Journal of Theoretical and Applied Information Technology
31st August 2018. Vol.96. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PROFILING FRAMEWORK IN IDENTIFYING CYBER VIOLENT EXTREMISM (CYBER-VE) ATTACK

[1]NURHASHIKIN MOHD SALEH, [2]SITI RAHAYU SELAMAT, [3]ZURINA SAA'YA
[1,2]Faculty of Information and Communication Technology
[1,2,3]Universiti Teknikal Malaysia Melaka (UTeM)
E-mail: [1]nurhashikinbtmohdsalleh92@gmail.com, [2]sitirahayu@utem.edu.my, [3]zurina@utem.edu.my

ABSTRACT

Cyber Violent Extremism (Cyber-VE) attack becomes topped at the international agenda and it still significant and concern to many governments in Southeast Asia and beyond. Cyber-VE becomes a threat to the country as the ongoing increase in online activities by the violent extremists group. The threat of Cyber-VE is still on the rise and the existing counters do not seem to be reducing this attack. Hence, the aim of this paper is to propose a new profiling framework in profiling Cyber-VE activities. This paper integrates between Cyber-VE traces classification and the components of criminology theory. Traces classification is generated through the process of identifying, extracting, and classifying traces. Two types of criminology theory which social are learning theory and space transition theory are used to explain and identify the criminal 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. The proposed profiling framework is evaluated and validated to verify its capabilities in profiling Cyber-VE activities. In experimental approach, the results from the dataset showed that the profiling framework is capable to profile Cyber-VE activities. In expert view, the results showed that the proposed profiling framework able to identify the activities that related to Cyber-VE attack. These findings will be used in helping the investigators in identifying any activities that related to Cyber-VE attack and help in profiling Cyber-VE attack.

Keywords: *Cyber Violent Extremism (Cyber-VE), Dark Web, Profiling Framework, Traces Classification, Criminology Theory*

1. INTRODUCTION

Violent extremism is a threat to the country as it impacts not only on the politics but also on the economics of the country involved [1]. Nowadays, extremism groups have expanded their authority through Internet and online social media with the objective to recruit new members [2] [3]. These groups use Internet to form online communities and spread their material without having relied on traditional media outlets [2] [4]. Extremist group activities involved in directed communication and advertisement, recruiting members on online social media like Second Life, Facebook, and web forums [2] [3]. It has been reported that the use of web technology to support extremism activities has increased dramatically [5] [6].

The ongoing increase in online activities by the violent extremist group along with the lack of mechanism that can be used to identify violent extremism activity could be considered as a major problem [7]. The problem arises when it is impossible for detecting and analyzing the possible terrorists. It creates a challenge in identifying, tracing, and detecting activities relates to violent extremism attack especially on the violent extremism that use cyber as the medium for the attack that known as Cyber-VE. As existing profiling only covered on criminal or offender, or crime itself, it still lacking as it could not be adopting in identifying Cyber-VE activities as the threat of terrorism is still on the rise and the existing counter terrorism policies do not seem to be reducing terrorism worldwide [10].

Therefore, a new profiling framework in identifying any activities that related to Cyber-VE attack needs to be developed. This paper is organized as the following: Section II discusses about the related work, Section III describes about methodology, Section IV discusses about the proposed profiling framework and Section V shows about analysis and findings. Lastly, Section VI explains about conclusion and future work.

2. RELATED WORK

In this section, cyber violent extremism (Cyber-VE), profiling framework, traces classification, and criminology theory are further explained.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.1 Cyber Violent Extremism (Cyber-VE)

Cyber-VE defined as an individual, group, or organization that put their ideology, extreme belief, or objective into violent action with intent to cause harm to the target by using cyberspace as their domain [12]. [7] stated extremists use violent methods to disrupt an established authority as they act with the specific goal of influencing public opinion or inciting political change. Extremist groups believed a violent method is justified in order to achieve their aim [13]. According to [14], extremists choose to use violent method because they want to create and exploit fear for political change. Besides, [15] stated weapon is one of tools that have been used by this group in order to do their attack. [16] [17] added extremist's use bomb as their tools to leave a greatest damage to the target. As the use of Internet as the main medium of communication, it has leads to the formation of cyber communities which become attractive to this group [7].

Violent extremism group used cyber communities as their medium to do illegal activities [2]. Coupled with the advent of web forums, it has facilitated an interaction among participants that allow extremists group to promote violence and distribute their propaganda materials known as Dark Web [18]. Dark web is a private website where extremist groups use to communicate and spread their message [19]. Extremist groups set up various web sites embedded in the public Internet to exchange ideology, spreading propaganda, and recruit a new member [18][19]. Extremists have created their own websites for spread and publish their agenda and the information about their activities to gain public attention [20]. These social media sites have value-add to extremists or terrorist's ability to communicate, organize, recruit, and even train the people to become terrorist's person [5].

