

# A REVIEW ON THE CRIMINOLOGY THEORY IN UNDERSTANDING CYBER VIOLENT EXTREMISM (CYBER-VE)

NM Salleh<sup>1</sup> and SR Selamat<sup>2</sup>

<sup>1</sup>Faculty of Information Technology & Multimedia  
Melaka International College of Science and Technology (MiCoST),  
Wisma Yayasan Melaka, BLOCK C, Lot 925, Jalan Hang Tuah,  
75300, Melaka, Malaysia.

<sup>2</sup>Faculty of Information & Communication Technology  
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian  
Tunggal, Melaka, Malaysia.

Corresponding Author's Email: [nurhashikin@micost.edu.my](mailto:nurhashikin@micost.edu.my)

**Article History:** Received 2 Mac 2022; Revised 19 April 2022; Accepted 30 May 2022

**ABSTRACT:** The Internet and social media are the most powerful tools used by extremists to spread violent extremism (VE) and ultimately cause conflict. This issue has become a global threat that directly impacts Malaysia's security. The threat of Cyber-VE is still on the rise, and the existing counter does not seem to be reducing this attack. As criminology theory is a philosophy used to study the causes of criminal behavior, therefore this research adopted this theory to explain and understand Cyber-VE behavior. This paper reviews and analyze several types of criminology theories and the capability of criminology. From the analysis, two theories have been identified: Social Learning Theory and Space Transition Theory, which consist of motive, method, tools, and medium components. Hence, understanding Cyber-VE behavior will help complement the existing mechanism in tracing Cyber-VE attacks and develop any policy or framework for dealing with it.

**KEYWORDS:** *Cyber Violent Extremism (Cyber-VE), Criminology theory, Behavior, Criminal.*

## 1.0 INTRODUCTION

Violent extremism is a threat to the country as it impacts the politics and economics of the country involved [1]. The growth of information technology has caused multiple problems since the Internet has

provided a medium for an attacker to attack. Extremist groups have expanded their authority through the Internet and social media, intending to recruit new members [2]. These groups focus on online communities and spread their material without relying on traditional media outlets [3]. The statistic reported that the use of web technology to support extremism activities had increased dramatically [4]. These activities are known as Cyber-VE attacks and have become a significant problem due to the lack of a mechanism to identify violent extremism activity. The problem arises when it is impossible to detect and analyze the possible terrorists. These create a challenge in tracing and detecting activities relates to Cyber-VE attacks. As criminology theory is the basic concept for understanding the causes of criminal behavior, this research used this theory to explain and understand cyber-VE behavior. It is essential to identify the possible motivations of all parties involved and a description of the criminal. The remainder of this paper is organized as follows; Section II discusses the related work on Cyber-VE and the criminology theory, Section III presents the classification of criminology theory components, Section IV discusses the discussion and findings, and Section V concludes and summarizes future directions of this work.

## **2.0 RELATED WORK**

In this section, Cyber Violent Extremism (Cyber-VE) and criminology theory are explained.

### **2.1 Cyber Violent Extremism (Cyber-VE)**

Cyber-VE is an individual, group, or organization that puts their ideology, extreme belief, or objective into violent action with the intent to cause harm to the target by using cyberspace as their domain [5]. This attack brings a severe threat to international peace and security as it can cause the target to become panic, fear, anxiety, chaos, and grief [6]. The violent extremism attack has resulted in the death of a civilian, including women and children [7]. It could disrupt an established authority as they act with the specific goal of influencing public opinion or inciting political change [8]. [9] stated that the method used by the extremist group could be in terms of threats, suicide bombing, or car bombing attacks. World Health Organization Geneva also revealed that extremist action covers a wide range of acts, going beyond physical acts to threats and intimidation. [10] and [11] explored that bombings are one of the methods used by violent extremist groups. People are willing to bomb themselves to achieve their extreme beliefs [12]. In addition, their activities are not always violent acts but include crimes

such as money laundering, weapons trade, and other minor criminal offenses [13]. Internet-enabled extremists connect and communicate with other extremists and provide verification in terms of identification through this online community [14]. Using cyber communities enables violent extremist groups to spread the materials, recruit and train members, exchange ideology, and even plan an attack.

