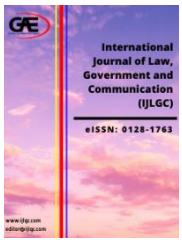
International Journal of Law, Government and Communication
EISSN : 0128-1763
IJLGC
Volume 6 Issue 22 (March 2021) PP. 168-178
DOI 10.35631/IJLGC.6220016



INTERNATIONAL JOURNAL OF LAW, GOVERNMENT AND COMMUNICATION (IJLGC)
www.ijlgc.com

SELECTED THEORIES ON CRIMINALISATION OF HACKING

Ani Munirah Mohamad[1]*, Zaiton Hamin[2], Mohd Zakhiri Md Nor[3], Nurhazman Abdul Aziz[4]

[1] School of Law and Center for Testing, Measurement and Appraisal, Universiti Utara Malaysia, Malaysia
Email: animunirah@uum.edu.my
[2] Faculty of Law, Universiti Teknologi MARA, Malaysia
Email: zaihamin1@gmail.com
[3] School of Law and Legal and Justice Research Center, Universiti Utara Malaysia, Malaysia
Email: zakhiri@uum.edu.my
[4] Office of Entrepreneurship Development, Republic Polytechnic, Singapore
Email: hazman_aziz@rp.edu.sg
* Corresponding Author

Article Info:

Article history:
Received date: 09.11.2020
Revised date: 15.11.2020
Accepted date: 10.12.2020
Published date: 10.03.2021

To cite this document:

Mohamad, A. M., Hamin, Z., Md Nor, M. Z., Abdul Aziz, N. (2021). Selected Theories on Criminalisation of Hacking. International Journal of Law, Government and Communication, 6 (22), 168-178.

DOI: 10.35631/IJLGC.6220016.

Abstract:

Hacking or unauthorised access is criminalised in many jurisdictions, including Malaysia, Singapore, the United Kingdom, Hong Kong, and a few other countries. Hacking is the act of gaining access through the computer system or network without proper authority or exceeding the original authority given to him. Many commentators and researchers have reported on the conceptual and legal aspects of hacking. However, hacking's theoretical, conceptual, and legal aspects have remained under-researched. Therefore, this paper's primary objective is to outline the various theories, which could inform the criminalisation of hacking. The theories of routine activities, deterrence theory, social learning and self-control, general strain theory, and deviant subcultures are deliberated in this paper alongside illustrations within the context of hacking. This paper will shed light on the body of literature and contribute to a better understanding of hacking criminalisation from various theories discussed in this paper. Future research should be directed to provide empirical evidence of applying the theory to hacking criminalisation.

Keywords:

Hacking, Criminality, Routine Activities Theory, Deterrence Theory, Social Learning And Self-Control Theory, General Strain Theory, Deviant Subcultures Theory

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 6 Issue 22 (March 2021) PP. 168-178
DOI 10.35631/IJLGC.6220016

Introduction

Hacking involves attempting to penetrate or tamper with digital devices such as computers, mobile devices and telephones (Scambray et. al., 2000). Moreover, while hacking may not always be for self-gain, nowadays most of the examples to hacking and hackers characterise it as a fraudulent activity by cybercriminals—motivated by monetary benefit, protest, data gathering (spying) and even just the "fun" of the game (Coleman, 2012). Hacking is typically a specialised technical activity (like creating malvertising that deposits malware in a drive-by attack requiring no user interaction). Hackers may use the information to trick people into installing malware or provide stolen information to third parties (Gunkel, 2018).

Cybercriminals can be categorised in computer programming circles as white hats, black hats, and grey hats (Al-Sharif et. al., 2016). Hackers who know how to hack a system to make it even more hack-proof. In most cases, they are under the same umbrella or parent company. Hackers hack to gain control of a computer for personal gain (Gaia, et. al., 2020). They can cause, steal, or prevent the introduction of approved devices into the system. They do this by understanding the unique strengths and weaknesses of the existing system. Some people prefer to call hackers crackers instead (Goerzen & Matthews, 2019).

