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

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

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 (Nasseret al., 2011). The threat of violent extremism immediately topped the international agenda (Guilain andLynn, 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 Africaregion 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.

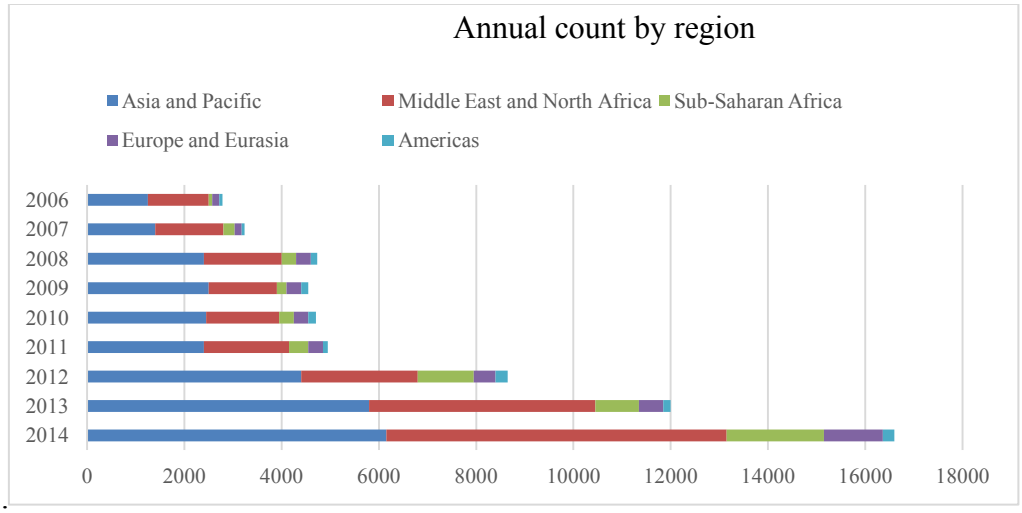

Figure 1.1: Terror attacks are on the rise around the world *(Sources: Global Terrorism Index, 2015)*

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 developedin 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(Scanlonand 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 aresome 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 (Saroha, 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