CYBERSTALKING AMONG GEN Z IN MALAYSIA: A QUALITATIVE STUDY ON PERCEPTIONS, EXPERIENCES, AND REPORTING BEHAVIOURS

NUR AAFREEN BINTI MOHAMMED PARWEZ ALAM

UNIVERSITI SAINS MALAYSIA

2026

CYBERSTALKING AMONG GEN Z IN MALAYSIA: A QUALITATIVE STUDY ON PERCEPTIONS, EXPERIENCES, AND REPORTING BEHAVIOURS

by

NUR AAFREEN BINTI MOHAMMED PARWEZ ALAM

Thesis submitted in fulfillment of the requirements for the degree of Bachelor of Science in Forensic Science (Honours)

FEBRUARY 2026

ACKNOWLEDGEMENT

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

DoSM	Department of Statistics Malaysia
FoCT	Fear of Crime Theory
FYP	Final Year Project
Gen Z	Generation Z
HREC	Human Research Ethics Committee
NT	Neutralization Theory
PCF	Participant Consent Form
PIS	Participant Information Sheet
RAT	Routine Activity Theory
SSIG	Semi-structured Interview Guide
USM	Universiti Sains Malaysia

CYBERSTALKING AMONG GEN Z IN MALAYSIA: A QUALITATIVE STUDY ON PERCEPTIONS, EXPERIENCES, AND REPORTING BEHAVIOURS

ABSTRAK

ABSTRACT

CHAPTER 1 - INTRODUCTION

1.0 INTRODUCTION

This Forensic Science Final Year Project (FYP) thesis examines the perceptions, lived experiences, and reporting behaviours of Generation Z (Gen Z) individuals in Malaysia in relation to cyberstalking. This study adopts a qualitative criminological approach to explore how Gen Z understands cyberstalking, navigate online risks, and decide whether or not to report such incidents. In addressing these issues, this thesis covers several key components, including the background of the study, the problem statement and research objectives, a review of relevant literature and criminological theories, the research methodology, data analysis, and the ethical considerations undertaken throughout the research process.

1.1 BACKGROUND

This section outlines the key contextual backgrounds of the study. It first addresses the increasing prevalence of cyberstalking in Malaysia, followed by the vulnerability of Generation Z (Gen Z) to cyberstalking in online spaces. The section also considers Gen Z's reporting behaviours in relation to cyberstalking, with particular attention to patterns of reporting and non-reporting.

1.1.1 RISING PREVALENCE OF CYBERSTALKING

Cyberstalking has become an increasingly visible issue in Malaysia, reflecting the broader rise in cybercrime within the country. National and academic reports have indicated a steady increase in online offences alongside the rapid expansion of digital platform use. Ariffin, Mohd, and Rokanatnam (2021), in their study on cyberbullying via social media, found that persistent online harassment could escalate into severe psychological harm, including suicide attempts. Although their research focused specifically on cyberbullying, this study argues that their findings are relevant to cyberstalking, as both forms of victimisation involve repeated and intrusive online behaviours that undermine victims' sense of safety.

The prevalence of cyberstalking is further shaped by limitations in legal awareness and institutional responses. UNICEF Malaysia (2020) reported that Malaysian adolescents were frequently exposed to online risks while lacking sufficient awareness of protective mechanisms or confidence in institutional support systems. The same report found that young people were often reluctant to report harmful online behaviours due to fear of stigma and distrust towards authorities. These findings highlight structural and perceptual barriers that may discourage formal reporting of cyberstalking incidents.

Broader analyses of cybercrime trends reinforce the urgency of addressing cyberstalking within the Malaysian context. Muharram et al. (2023) reported that cybercrime cases in Malaysia increased sharply between 2020 and 2022, involving thousands of complaints and substantial financial losses. While financial crimes constituted the majority of reported cases, Muharram et al. (2023) identified harassment and stalking as emerging threats within the wider cybercrime landscape. This suggests that non-financial forms of cybercrime warrant greater academic and policy attention.

Taken together, these studies suggest that underreporting and the normalisation of harmful online behaviours remain significant challenges. From the perspective of the present study, the rapid growth of digital platforms has created opportunities for offenders to monitor, harass, and intimidate victims through social media and messaging applications. For Gen Z,

who spend substantial amounts of time online, this gap in protection may increase exposure to cyberstalking. Accordingly, this study contends that targeted qualitative research is necessary to understand Gen Z's perceptions, experiences, and responses to cyberstalking within the Malaysian context.

1.1.2 THE CYBERSTALKING VULNERABILITY OF GEN Z

Cybersecurity analyses have highlighted the heightened vulnerability of young people in Malaysia's digital environment. The PIKOM Cybersecurity Report (2024) reported that Malaysia experienced a 144% increase in data breaches in 2023, placing the country among the top ten most breached globally. Although the report primarily focused on data breaches, it identified harassment and stalking as emerging risks within the broader cybercrime landscape. This study argues that these findings are particularly relevant to Gen Z, who represent the most digitally active cohort and are therefore exposed to cyberstalking alongside other online threats.

Gen Z's vulnerability to cyberstalking has been closely linked to their digital lifestyles and sustained online presence. A narrative systematic review by Bussu et al. (2024) examining cyberbullying and cyberstalking risks among university students found that younger cohorts were disproportionately exposed to these harms due to their reliance on social networking sites. The review further reported that the convergence of cyberbullying and cyberstalking behaviours intensified harm, particularly among students with limited awareness of protective strategies (Bussu et al., 2024). These findings suggest that routine online activities may increase both exposure to and the impact of cyberstalking.

The psychological consequences of cyberstalking for Gen Z have also been well documented as substantial and multifaceted. Henry and Flynn (2022), in their study on technology-facilitated abuse, found that victims of online harassment frequently experienced anxiety, distrust, and social withdrawal. Their findings demonstrated that such harms extended beyond the digital sphere, affecting academic performance, interpersonal relationships, and overall wellbeing (Henry & Flynn, 2022). Similar conclusions were reported by Janickyj, Blom, and Tanczer (2025), who found that technology-facilitated abuse resulted in significant psychological harm, behavioural withdrawal, and institutional challenges for victims. Both studies demonstrate that cyberstalking is both a behavioural and a mental-health concern for Gen Z.

Taken together, these studies highlight how Gen Z's online routines and digital dependence may increase susceptibility to persistent harassment. From the perspective of the present study, cyberstalking constitutes not only a behavioural issue but also a mental health concern for Malaysia's Gen Z population. Given the limited local qualitative research examining how Malaysian Gen Z individuals perceive, experience, and respond to cyberstalking, this study argues that targeted qualitative inquiry is necessary to fill a critical gap in understanding. The findings are expected to inform more effective prevention, support, and policy strategies tailored to Gen Z's needs.

1.1.3 THE REPORTING BEHAVIOURS OF CYBERSTALKING

Gen Z's reporting behaviours in relation to cyberstalking remain poorly understood, despite their high exposure to online risks. Wan Rosli et al. (2021) analysed Malaysia's historical non-criminalisation of cyberstalking and demonstrated that unclear enforcement pathways and limited legal recognition discouraged victims from making formal reports. The study found that young victims frequently anticipated inadequate follow-up or institutional

inaction, which fostered reliance on informal coping strategies over official reporting (Wan Rosli et al., 2021). This context helps to explain persistent underreporting, even when harm is recognised.

Digital norms further shape Malaysian youths' responses to online abuse. Nasruddin et al. (2023) reported that victims of cyberbullying commonly relied on peer networks, blocking, and platform-based self-management rather than institutional mechanisms. Such informal strategies reduce the visibility of incidents within formal systems and constrain available data on prevalence and impact (Nasruddin et al., 2023). For cyberstalking, this pattern suggests that trust in authorities, clarity of reporting procedures, and accessibility of reporting channels are critical determinants of whether youths engage in formal processes.

International evidence on technology-facilitated abuse further reinforces why young victims hesitate to report. Henry and Flynn (2022) highlighted how platform affordances, anonymity, and cross-jurisdictional complexity impeded help-seeking and diminished confidence in institutional effectiveness. Their study showed that victims prioritised immediate safety strategies, such as evidence capture, privacy adjustments, and community support, over formal complaints when reporting systems were perceived as opaque or unresponsive (Henry & Flynn, 2022). These findings indicate that perceived institutional opacity and limited recourse shape reporting decisions across contexts.

These insights underscore the need for youth-centred, streamlined reporting pathways and enhanced institutional communication in Malaysia. Recent legal reforms and amendments to the Penal Code (Act 574) have begun to provide clearer legal recognition of stalking and harmful communications, including online conduct. From the perspective of the present study, evaluating Gen Z's awareness of, trust in and utilisation of these reforms is essential to closing the reporting gap. This thesis, therefore, contends that understanding Gen Z's reporting behaviours will inform more effective, accessible, and youth-appropriate reporting mechanisms and support services.

1.2 PROBLEM STATEMENT

This study identifies two interrelated problems emerging from the literature review. First, despite statutory provisions such as Act 574, little is known about how Malaysia's Gen Z perceive and interpret cyberstalking; existing evidence does not adequately capture their lived experiences, meanings and reporting decisions. Second, current institutional structures and reporting mechanisms do not reflect Gen Z's digital norms and everyday practices, which may discourage formal help-seeking and perpetuate underreporting.