From the other side of the coin, grey hat hackers are people with enough computer language expertise to hack into a person's system and find vulnerabilities (Goerzen & Matthews, 2019). Black hats are different from grey hats. The former discloses the loopholes in the system, which gets passed on to the system's administrator, while the latter only seek personal benefits. All hacking practises and activities are considered illegal unless done by white hat hackers (Radziwil et. al., 2015).

Nevertheless, the theories behind the criminalisation of hackers are often under-researched. Past research generally investigated the nature and legal position of hacking without diving into its theoretical aspects. Based on this premise, this paper is produced, primarily to address the main objective of outline the selected theories on hacking criminalisation.

In essence, this paper begins with the conceptualisation of hacking and its criminalisation. For this purpose, few jurisdictions are chosen to illustrate the criminalisation of hacking in the nation. Accordingly, five theories are analysed in this paper: (i) routine activities theory, (ii) deterrence theory, (iii) social learning and (iv) self-control, general strain theory and (v) deviant subcultures. The paper concludes by highlighting the future agenda for the criminalisation of hacking and future research recommendations.

Hacking and Its Criminalisation

This part elaborates on the main concepts engaged in this study: hacking and its criminalisation in few selected jurisdictions.

What is Hacking?

Hacking is attempting an unauthorised entry into a computer system. Cracking passwords and clearing security codes allows access to private, protected, and/or over-secured systems (Palmer, 2001). Cracking technique refers to how an encrypted password is discovered. The individual who engages in hacking is called a hacker. The hacking can be done on a single computer, a group of computers, a local area network or a website. The hackers gain access to the system by exploiting the password system (Hamin, 2000).

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 6 Issue 22 (March 2021) PP. 168-178
DOI 10.35631/IJLGC.6220016

Many people and businesses use computers and laptops daily (Harper et al., 2011). Organisations must have access to a variety of resources like computers and the Internet. Because of this, these networks are vulnerable to hackers (Koval, 2015). Hacks are mostly intentional acts for fraudulent or malicious reasons. Misleading information and business disruptions which are socially injurious are a crime (Jordan, 2008).

Ramifications of Hacking

The various ramification of hacking exist. Hackers can gain access to systems using the real usernames and passwords of actual users so that they can alter and manipulate the systems (Beale & Berris, 2017). They can either predict passwords if they use poor or obvious passwords or steal them through fraudulent tactics. Phishing messages are messages sent to trick people into revealing their usernames and passwords which can be sent via e-mail, messaging apps, or other technologies (McClure et al., 2009).

Another common adverse effect of hackers is the stealing of confidential data. Those who hack into systems can access passwords, banking information, personal information, and other sensitive details. They could do this for personal profit or because they are passionate about it (Wilson, 2001).

Theft of data can have severe consequences for entities and people. The inability to secure data will lead to a decline in productivity and growth for the economy. It can also have legal implications whenever the data are covered by both the client and the third party (Buchanan, 2016). Suppose private conversations such as texting or e-mail messages are stolen. In that case, the confidentiality of the individuals involved is at risk.

Similarly, suppose the stolen data contains username and passwords for multiple systems. In that case, the stolen data can be used to access each of these systems (Futter, 2018). If a bank or credit card data is stolen, the information available can be used to make fraudulent transactions or steal money.

It is even possible to damage, both digital and physical equipment physically. Some hackers are capable of damaging their targets deliberately. Also, sensitive information can be inadvertently lost or not saved by hacking tools and hacker applications (Jordan, 2017). Data can be encrypted and kept hostage for ransom if hackers do not receive payment. Hackers may also use remote monitoring and control devices to destroy the target's connected devices.