## **2.2 Criminology Theory**

Criminology theory is the theory use to study crime [15]. It refers to the origins of criminal behaviors, either individual or groups of people, and it has been a general theory of criminal behavior [16]. Generally, criminology theories assist in understanding why criminals commit crimes to achieve their goals [17]. It explores the causes that lead to criminal behavior and the factors contributing to the crime [18]. According to [19], criminology theory is the basic concept for understanding the causes of criminal behavior. This theory considers the characteristics of individuals and a society that results in crime. Criminology theory will give direction to researchers and provide a framework for understanding the significance of knowledge acquired about crime in the past. Criminology is used to study the criminal, why individuals commit crimes, and why they behave in certain situations. Understanding why a person or group commits a crime will help develop a way to control, handle, and prevent the criminal [17]. Criminology theory is essential for developing any policy, framework, or treatment for dealing with criminals. This role will help make predictions about the criminal that can be used as a technique to deal with criminals [20]. [21] using the existing criminological theories will help develop a better understanding of the causes and possible measures against cyberbullying.

## **3.0 CLASSIFICATION OF CRIMINOLOGY THEORY COMPONENTS**

Rational choice theory was introduced in the 1970s by [22] when exact crimes producing traits and factors that can be found and treated began to reduce. Rational choice theory argues that the offender makes a rational choice to commit the offense. The offender has weighed the benefits of the crime against the cost of being caught and punished. This theory states that a choice is made during the commission of a crime, whether to continue or not. The offender must weigh the benefits of the next step with the punishment if caught. [23] also uses the rational choice theory to elaborate on people that are entirely rational when deciding to commit a crime. [24] agreed, an individual

decision to commit a crime is based on the cost and benefit proportion. Rationality means that an individual balances cost and benefit to determine an action that maximizes personal benefit. [25] added rational choice theory is one approach that can handle cognitive and behavioral factors and situational factors. [26] has combined rational choice theory and self-control theory to explain cyberbullying perpetration. The rational choice theory states that deviant behavior results from an assessment of costs and benefits whereby the benefits outweigh the costs, while self-control theory is used to determine why some youth make the rational decision to cyberbully while others do not. Self-control theory assumes that engagement in deviant behavior depends on a person's extent of self-control [26]. It has been supported by [27] using rational choice theory to prevent cyberbullying. [19] agreed people make a fundamental decision to commit a crime or not based on a simple cost-benefit analysis. This theory focuses on non-sociological factors that can influence the decision of a criminal to commit a crime. Rational choice theory helps to focus on the individual's decision and control over who they are and what they will be.

A routine activity theory is a theory that was developed by [22] that explain the increase in the rate of property and predatory crimes. This theory states crime is normal and it just needs opportunity to happen. Crime happens when three things are gathered which are the offenders must be motivated, there must be a suitable target and there must be the absence of a capable guardian. A capable guardian could be to protect the target or is the guardian of the offender; for example, parent or teacher. [22] argued crime happens when there is a convergence in space and time between a motivated offender, a suitable target, and an absence of a capable guardian. Routine activities theory help to predict the risk of victimization according to the victim's lifestyle, behavior, and demographic characteristics. [21] and [19] has explained more about routine activity theory. For a crime to be committed, there are some criteria must be concurrently present. First is a suitable target must be available. The suitable target could be person, object, or place.

Second is the lack of a guardian to prevent the crime from happens. The guardian refers to a deterrent, security guards, neighborhood watch, door staff, vigilant staff and coworkers, friends, neighbors and CCTV systems. Lastly is motivated offender being present. There can be no victim without the intentional actions of another individual [19]. It has been supported by [28] who used routine activities theory to explain the specific behavior of cyberbullying. While, [29] stated this theory found to be relevant to Nigerian cybercrime. Routine activities

theory states if target is attractive enough, crime will happen [17]. [30] exposed that the reason for criminal behavior is related to the connection between society and the individual. More than that, it is more influential and motivating for someone to become a criminal and pick crime as a career if that person is identified as a criminal from an early age. While [31] explained social theory as one of the criminology theories used to understand how people act and what should be done about those actions. [32] stated social theory focuses on learning also criminal techniques and the role of drivers, motives, and rationalizations. This theory also applies to understanding other types of non-traditional crimes, such as computer crime [32]. The social theory showed that criminality is a function of individual socialization.

[33] explained that social theory explains specific phenomena based on behaviorism and phenomenology. [30] introduced social control theory as a theory used to exploit the socialization and social learning process, builds self-control, and reduces the inclination to indulge in behavior recognized as antisocial. This theory focuses on society's role in controlling criminal behavior. Social control theory focuses on the fact that most delinquent behavior results from unmonitored social control of the authorities and the family. For example, very little crime is committed by young children because they are constantly under adult control compared to adolescents and young people who are free from adult control. As a result, those who experience less social control tend to engage in cybercrimes.