2.2 Profiling Framework

[21] defined profiling 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. Profiling describe about the criminal characteristics without knowing the identity of the criminal. It is a psychological assessment of define characteristics that are common in a particular of criminals [22]. Besides, according to [23], profiling is the recording and analysis of a person's psychological and behavioral characteristics to assess or predict their capabilities in order to assist in identifying categories of people. While, [24] defined profiling as the activity of collecting information about someone in order to give a description about them. However, in 2015, [25] research defined 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 identify of the cybercriminal. The existing profiling framework uses different terms to define the same steps of developing profiling. It also been identified that the processes used by researchers are not in the same sequences. The previous process shows there are three main processes namely identifying and analyzing crime and evidence, understanding and analyzing about victim, and identifying and analyzing about offender. However, not all processes are included in researcher's study. Therefore, these processes will be used as a guideline in developing Cyber-VE profiling framework.

2.3 Traces Classification

Cyber-VE traces consists of the keyword that usually used by the extremist groups. Using these traces, attributes and components of Cyber-VE can be identified. Cyber-VE traces plays an important role as it can be used in identifying the origin of the attack. In traces classification, the Cyber-VE traces are classified in order to determine the activities of Cyber-VE attack. [26] discovered traces are meaningless without knowing the relation between them. Therefore, it is very important to identify the relationship between the discovered traces. The relationship between traces should be identified in order to form the complete traces. This traces classification is used to profile Cyber-VE attack by developing profiling framework.

2.4 Criminology Theory

Criminology theory is used to understand about why criminal commit crime. It covers on different subject domain such as law, social, psychological, computing and information security. It attempts to explore about the causes that leading to criminal behavior and also the factors contribute to crime. Criminology theory will help this research to describe about the characteristics of an individual and society that lead them to do crime. This theory describes on what is important to look for understand, explain, predict, and handle it. By using criminology theory, it helps to design effective crime control strategies. It has been identified theories used by the previous researches are rational choice theory, routine activities theory, social learning theory,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

social control theory, space transition theory, opportunity theory, and crime displacement theory. Although all theories discussed are related to crime activities, this research has identified two related theories to be used namely Social Learning Theory and Space Transition Theory in order to develop a better understanding the causes that leading to criminal behavior and possible measures against Cyber-VE attack. From the both theories, the potential conceptual components are identified. These components are used to profile Cyber-VE attack by developing profiling framework.

2.5 Profiling Cyber Violent Extremism

Currently, there are a number of research in cyber criminal that are using various approaches to profile the criminal. For example, using metrics to identify criminal behavior and characteristics [46] and case-based reasoning to measure an attacker's characteristics [47]. In this work, we specifically focus on profiling the violence activities such as action to disrupt an established internet service. Basically, profiling cyber violence differs from profiling cyber criminal in various ways. For example, profiling criminal mostly cover only on criminal or offender, or crime itself while in our research the main idea is to identify activities that have intention to cause harm.

3. METHODOLOGY

There are three phases involved in developing Cyber-VE profiling framework in order to identify Cyber-VE activities. The explanations of these phases will be explained below.

3.1 Cyber-VE Traces Classification Phase

Traces classification is the important phase that enables us to identify the origin of the attack. During this phase, the keyword extraction technique is used in order to identify, extract, and classify the traces. As our dataset consists of the potential extremist's website, therefore, term frequency (TF) is used to identify the keyword that usually used by the extremist groups. The keyword is based on its frequency. After keywords are selected, these keywords will be classified into Cyber-VE attributes and components. As keyword plays an important role in producing a short summary about the content, therefore one of measures to determine the importance of a word in a document is term frequency. This measure will calculate the total number of times a word occurs in a document [38]. With these keywords, the attributes and components of Cyber-VE attack can be identified.

3.2 Criminal Behavior Phase

In identifying criminal behaviors, two types of criminology theory are used namely social learning theory and space transition theory. Social learning theory states that people commit a crime by learning a new behavior by watching other people. People learn a new behavior through the observational learning of the social factors in their environment [21]. This theory helps this research to focus on how criminal commit crime through the people they associate with [39]. Social theory not only focuses on the learning of techniques but it also focuses on the role of drivers, motives, and rationalizations of the attacker [40]. While, space transition theory helps to explain about the nature of the person behavior who bring out their conforming and non-conforming behavior in the physical space and cyberspace. This theory explains about the movement of persons from one space to another space, for example; from cyberspace to physical space [41]. This theory explains how people like to unite in cyberspace to commit crimes in physical space. The behavior of criminal in cyberspace is likely to be imported to the physical space, and criminal behavior in physical space also may be exported to cyberspace as well [42]. The criteria used in explaining the behavior of criminal is identified.

3.3 Develop Cyber-VE Profiling Framework Phase

After completing the previous phases, Cyber-VE profiling framework will be developed. This research proposes to integrate between Cyber-VE traces classification and the components of criminology theory in order to be used in developing Cyber-VE profiling framework.

4. PROPOSED CYBER-VE PROFILING FRAMEWORK

This paper proposed Cyber-VE profiling framework by integrating between Cyber-VE traces classification and the components of criminology theory. The purpose of the proposed profiling framework is to assist forensic investigators in identifying any activities that related to Cyber-VE attack. This paper proposed Cyber-VE profiling

Journal of Theoretical and Applied Information Technology
31st August 2018. Vol.96. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

framework as shown in Figure 1, Figure 2, Figure 3, and Figure 4.