1.2.1 KNOWLEDGE GAP

Despite the introduction of legal provisions in Malaysia aimed at addressing stalking, research on how Gen Z perceive and report cyberstalking remains limited. Wan Rosli et al. (2021) highlighted that the historical non-criminalisation of cyberstalking hindered justice for victims, leaving enforcement pathways unclear and discouraging formal disclosure. Their study further suggested that these institutional gaps contributed to persistent underreporting, even when harm was recognised (Wan Rosli et al., 2021). From the perspective of the present study, these findings indicate a need to investigate how young Malaysians interpret and act upon cyberstalking experiences within evolving legal frameworks.

Recent studies have further emphasised the persistence of informal coping strategies and underreporting among youths. Sani, Yatim, and Azizi (2025) found that while awareness

of cyberbullying risks was relatively high among Malaysian students, reporting behaviours remained inconsistent, with peer-based support often replacing formal reporting. On a regional level, Sari (2024) observed that underreporting remains a significant barrier to effective enforcement of cybercrime laws across ASEAN, limiting institutional responses. Taken together, these studies highlight a clear knowledge gap: existing laws and enforcement mechanisms may not adequately capture the reporting behaviours of Malaysia's Gen Z, necessitating qualitative inquiry into their perceptions, experiences, and practices.

1.2.2 EXISTING STRUCTURES FAIL TO REFLECT GEN Z'S SOCIAL NORMS

Existing structures and legal frameworks often fail to capture the digital realities of Gen Z in Malaysia. While statutory provisions such as Act 574 provide a foundation for addressing cybercrime, they are frequently designed with traditional contexts in mind and overlook the complexities of online interactions among younger generations. Zhang, Ma'rof and Azam (2024) found that social comparison, fear of missing out and cyberbullying via social media significantly contributed to social anxiety among Malaysian youth, highlighting how institutional safeguards remain misaligned with lived experiences. Earlier, UNICEF Malaysia (2020) reported that adolescents often prioritised peer acceptance and digital identity over formal safety structures, revealing gaps between policy frameworks and youth practices.

Research further demonstrates that Gen Z's social norms are shaped by constant connectivity, fluid online identities and evolving digital cultures, which existing structures struggle to accommodate. Ariffin, Mohd and Rokanatnam (2021) presented case studies of cyberbullying via social media in Malaysia, showing that victims frequently relied on informal coping strategies rather than institutional reporting mechanisms. More recently, Saruddin et al. (2023) documented high prevalence rates of cyberbullying among Malaysian high school students, with nearly half reporting victimisation but few engaging formal channels. Taken together, these findings underscore the necessity of research that foregrounds Gen Z's perspectives in order to inform responsive policies and interventions that align with their social norms and digital practices.

1.3 RESEARCH QUESTIONS

This study is guided by a set of research questions designed to explore Gen Z's understanding, experiences and responses to cyberstalking within the Malaysian context. These questions provide the framework for qualitative inquiry and will be addressed through semi-structured interviews, enabling deeper insights into the social and psychological dimensions of cyberstalking among young people. By focusing on perceptions, lived experiences and reporting behaviours, the study seeks to capture how Gen Z interpret and act upon cyberstalking in relation to evolving legal and institutional structures. The research questions are as follows:

1. How do Gen Z Malaysians perceive cyberstalking?
2. What are Gen Z experiences with cyberstalking?
3. How open are Gen Z to reporting cyberstalking incidents to authorities or social media platforms?

1.4 OBJECTIVES

This section outlines the general and specific objectives that define the study's overall purpose and direction. The general objective states the broad aim of the research, while the specific objectives break that aim into focused areas of inquiry that guide data collection and

analysis. Together, these objectives ensure the study systematically examines Gen Z's perceptions, experiences and reporting behaviours in relation to cyberstalking within the Malaysian context.

1.4.1 GENERAL OBJECTIVE

The general objective of this qualitative study is to examine Gen Z's perceptions, experiences and reporting behaviours in relation to cyberstalking within Malaysia. This objective frames the study's broad aim to understand how young people interpret, respond to and disclose incidents of cyberstalking in the context of evolving legal and institutional arrangements. This study contends that generating in-depth, qualitative insights will help address existing knowledge gaps and inform more effective, youth-centred prevention and support strategies.

1.4.2 SPECIFIC OBJECTIVES

This study has three specific objectives that guide the formulation of exploratory themes and the semi-structured interview schedule. These specific objectives are listed below.

1. To explore how Malaysian Gen Z conceptualise and make sense of cyberstalking in digital contexts.
2. To examine the lived experiences of Gen Z individuals who have encountered or witnessed cyberstalking.
3. To understand the factors that influence Gen Z's willingness or reluctance to report cyberstalking incidents to authorities or social media platforms.

1.5 OPERATIONAL DEFINITIONS

This section defines key terms used throughout the study to ensure clarity and consistency in interpretation within the Malaysian context. The terms defined are cyberstalking, online harassment, Gen Z, reporting behaviours, and digital contexts. Precise operationalisation will distinguish cyberstalking from broader forms of online abuse, specify the birth-year range used for Gen Z, differentiate formal, institutional reporting from informal, peer-based or platform-level reporting behaviours, and outline the various digital contexts that shape online interactions and victimisation. These definitions are intended to avoid ambiguity in data collection and analysis.

1.5.1 CYBERSTALKING

Kaur, Dhir, Abohassan, Alzeiby, and Tandon (2021) define cyberstalking as a persistent form of online victimisation that exploits social media, messaging platforms, and other digital tools to intrude upon privacy and cause psychological distress. Key features such as impersonation, doxing, location tracking, and anonymity are emphasised, as these elements intensify harm and complicate detection and reporting (Kaur, et al, 2021). This definition highlights cyberstalking as a distinct form of victimisation in the digital age, which requires tailored and specific responses.

Under Malaysian law, cyberstalking has recently been recognised as a criminal offence through amendments to Act 574. Section 507A, introduced in 2023, defines stalking as repeated acts of harassment intended or likely to cause distress, fear, or alarm to any person. This section explicitly covers both physical and online conduct, with penalties of up to three years' imprisonment, fines, or both. The provisions under Section 507A reflect the growing awareness of cyberstalking as a significant issue, necessitating legal measures to address online harassment. Specifically, section 507A of Act 574 states:

(1) Whoever repeatedly by any act of harassment, intending to cause, or knowing or ought to know that the act is likely to cause, distress, fear or alarm to any person of the person's safety, commits an offence of stalking.
(2) For the purposes of subsection (1), the act of harassment may include the following:
(a) following or tracking a person in any manner or by any means;
(b) communicating or attempting to communicate with a person in any manner or by any means;
(c) loitering at the place of residence or business of a person;
(d) giving or sending any thing to a person in any manner or by any means.
(3) Whoever commits the offence of stalking shall be punished with imprisonment for a term which may extend to three years or with fine or with both.
(4) In this section, "repeatedly" shall refer to at least two occasions

Complementary provisions in the Communications and Multimedia Act 1998 (Act 588) regulates online behaviour, criminalising the improper use of network services to harass or threaten others. Section 233(1)(a) of Act 588 specifically prohibits the use of network facilities or services to transmit any communication that is obscene, indecent, false, menacing, or offensive in nature, with intent to annoy, abuse, threaten, or harass. The penalties under this section include a fine not exceeding RM50,000, imprisonment for up to one year, or both, with an additional fine of RM1,000 for each day the offence continues after conviction. These provisions provide a legal framework for addressing the various forms of cyberstalking that occur online. Specifically, section 233 of Act 588 states:

(1) A person who—
(a) by means of any network facilities or network service or applications service knowingly—
(i) makes, creates or solicits; and
(ii) initiates the transmission of,
any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or
(b) initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address,
commits an offence.
(2) A person who knowingly—
(a) by means of a network service or applications service provides any obscene communication for commercial purposes to any person; or
(b) permits a network service or applications service under the person's control to be used for an activity described in paragraph (a),
commits an offence.
(3) A person who commits an offence under this section shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of one thousand ringgit for every day during which the offence is continued after conviction.