The Criminalisation of Hacking in Various Jurisdictions

Given the grievous ramifications of hacking, various jurisdictions have outlawed this crime. The laws have been passed to criminalise hacking—this following Table 1 outlines a few selected jurisdictions' initiatives to criminalise hacking:

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 6 Issue 22 (March 2021) PP. 168-178
DOI 10.35631/IJLGC.6220016

Table 1: Laws On Hacking In Selected Jurisdictions

Country	Law	Provision on criminalisation of hacking
Malaysia	Section 3 of Computer Crimes Act 1997	1. Causing a computer to perform any function with intent to secure access to any program or data held in any computer; 2. The access he intends to secure is unauthorised; and 3. Knowledge at the time when he causes the computer to perform the function that is the case.
Singapore	Section 3 of Computer Misuse Act 1993	Any person who knowingly causes a computer to perform any function to secure access without authority to any program or data held in any computers.
Hong Kong	Section 27A of Telecommunications Ordinance 1963	Any person who, by telecommunications, knowingly causes a computer to perform any function to obtain unauthorised access to any program or data held in a computer
Philippines	Section 4 of Cybercrime Prevention Act 2012	The access to the whole or any part of a computer system without rights.
Australia	Section 477.1 of Cybercrime Act 2001	1. Causing any unauthorised access to data held in a computer; 2. The unauthorised access … is caused by means of a telecommunications service; 3. The person knows the access … is unauthorised; and 4. The person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory (whether by that person or another person) by the access.
New Zealand	Section 249 of Crimes Act 1961	Access to any computer system and thereby, dishonestly or by deception, and without claim of right, (a) obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or (b) causes loss to any other person.

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 6 Issue 22 (March 2021) PP. 168-178
DOI 10.35631/IJLGC.6220016

Country	Law	Provision on criminalisation of hacking
United Kingdom	Section 1 of Computer Misuse Act 1990	1. Causing a computer to perform any function with intent to secure access to any program or data held in any computer 2. The access he intends to secure is unauthorised; and 3. Knowledge that at the time when he causes the computer to perform the function that that is the case.

What could be gathered from the list of legal provisions on the criminalisation of hacking, or legally termed as 'authorised 'access', is that many jurisdictions agree that hacking is a criminal activity. Hence these jurisdictions formalised the criminalisation of such offence in the form of national laws.

Theorising the Criminalisation of Hacking

Several theories can be used to understand the criminalisation of hacking. This section elaborates on five of such theories: routine activities theory, deterrence theory, social learning and self-control, general strain theory and deviant subcultures.

Routine Activities Theory

Routine activities theory suggests crime-related behaviour patterns (Holt & Bossler, 2008), different from other crime theories. It focuses on how criminals carry out their actions rather than the underlying motives. This distinction is not insignificant, but rather it has crucial implications on how we make decisions and how we prevent crime (Finkelhor & Asdigian, 2008).

The theory proposes that the pattern of taking advantage of the opportunity is created through daily repetition (Branic, 2015). Crime is affected by a variety of daily activities, including where people work, the routes they take to and from school, the groups with which they socialise, the shops and stores where they frequent, etc. Criminal habits may be convenient, complicated, or safe, depending on the situation. Consideration of possibilities varies over time, space, and by individuals. As a result, criminal acts are more probable (Reyns et al., 2015). Research that results from routine activities theory is most relevant, typically investigates daily opportunities for criminal activity; prevention of criminal behaviour is informed by routine activities theory (Arntfield, 2015).

Routine activities theory is used to look at changes over time in crime patterns. Nowadays, many people use it to understand and prevent crimes (Navarro & Jasinski, 2012). Researchers have tested the hypothesis and various methods to prove the theory. The theory has now been strongly connected with the ecological criminology paradigm since its beginnings, which focuses on factors that influence crime rates or how it occurs (Tillyer, 2011).

Routine activities theory is rightly applicable in hacking cases because the perpetrator might be involved in specific routine activities, space and time. For example, when an individual is left alone in a room where he might have ample space and time, he might use this opportunity

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 6 Issue 22 (March 2021) PP. 168-178
DOI 10.35631/IJLGC.6220016

to hack into a computer system or network. In some other situations, the perpetrator might end up in a routine group of people who also engage in hacking activities, allowing him to commit hacking. This scenario is summarised into Figure 1 below.