Social learning theory is a general theory that explains the acquisition, maintenance, and change in criminal and deviant behavior that embraces social, nonsocial, and cultural factors operating to motivate and control criminal behavior and promote and undermine conformity [34]. Social learning theory explains that people learn new behavior through observational learning of the social factors in their environment [35]. This theory explained that people could learn further information and behaviors by watching others [35]. If individuals observe positive, desired outcomes in the observed behavior, they are more likely to model, imitate, and adopt the behavior themselves. [36] suggested that individuals who associate with deviant peers will be more likely to encourage them to commit a crime, and the anticipated rewards and punishments reinforce these. [36] added whether the individuals can learn the illegal behaviors depends on their characteristics, the offenders' characteristics through the people who have been observed, and on the consequences who follow the offenders' behaviors.

Besides, [37] stated that social learning theory views the learning process as operating within the context of interactions, social structure, and situations. [37] also suggested that the conforming or criminal behavior resulting from the learning process is a function of reinforcement and other variables associated with the social learning process. [38] Social learning theory is based on operant conditioning and observational learning principles. The operant conditioning uses reinforcements and punishments to explain how to learn the characteristics through positive and negative reinforcement. Positive reinforcement involves receiving something suitable for an action that reinforces or encourages the behavior to be repeated. While negative reinforcement consists of removing a burden or something terrible, when a particular behavior is reproduced, this again reinforces that behavior to be repeated. Based on these principles, social learning theory would expect most criminals who commit a second crime to have committed the same crime twice, rather than two different crimes. Social learning theory has significant intrinsic value for understanding cybercrime. The offenders not only learn how to operate with equipment but also its specific procedures, programming, and techniques for using the computer illegally [38]. Social learning theory explains that if the person observes other people's behavior either in terms of what they do and how they do it or what they say and say it, it may affect whether the person is imitated or not. In the crime aspect, this theory clarifies that people can learn new information and behavior by only watching other people [19]. It has been supported by [39], who claimed this theory is appropriate to explain the new forms of deviance like cyberbullying. It is true that the social learning theory will help to explain how people's associations with other criminals help them to develop the motivation and skills to commit crimes [40].

In 2007, [41] introduced space transition theory to explain the causation of crimes in cyberspace. A space transition theory explains the nature of the behavior of the persons who bring out their conforming and non-conforming behavior in the physical space and cyberspace [42]. The space transition theory involves the movement of persons from one space to another, for example, from physical space to cyberspace and from cyberspace to physical space. It also states that criminal behavior in cyberspace is likely to be imported to physical space, which in physical space may also be exported to cyberspace. Virtual space provides the space where an individual can express his feelings and even give out his anger against anyone. Cyberstalking and cyber defamation are examples where offenders use cyberspace because of its anonymity and widespread approach. This theory states that people who endure criminal behavior in the physical space tend to commit a



crime in cyberspace; otherwise, they would not commit in physical space due to their status and position. [43] added space transition theory does not explain physical crime but only focuses on cybercrime. This theory understands how people move and behave from one space to another. It requires persons with repressed criminal behavior in the physical space tending to commit a crime in cyberspace.

[44] have introduced opportunity theory to be used to assist in understanding the crime. Opportunity theory is a theory that not only focuses on the events but also on the opportunities that emerged and contributed to crime. [44] argued that crimes transverse between location, time, target, direction, and method of committing the crime. This theory states that the opportunity to commit a crime is a root cause of crime. This theory also states that no crime can occur without physical opportunity. Therefore, opportunity plays a role in all crimes, not just those involving physical property, thereby reducing the opportunity of crime. [45] explained more about crime opportunity theory which states a person intends to commit a crime, but the crime can be barred by solid determination. Another theory is the crime displacement theory, which focuses primarily on reducing the opportunity to commit a crime. The efforts tend to displace or move the crime from one location to another [44]. Crime displacement theory may involve:

- Geographical Movement: Moving crime from one location to the other;
- Temporal Movement: Moving crime from one time to the other;
- Target Movement: Changing the approach to committing the crime from one to the other; and
- Crime Type: Changing the type of crime that is to be committed.