Section 211 further reinforces this by prohibiting the distribution of content that is indecent, obscene, false, or offensive, especially when such content targets individuals or groups. This provision offers legal grounds to address cyberstalking behaviours, particularly

when they involve harmful content directed at specific individuals. Section 211 of Act 588 states:

> *(1) No content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.*
> *(2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of one thousand ringgit for every day or part of a day during which the offence is continued after conviction.*

Recent updates to the law have further strengthened protections against cyberstalking and related behaviours. Further amendments to Act 574 in 2025 introduced heavier penalties for offences such as doxing, stalking, and mental harassment, reflecting recognition of the growing prevalence of online harms and the need for proportionate punishment. These amendments offer clearer legal recourse for victims of cyberstalking and align penalties with the severity of such offences. Sections 507B to 507G of Act 574 states:

> *"Causing harassment, distress, fear or alarm*
> *507b. Whoever, in any manner or by any means, uses or makes any threatening, abusive or insulting words or communication, or engages in any threatening, abusive or insulting act, with intent to cause, or knowing or ought to know that the words, communication or act are likely to cause harassment, distress, fear or alarm to a person, shall be punished with imprisonment for a term which may extend to three years or with fine or with both.*
>
> *Causing harassment, distress, fear or alarm to a person likely to feel harassed, distressed, fear or alarmed*
> *507c. (1) Whoever, in any manner or by any means, uses or makes any threatening, abusive or insulting words or communication, or engages in any threatening, abusive or insulting act, and such words, communication or act are heard, seen or otherwise perceived by a person who is likely to feel harassed, distressed, fear or alarmed by such words, communication or act, shall be punished with imprisonment for a term which may extend to one year or with fine or with both.*
> *(3) It shall be a defence to a charge against a person under this section if it is proved that he had no reasonable grounds to believe that the words or communication used or made by him, or his act, would be heard, seen or otherwise perceived by a person who was likely to feel harassed, distressed, fear or alarmed by such words, communication or act.*
>
> *Causing a person to believe that harm will be caused*
> *507d. (1) Whoever, in any manner or by any means, uses or makes any threatening, abusive or insulting words or communication against any person, or engages in any threatening, abusive or insulting act towards any person, with intent to cause, or knowing or ought to know that the words, communication or act will cause the person to believe that harm will be caused to himself or to any other person, shall be punished with imprisonment for a term which may extend to one year or with fine or with both.*
> *(2) Whoever, in any manner or by any means, uses or makes any threatening, abusive or insulting words or communication against any person, or engages in any*

threatening, abusive or insulting act towards any person, with intent to provoke the person to cause harm to himself or to any other person, or knowing or ought to know that the words, communication or act are likely to provoke the person to cause harm to himself or to any other person, shall be punished with imprisonment for a term which may extend to one year or with fine or with both; and if the person so provoked attempts to commit suicide or commits suicide as a result of such provocation, shall be punished with imprisonment for a term which may extend to ten years or with fine or with both.

Publishing, etc., any identity information to cause harassment, distress, fear or alarm
507e. Whoever, in any manner or by any means, publishes, circulates or makes available or causes to be published, circulated or made available, any identity information of a person with intent to cause, or knowing or ought to know that the publication, circulation or availability is likely to cause harassment, distress, fear or alarm to the person, shall be punished with imprisonment for a term which may extend to three years or with fine or with both.

Publishing, etc., any identity information to cause a person to believe that harm will be caused
507f. (1) Whoever, in any manner or by any means, publishes, circulates or makes available or causes to be published, circulated or made available, any identity information of a person with intent to cause, or knowing or ought to know that the publication, circulation or availability will cause the person to believe that harm will be caused to him or to his related person, shall be punished with imprisonment for a term which may extend to one year or with fine or with both.
(3) Whoever, in any manner or by any means, publishes, circulates or makes available or causes to be published, circulated or made available, any identity information of a person with intent to facilitate, or knowing or ought to know that the publication, circulation or availability is likely to facilitate, the causing of harm to the person or to his related person, shall be punished with imprisonment for a term which may extend to one year or with fine or with both.

Definitions of "harm", "identity information" and "related person"
507g. (1) For the purposes of sections 507d and 507f, "harm" means harm to a person's body, mind, reputation or property, including psychological harm.
(2) For the purposes of sections 507e and 507f, "identity information" means any information that identifies or purports to identify a person.
(3) For the purposes of section 507f, "related person" means, in relation to a person, any person whose safety or well-being would reasonably be expected to be of concern of the first-mentioned person.".

Complementing the legal framework, Harewell, Pina, and Storey (2022) synthesise the prevalence, characteristics, and impacts of cyberstalking. Their analysis distinguishes cyberstalking from traditional stalking by emphasising its reliance on electronic communication and the perceived anonymity of offenders (Harwell, et al., 2022). This distinction is crucial in understanding how cyberstalking manifests in the digital age and why it demands separate attention from other forms of abuse.

There is no single, universally accepted operational definition of cyberstalking in the literature. Studies vary on criteria such as incident count, required victim fear and timeframe

(Kaur et al., 2021). For the purposes of this study, cyberstalking is defined as the repeated and intentional use of digital communication technologies, such as social media, messaging platforms, email and network services, to harass, monitor, threaten or intrude upon another individual's privacy, thereby causing fear, distress or disruption to daily life. Consistent with the definition in Act 574, the term "repeated" is taken to mean at least two occasions. This definition aligns scholarly characterisations with the current Malaysian statutory framework and clarifies the criteria used during participant interviews and thematic coding (Kaur et al., 2021; Harewell et al., 2022; Act 574; Act 588).

1.5.2 ONLINE HARASSMENT

Henry and Flynn (2022) highlighted that technology-facilitated abuse encompasses a wide spectrum of behaviours including abusive messages, threats, identity misuse, and public shaming, all of which undermine victims' psychological well-being. Schoenebeck, Lampe, and Triệu (2023) further emphasised that online harassment is persistent and diverse, with harms ranging from reputational damage to long-term emotional distress. These definitions underscore online harassment as a distinct form of victimisation in the digital age that requires a nueanced response.

Under Malaysian law, online harassment is addressed through both Act 574 and Act 588. Amendments to Act 574 in 2023 introduced Section 507A (see 1.5.1), criminalising stalking and harassment, including acts committed online, with penalties of up to three years' imprisonment, fines, or both. Further amendments in 2025 expanded provisions under Sections 507B–507G (see 1.5.1) to cover bullying, insults, and identity misuse, reflecting the growing prevalence of online harassment. Act 588 regulates improper use of network services, with Section 233 (see 1.5.1) prohibiting the transmission of offensive, threatening, or indecent content, and recent amendments have strengthened penalties for online abuse. Together, these laws provide a comprehensive framework for addressing online harassment in Malaysia.

It is also important to distinguish online harassment from related forms of digital victimisation, such as cyberstalking. Davidovic, Talbot, Hamilton-Giachritsis, and Joinson (2023) found that young adults often perceive online harassment as sporadic or situational, requiring context-specific interventions, whereas cyberstalking involves persistent monitoring or pursuit that creates fear and an invasion of privacy. Based on the existing literature by Davidovic et al. (2023), online harassment can be understood as hostile digital behaviours that may be broader and less sustained, such as sending offensive messages or posting harmful content. In contrast, cyberstalking is characterised by its ongoing nature and intent to control or intimidate.

Based on the studies and legal statues referenced above, online harassment is broadly defined as repeated, unwanted, and hostile behaviour conducted through digital platforms, often intended to cause distress or harm (Henry and Flynn, 2023; Schoenebeck et al., 2023; Davidovic et al., 2023; Act 574; Act 588). In this study, online harassment refers to the repeated or sustained use of digital communication technologies, such as social media, messaging platforms, email, and online forums, to send unwanted, offensive, threatening, or abusive content that causes distress, fear, or disruption to the targeted individual's wellbeing.

1.5.3 GENERATION Z

Generation Z (Gen Z) is commonly defined as the cohort born between the mid-1990s and early 2010s, representing the first generation to grow up entirely in a digitally mediated

environment (Zahra, Handoyo, & Fajrianthi, 2025). The Department of Statistics Malaysia (DoSM, 2025) identifies Gen Z as individuals aged 12–28 in 2025 and estimates they comprise nearly 27% of the national population, giving them substantial influence as consumers, employees and digital citizens. UNICEF Malaysia (2020) characterised this cohort as digital natives who rely on technology for education, socialisation and civic engagement, a profile that shapes both risk exposure and help-seeking behaviours online.

Gen Z's distinctiveness lies in high digital fluency and rapid adaptation to emerging technologies. Chardonnens (2025) noted that Gen Z students quickly adapted to artificial intelligence and metacognitive learning strategies, reflecting their comfort with emerging technologies and innovative learning environments. Germe and Carado (2025) found that Gen Z's communication patterns are heavily influenced by social media and cultural trends, shaping both formal and informal language use. These findings make Gen Z particularly relevant for research into online behaviours such as cyberstalking and online harassment.

Operationally, this study defines Generation Z as individuals born between 1995 and 2010, consistent with DoSM and UNICEF demographic framing. For analytical clarity, Gen Z in this study is described as Malaysia's digitally native youth cohort, characterised by high digital engagement, entrepreneurial tendencies and pronounced social awareness. These defining attributes are treated as contextual factors when interpreting perceptions of cyberstalking and reporting behaviours.

1.5.4 REPORTING BEHAVIOURS

Van de Weijer, Leukfeldt and Van der Zee (2020) found that decisions to report cybercrime victimisation are shaped by perceptions of police effectiveness, prior experiences and personal motives, with many victims reluctant to engage formal systems. Henry and Powell (2021) demonstrated that the reporting of technology-facilitated abuse is influenced by both structural factors, such as legal frameworks and institutional support, and individual factors, such as resilience and social networks. Janickyj et al. (2025) further emphasised that cultural attitudes towards criminalisation and levels of institutional trust play a critical role in reporting decisions, as victims often weigh the risks of retaliation or stigma before disclosing their experiences. These studies collectively suggest that reporting behaviours are complex and influenced by a combination of social, cultural, and psychological factors.

Generational differences are particularly evident in the reporting behaviours of younger cohorts. Bussu et al. (2024) found that many university students prefer informal coping strategies, such as blocking offenders or confiding in peers, over engaging with formal reporting systems. Their study reported that this reluctance is often rooted in concerns about confidentiality and the perceived inefficiency of institutional responses (Bussu et al., 2024). These findings highlight the importance of examining reporting behaviours specifically within the context of Gen Z, whose digital norms, expectations of platform governance and help-seeking practices differ from older cohorts. Understanding these generational patterns is therefore central to interpreting how and why young people disclose cyberstalking incidents.

