman and Potter, 2000). This theory considers about the characteristics of individuals and also a society that results in crime by explaining and analyzing about the criminal activities and the behaviors