On the other hand, the deindividuation theory proposed by [46] explained that the individual's immersion within a group results in a loss of self-identity and, ultimately, a behavior that the group represents. It could be ideal for cyber criminals who find themselves on the Internet without an identity and as part of a group who indulge in cybercrime. [27] used uses and gratifications theory as a theoretical theory in understanding cyberbullying perpetration. Another theory is a technology, which relies on using cryptography, steganography, network protocols, and software engineering process to develop systems that offer some form of protection for users and the

information infrastructure [47]. Previous researchers have applied criminology theories to understand crime activities and the behavior of criminals. These findings summarize each theory's concepts and potential conceptual components, as shown in Table 1.

Table 1: Summarization of Criminology Theories

Criminology Theories	Researchers	Concepts	Potential Conceptual Components
Rational Choice Theory	[44]	<ul style="list-style-type: none"> <li>•The offender makes a rational choice to commit the offense by weighted up the benefits of the crime against the cost of being caught and punished.</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> <li>•Impact</li> </ul>
	[48]	<ul style="list-style-type: none"> <li>•Offender are completely rational when making the decision to commit a crime.</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> </ul>
	[49]	<ul style="list-style-type: none"> <li>•Individual decision to commit crime is based on the cost and benefit proportion.</li> <li>•Individual balances cost and benefits to arrive at action that maximizes the personal benefit.</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> <li>•Impact</li> <li>•Objective</li> </ul>
	[36]	<ul style="list-style-type: none"> <li>•The deviant behavior is the result of an assessment of costs and benefits whereby the benefits outweigh the costs</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> <li>•Impact</li> </ul>
	[19]	<ul style="list-style-type: none"> <li>•People make a basic decision to commit a crime or not based on a simple-cost benefit analysis</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> <li>•Impact</li> </ul>
	[40]	<ul style="list-style-type: none"> <li>•People make decision to commit crime after taking some consideration about risks including caught and punished.</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> <li>•Impact</li> </ul>
Routine Activities Theory	[44]	<ul style="list-style-type: none"> <li>•Crime is normal and it just needs opportunity to happen.</li> <li>•Crime happens when three things are gather; the offender must be motivated, there must be a suitable target, and there must be the absence of a capable guardian.</li> </ul>	<ul style="list-style-type: none"> <li>•Opportunity</li> <li>•Offender</li> <li>•Motive</li> <li>•Target</li> <li>•Guardian</li> </ul>
	[26]	<ul style="list-style-type: none"> <li>•For a crime to be committed, there are some criteria must be concurrently present. The criteria:                             <ul style="list-style-type: none"> <li>i-The suitable target must be available and it could be person, object, or place.</li> <li>ii-The lack of guardian to prevent crime from happen.</li> <li>iii-Motivated offender being present.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>•Target (person, object, or place)</li> <li>•Guardian</li> <li>•Offender</li> <li>•Motive</li> </ul>
	[17]	<ul style="list-style-type: none"> <li>•If target is attractive enough, crime will happen.</li> </ul>	<ul style="list-style-type: none"> <li>•Target</li> </ul>



Social Theory	[30]	The reason of criminal behavior is relate to the connection between society and individual. If an individual is already labelled as a criminal from his young age, then it will motivate that individual to become a criminal.	Criminal
	[32]	<ul style="list-style-type: none"> <li>•This theory is not only focuses on the learning of criminal techniques but also the role of drivers, motives, and rationalizations.</li> </ul>	<ul style="list-style-type: none"> <li>•Skills</li> <li>•Motives</li> <li>•Offender</li> </ul>
	[48]	<ul style="list-style-type: none"> <li>•Criminal is a function of individual socialization.</li> <li>•The interactions people relate to organizations, institutions, and process of society.</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> </ul>
Social Control Theory	[30]	<ul style="list-style-type: none"> <li>•Stress on the role of society in the control of criminal behavior.</li> <li>•This theory stresses on the fact that most delinquent behavior is the result of unmonitored social control by the authorities and primarily; like family</li> </ul>	<ul style="list-style-type: none"> <li>•Criminal</li> <li>•Society</li> </ul>
Social Learning Theory	[35]	<ul style="list-style-type: none"> <li>•People learn new behavior through observational learning of the social factors in their environment.</li> <li>•People can learn new information and behaviors by watching other people</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> <li>•Skills</li> </ul>
	[36]	<ul style="list-style-type: none"> <li>•Individuals can learn the illegal behaviors are depends on:                             <ul style="list-style-type: none"> <li>i-Their own characteristics</li> <li>ii-The offender's characteristics which through the people who has being observed</li> <li>•iii-The consequences who follow the offender's behaviors</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> <li>•Skills</li> </ul>
	[38]	<ul style="list-style-type: none"> <li>•Offenders must learn not only how to operate an equipment but also specific procedures, programming, and techniques for using the computer illegally.</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> <li>•Skills</li> </ul>
	[19]	<ul style="list-style-type: none"> <li>•If the person observes other people's behavior it may affect the person to imitate.</li> <li>•People can learn new information and behavior by only watching other people.</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> <li>•Skills</li> </ul>
	[40]	<ul style="list-style-type: none"> <li>•How people develop motivation and skills to commit crime through the people they associate it.</li> </ul>	<ul style="list-style-type: none"> <li>•Motivation</li> <li>•Skills</li> </ul>