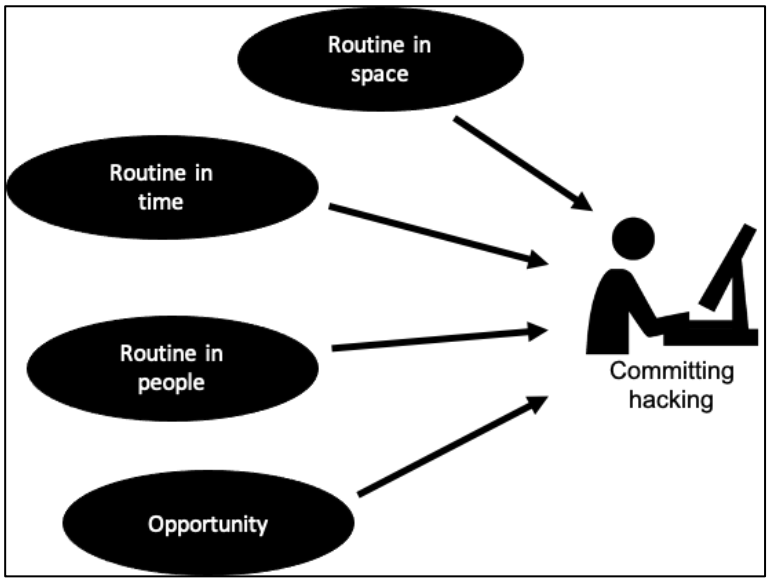


Figure 1: Routine Activities Theory And Hacking

Deterrence Theory

This theory suggests that an inferior force, employing the destructive power of their weapons of force, could discourage a more complex oppressor, provided that their force could be safeguarded by an attack at a time of their choosing (Bendie, & Merzger, 2015). This doctrine has gained popularity as a war strategy during the Cold War concerning the use of atomic warheads and is related, but distinct from, to the concept of nuclear annihilation, modelling what would happen in a nuclear war if both sides started using nuclear weapons (Brantly, 2018). Deterrence is a strategy used to dissuade an adversary from action that is not yet occurring through retaliation threats or stopping something the adversary wants to do. The same cognitive concept is the basis of this strategy.

The use of foreign aggression as a means of relieving international crises and wars has been a central theme of international security research for at least 200 years (Guitton, 2012). The research examines whether and under what circumstances conventional deterrence will be successful or fail. Alternative psychological models challenge rational persuasion theory and illustrate how cognitive processes determine actions.

The philosophy of deterrence can be portrayed as provocations to compel someone from committing a crime (Hua & Bapna, 2012). The threat serves as a deterrent to the degree that it scares the target so, it convinces him not to carry out the intended action. In international security, deterrence refers to the risk of military revenge attacks by the leaders of one state to the leaders of another state to prevent the other state from succumbing to the threat of military force (Cheng et. al., 2013; Tor, 2017).

Within the context of hacking, rules and regulations play a vital role in deterring people from committing the offence. In this regard, any law passed by the government in criminalising

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 6 Issue 22 (March 2021) PP. 168-178
DOI 10.35631/IJLGC.6220016

hacking would be an effective method to deter people from committing hacking. Such a situation is right because the punishment and the legal sanctions against hacking are severe and heavy in the potential perpetrators' minds. In the end, the entire community is deterred from committing hacking. This situation is illustrated in **Figure 2** below.