Operationally, reporting behaviours in this study are defined as the processes by which Gen Z victims of cyberstalking decide whether, how, and to whom they disclose their experiences. This definition integrates existing academic perspectives with the Malaysian context, recognising that reporting behaviours encompass both formal channels, such as the police and university authorities, and informal channels, such as friends and online

communities, as well as that disclosure decisions are shaped by perceived costs and benefits. This operational definition provides clarity for the study, ensuring a structured examination of Gen Z's responses to cyberstalking victimisation.

1.5.5 DIGITAL CONTEXTS

Stoilova, Livingstone, and Nandagiri (2020) highlighted that digital contexts involve governance structures, such as platform policies and national regulations, which influence the safety or risk associated with these environments. Chen, Saharuddin, Yasin, and Wang (2025) argued that digital contexts are not neutral; rather, they actively shape social norms, identity formation, and power relations, particularly through practices of online deviance and technology-facilitated abuse. This perspective makes digital contexts especially relevant to criminological research, where online environments can facilitate both positive engagement and harmful behaviours, such as harassment or stalking (Chen et al., 2025).

Salza and Samuel (2025) emphasised the complexity of digital contexts in shaping youth experiences, noting that young people's digital engagement is driven by educational needs, social interaction, and entertainment. They found that digital contexts are shaped by socioeconomic inequalities that affect access, motivation, and mastery (Salza & Samuel, 2025). Their scoping review demonstrated how digital contexts create both opportunities and risks, blurring the boundaries between public and private spheres (Salza & Samuel, 2025). Kalyani (2025) further emphasised that digital contexts are dynamic, constantly evolving with technological innovation and cultural adaptation, requiring researchers to treat them as fluid environments rather than static ones.

For this study, digital contexts are defined as the environments created by digital technologies in which Gen Z's social, cultural, and behavioural interactions occur. By adopting this definition, the study ensures clarity in examining how digital contexts contribute to Gen Z's vulnerability and reporting behaviours in relation to cyberstalking. Based on the available literature, digital contexts encompass online platforms, communication tools, and virtual spaces that shape how individuals engage with information and interact with one another (Stoilova et al., 2025; Chen et al., 2025; Salza & Samuel, 2025; Kalyani, 2025).

CHAPTER 2 - LITERATURE REVIEW

This chapter critically reviews existing literature on cyberstalking and its criminological underpinnings to establish this study's conceptual foundation. It first presents the theoretical framework, outlining the key criminological theories that inform the research perspective and interpretive lens. It then synthesises empirical studies that have applied these theories to online victimisation and offender behaviour, emphasising findings that are directly relevant to Gen Z and digital contexts. This chapter concludes by identifying empirical and conceptual gaps in the literature and explaining how the present study addresses those gaps.

2.1 THEORETICAL FRAMEWORK

This section discusses the theoretical framework that guides this study. Three theories are discussed: the Routine Activity Theory (Cohen & Felson, 1979), the Neutralization Theory (Sykes & Matza, 1957), and the Fear of Crime Theory (Ferraro, 1995). Together, they provide an ecological lens that links situational opportunity, offender justification, and victim perceptions of risk, each of which is crucial for understanding the dynamics of cyberstalking.

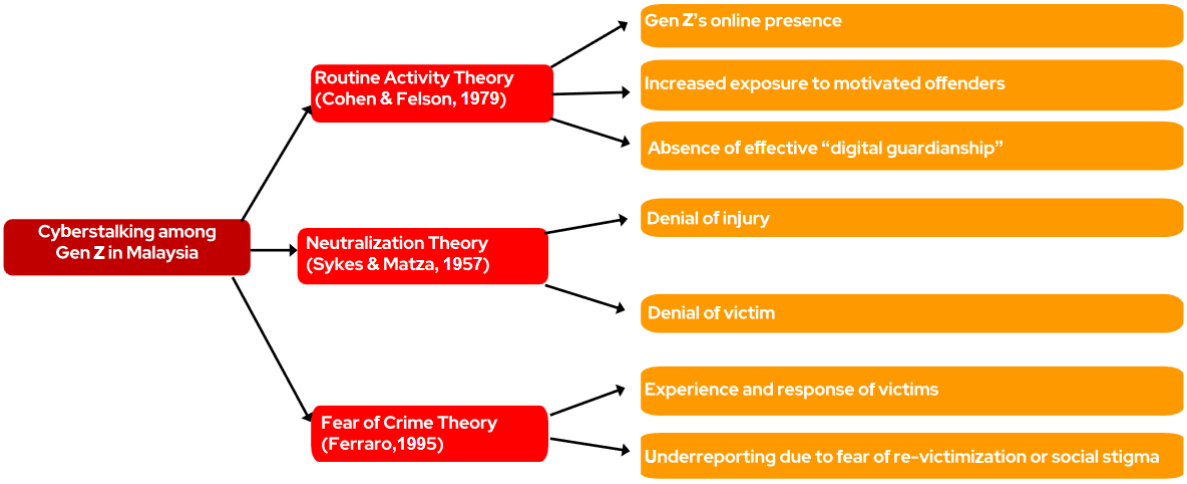

Figure 1: The proposed theoretical framework

2.1.1 ROUTINE ACTIVITY THEORY

The Routine Activity Theory (RAT), introduced by Cohen and Felson (1979), is a central framework in criminology for analysing crime rate trends and cycles. The core proposition of RAT (Cohen & Felson, 1979) is that crime occurs when three elements converge: a motivated offender, or likely offenders, a suitable target, which can be a person or an object, and the absence of capable guardians against a violation. Cohen and Felson (1979) confined their analysis to direct-contact predatory violations, where the offender intentionally harms or takes another person's property. These violations specifically involve direct physical contact between at least one offender and at least one person or object the offender seeks to take or damage. In the context of this study, cyberstalking is viewed through this lens, where the offender's motivations, the victim's visibility, and the lack of protective mechanisms contribute to the likelihood of victimisation.

A motivated offender is an individual with both criminal inclinations and the ability to carry out those inclinations. RAT (Cohen & Felson, 1979) assumes that criminal inclination is an inherent factor and focuses instead on how social activities facilitate the opportunity for offenders to act on these inclinations. In this study, the motivated offender would be the cyberstalker, whose behaviours could be driven by jealousy, control, revenge, or obsession.

A suitable target is a person or object that provides an opportunity for the offender. Target suitability is a crucial factor influencing the likelihood of a crime occurring. According to Cohen and Felson (1979), factors such as the target's value, visibility, access, and resistance to illegal treatment (VIVA) influence suitability. In the digital context, Gen Z individuals, characterised by their high online visibility, are particularly vulnerable to cyberstalking. The structure of their daily online routines, which often include sharing personal information, geotagging, and frequent social media interactions, increases their exposure to online threats (Nutter, 2021).

Capable guardians refer to the protective presences capable of preventing violations. The presence of these guardians is often implied in everyday life and is usually only noticed by the absence of violations (Cohen & Felson, 1979). In the context of online environments, this includes both technological safeguards, such as privacy settings, and institutional protections, such as law enforcement and reporting systems, as well as informal guardianship from supportive peers and platform moderators. However, ineffective reporting systems,

weak law enforcement responses, and peer inaction in online spaces create a lack of guardianship. The absence of such protective measures increases the risk of cyberstalking victimisation, as offenders are emboldened by the lack of consequences.

While not an element, RAT (Cohen & Felson, 1979) also highlights the significance of convergence, which is the simultaneous occurrence of motivated offenders, suitable targets, and a lack of guardianship at a specific time and place. Changes in the structure of routine activities can alter the likelihood of this convergence, potentially leading to large increases in crime rates even without requiring any increase in the structural conditions that motivate individuals to engage in crime (Cohen & Felson, 1979).

Examining these components allows the RAT (Cohen & Felson, 1979) approach to link illegal and legal activities within a single conceptual framework, offering valuable insights into the dynamics of crime. By focusing on situational opportunities rather than offender characteristics, RAT (Cohen & Felson, 1979) provides a powerful lens for understanding how predatory acts emerge in both physical and digital environments. This approach is particularly useful for studying cyberstalking in the context of Gen Z.

In the context of cyberstalking, RAT (Cohen & Felson, 1979) has been increasingly applied to explain how online routines and visibility create opportunities for victimisation, particularly among younger generations. Nutter (2021) observed that Gen Z's high online visibility increases target suitability by making individuals more accessible to offenders in cyberspace. This situational vulnerability reflects RAT's (Cohen & Felson, 1979) principle that crime is facilitated when targets are both visible and accessible, underscoring the need to consider generational differences in online routines when analysing cyberstalking victimisation.

As an offshoot to RAT (Cohen & Felson, 1979), Raj and Caeiro (2024) reviewed the application of Lifestyle-Routine Activity Theory in cyber criminology, noting that offenders are often drawn to victims who maintain highly visible online profiles. This aligns with RAT's (Cohen & Felson, 1979) emphasis on opportunity structures, as offenders are motivated not by unique psychological traits but by the ease of access to potential victims. This situational framing highlights the importance of examining offender behaviour in relation to digital environments rather than focusing solely on individual pathology.