Space Transition Theory	[42]	<ul style="list-style-type: none"> <li>•Criminal behavior in cyberspace is likely to be imported to physical space which in physical space may be exported to cyberspace as well.</li> </ul>	<ul style="list-style-type: none"> <li>•Medium</li> <li>•Criminal</li> </ul>
Space Transition Theory	[43]	<ul style="list-style-type: none"> <li>•How people move and behave from one space to other space</li> <li>•Persons with repressed criminal behavior in the physical space tending to commit crime in cyberspace.</li> </ul>	<ul style="list-style-type: none"> <li>•Medium</li> <li>•Criminal</li> </ul>
Opportunity Theory	[22]	<ul style="list-style-type: none"> <li>•Crimes transverse between location, time, target, direction, and method of committing the crime.</li> <li>•Opportunity to commit a crime is a root cause of crime</li> </ul>	<ul style="list-style-type: none"> <li>•Opportunity</li> <li>•Time</li> <li>•Target</li> <li>•Method</li> <li>•Location</li> </ul>
Crime Opportunity Theory	[45]	<ul style="list-style-type: none"> <li>•People intent to commit a crime but the crime can be barred by strong determination.</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> </ul>
Crime Displacement Theory	[22]	<ul style="list-style-type: none"> <li>•Focuses primarily on the reduction of the opportunity to commit crime. The efforts tend to displace or move the crime from one location to another location</li> </ul>	<ul style="list-style-type: none"> <li>•Opportunity</li> </ul>
Deindividuation Theory	[46]	<ul style="list-style-type: none"> <li>•The immersion of the individual within a group results in a loss of self-identity and ultimately a behavior that is represented by the group.</li> </ul>	<ul style="list-style-type: none"> <li>•Offender</li> </ul>
Technology Theory	[47]	<ul style="list-style-type: none"> <li>•Rely on the use of cryptography, steganography, network protocols, and the use of software engineering process to develop systems that offer some form of protection for users and the information infrastructure.</li> </ul>	<ul style="list-style-type: none"> <li>•Security</li> </ul>

#### 4.0 DISCUSSION AND ANALYSIS

In the previous study, a few researchers such as [19], [50], [51], and [52] used this criminology theory to study and understand cybercrimes. Based on the analysis in Section 3.0, this research combines social learning theory and space transition theory to explain and understand Cyber-VE behavior. This research aims to understand better the causes that lead to criminal behavior and possible measures against Cyber-VE attacks, as described in the following subsection.

## 4.1 Social Learning Theory

Social learning theory states that people commit crimes by learning a new behavior from watching other people. This theory helps this research focus on how the attackers commit attacks through the people they associate with. In addition, this theory not only focuses on learning techniques but also on the role of drivers, motives, and rationalizations of the attacker. From the analysis, this research has identified several components which is essential to be used to explain and understand criminal behavior. The components are offender, motivation, and skills. In skills components, this research identified there are sub-components which are method, tools, and medium.

## 4.2 Space Transition Theory

A space transition theory is a theory that explains how people move and behave from one space to another space. This theory explains how people like to unite in cyberspace to commit crimes in physical space. The behavior of criminals in cyberspace is likely to be imported into the physical space, and criminal behavior in physical space may also be exported to cyberspace. From this theory, physical space or cyberspace refers to the medium. The significance of social learning theory and the space transition theory is that they focus on how the environment influences criminal behavior and the capabilities of criminals to perform the crime. The combination of these theories is shown in Figure 1.