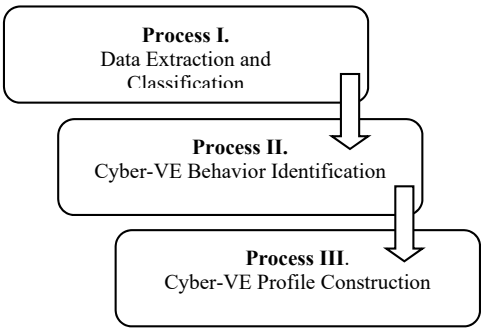

Figure 1: Proposed Cyber-VE profiling framework

From the Figure 1, it demonstrates the proposed Cyber-VE profiling framework consists of three main processes namely i) Data extraction and classification ii) Cyber-VE behavior identification and iii) Cyber-VE profile construction. The description about each process will be explained below.

4.1 Data Extraction and Classification

The first process starts by extracting and classifying data as depicted in Figure 2. Based on the Figure 2, data extraction and classification process consists of three sub-process which are data identification, traces identification, and traces classification. The sub-process starts with filtering the collected data by removed irrelevant data. In this sub-process, this research manually filtering as it can achieve high precision but surely less efficient [43]. The relevant data will be determined whether its content potentially risks or not to be used as our evidence source.

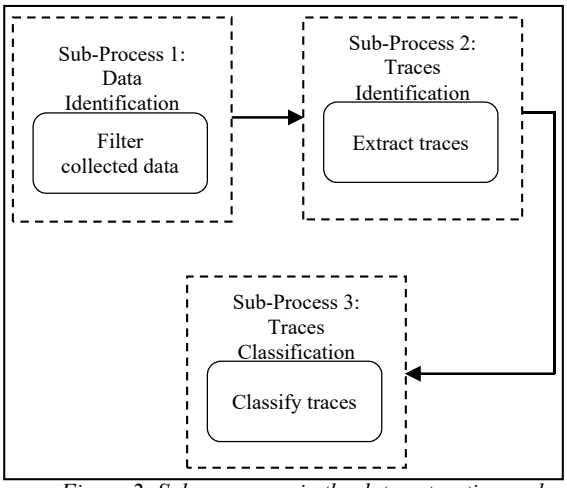

Figure 2: Sub-processes in the data extraction and classification process

The next sub-process is to identify the traces which directly referring to the keyword that usually used by the extremist groups. This sub-process is conducted using term frequency (TF) technique. Then, using traces found, the process of identifying attributes and components is conducted. This sub-process is important in order to identify the origin of the attack. If traces are belonging to $attribute_1$, then traces are classified into $attribute_1$. If not, traces are classified into other $attribute_{n+1}$. Next, if attribute1 is belongs to $component_1$, then $attribute_1$ are classified into $component_1$. If not, $attribute_1$ is classified into other $component_{n+1}$.The proposed Cyber-VE components by [44] will be used as our references in order to classify traces. The components consist of attacker, motivation, intention, method, tools, medium, target, and impact. While, attributes consist of individual, group, organization, ideology, extreme belief, objective, harm, violent, weapon, social media, digital form, publication, cyberspace, traditional space, public, target place, physical, psychological, social, economic, and emotional.

4.2 Cyber-VE Behavior Identification

After completing the data extraction and classification process, the next process is to identify Cyber-VE behavior. The process is represented in Figure 3.

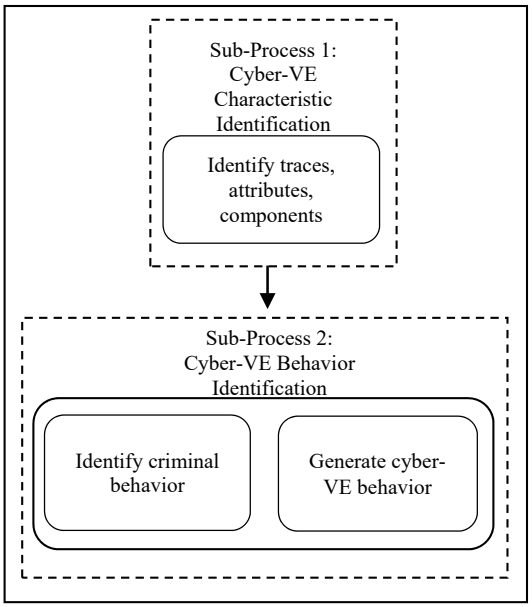

Figure 3: Sub-processes in Cyber-VE behavior identification process

Figure 3 presents two sub-processes which are Cyber-VE characteristic identification and Cyber-

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

VE behavior identification. In the first sub-process, Cyber-VE trace pattern will be generated as it can be representing the activities of Cyber-VE. The purpose of this sub-process is to identify the details about how the Cyber-VE attack happened. This sub-process also will determine the characteristics of Cyber-VE attack. The conceptual of criminology theories is reviewed in order to understand about the criminal behavior. Using social learning theory and space transition theory, four conceptual components consists if motive, method, tools, and medium are used in understanding about criminal behavior. Then, the process of generating Cyber-VE behavior is conducted.