Equally critical is the absence of capable guardianship in cyberspace. Smith and Haines (2025) argued that ineffective reporting systems, lack of law enforcement action, and peer inaction contribute significantly to the persistence of cyberstalking. Smith and Haines (2025) noted that while victims often report incidents, institutional responses are inadequate, leaving offenders unchecked and victims unprotected. This mirrors RAT's (Cohen & Felson, 1979) third element, where the absence of guardianship creates fertile ground for predatory acts. This highlights the importance of evaluating systemic failures in protective mechanisms, including both technological safeguards and institutional responses.

Based on the above descriptions, RAT (Cohen & Felson, 1979) provides a robust framework for analysing cyberstalking by situating crime within the convergence of motivated offenders, suitable targets, and absent guardianship. Contemporary studies between 2020 and 2025 have demonstrated its applicability, showing how cyberstalkers exploit the visibility of Gen Z individuals in environments where protective mechanisms are weak or

absent. This situational analysis is invaluable, as it bridges traditional criminological theory with modern digital realities.

2.1.2 NEUTRALIZATION THEORY

The Neutralization Theory (NT), developed by Sykes and Matza (1957), challenges the assumption that juvenile delinquents operate under a value system entirely opposed to conventional society. Instead, Sykes and Matza (1957) proposed that delinquents employ techniques such as Denial of Responsibility, Denial of Injury, Denial of the Victim, Condemnation of the Condemners, and Appeal to Higher Loyalties to justify their actions temporarily suspend their internalised conventional norms. Sykes and Matza (1957) posit that social rules or norms are rarely absolute but function as qualified guides for action, limited in their applicability by time, place, persons, and social circumstances. Sykes and Matza (1957) relate this concept to criminal laws, which provide defences to crimes, such as nonage, necessity, or self-defence, that allow an individual to avoid moral culpability.

The Techniques of Neutralization (Sykes & Matza, 1957) extend traditional defences of criminal acts, serving as justifications for deviance that are accepted by the delinquent but not by society or the legal system. These techniques (Sykes & Matza, 1957) precede deviant behaviour, making the act possible, rather than merely rationalising it afterwards. According to Sykes and Matza (1957), the techniques allow delinquents to deflect disapproval by neutralising internalised norms and social controls, thus enabling them to maintain their commitment to the dominant normative system. By qualifying societal rules, these techniques make violations appear acceptable, positioning the delinquent as someone who views themselves as more sinned against than sinning, rather than as an outright opponent of the law (Sykes & Matza, 1957).

The Denial of Responsibility technique (Sykes & Matza, 1957) allows the delinquent to view themselves as lacking control over their deviant actions, thereby mitigating disapproval from both themselves and others. This technique (Sykes & Matza, 1957) extends beyond simply claiming the act was accidental, suggesting that external forces, such as bad companions, unloving parents, or a disadvantaged neighbourhood, were to blame. By adopting this rationalisation, delinquents can engage in deviant behaviour without directly challenging societal norms, as it is framed as a consequence of uncontrollable external factors (Sykes & Matza, 1957).

The Denial of Injury technique (Sykes & Matza, 1957) operates on the perception that the deviant action does not result in significant harm. The delinquent rationalises that while the act violates the law, it does not cause substantial harm (Sykes & Matza, 1957). Examples given by Sykes and Matza (1957) include defining vandalism as mere mischief because the victim can afford the loss or viewing auto theft as merely borrowing. Denial of Injury (Sykes & Matza, 1957) effectively breaks the link between the illegal act and its consequences, making the behaviour appear less harmful and thus more socially acceptable.

When employing the Denial of Victim technique (Sykes & Matza, 1957), the delinquent neutralises moral indignation by framing the injury as justified under the circumstances. According to Sykes and Matza (1957), the victim is redefined as deserving of harm, with the act framed as rightful retaliation or punishment. Sykes and Matza (1957) further noted that the victim's presence may be diminished, especially in property crimes, when the victim is absent, unknown, or viewed as an abstract concept. This allows the

delinquent to rationalise their actions by displacing any moral responsibility (Sykes & Matza, 1957).

The Condemnation of the Condemners technique (Sykes & Matza, 1957) enables the delinquent to deflect attention from their own actions by focusing on the motives and behaviours of those who disapprove. This technique (Sykes & Matza, 1957) often evolves into a bitter cynicism directed towards authority figures, such as law enforcement. By attacking the critics, the delinquent can suppress or disregard the wrongfulness of their own behaviour, deflecting any moral or social guilt onto those who condemn them (Sykes & Matza, 1957).

Finally, the Appeal to Higher Loyalties technique (Sykes & Matza, 1957) neutralises both internal and external social controls by prioritising the demands of smaller social groups, such as friendship cliques, over the larger society. According to Sykes and Matza (1957), the delinquent does not necessarily reject the dominant norms but views themselves as caught in a dilemma where violating the law is necessary to meet the demands of the smaller group. The delinquent perceives the norms of this smaller group as more pressing or involving a higher loyalty than the broader societal norms (Sykes & Matza, 1957).

Traditionally, from the current researcher's observation, these techniques (Sykes & Matza, 1957) have been studied as rationalisations used by offenders. However, recent studies, such as those listed in this section, have extended the theory to victims, suggesting that Neutralization Techniques (Sykes & Matza, 1957) can also function as coping mechanisms to mitigate fear, insecurity, and other negative emotions following victimisation.

A significant reinterpretation of NT (Sykes & Matza, 1957) is offered by Dreißigacker, Müller, Isenhardt, and Schemmel (2024), who examined online hate speech victimisation and its consequences for victims' feelings of insecurity. Their study redefined two of the original techniques introduced by Sykes and Matza (1957): *Denial of Injury* (Sykes & Matza, 1957) became *Denial of Serious Harm*, and *Denial of the Victim* (Sykes & Matza, 1957) was reframed as *Denial of One's Innocence*. This reframing demonstrates how victims, rather than offenders; may employ neutralisation strategies to reduce the psychological impact of victimisation. By minimising harm or questioning their own innocence, victims attempt to preserve agency and reduce vulnerability, showing the adaptability of NT (Sykes & Matza, 1957) beyond its original offender-focused scope (Dreißigacker et al., 2024).

Based on the above descriptions, NT (Sykes & Matza, 1957) continues to serve as a robust framework not only in analysing juvenile delinquency but also in understanding victim coping strategies. By incorporating reinterpretations such as Dreißigacker et al.'s (2024) reframing of denial techniques, both the traditional and contemporary applications of NT (Sykes & Matza, 1957) can be critically engaged. This dual perspective highlights the complex interplay between offenders' justifications and victims' psychological resilience. For this study, NT (Sykes & Matza, 1957) will be used to explain both the victims' and perpetrators' perspectives.

2.1.3 FEAR OF CRIME THEORY

The Fear of Crime Theory (FoCT), developed by Ferraro (1995), is based on the Risk Interpretation Model (Ferraro, 1995), which integrates symbolic interactionist perspectives with traditional criminological approaches to explain how individuals interpret victimisation

risk. Ferraro (1995) understood fear as a fundamentally psychological experience. It is highly emotive and activates corresponding physiological changes in the body, alerting the actor to the possibility of danger (Ferraro, 1995). FoCT (Ferraro, 1995) distinguishes between perceived risk, the cognitive assessment of the likelihood of victimisation, and fear of crime, the emotional response to that perceived risk. The importance of FoCT (Ferraro, 1995) remains to this day due to its adaptability to both traditional and digital contexts (Zhang, Zhai, & Wu, 2024).

The Risk Interpretation Model (Ferraro, 1995), the central framework of FoCT (Ferraro, 1995), integrates symbolic interactionist theory with traditional criminological perspectives to interpret risk. According to Ferraro (1995), both constrained behaviour and fear of crime are responses that occur when individuals perceive their victimisation risk as high. The model (Ferraro, 1995) distinguishes between these two related concepts, with perceived risk being central to the interpretive process. According to Ferraro (1995), perceived risk involves an individual's assessment of the likelihood of being victimised, while fear of crime represents the emotional response to this perceived risk. Ferraro (1995) argues that perceived risk is the most significant determinant of fear, particularly in the context of property or personal crime, and that fear often shapes behavioural intentions aimed at reducing risk.

The Generic Model of Fear of Crime Based on a Risk Interpretation Approach (Ferraro, 1995) identifies three key factors that influence an individual's perception of risk: ecological (macro) factors, neighbourhood factors, and personal (micro) factors. According to Ferraro (1995), these factors shape how individuals perceive risk, which, in turn, leads to either fear or constrained behaviour, such as actions taken to reduce exposure to risk. Constrained behaviour is associated with high levels of perceived risk and fear (Ferraro, 1995).

Ferraro (1995) stated that ecological factors include objective crime prevalence in the larger community and broader community characteristics. Neighbourhood factors encompass perceptions of incivility, community cohesion, and the presence of crime-watch programs (Ferraro, 1995). Notably, Ferraro (1995) found that neighbourhood incivility, which refers to low-level breaches of community norms, is often the most significant predictor of perceived risk. Personal factors involve characteristics such as gender, race, victimisation history, and residential characteristics (Ferraro, 1995). Direct experiences of victimisation, particularly in property crime, tend to increase an individual's perception of risk (Ferraro, 1995).