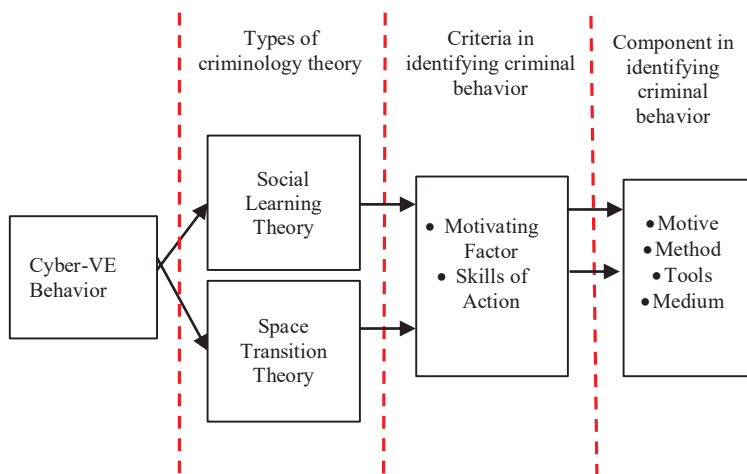


Figure 1: Components in explaining and understanding Cyber-VE behavior

Figure 1 shows the combination of two criminology theories; social learning theory and space transition theory. From these theories, criteria and components in identifying criminal behavior are identified. Criteria are defined as a standard by which something is judged or decided while the component is a part of a process. Two criteria are found; motivating factors and skills of action. While components found are; motive, method, tools, and medium. Using these components will help to identify and analyze the offender, which will directly understand cyber-VE behavior.

## **5.0 CONCLUSION AND FUTURE WORK**

This study examines the existing criminology theories to explain and understand criminal behavior and attempts to apply them to Cyber-VE. This paper provides some insights on how these theories explain the causation of Cyber-VE activities. From the analysis, two theories have been identified: social learning theory and space transition theory, which consists of motive, method, tools, and medium components. Furthermore, the components can be used to assist the forensic investigator in understanding Cyber-VE behavior as it refers to the process of identifying and analysis about the offender. In the future, this research aims to interview experts to gain their opinion and insight on these theories.

## **ACKNOWLEDGMENT**

The authors would like to thank Melaka International College of Science and Technology (MiCoST) and Universiti Teknikal Malaysia Melaka (UTeM) for the support.

## **REFERENCES**

- [1] Georgian Center for Security and Development. (2018). The Roots of Violent Extremism and Radicalization in Azerbaijan and Georgia. [Online]. Available at: <http://library.fes.de/pdf-files/bueros/georgien/14736.pdf> [Accessed 2 March 2021].
- [2] L. A. Overbey, G. McKoy, J. Gordon, and S. McKittrick, "Automated sensing and social network analysis in virtual worlds", 2010 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 179-184, 2010.

- [3] I. Awan, "Cyber-Extremism: Isis and the Power of Social Media, Social Science and Public Policy", *Soc*, vol. 54, pp. 138-149, 2017.
- [4] J. R. Scanlon, and M. S. Gerber, "Forecasting Violent Extremist Cyber Recruitment", *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp.2461-2470, 2015.
- [5] N. M. Salleh, S. R. Selamat, Z. Saaya, R. Ahmad, and Z. Masúd, "A New Taxonomy of Cyber Violent Extremism (CyberVE) Attack" in 2016 6th International Conference on Information and Communication Technology for The Muslim World (ICT4M), 2016, pp. 234- 239.
- [6] M. Nasser-Eddine, B. Garnham, K. Agostino, and G. Caluya, "Countering violent extremism (CVE) literature review", Defence Science and Technology Organisation Edinburgh, Australia, 2011.
- [7] M. Abrahms, M. Ward, and R. Kennedy, "Explaining civilian attacks: Terrorist networks, principal-agent problems and target selection", *Perspectives on Terrorism*, vol. 12, no. 1, pp. 23-45, 2018.
- [8] J. R. Scanlon and M. S. Gerber, "Automatic detection of cyber-recruitment by violent extremists", *Security Informatics*, vol. 3, no. 1, pp.1-10, 2014.
- [9] E. Kohlmann, 2011. *The Anti-Social Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations*. [Online]. Available at: [http://www.foreignpolicy.com/articles/2011/05/23/the\\_antisocial\\_network](http://www.foreignpolicy.com/articles/2011/05/23/the_antisocial_network) [Accessed on 16 September 2016].
- [10] L. R. Iannaccone and E. Berman, "Religious extremism: The good, the bad, and the deadly", *Public choice*, vol. 128, no. 1-2, pp.109-129, 2006.
- [11] K. Ramakrishna, (2014). "*Islamist terrorism and militancy in Indonesia: The power of the Manichean Mindset*", Singapore: Springer.
- [12] C. E. Quintero, (2014). "*A Typology of Homegrown Terrorists*", Master Thesis, California State University, San Bernardino.
- [13] S. Zeiger, and A. Aly. (2015). "*Countering violent extremism: Developing an evidence-base for policy and practice*". Translated from Curtin University.
- [14] C. Haynes and J. Mangas. (2015). "*Countering extremism: an understanding of the problem, the process and some solutions*". Doctoral dissertation, Monterey, California: Naval Postgraduate School.
- [15] F. A. Zuhri. (2017). *Why are Cybercriminals Attracted to Commit Crimes* [Online]. Available: <https://digitalforensicsmagazine.com/blogs/wp-content/uploads/2017/05/Why-Are-Cybercriminals-Attracted-To-Commit-Crimes.pdf> [Accessed 12 November 2017].
- [16] J. D. Alston, (1994). "*The serial rapist's spatial pattern of target selection*" (Doctoral dissertation, Theses (School of Criminology)/Simon Fraser University).