4.3 Cyber-VE Profile Construction

Move into the next process is to construct Cyber-VE profile. The process is depicted in Figure 4.

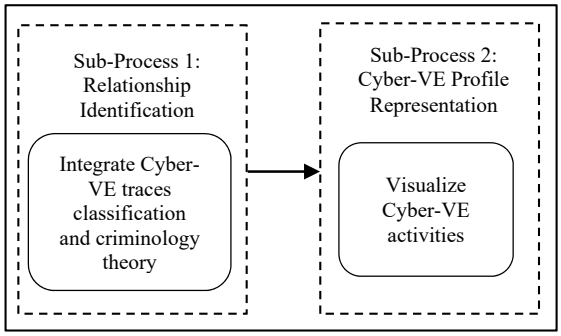

Figure 4: Sub-processes in Cyber-VE profile construction process

Table 1: Eight major categories for Cyber-VE profile

Category	Explanation
Potential attacker	The person who commit, support, promote, and encourage the attack
Motivating factor	Attacker motive for the attack
Aim of attack	Intention to do certain things either good or bad
Tools of action	Tools used to commit, support, promote, and encourage the attack
Method of action	Illegal and unlawful acts taken to carry out the attack
Medium of communication	The medium used to commit, support, promote, and encourage the attack
Target involved	The person targeted by the attack
Attack impact	The consequences of the attack to the target

From Figure 4, the first sub-process starts by integrating the Cyber-VE traces classification and criminology theory. The purpose of this sub-process is to determine the relationship between them. Both traces classification and criminology theory were first gathered together to identify the common categories under which components, attributes, and traces found could be classified. Then, the categories which emerged were suitably titled as the major categories contributing to the final profile of Cyber-VE. Thus, all the components, attributes, and traces found were classified under eight major categories as shown in Table 1.

The next sub-process is to visualize Cyber-VE activities. The Cyber-VE profile is presented in the form of figure.

5. ANALYSIS AND FINDINGS

The data used consists of the potential extremist's website known as "Dark Web". Dark web known as a place where extremist organization and their sympathizers exchange ideology, spread propaganda, recruit members, and even plan attacks. As this research only focus on Malay and Indonesia Language, any irrelevant websites are removed. The website covered from 2014 until 2016 in order to be considered relevant to contemporary anti-extremist efforts [7]. The validity and generalizability of our results are subject to assumption about this data. First, we assume that web sites that we refer to contain valid content. Second, as we limit out dataset to Malay and Indonesian languages and the data is from year 2014 to 2016 so the text consist in the websites are in the context of these languages and years. The description of each dataset (DS) are depicted as in Table 2.

Table 2: Description of Dataset (DS)

Dataset (DS)	Description
DS1	Website Type: Forum Website Website Name: Anonymous W1 URL: Anonymous U1
DS2	Website Type: Web Blog Website Name: Anonymous W2 URL: Anonymous U2
DS3	Website Type: Forum Website Website Name: Anonymous W3 URL: Anonymous U3

From Table 2, it shows DS1 and DS3 are classified as forum website while DS2, DS4, and DS5 are classified as web blog types. Information of the websites is hidden due to sensitive issues. All these DS will be used in order to generate Cyber-VE traces classification and indirectly identify Cyber-VE activities. In order to identify Cyber-VE traces, term frequency (TF) is used to trace traces from the website. In this paper, traces are known as a keyword that usually used by the extremist groups. The lists of traces for each DS are listed in Table 3. However,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

due to the sensitive data, the keyword traced in this paper is represented as k_1 to k_{n+1}.

Table 3: Traces identification for DS1, DS2, and DS3

Dataset (DS)	Keywords
DS1	k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}, k_{11}, k_{12}, k_{13}, k_{14}, k_{15}, k_{16}, k_{17}, k_{18}
DS2	k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}, k_{11}, k_{12}, k_{13}, k_{14}, k_{15}, k_{16}, k_{17}, k_{18}
DS3	k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}, k_{11}, k_{12}, k_{13}, k_{14}, k_{15}, k_{16}, k_{17}

Table 3 shows traces found in each DS using term frequency (TF) technique. Using these traces, the process of classifying traces into Cyber-VE attributes and components are conducted. The aim of this process is to get the relationship between traces found. The example of traces classification for DS1 is shown in Table 4.