Ecological (macro) factors in the context of cybercrime include global prevalence rates, media coverage, and the visibility of high-profile cases (Fakhrou et al., 2022). Fakhrou, Adawi, and Moussa (2022) found that widespread reporting of cyber threats significantly influenced students' perceived risk of victimisation, even when they had not been directly targeted. That study (Fakhrou et al., 2022) found that, in cyberstalking, ecological factors manifest through the global recognition of online harassment as a pervasive issue, shaping collective perceptions of insecurity. It is the opinion of the current researcher that macro-level influences demonstrate how fear can be socially constructed through exposure to information and discourse surrounding cybercrime.

Personal (micro) factors remain central to FoCT (Ferraro, 1995), as individual characteristics shape how risk is interpreted. Obermaier and Schmuck (2022) found that victims of online hate speech reported heightened insecurity when personal vulnerabilities,

such as age or gender, intersected with digital exposure. Earlier, Nutter (2021) observed that cyberstalking victims often experienced fear due to personal routines, such as frequent social media use, which increased visibility and perceived risk. These micro-level factors demonstrate how personal behaviours and demographics interact with ecological and neighbourhood influences to produce fear and constrained behaviour.

From the available literature, FoCT (Ferraro, 1995) and the Risk Interpretation Model (Ferraro, 1995) provide a robust framework for understanding fear in both traditional and digital contexts. FoCT (Ferraro, 1995), when applied to cybercrime and cyberstalking, reveals that ecological factors such as media and global prevalence, neighbourhood factors such as online community dynamics, and personal factors such as individual routines and vulnerabilities could collectively shape perceived risk and fear. Recent studies reaffirm FoCT's (Ferraro, 1995) relevance, demonstrating that fear of cybercrime is not only a product of victimisation but also of how individuals interpret risk within complex digital environments. This situational and interpretive approach is invaluable in analysing both the psychological impact of cybercrime and the behavioural responses it provokes amongst Malaysian Gen Z.

2.2 PAST STUDIES

This section critically reviews prior research on cybercrime and related online harms, with particular emphasis on empirical studies that have applied the criminological theories outlined in the theoretical framework. Given the limited number of recent, focused studies on cyberstalking, this review draws from broader cybercrime research to extract theoretical insights, methodological approaches, and empirical findings relevant to the study of cyberstalking. The aim is to show how existing evidence helps illuminate patterns of online victimisation, offender behaviour, and reporting, while also identifying methodological and conceptual gaps that justify the present study's focus on Gen Z, digital contexts, and reporting behaviours.

2.2.1 PAST STUDIES ABOUT CYBERCRIME

This section reviews four Malaysian studies that inform understanding of cybercrime and cyberstalking among young people, comparing their perspectives, empirical contributions and methodological limitations. It summarises each study's focus and evaluates how their findings relate to the study's theoretical framework. The review also highlights common methodological weaknesses such as limited theoretical engagement.

Saharrudin and Ghazali (2020) explored the psychological impacts of cyberbullying, focusing on victim experiences and emotional distress. Their work (Saharrudin & Ghazali, 2020) highlights how Gen Z individuals often internalise online harassment, leading to anxiety and social withdrawal. However, Saharrudin and Ghazali's (2020) study is largely descriptive and lacks a strong theoretical framework, limiting its ability to explain structural or behavioural drivers of cybercrime. Moreover, the absence of longitudinal or comparative data restricts the study's (Saharrudin & Ghazali, 2020) capacity to capture the evolving nature of online victimisation across different contexts. Nonetheless, that study (Saharrudin & Ghazali, 2020) remains useful for contextualising the emotional consequences of cyberbullying among digital natives.

Rani et al. (2022) examined cyberstalking behaviours via social media, emphasising how youth online routines increase exposure to predatory acts. The study's (Rani et al., 2022) strength lies in its empirical evidence linking visibility and oversharing to heightened risk,

which is particularly relevant for Gen Z. Unfortunately, the study (Rani et al., 2022) pays limited attention to systemic guardianship failures such as weak platform regulation. Futhermore, the study's (Rani et al., 2022) narrow focus on individual behaviours overlooks broader socio-cultural and institutional factors that shape vulnerability, limiting the explanatory depth of its analysis. However, Rani et al.'s (2022) findings align with situational criminological perspectives, showing how everyday digital behaviours create opportunities for cybercrime.

Building on this, Rani et al. (2023) analysed stalking alongside problematic social media behaviours, such as compulsive engagement and dependency. That particular study (Rani et al., 2023) recognised how digital addiction intertwines with victimisation risk, offering insight into the behavioural ecology of Gen Z. However, the study (Rani et al., 2023) risks conflating problematic use with stalking victimisation, which may obscure distinct mechanisms of harm. A stronger theoretical framing could have clarified how perceived risk translates into fear and constrained behaviour.

Samsudin et al. (2023) adopted a public health perspective, linking cyberbullying victimisation to family dysfunction, health behaviours, and psychological distress. Samsudin et al.'s (2023) cross-sectional study situates cybercrime within broader socio-ecological contexts, highlighting how personal vulnerabilities intersect with digital victimisation. While valuable, the study's (Samsudin et al., 2023) design limits causal inference and lacks integration with criminological theory. In addition, the study's (Samsudin et al., 2023) reliance on self-reported measures raises concerns about response bias and the accuracy of victimisation data. Nevertheless, the study (Samsudin et al., 2023) contributes significantly to understanding the psychosocial consequences of cybercrime among young adults in Malaysia.

Taken together, these studies illustrate the multifaceted nature of cybercrime among Gen Z, spanning emotional, behavioural and socio-ecological dimensions. Saharrudin and Ghazali (2020) emphasised psychological impacts, Rani et al. (2022, 2023) focused on behavioural risks and stalking, while Samsudin et al. (2023) highlighted family and health-related vulnerabilities. A common limitation across these studies is the underuse of criminological theory, which could strengthen explanations of risk and coping. Collectively, these studies demonstrate that Gen Z's vulnerability arises from a combination of high online visibility, problematic digital routines, and personal or familial vulnerabilities, making them a critical demographic for forensic science research into cybercrime.

2.2.2 PAST STUDES THAT USED THE ROUTINE ACTIVITY THEORY

This section reviews three international studies that applied RAT (Cohen & Felson, 1979) to cybercrime and cyberstalking. It compares how each study utilises RAT (Cohen & Felson, 1979) constructs. The review also highlights each studies weakness.

Özaşçılar, Çalıcı, and Vakhitova (2024) applied RAT (Cohen & Felson, 1979) to examine cybercrime victimisation among Turkish women, focusing on cyberstalking, hacking, and identity theft. Their study (Özaşçılar et al., 2024) highlighted how online routines, visibility, and accessibility increase vulnerability, with weak guardianship amplifying risks. While the findings are robust in situational analysis, the focus on women limits generalisability to Gen Z more broadly, who share similar risks due to high online activity. The study demonstrates RAT's (Cohen & Felson, 1979) adaptability but does not fully address psychological consequences such as fear and coping strategies. Furthermore, the study's (Özaşçılar et al., 2024) reliance on a single national context restricts cross-cultural

applicability, overlooking how different regulatory and cultural environments may shape cybercrime dynamics.

Earlier, Akgül (2021) investigated cyberbullying victimisation among Turkish adolescents using RAT (Cohen & Felson, 1979), emphasising how target suitability and lack of guardianship predict online victimisation. This study (Akgül, 2021) is highly relevant to Gen Z, as it shows how everyday digital routines, such as social media use, create opportunities for offenders. Compared to Özaşçılar et al. (2024), Akgül's (2021) work focused more directly on youth, highlighting developmental vulnerabilities. However, both Özaşçılar et al. (2024) and Akgül (2021) share a limitation in prioritising situational opportunity structures over emotional and psychological impacts. Additionally, the reliance on cross-sectional data constrains the ability to capture how risks and coping strategies evolve over time, limiting the studies' (Özaşçılar et al., 2024; Akgül, 2021) longitudinal relevance.

Walsh, Finkelhor, and Turner (2024) explored cyberstalking victimisation among juveniles and young adults in the United States of America (USA), applying RAT (Cohen & Felson, 1979) to highlight how visibility and accessibility online increase risks. Their study (Walsh et al., 2024) revealed that Gen Z victims often face multiple perpetrators and violent threats, with few reporting incidents to authorities. Walsh et al. (2024) highlight systemic failures in guardianship and institutional responses, underscoring the importance of combining situational and institutional perspectives in understanding cybercrime. Nonetheless, the reliance on retrospective self-reports introduces recall bias, which may limit the accuracy of the study's (Walsh et al., 2024) findings on victimisation dynamics.

Taken together, these studies confirm RAT's (Cohen & Felson, 1979) utility for explaining how digital routines and platform affordances create opportunities for cyberstalking. While Özaşçılar et al. (2024) and Akgül (2021) emphasised on situational opportunities through RAT (Cohen & Felson, 1979), Walsh et al. (2024) highlighted systemic failures and behavioural consequences. A recurring theme across the studies is the vulnerability of Gen Z due to high online visibility and weak guardianship, though the studies differed in whether they prioritise offender opportunity structures or institutional shortcomings. Collectively, these studies display the need for an integrated approach that considers situational, psychological, and systemic dimensions in understanding cyberstalking and cybercrime in the digital age.