- [16] J. D. Alston, (1994). “*The serial rapist's spatial pattern of target selection*” (Doctoral dissertation, Theses (School of Criminology)/Simon Fraser University).
- [17] Tania, (2014). *Criminology Theories: The Varied Reasons Why People Commit Crimes*. [Online]. Available: <https://blog.udemy.com/criminology-theories/> <https://blog.udemy.com/criminology-theories/> [Accessed 17 September 2015].
- [18] Ronald L. Akers and Christine S. Sellers, *Criminological Theories: Introduction, Evaluation, Application*, Oxford (8th Edition). (2020).
- [19] F. Wada, O. Longe, and P. Danquah, “Action speaks louder than words—understanding cybercriminal behavior using criminological theories”, *The Journal of Internet Banking and Commerce*, vol.17, no. 1, pp.1-12, 2012.
- [20] R. V. Clarke, and M. Felson, “*Introduction: Criminology, routine activity, and rational choice*” in *Routine activity and rational choice*, pp. 1-14, Routledge, New York, 2017.
- [21] S. Veenstra, “Cyberbullying: an explanatory analysis”. Unpublished doctoral thesis. University of Leicester, Leicester, United Kingdom. 2011.
- [22] L. E. Cohen, and M. Felson, “Social Change and Crime Rate Trends: A Routine Activity Approach”, *American Sociological Review*, vol. 44, No. 4, pp. 588-608, 1979.
- [23] J. Ahmad and T. Q. Emeka, (2014). Rational choice theory. *The Encyclopedia of Criminology and Criminal Justice*, pp. 1-5.
- [24] R. Willison and P. B. Lowry, “Disentangling the motivations for organizational insider computer abuse through the rational choice and life course perspectives”, *ACM SIGMIS Database: The database for advances in information systems*, vol. 49, SI, pp. 81-102, 2018.
- [25] H. Li, X. R. Luo, J. Zhang, and R. Sarathy, “Self-control, organizational context, and rational choice in Internet abuses at work”, *Information & Management*, vol. 55, no.3, pp. 358-367, 2018.
- [26] S., Veenstra, (2011). *Cyberbullying: an explanatory analysis*, Translated from University of Leicester, Leicester, United Kingdom.
- [27] T. Tanrikulu, “Cyberbullying from the perspective of choice theory”. *Educational research and reviews*, vol. 9, no. 18, pp. 660-665, 2014.
- [28] C. Lee, (2013). Deviant peers, opportunity, and cyberbullying: A theoretical examination of a new deviance. Translated from Southern Illinois University at Carbondale.
- [29] O. J. Olayemi, “*A socio-technological analysis of cybercrime and cyber security in Nigeria*”, *International Journal of Sociology and Anthropology*, 6(3), pp.116-125. 2014.