Table 4: Traces classification for DS1

Components	Attributes	Traces	Frequency
Attacker	Group	k_1	5
		k_2	2
	Organization	k_3	26
Motivation	Ideology	k_4	38
	Extreme belief	k_5	10
		k_6	11
Intention	Harm	k_7	8
Method	Violent	k_8	4
Tools	Social media	k_9	3
Medium	Cyberspace	k_{10}	2
Target	Group of people	k_{11}	4
	Target Place	k_{12}	2
		k_{13}	4
		k_{14}	13
		k_{15}	13
Impact	Physical	k_{16}	2

Table 4 shows the process of classifying traces into Cyber-VE components and attributes for DS1. In attacker component, k_1 and k_2 are classified as group attribute and k_3 is classified as organization attribute. For motivation component, k_4 is classified as ideology attribute. While, k_5 and k_6 are classified as extreme belief attribute. Table 4 also shows intention component consists of harm attribute which referred to the keyword k_7. For method component, k_8 is one of keyword found that usually used by the extremist groups. K_9 is classified as violent attribute and method component. In medium component, k_{10} is classified as cyberspace attribute. For target component, k_{11} is classified as group of people attribute while k_{12}, k_{13}, k_{14}, and k_{15} are classified as target place attribute. Lastly, k_{16} is keyword that classified as physical attribute and impact component. Then, the Cyber-VE traces classification for DS1 is constructed as shown in Figure 5.

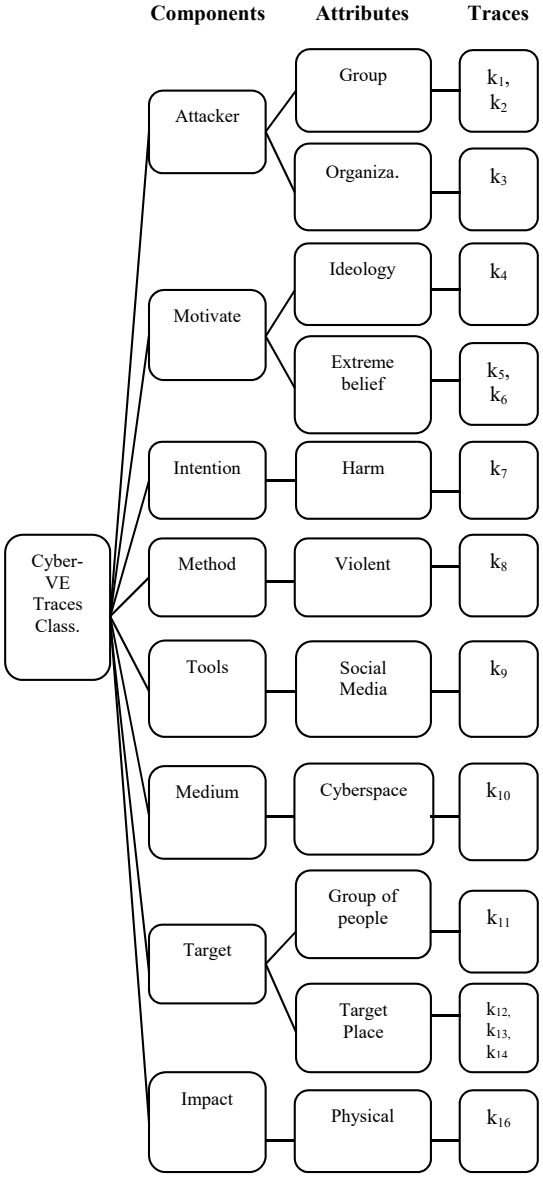

Figure 5: Cyber-VE traces classification for DS1

Figure 5 shows Cyber-VE traces classification for DS1 consist components, attributes, and traces extracted. The components are attacker, motivation, intention, method, tools, medium, target, and impact. While, the attributes are group, organization, ideology, extreme belief, harm, violent, social media, cyberspace, physical, group of people, target place, and physical. This traces classification indicates the activities of Cyber-VE. In order to identify Cyber-VE behavior, the causes that leads to criminal behaviors is identified. Then, the behavior

Journal of Theoretical and Applied Information Technology
31st August 2018. Vol.96. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of Cyber-VE is generated based on traces classification and criminology theory. In order to construct Cyber-VE profile, this research proposed to integrate between the Cyber-VE trace pattern and criminology theory as shown in Figure 6.

Figure 6 shows the integration between Cyber-VE traces classification and criminology theory. Based on this proposed profiling framework, this research represents Cyber-VE profile in the form of figure as shown in Figure 7.

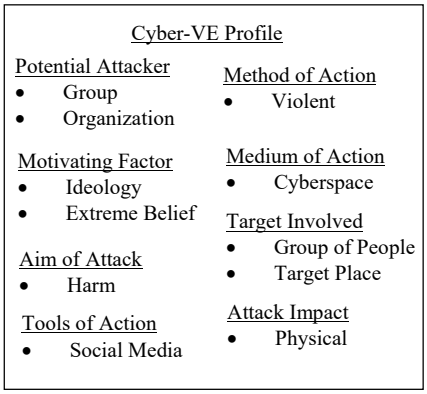

Figure 7: Cyber-VE profile

Figure 7 shows the profile of Cyber-VE under eight major categories. The categories are potential attacker, motivating factor, aim of attack, method of action, tools of action, medium of action, target involved, and attack impact. In potential attacker component, three attributes are found which are group and organization. While in motivating factor component, ideology and extreme belief attributes are found. Harm and violent attributes was found in aim of attack and method of action component respectively. Besides, in tools of action component, the attribute found is social media. While, medium of action consists of cyberspace attribute. Target component consists of group of people and target place attributes. Lastly, for attack impact component, physical is one of the attribute.