2.2.3 PAST STUDIES THAT USED THE NEUTRALIZATION THEORY

This section reviews four international studies that applied NT (Sykes & Matza, 1957) to cybercrime and cyberstalking. It summarises their contributions, methodological limitations and relevance to a Gen Z sample. The review also compares how each study utilises Neutralization Techniques (Sykes & Matza, 1957).

Van Baak et al. (2022) examined cyber harassment through the dual lens of power and control dynamics alongside Techniques of Neutralization (Sykes & Matza, 1957). Their study (Van Baak et al., 2022) highlighted how American perpetrators rationalise harmful behaviour by denying responsibility, minimising injury, or condemning victims, thereby maintaining a sense of legitimacy. While the focus is primarily on offenders, the findings (Van Baak et al., 2022) are relevant to Gen Z as both perpetrators and victims often engage in online spaces where harassment is normalised. The study's (Van Baak et al., 2022) strength lies in linking neutralisation to broader power structures, but it pays less attention to how

victims themselves may adopt neutralisation strategies to cope. Furthermore, the study's (Van Baak et al., 2022) reliance on a single cultural context limits the applicability of its conclusions to diverse online environments where norms and power relations may differ.

Dreißigacker et al. (2024) reinterpreted NT (Sykes & Matza, 1957) in the context of online hate speech victimisation in Germany, reframing Denial of Injury (Sykes & Matza, 1957) as Denial of Serious Harm and Denial of the Victim (Sykes & Matza, 1957) as Denial of One's Innocence. This victim-centred approach demonstrates how individuals rationalise their experiences to reduce insecurity and fear. Unlike Van Baak et al. (2022), which focuses on offender justifications, Dreißigacker et al. (2024) highlight victim coping strategies, making that particular study relevant to Gen Z who often face online hostility. The strength of this work lies in extending neutralisation beyond perpetrators, despite its limited scope to hate speech. However, its conceptual reframing remains underdeveloped, lacking empirical validation across diverse forms of cybervictimisation such as cyberstalking or online harassment.

Connolly, Borrion, and Arief (2025) analysed ransomware crime through NT (Sykes & Matza, 1957) in the United Kingdom (UK), showing how organised cybercriminal groups justify attacks by denying injury, appealing to higher loyalties, or condemning condemners. Although focused on offenders, the study (Connolly et al., 2025) illustrates how the Neutralization Techniques (Sykes & Matza, 1957) are embedded in cybercrime operations, including Ransomware-as-a-Service. Compared to Van Baak et al. (2022), Connolly et al. (2025) emphasised business-like rationalisations rather than interpersonal power dynamics. This contrast demonstrates the versatility of NT (Sykes & Matza, 1957) across different forms of cybercrime, although its victim-centred implications remain underexplored. Moreover, the reliance on secondary case materials rather than direct offender narratives limits the depth of insight into how neutralisation is actively constructed and maintained in practice.

Aslam and Mustafa (2025) investigated how cybercriminals in Pakistan adapt Neutralization Techniques (Sykes & Matza, 1957) to expand fraudulent operations, including online scams and cryptocurrency theft. Their study (Aslam & Mustafa, 2025) highlighted Denial of Injury and Denial of Responsibility (Sykes & Matza, 1957) as central strategies for offenders to maintain moral disengagement. Unlike Dreißigacker et al. (2024), who focused on victims, Aslam and Mustafa (2025) emphasise offender rationalisations in the context of financial cybercrime. This comparison shows how neutralisation operates differently depending on whether the focus is victim coping or offender justification, both of which are relevant to Gen Z's experiences of cybercrime. However, the study's (Aslam & Mustafa, 2025) limited empirical grounding and reliance on conceptual analysis reduce its explanatory power for understanding the lived realities of offenders and victims in diverse digital contexts.

Taken together, these studies illustrate the dual application of NT (Sykes & Matza, 1957) to both offenders and victims within cybercrime contexts. Van Baak et al. (2022) and Connolly et al. (2025) highlighted offender rationalisations, while Dreißigacker et al. (2024) and Aslam and Mustafa (2025) demonstrated victim coping and offender expansion strategies respectively. A common theme across these studies is the normalisation of harmful behaviour in digital environments. Collectively, these studies highlight the importance of understanding how Gen Z's vulnerability to cybercrime is shaped not only by offender justifications but also by the ways victims reinterpret harm in order to manage fear and insecurity.

2.2.4 PAST STUDIES THAT USED THE FEAR OF CRIME THEORY

This subsection reviews four international studies that apply FoCT (Ferraro, 1995) to cybercrime and cyberstalking. It summarises their contributions, methodological limitations and relevance to a Gen Z sample. The review also evaluates the robustness of the measurement and analytic approaches of these studies.

Fakhrou, Adawi, and Moussa (2022) examined cybercrime risk fear among university students in Qatar using social networking sites, testing the validity and reliability of fear of crime measures in digital contexts. Their study (Fakhrou et al., 2022) highlighted how perceived risk of victimisation strongly influenced fear, with constrained behaviours such as limiting online activity emerging as coping strategies. This work (Fakhrou et al., 2022) is particularly relevant to Gen Z, who are highly active on social media and therefore more exposed to cyber threats. However, Fakhrou et al.'s (2022) focus on measurement reliability limited its exploration of broader ecological and institutional factors shaping fear. By prioritising psychometric validation, their study (Fakhrou et al., 2022) overlooked how structural elements such as university policies, law enforcement practices, and platform governance interact with individual perceptions to shape fear.

McNealey, Figueroa, and Burden (2025) compared fear of crime across offline and online contexts in USA, showing that victimisation experiences in one domain influenced fear in the other. Their findings (McNealey et al., 2025) emphasised that Gen Z's fear of cybercrime is not isolated but interconnected with broader perceptions of insecurity. Unlike Fakhrou et al. (2022), who concentrated on measurement, McNealey et al. (2025) explored cross-contextual dynamics, offering a more holistic view of how fear operates across environments. This contrast demonstrates the importance of situating FoCT (Ferraro, 1995) within both digital and physical realities. Nevertheless, the study's (McNealey et al., 2025) reliance on self-reported survey data constrains its ability to capture the nuanced emotional and behavioural processes underlying fear across contexts.

Janickyj et al. (2025) analysed online and offline stalking victimisation in the UK using Crime Survey data from England and Wales, applying FoCT (Ferraro, 1995) to interpret victims' perceptions of insecurity. Their study (Janickyj et al., 2025) revealed that cyberstalking significantly heightened fear among younger cohorts, including Gen Z, who reported constrained behaviours and calls for stronger criminalisation. Compared to McNealey et al. (2025), who examined cross-contextual fear, Janickyj et al. (2025) focused specifically on stalking, making their findings highly relevant to the current study. Both studies extend FoCT (Ferraro, 1995) beyond its traditional role as a measurement tool by demonstrating how fear operates within lived victimisation experiences. McNealey et al. (2025) show that fear transcends boundaries between offline and online contexts, while Janickyj et al. (2025) illustrate how specific forms of cybervictimisation, such as stalking, intensify insecurity and shape demands for criminalisation. Together, they highlight the theory's explanatory power in capturing the dynamic interplay between victimisation, behavioural responses, and broader perceptions of safety.

Zhang, Zhai, and Wu (2024) provided a theoretical review of FoCT (Ferraro, 1995), discussing antecedent variables and its significance in contemporary crime research, including cybercrime. Their work (Zhang et al., 2024) synthesised ecological, neighbourhood, and personal factors, showing how these shape perceived risk and fear in digital environments particularly within China's socio-cultural context. Unlike the empirical focus

of Fakhrou et al. (2022) and Janickyj et al. (2025), Zhang et al. (2024) offered a conceptual framework that reinforces FoCT's (Ferraro, 1995) applicability to cybercrime. This theoretical contribution complements empirical findings by clarifying how risk interpretation processes underpin fear among Gen Z. Yet, this study's (Zhang et al., 2024) lack of empirical validation restricts the generalisability of the framework, leaving questions about how these antecedent variables operate across different cultural and technological contexts.

Taken together, these studies highlight the adaptability of FoCT (Ferraro, 1995) in understanding cybercrime and cyberstalking. Fakhrou et al. (2022) emphasised measurement reliability, McNealey et al. (2025) highlighted cross-contextual fear, Janickyj et al. (2025) focused on stalking victimisation, and Zhang et al. (2024) provided a theoretical framework for risk interpretation. A common theme across these studies is the centrality of perceived risk in shaping fear and constrained behaviour. Collectively, they demonstrate that FoCT (Ferraro, 1995) offers a powerful framework for understanding Gen Z's vulnerability to cybercrime, though it requires an integration of both empirical and theoretical perspectives to fully capture the complexity of fear and coping behaviours in digital contexts.

2.3 GAPS IN KNOWLEDGE

This section identifies the principal gaps in the literature on cyberstalking among Gen Z in Malaysia. Although existing work documents prevalence and psychological impacts, it provides limited insight into victims' perceptions, lived experiences and the decision-making processes that shape disclosure and reporting. By reviewing current research trends and limitations, this section highlights three major areas that require further investigation to enhance theoretical understanding and improve practical interventions. The gaps are: the lack of qualitative studies on the cyberstalking perceptions and lived experiences of Gen Z, the limited focus on the reporting behaviours of Gen Z and the institutional barriers, and the fragmented application of criminological theories in cyberstalking research. These gaps form the foundation upon which the present study is built and underscore the significance of conducting a qualitative investigation into the phenomenon.