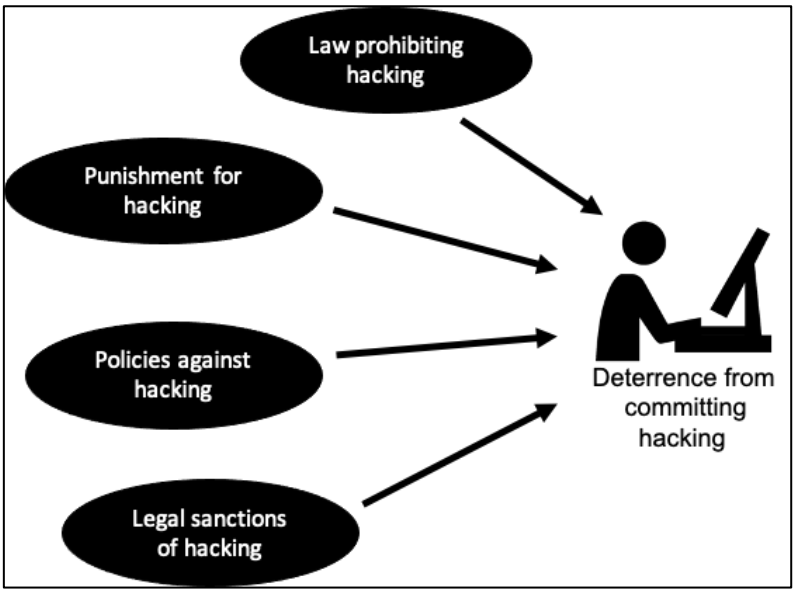


Figure 2: Deterrence Theory And Hacking

Social Learning and Self Control

Social learning theory suggests that individuals can learn new behaviours via observation and imitation of their environment (Nodeland & Norris, 2020). Even in the absence of motor reproduction or instruction, learning is a cognitive process in a social context and occurs solely through observation (Holt et al., 2010). In addition to observing behaviour directly, learning also becomes apparent through the observation of rewards and punishments. If an action is rewarded often and consistently, it will continue; if the action is repeatedly punished and is discouraged, it will eventually stop (Morris & Higgins, 2010).

The 'self-control' theory is a criminological theory about the lack of individual's self-control as a common underlying factor behind criminal behaviour. The general theory of crime is often referred to as the general crime theory (Higgins & Wilson, 2006). The crime theory of behaviour indicates that people who were parented inadequately during childhood develop less self-control than people of a similar age who were parented more effectively. Several studies have found that lower self-control levels increase the probability of criminal and impulsive behaviour (Yarbrough et al., 2012).

Within a broader context, humans are social learners. They learn from various teachers in their life beginning with learning from their parents when they are still small. When they grow older, they learn from their peers and social media. Humans also know from other sources such as what they see, what they feel, and what they hear. Their behaviours are much influenced by what they learn. Therefore, assuming that the potential perpetrator learns from their parents or peers or social media, how to hack, chances are they would also commit hacking. On the other hand, if they are surrounded by ethical people, who do not engage in hacking, they would also not get involved with hacking. This example is illustrated in the following **Figure 3.**

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 6 Issue 22 (March 2021) PP. 168-178
DOI 10.35631/IJLGC.6220016