- [30] T. Hirschi. (1969). *Key idea: Hirschi's social bond/social control theory in Criminology and Criminal Justice*, (1969), pp. 55-69.
- [31] R. Paternoster. (2001). *Explaining criminals and crime: Essays in contemporary criminological theory*. Roxbury Publishing Company.
- [32] M. K. Rogers. (2001). "A social learning theory and moral disengagement analysis of criminal computer behaviour: An exploratory study", Doctoral dissertation, University of Manitoba.
- [33] J. D. Alston, (1994). "The serial rapist's spatial pattern of target selection", Doctoral dissertation, Theses (School of Criminology)/Simon Fraser University.
- [34] F. T. Cullen, J., Wright K. Blevins. "Taking stock: The status of criminological theory", Transaction Publishers, 2011.
- [35] R. L. Burgess and R. L. Akers, "A differential association-reinforcement theory of criminal behavior". *Social problems*, vol. 14, no. 2, pp. 128-147, 1966.
- [36] R. L. Akers, "Social learning and social structure: A general theory of crime and deviance", Boston, MA: Northeastern University Press, 1998.
- [37] S. A. Mohammed, S. Abdullah, D. Ghawanmeh, and D. Alqaadan, (2020). *Theory of Planned Behavior, Human Capital Theory, and Social Learning Theory Towards Entrepreneurial Intention. The Role of Islamic Perspective Entrepreneurship, An Attempt Towards Discussion: A General-Review Paper*. *International Journal of Management*, 11(11).
- [38] R. L. Akers and G. F. Jensen, *Social learning theory and the explanation of crime* [Online], Available: <http://www.smartalevels.co.uk/Psychology/mod3unit2/2-3-social-learning-theory-as-an-explanation-of-crime.pdf>. [Accessed 7 November 2016] (Eds.), 2011.
- [39] C. Lee, 2013. *Deviant peers, opportunity, and cyberbullying: A theoretical examination of a new deviance*. Southern Illinois University at Carbondale.
- [40] M. Chermak Steven and Jeffrey A. Gruenewald, "Laying a Foundation for the Criminological Examination of Right-Wing, Left-Wing, and Al Qaeda-Inspired Extremism in the United States," *Terrorism and Political Violence*, vol. 27, pp. 133–159, 2015.
- [41] K. Jaishankar, "Establishing a theory of cybercrimes", *International Journal of Cyber Criminology*, vol. 1, no. 2, pp. 7-9, 2007.
- [42] K., Jaishankar, (2008). "Space Transition Theory of cybercrimes". In Schmallerger, F., & Pittaro, M. (Eds.), *Crimes of the Internet*. (pp.283-301) Upper Saddle River, NJ: Prentice Hall.
- [43] F. Schmallegger and M. Pittaro. (2009). *Crimes of the Internet*. Pearson Prentice Hall.

- [44] L.E. Cohen, and M. Felson, “Social Change and Crime Rate Trends: A Routine Activity Approach”, *American Sociological Review*, vol. 44, pp.588–608, 1979.
- [45] D. Y. Chiu, T. T. Chung, and C. S. Wang, “Attacking and Defending Perspective of E-Crime Behavior and Psychology: A Systemic Dynamic Simulation Approach”, *2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC)*, pp. 1035-1039, 2009.
- [46] E. Diener, S. C. Fraser, A. L. Beaman and R. T. Kelem, “Effects of deindividuation variables on stealing among Halloween trick-or-treaters”, *Journal of personality and social psychology*, vol. 33, no. 2, pp.178, 1976.
- [47] F. Wada, O. Longe and P. Danquah, “Action speaks louder than words-understanding cybercriminal behavior using criminological theories”, *The Journal of Internet Banking and Commerce*, vol. 17, no. 1, pp.1-12, 1970.
- [48] A. B. Dechant, (2009). *The psychology of criminal behavior: theories from past to present*. Retrieved from Coastline Journal [Online] Available: <http://coastlinejournal.org/2009/04/13/the-psychology-of-criminal-behaviour-theories-from-past-to-present>.
- [49] D. B. Cornish and R. Clarke, (2010). *Understanding Crime Displacement: An Application of Rational Choice Theory*. In *Classics in Environmental Criminology* (pp. 367-380). Routledge.
- [50] E. R. Leukfeldt and M. Yar, “Applying routine activity theory to cybercrime: A theoretical and empirical analysis”, *Deviant Behavior*, vol. 37, no. 3, pp. 263-280, 2016.
- [51] O. Wori, “Computer crimes: factors of cybercriminal activities”, *International Journal of Advanced Computer Science and Information Technology*, vol. 3, no. 1, pp. 51-67, 2014.
- [52] Vienna. (2013). *Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime*. [Online]. Available: [https://www.unodc.org/documents/organized-crime/unodc\\_ccpcj\\_eg.4\\_2013/cybercrime\\_study\\_210213.pdf](https://www.unodc.org/documents/organized-crime/unodc_ccpcj_eg.4_2013/cybercrime_study_210213.pdf) [Accessed on 16 September 2016].