Profile Identification

The capabilities of the proposed profiling framework are evaluated to determine either Cyber-VE profile can be identified or not (*Profile Identification*). To achieve it, the major categories needs to be identified first either it found or not during the integration process (*Category Identification*) as the major categories are contributing to the final profile of Cyber-VE. Based on the eight major categories consists of Potential Attacker, Motivating Factor, Aim of Attack, Tools of Action, Method of Action, Medium of Communication, Target Involved, and Attack Impact, the result of *Profile Identification* and *Category Identification* for DS1, DS2, DS3 is shown in Table 5.

Table 5: Result of Profile Identification for DS1, DS2, and DS3
(√ = Category Found, X = Category Not Found)

DS	Category								Cyber-VE Profile Identification (Y= Yes, N=No)
	Potential	Motivating	Aim of Attack	Method of	Tools of Action	Medium of Communication	Target Involved	Attack Impact	
DS1	√	√	√	√	√	√	√	√	Y
DS2	√	√	√	√	√	√	√	√	Y
DS3	√	√	√	√	√	√	√	√	Y

Table 5 shows the results of Category Identification for DS1, DS2, and DS3 which all the major categories are found in all DS. It can be concluded all the major categories are used to describe about the activities of Cyber-VE. It also indicates that these major categories are important in providing the specific information about the attacker who commits Cyber-VE attack. Besides, it indicates that Cyber-VE profile is identified using the proposed profiling framework.

6. DISCUSSION AND FUTURE WORK

From the analysis and findings, this research found the proposed profiling framework is capable to profile Cyber-VE activities and able to identify any activities that related to Cyber-VE attack. It also proves that by using Social Learning Theory and Space Transition Theory, it can contribute better understanding about the causes of Cyber-VE attack. Consistent with the theory, the results indicate that due to the ideology and extreme belief that has been spread through social media, it motivates and create inspiration to the people who has exposed about extremist's motive. Through Internet, people can learn and develop their skills on how to conduct Cyber-VE attack. The finding also supports both theories as extremists use cyberspace to plan an attack and launch it in physical space. In the future, we aim to conduct an interview with the experts to validate and to obtain their opinion and insight on the proposed framework.

7. CONCLUSION AND FUTURE WORK

This paper proposes Cyber-VE profiling framework consists of three main processes which are data extraction and classification, Cyber-VE

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

behavior identification, and Cyber-VE profile construction. In order to achieve it, this paper integrates between Cyber-VE traces classification and criminology theory. This research used Dark Web as our dataset in order to identify the activities of Cyber-VE. Our findings indicate that by developing this profiling framework, it can assist the forensic investigators in identifying any activities that related to Cyber-VE attack. Using this proposed profiling framework, Cyber-VE attack can be profile.

ACKNOWLEDGEMENT

Authors are grateful to INSFORNET Research Group, C-ACT, Fakulti Teknologi Maklumat & Komunikasi, Universiti Teknikal Malaysia Melaka and this work is funded by CyberSecurity Malaysia through the Industry Research Grant Scheme [GLUAR/CSM/2016/FTMK-CACT/I00013].

REFERENCES

[1] Quintero, C. E. (2014). A Typology of Homegrown Terrorists. Electronic Theses, Projects, and Dissertations. Paper 109.

[2] Robyn T. (2010), "Make A Bomb in Your Mums Kitchen": Cyber Recruiting and Socialisation of 'White Moors' and Home Grown Jihadist, Australian Counter Terrorism Conference School of Computer and Information Science, Edith Cowan University Perth, Western Australia, pp. 54–61.

[3] Overbey, L. A., McKoy, G., Gordon, J., & McKitrick, S. (2010). Automated sensing and social network analysis in virtual worlds. In Intelligence and Security Informatics (ISI), 2010 IEEE International Conference on (pp. 179-184). IEEE.

[4] O'Rourke, S. (2007). Virtual radicalisation: Challenges for police, Proceedings of The 8th Australian Information Warfare and Security Conference, pp. 29-35.

[5] Weimann, G. (2012), Lone wolves in cyberspace, Journal of Terrorism Research, Vol. 3(2), pp. 75-90.

[6] Jacob R. S. and Matthew S. G. (2015), Forecasting Violent Extremist Cyber Recruitment, IEEE Transactions on Information Forensics and Security, Vol. 10(11), pp. 1- 10.

[7] Jacob R. S. and Matthew S. G. (2014), Automatic detection of cyber-recruitment by violent extremists, Scanlon and Gerber Security Informatics 2014, Vol.3 (5), pp. 1-10.

[8] Lisa R. Wulan, (2011), ENHANCING THE ROLE OF WOMEN IN INDONESIA TO COUNTER TERRORISM, pp. 1-14.

[9] Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtenson, C., & Svenson, P. (2012). Analysis of weak signals for detecting lone wolf terrorists. In Intelligence and Security Informatics Conference (EISIC), 2012 European (pp. 197-204). IEEE.