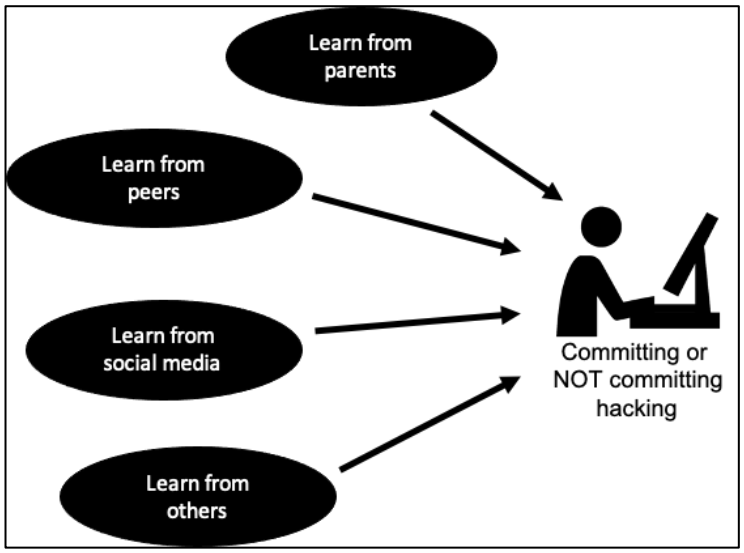


Figure 3: Social Learning And Self-Control Of Hacking

General Strain Theory

The general strain theory has accrued a large amount of scientific data. Providing explanations of phenomena outside of criminal activity has extended its primary scope (Pasculli, 2020). The theory consists mainly of three strains: the inability to attain positively valued targets, the elimination of positive stimuli and the implementation of negative stimuli, and eventually, the theory recognises that incidents that are considered by those who encounter them to be overwhelmingly negative are positively associated with a greater probability of criminal activity (Hay & Ray, 2020). The theory of strain is often used to describe several criminal occurrences.

For hackers, the general strain theory could also be applicable. An example situation is when the potential perpetrator is unable to attain meaningful positivity is in life. He could encounter difficulties in his life, involving his work, family, or relationship with his friends. He might resort to negativities. In this situation, he would first eliminate positive stimuli by distancing himself from family, peers at work and friends. Next, he would implement negative issues such as thinking about the worst-case scenario. The result is that he might commit hacking, which illustrates the application of general strain theory to such crime, as shown in **Figure 4** below.

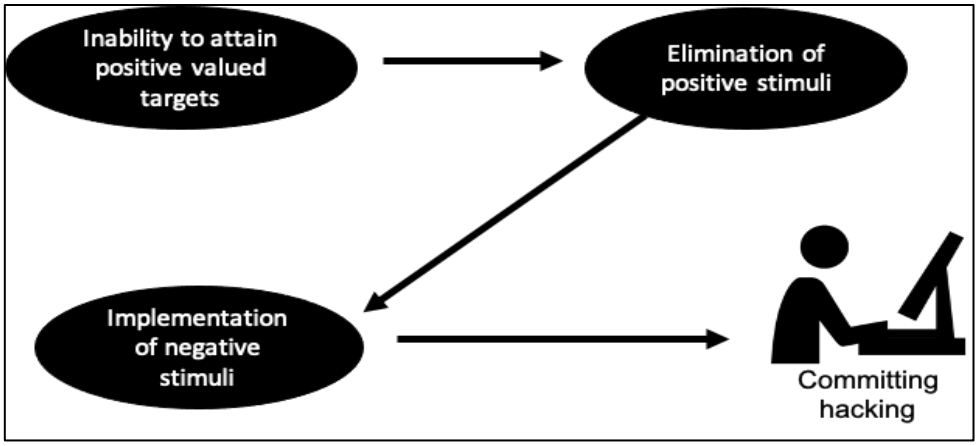


Figure 4: General Strain Theory And Hacking

International Journal of Law, Government and Communication
EISSN : 0128-1763
IJLGC
Volume 6 Issue 22 (March 2021) PP. 168-178
DOI 10.35631/IJLGC.6220016

Deviant Subcultures

Deviant subculture theory suggests that crime is a product of the individuals' grouping into subcultures predisposed to deviant behaviours. The subcultural theory became the most influential theoretical paradigm (Holt & Bossler, 2008). Concerning juvenile offenders, the basic presumption is that the vast majority are members of delinquent subcultures. Subcultures are characterised as subgroups or countercultures with their distinct attitudes, values, and norms that often oppose society's prevailing norms. (Williams, 2011). In this regard, young people's union is the product of their adjustment to the current capitalist class society's social inequality. Due to the particular and unique subculture, the subculture's behaviour is radically different from outside the subculture (Blackman, 2014). People also consider society as a whole as deviant, typically criminal.

For hacking situations, deviant subcultures could be applicable in criminalisation, which would happen when the potential perpetrator gets involved with deviant groups. He could also be involved with delinquent juveniles or other deviant subcultures who also engage in social problems or other cybercrimes. The result is that the person could be committing hacking. This scenario is produced in **Figure 5** below.