2.3.1 LACK OF QUALITATIVE STUDIES OF GEN Z'S PERCEPTIONS AND LIVED EXPERIENCES

Most existing studies, such as those by Özaşçılar et al. (2024) and Walsh et al. (2024), predominantly utilise quantitative surveys or statistical modelling to examine cybercrime victimisation. While these approaches are effective at identifying correlations between factors such as online routines, guardianship deficits, and victimisation risk, they often fail to capture the nuanced perceptions, contextualised meanings that victims attach to their experiences. As a result, there remains a significant gap in understanding how Gen Z interprets risk, rationalise harm, and emotionally respond to cyberstalking in their daily digital interactions.

To fill this gap, a qualitative approach is necessary to uncover the subjective meanings behind experiences such as fear, coping strategies, and reporting behaviours. By focusing on the lived experiences of Gen Z, this study can explore how individuals negotiate their online identities and visibility, weigh the costs and benefits of disclosure, and use frameworks such as NT (Sykes & Matza, 1957) to rationalise their encounters with online harm. This approach provides valuable psychological and social insights into cyberstalking by illuminating the psychological and social mechanisms that underlie reporting decisions and help-seeking behaviours. Thus, enriching the quantitative findings that currently dominate the field.

2.3.2 LIMITED FOCUS ON REPORTING BEHAVIOURS AND INSTITUTIONAL BARRIERS

Existing Malaysian and international studies, such as Samsudin et al. (2023) and Rani et al. (2022, 2023), highlight the prevalence of cyberbullying and stalking but devote comparatively little attention to how victims engage with reporting mechanisms. Walsh et al. (2024) noted low rates of formal disclosure among young victims, yet the empirical literature rarely interrogates the reasons for non-reporting or the pathways through which reporting, or its absence, shapes institutional responses. This gap is critical, as reporting behaviours directly influence institutional responses and the effectiveness of guardianship in digital environments as when victims do not disclose incidents, platforms and law enforcement cannot intervene, institutional responsiveness is reduced, and situational opportunities for repeat victimisation persist.

For Gen Z in Malaysia, reporting decisions are likely shaped by a combination of cultural norms, trust in institutions, legal awareness and peer-level dynamics. A deeper investigation into these reporting behaviours would reveal specific barriers such as fear of stigma, concerns about privacy and reputational harm, perceived futility of enforcement, or the normalisation of online harassment within peer networks. Addressing this gap strengthens the application of RAT (Cohen & Felson, 1979) by linking guardianship failures to victim decision-making and institutional responses, particularly by showing how institutional and platform-level failures translate into reduced protective presence in digital spaces.

2.3.3. FRAGMENTED APPLICATION OF CRIMINOLOGICAL THEORIES

Existing studies tend to apply criminological theories in isolation, with RAT (Cohen & Felson, 1979) used to explain situational risks (Özaşçılar, 2024; Akgül, 2021), NT (Sykes & Matza, 1957) addressing offender rationalisations (Baak, 2022; Connolly, 2025), and FoCT (Ferraro, 1995) focusing on victim perceptions (Fakhrou, 2022; McNealey, 2025). While each theory offers valuable insights into different aspects of cyberstalking, the fragmented approach limits the ability to comprehensively explain the complex dynamics of cyberstalking within Gen Z populations. There is a need for integrated frameworks that combine the situational, psychological, and behavioural factors that collectively shape cyberstalking experiences.

By synthesising RAT (Cohen & Felson, 1979), NT (Sykes & Matza, 1957), and FoCT (Ferraro, 1995), this study can better explain how offender opportunities, victim rationalisations, and fear interact to influence the cyberstalking experiences of Gen Z. For example, Gen Z's high online visibility, RAT (Cohen & Felson, 1979), increases the risk of victimisation, while victims may downplay or rationalise harm, NT (Sykes & Matza, 1957), yet still exhibit constrained behaviour in response to their fears, FoCT (Ferraro, 1995). Addressing this gap allows a holistic understanding of cyberstalking, contributing to both theoretical and practical advancements in criminology and forensic science in Malaysia, and providing more effective frameworks for intervention and prevention.

CHAPTER 3 - RESEARCH METHODOLOGY

3.0 RESEARCH METHODOLOGY

This section outlines the research methodology employed in this study. It begins with a description of the research design, followed by the sampling strategy, research tools, and data collection procedures. The methodology section also includes a study flow chart and a

Gantt chart, which illustrate the research process and timeline. Finally, this section concludes with an overview of the ethical considerations involved in conducting the study.

3.1 RESEARCH DESIGN

This study employs a qualitative, cross-sectional research design, using semi-structured interviews to explore the perceptions, experiences, and reporting behaviours of Malaysian Gen Z regarding cyberstalking. Qualitative research is particularly suitable for this investigation as it enables a deeper understanding of the nuanced attitudes and lived experiences of participants, which quantitative methods, such as surveys, may not fully capture (Frechette et al., 2020). Prior to conducting the pilot study and data collection, ethical approval was sought from the Human Research Ethics Committee (HREC) at the USM Health Campus to ensure the study adheres to ethical guidelines.

3.2 SAMPLING

This section outlines the sampling approach employed in this study, detailing the study location, target population, and participant selection criteria. The inclusion, exclusion, and withdrawal criteria are explicitly defined to ensure a clear and ethical recruitment process, preserving the integrity and validity of the research. By adhering to this structured sampling framework, the study aims to capture a representative range of insights that reflect the lived experiences of Malaysian Gen Z in relation to cyberstalking, ensuring the findings are both meaningful and contextually relevant.

3.2.1 STUDY LOCATION

This study is conducted in Malaysia due to the limited research on cyberstalking within the country. Stalking, both online and offline, was officially criminalised in Malaysia under Section 507A of Act 574, effective from 31st May 2023. Subsequent amendments, including the introduction of Sections 507B to 507F, came into effect on 11th July 2025, broadening the legal framework to include various forms of harassment and the unauthorised sharing of personal information which are issues closely related to cyberstalking. The legal context makes Malaysia an appropriate setting for examining cyberstalking and its impacts, particularly in the context of Gen Z's digital engagement.

3.2.2 STUDY POPULATION

The study focuses on Gen Z Malaysians, defined as individuals born between 1995 and 2010 (see section 1.5.3). As such, the participants in this study are aged between 18 and 28 years old. This demographic was selected due to their high engagement with social media platforms, which distinguishes them from other age groups. Given Gen Z's substantial online presence, they represent a key population for investigating the perceptions, experiences, and reporting behaviours related to cyberstalking in Malaysia.

3.2.3 PARTICIPANT SELECTION

The selection of participants for this study was guided by a set of inclusion, exclusion, and withdrawal criteria to ensure both the ethical integrity and validity of the research. These criteria are outlined below, with the purpose of capturing a sample that reflects the lived experiences of the target population while safeguarding participants' wellbeing.

The inclusion criteria listed in the table below (Table 1) were used to select participants for this study.

CRITERIA	DESCRIPTION
Nationality	Malaysian
Sociodemography	Gen Z (18-28), regardless of gender identities and expressions
Experience / Awareness	Personally experienced, witnessed, or are aware of cyberstalking incidents
Platform Use	Active users of social media or digital communication platforms (e.g., Instagram, X, TikTok, etc.)
Language Proficiency	Able to communicate in English or Bahasa Malaysia
Consent	Voluntarily agree to participate and sign the informed consent forms

Table 1: Participant inclusion criteria

The exclusion criteria listed in the table below (Table 2) were applied to ensure the safety and suitability of participants.

CRITERIA	DESCRIPTION
Sensitive Mental State	Currently in severe emotional distress or active trauma that may be exacerbated by discussing the topic
Mental & Physical Conditions	Currently facing mental health issues (e.g., anxiety, depression) On substances that could impair memory (e.g., alcohol)
Education	All students that are currently studying either USM's Forensic Science undergraduate or postgraduate programme

Table 2: Participant exclusion criteria

Participants were informed of their right to withdraw from the study at any stage without consequence. The withdrawal criteria listed in the table below (Table 3)

CRITERIA	DESCRIPTION
Voluntary Withdrawal	Respondents may withdraw at any time without penalty or justification
Emotional Distress	Respondents who experience discomfort, anxiety, or emotional distress during the interview will be allowed to stop or discontinue participation
Non-response	Respondents who fail to attend scheduled interviews or stop responding after multiple follow-ups will be withdrawn from the study

Table 3: Participant withdrawal criteria

3.2.4 SAMPLE SIZE ESTIMATION

According to the DoSM (2025), Gen Z constitutes approximately 27% of the total population in Malaysia as of 2025. Of this demographic, individuals aged 18 to 28 years make up about 78%, representing a significant proportion of Malaysia's Gen Z population. Given that this study adopts a qualitative research design, the sample size was determined based on the principle of data saturation, where further data collection will cease once no new themes or insights emerge from the interviews.

For this study, the anticipated sample size is 15 participants. This estimate is informed by previous qualitative studies on similar topics, such as those conducted by Rani et al. (2022) and Rani et al. (2023), where similar sample sizes were deemed adequate to achieve data saturation and provide meaningful insights into the phenomena under investigation.

3.2.5 SAMPLING METHOD