[10] Crelinsten, R. (2014). Perspectives on Counterterrorism: From Stovepipes to a Comprehensive Approach. Perspectives on Terrorism, Vol.8(1).

[11] Zeiger, S., & Aly, A. (2015). Countering Violent Extremism: Developing an Evidence-base for Policy and Practice. Curtin University.

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

[13] Haynes, C., & Mangas, J. (2015). Countering extremism: an understanding of the problem, the process and some solutions (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

[14] Fenstermacher, L., Leventhal, T., & Canna, S. (2011), Countering Violent Extremism: Scientific Methods & Strategies, AIR FORCE RESEARCH LAB WRIGHT-PATTERSON AFB OH, pp. 1-206.

[15] Ganor, B. (2009). Trends in modern international terrorism. In To Protect and To Serve (pp. 11-42). Springer New York.

[16] Ramakrishna, K., 2015. Islamist terrorism and militancy in Indonesia: The power of the manichean mindset,

[17] Khan, M. M. (2015). Understanding and Identifying Violent Extremism. Institute of Strategic Studies (ISSI) Issue Brief.

[18] Yulei Z., Shuo Z., Li F., Yan D., Catherine A. L., and Hsinchun C. (2009), Dark Web Forums Portal: Searching and Analyzing Jihadist Forums, Intelligence and Security Informatics, 2009, pp.71-76.

[19] Sachan, A. (2012, July). Countering terrorism through dark web analysis. In Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on (pp. 1-5). IEEE.

[20] Sujoyini M. and Ee P. L. (2008), Second life: Limits of creativity or cyber threat? Proc. IEEE Conf. Technol. Homeland Secur, pp. 498–503.

[21] Douglas, J. E., Ressler, R. K., Burgess, A. W., & Hartman, C. R. (1986). Criminal profiling from crime scene analysis. Behavioral Sciences & the Law, Vol.4(4), pp401-421.
[22] Rashmi S. (2014). Profiling a Cyber Criminal. International Journal of Information and Computation Technology,Vol.4(3), pp. 253-258.
[23] Oxford dictionary. (2015), Available at: http://www.oxforddictionaries.com/ [Accessed October 30th 2015].
[24] Cambridge Dictionary (2016). Available at: http://dictionary.cambridge.org/ [Accessed January 10th 2016]
[25] Alazab, M., 2015. The Journal of Systems and Software Profiling and classifying the behavior of malicious codes. , 100, pp.91–102.
[26] Selamat, S. R., Yusof, R., Sahib, S., Mas' ud, Z., Abdollah, M. F., & Zainal Abidin, Z. (2010). Advanced trace pattern for computer intrusion discovery. Journal of Computing, 2(6), 200-2007.
[27] Selamat, S. R., Yusof, R., Sahib, S., Roslan, I., Abdollah, M. F., & Mas' ud, M. Z. (2011). Adapting Traceability in Digital Forensic Investigation Process.
[28] Selamat, S. R., Salleh, N. M., Yusof, R., & Sahib, S. (2015). 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)
[29] Gennaro F. V., Jeffrey R. M., Ronald M. H. (2005). Criminology: Theory, Research, and Policy (Second Edition).
[30] Lilly, Robert J., Francis T. Cullen, Richard A. Ball. (2007). Criminological Theory: Context and Consequences (4th ed.). Thousand Oaks, CA: Sage Publications.
[31] Tania. (2014). Criminology Theories: The Varied Reasons Why People Commit Crimes. Available at: https://blog.udemy.com/criminology-theories/https://blog.udemy.com/criminology-theories/ [Accessed September 17th 2015]
[32] Ronald L. Akers and Christine S. Sellers. (2013). Criminological Theories: Introduction, Evaluation, Application (Sixth Edition)
[33] Lyman, M. D., & Potter, G. W. (2000). Organized crime. Upper Saddle River, NJ: Prentice Hall. Available at: http://wps.pearsoncustom.com/wps/media/objects/6904/7070214/CRJ455_Ch02.pdf [Accessed September 17th 2015]
[34] Wada, F., Longe, O., & Danquah, P. (2012). Action Speaks Louder than Words-Understanding Cyber Criminal Behavior Using Criminological Theories. Journal of internet banking and commerce, Vol.17(1), 1.
[35] Paternoster, R., & Bachman, R. (2001). Explaining criminals and crime. Los Angeles: Roxbury. Available at: http://www.rbtaylor.net/pub_paternoster_2001.pdf [Accessed October 17th 2015]
[36] Marsh, I., Cochrane, J., & Melville, G. (2004). Criminal justice: An introduction to philosophies, theories and practice. Psychology Press.
[37] Jonathan D. Alston, "The Serial Rapist's Spatial Pattern of Target Selection," in Godwin, 2001
[38] Siddiqi, S., & Sharan, A. (2015). Keyword and keyphrase extraction techniques: a literature review. International Journal of Computer Applications, 109(2).
[39] Steven B. (2015). Important Theories in Criminology: Why People Commit Crime.
[40] Rogers, M. K. (2001). A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study (Doctoral dissertation, University of Manitoba).
[41] Jaishankar, K. (2007). Establishing a theory of cybercrimes. International Journal of Cyber Criminology, 1(2), 7-9.
[42] Schmalleger, F., & Pittaro, M. (2009). Crimes of the Internet, Pearson Prentice Hall.
[43] Alghamdi, H. M., & Selamat, A. (2012). Topic detections in Arabic dark websites using improved vector space model. In 2012 4th Conference on Data Mining and Optimization (DMO). pp. 6-12, IEEE.Chicago.
[44] Salleh, N. M., Selamat, S. R., Saaya, Z., Ahmad, R., & Masúd, Z. (2016). Identifying Cyber Violent Extremism (Cyber-VE) Components by Exploring Dark Web. International Journal of Computer Science and Information Security, 14(9)
[45] Gadelrab, M. S., & Ghorbani, A. A. (2016). Cyber Criminal Profiling. In Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare (pp. 49-67). IGI Global.
[46] Warikoo, A. (2014). Proposed methodology for cyber criminal profiling. Information Security Journal: A Global Perspective, 23(4-6), 172-178.
[47] Kapetanakis, S., Filippoupolitis, A., Loukas, G., & Al Murayziq, T. S. (2014). Profiling cyber attackers using case-based reasoning.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