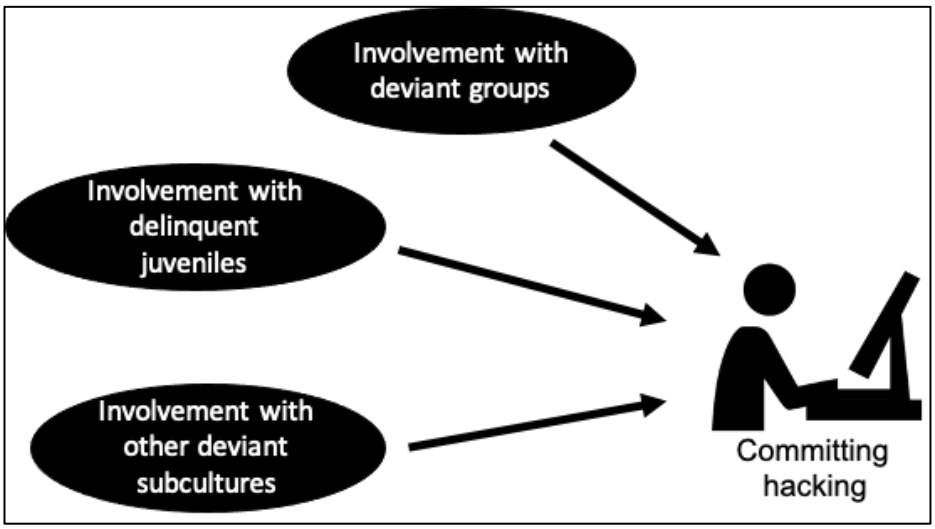


Figure 5: Deviant Subcultures And Hacking

Conclusion and Future Agenda for Criminalisation of Hacking

This paper examines the various theories which could inform the criminalisation of hacking. Each of the theories of routine activities theory, deterrence theory, social learning and self-control, general strain theory and deviant subcultures seem to point to the direction that the factors surrounding the perpetrator of hacking play a vital role shaping the criminal behaviour of the hacker. Accordingly, various jurisdictions took the initiative to launch its legal provisions to criminalise hacking, following its grievous ramifications to society.

Future research should be directed to examine and scrutinise each of these theories to understand better and analyse the behavioural choice of hacking criminals and its regulation under the respective countries' laws. Another direction of future research would be to carry out the case study of hackers' criminal behaviour focusing on the different parties involved in the offence, being the regulator, the enforcement officers, the perpetrators and the victims. Such

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 6 Issue 22 (March 2021) PP. 168-178
DOI 10.35631/IJLGC.6220016

research would provide a meaningful description and understanding of hacking criminalisation in the broader context.

Acknowledgement

This research was supported by Ministry of Education (MOE) Malaysia through Fundamental Research Grant Scheme For Research Acculturation of Early Career Researchers **(RACER/1/2019/SSI10/UUM//1)**.

References

Al-Sharif, S., Iqbal, F., Baker, T., & Khattack, A. (2016, November). White-hat hacking framework for promoting security awareness. In *2016 8th IFIP international conference on new technologies, mobility and security (NTMS)* (pp. 1-6). IEeE.

Arntfield, M. (2015). Towards a cybervictimology: Cyberbullying, routine activities theory, and the anti-sociality of social media. *Canadian Journal of Communication*, *40*(3).

Beale, S. S., & Berris, P. (2017). Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses. *Duke L. & Tech. Rev.*, *16*, 161.

Bendiek, A., & Metzger, T. (2015). Deterrence theory in the cyber-century. *INFORMATIK 2015*.

Blackman, S. (2014). Subculture theory: An historical and contemporary assessment of the concept for understanding deviance. *Deviant behavior*, *35*(6), 496-512.

Branic, N. (2015). Routine activities theory. *The encyclopedia of crime and punishment*, 1-3.

Brantly, A. F. (2018, May). The cyber deterrence problem. In *2018 10th International Conference on Cyber Conflict (CyCon)* (pp. 31-54). IEEE.

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organisations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447-459.

Coleman, E. G. (2012). *Coding freedom: The ethics and aesthetics of hacking*. Princeton University Press.