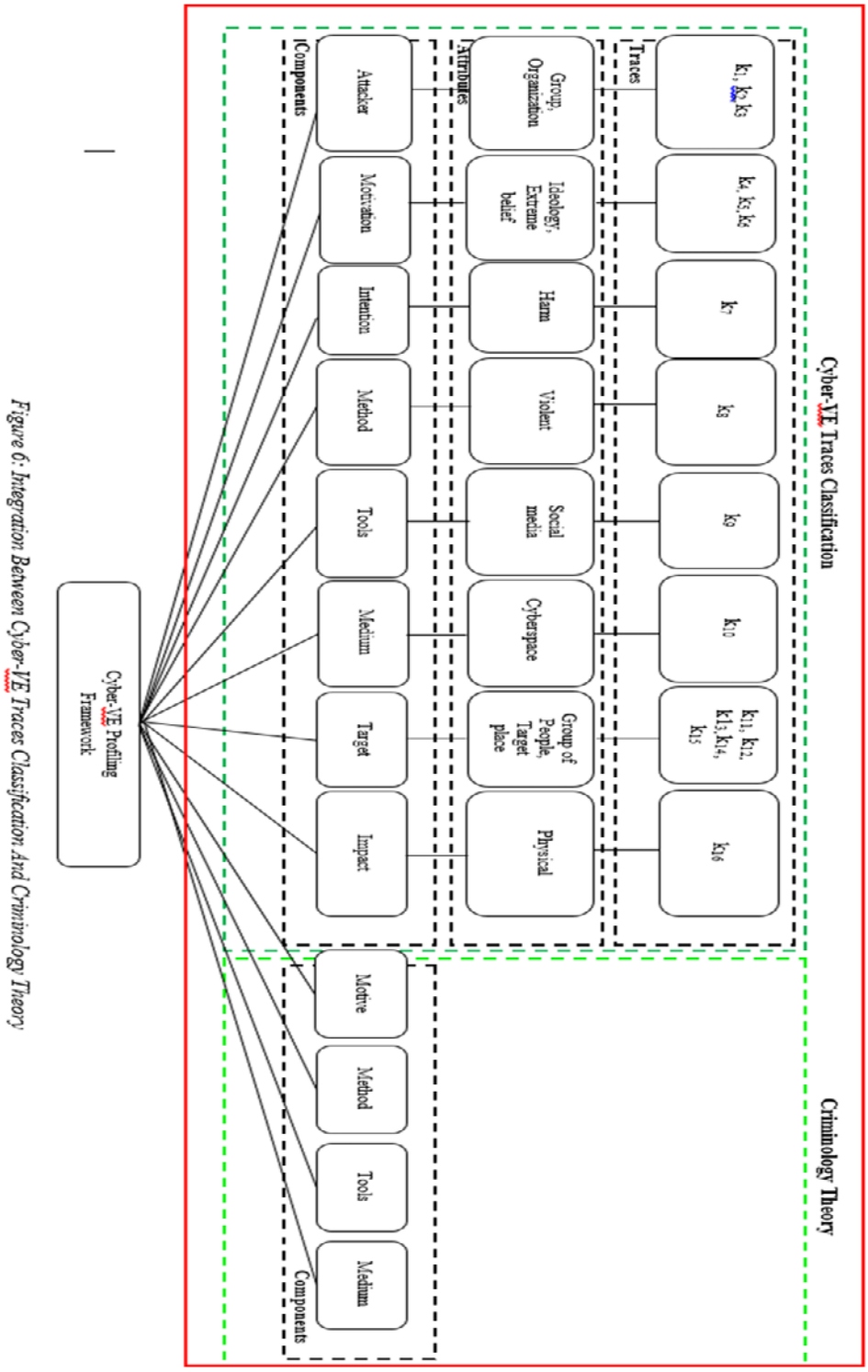

Figure 6: Integration Between Cyber-VE Traces Classification And Criminology Theory