Finkelhor, D., & Asdigian, N. L. (1996). Risk factors for youth victimisation: Beyond a lifestyles/routine activities theory approach. *Violence and victims*, *11*, 3-20.

Futter, A. (2018). *Hacking the bomb: cyber threats and nuclear weapons*. Georgetown University Press.

Gaia, J., Ramamurthy, B., Sanders, G., Sanders, S., Upadhyaya, S., Wang, X., & Yoo, C. (2020, January). Psychological Profiling of Hacking Potential. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Goerzen, M., & Matthews, J. (2019). Black Hat Trolling, White Hat Trolling, and Hacking the Attention Landscape. FATES.

Guitton, C. (2012). Criminals and Cyber Attacks: The Missing Link Between Attribution and Deterrence. *International Journal of Cyber Criminology*, *6*(2).

Gunkel, D. J. (2018). *Hacking cyberspace*. Routledge.

Hamin, Z. (2000). Insider cyber-threats: Problems and perspectives. *International Review of Law, Computers & Technology*, *14*(1), 105-113.

Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., & Williams, T. (2011). *Gray hat hacking the ethical hackers handbook*. McGraw-Hill Osborne Media.

Hay, C., & Ray, K. (2020). General Strain Theory and Cybercrime. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 583-600.

International Journal of Law, Government and Communication
EISSN : 0128-1763
IJLGC
Volume 6 Issue 22 (March 2021) PP. 168-178
DOI 10.35631/IJLGC.6220016
Higgins, G. E., & Wilson, A. L. (2006). Low self-control, moral beliefs, and social learning theory in university 'students' intentions to pirate software. *Security Journal*, *19*(2), 75-92.
Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimisation. Deviant Behavior, 30(1), 1-25.
Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, *33*(2), 31-61.
Hua, J., & Bapna, S. (2012). How can we deter cyber terrorism?. Information Security Journal: A Global Perspective, 21(2), 102-114.
Jordan, T. (2008). *Hacking: Digital media and technological determinism*. Polity.
Jordan, T. (2017). A genealogy of hacking. *Convergence*, *23*(5), 528-544.
Koval, N. (2015). Revolution hacking. *Cyber War in Perspective: Russian Aggression Against Ukraine*, 55-58.
McClure, S., Scambray, J., Kurtz, G., & Kurtz. (2009). Hacking exposed: network security secrets and solutions.
Morris, R. G., & Higgins, G. E. (2010). Criminological theory in the digital age: The case of social learning theory and digital piracy. *Journal of Criminal Justice*, *38*(4), 470-480.
Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum*, *32*(1), 81-94.
Nodeland, B., & Morris, R. (2020). A test of social learning theory and self-control on cyber offending. *Deviant Behavior*, *41*(1), 41-56.
Palmer, C. C. (2001). Ethical hacking. *IBM Systems Journal*, *40*(3), 769-780.
Pasculli, L. (2020). The Global Causes of Cybercrime and State Responsibilities. Towards an Integrated Interdisciplinary Theory. *Journal of Ethics and Legal Technologies*, *2*(1).
Radziwill, N., Romano, J., Shorter, D., & Benton, M. (2015). The Ethics of Hacking: Should It Be Taught?. *arXiv preprint arXiv:1512.02707*.
Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimisation. Criminal justice and behavior, 38(11), 1149-1169.
Scambray, J., McClure, S., & Kurtz, G. (2000). *Hacking exposed*. McGraw-Hill Professional.
Tillyer, M. S., & Eck, J. E. (2011). Getting a handle on crime: A further extension of routine activities theory. *Security Journal*, *24*(2), 179-193.
Tor, U. (2017). 'Cumulative 'deterrence' as a new paradigm for cyber deterrence. *Journal of Strategic Studies*, *40*(1-2), 92-117.
Williams, J. P. (2011). Subcultural theory: Traditions and concepts. Polity.
Wilson, Z. (2001). Hacking: the basics. *online at http://rr. sans. org/toppapers/hack_basics. php*.