Criminal Victimisation in Taiwan:
an opportunity perspective

by

Tien-Li Kuo

A dissertation submitted in fulfilment
of the requirements for the degree of

Doctor of Philosophy

of University College London.

UCL Department of Security and Crime Science

London, UK

7 December 2021

Declaration

I, *Tien-Li Kuo*, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Signed ___________________

Date 7 December 2021

Abstract

Environmental criminology concerns the role of opportunities (both people and objects) existing in the environment that make crimes more likely to occur. Research consistently shows that opportunity perspectives (particularly with regard to individuals' lifestyles and routines) help in explaining the prevalence and concentration of crimes. However, there is a paucity of studies investigating crime patterns from an opportunity perspective both outside western countries and in relation to cybercrimes. Hence, it is not clear whether non-Western and online contexts exhibit similar patterns of crime as would be predicted by an opportunity perspective.

This thesis is concerned with criminal victimisation in Taiwan – a less researched setting in the field of environmental criminology. It covers both offline victimisation (with a focus on burglary) and online victimisation from the aforementioned opportunity perspective. The goal of this thesis is to identify individual- and area-level characteristics that affect the patterns of victimisation in Taiwan. To achieve this, the thesis draws on a range of secondary datasets, including police recorded crime statistics, the Taiwan Area Victimisation Survey, and the Digital Opportunity Survey for Individuals and Households.

With the application of quantitative modelling, the thesis suggests that the generalisability the lifestyle-routine activity approach in explaining crime patterns in Taiwan should be taken with caution. The findings provide partial support for its applicability in relation to burglary and cybercrime in Taiwan. Furthermore, the findings reported here in relation to patterns of repeat and near repeat victimisation depart from those observed in the western literature. The thesis concludes by discussing the implications of the findings for academic research and practice in crime prevention.

Impact statement

This thesis concerns patterns and mechanisms of criminal victimisation in Taiwan. Specifically, the research examines patterns of burglary, repeat and near repeat burglary, cybercrime and online poly-victimisation – defined here as falling victim to different types of cybercrime.

The thesis has important academic and practical implications. From an academic perspective, it adds knowledge to the field of environmental criminology, particularly with regard to the applicability of the lifestyle-routine activity approach (LRAA) in both a non-western setting and in relation to cybercrime. Whilst the consistencies found here reinforce LRAA's theoretical applicability across contexts, the identified inconsistencies reflect the unique and complex nature of online and offline crime in Taiwan. Therefore, on the basis of this thesis, it is argued that the generalisability of LRAA should be taken cautiously in countries where crime and/or culture is of a fundamentally different nature to those settings which form the bulk of environmental criminology research.

Moreover, the thesis informs practical crime prevention. Firstly, the authority may choose to focus greater attention on tackling direct repeats rather than spatial near-targets in Taiwan, at least until further research can provide an explanation for some of the spatial irregularities observed here concerning the spread of (burglary) risk. Secondly, based on the risk factors identified in the thesis, situational crime prevention strategies might be expected to work both offline (burglary in particular) and online (verbal abuse, identity theft, fraud, virus, and poly-victimisation). Hence, this thesis could usefully inform stakeholders involved in the practical task of reducing crime in Taiwan (e.g. citizens/potential victims, social enterprise, public service, public policy designers, law enforcement, etc.) .

The impact of this thesis could occur locally and nationally within Taiwan, as the thesis would provide crime prevention insights to individuals, communities, organisations and further to the whole society across both offline and online context. The impact could also occur internationally, especially in the academic context, where the research findings from this thesis have been presented at several major conferences, included the 2018 American Society of Criminology Conference and the 2019 British Society of Criminology Conference. Submissions of findings were also accepted in the 2019 EUROCRIM and the 2020 Stockholm Criminology Symposium. However, these presentations were unfortunately cancelled due to unforeseen personal circumstances and the Covid-19 pandemic, respectively. Furthermore, the research reported here on repeat victimisation in Taiwan has been published by the Asian Journal of Criminology (doi: https://doi.org/10.1007/s11417-022-09364-9). I plan to disseminate the other findings from this thesis in other top-tier journals.

Acknowledgements

Dedicated to my deeply missed Mum who left
me and my family on 26 September 2019.
Forever you remain in my soul.

After several years of service in the Taiwanese police force, I decided to pursue a PhD to study the patterns of criminal victimisation in Taiwan. I started my academic journey with the MSc Crime Science Programme at the UCL Department of Security and Crime Science. I then stepped into the solitary endeavour within the same department.

Throughout the long PhD journey, I have however received a lot of support from a great number of people. My first and deepest appreciation goes to my supervisors, Professor Richard Wortley and Dr Aiden Sidebottom, for their initial interest in my proposal for the PhD research, their generous support and guidance, and their exceptionally helpful feedback and insights. Whenever I felt depressed, you were always there to help me out of the darkness. I will be forever grateful for being your student.

I would also like to express my gratitude to the Taiwanese government for funding my postgraduate programmes. Moreover, I have received a lot of assistance and warmth from the Education Division of the Taipei Representative Office in London, particularly from Eileen and Huichun. I would like to extend the gratitude to Professor Tien-Muh Tsai at the Central Police University, for sharing the Taiwanese victim survey dataset and providing me with an opportunity to work as a research assistant on his funded project about drug issues in Taiwan. All this makes my PhD possible.

My PhD programme was enriched by the opportunity to work as a postgraduate teaching assistant at UCL and research assistant for the 'What works in Crime Reduction Toolkit' project funded by the College of Policing. Thus, I would like to express my gratitude to Dr Jyoti Belur, Dr Sandy Shuman, Dr Amy Thornton, Dr Lisa Tompson, Dr Sanaz Zolghadriha. It was indeed my pleasure to work with you. I am especially thankful to Dr Lisa Tompson, for our collaboration in teaching and the funded research project, and even more so for her invaluable feedback at my upgrade viva. Wishing you all the best for your new endeavour at the University of Waikato.

My life in the UK has been coloured since I met my partner Jason. We have been through every happiness and difficulty. I am extremely grateful to you for making me feel loved, particularly when my mum left me in 2019 and when the pandemic broke out in the beginning of 2020. Since then, I have moved from London to Cambridge to stay with you and you are always by my side whenever I need a hug, support or even just a piece of advice for an email draft. Thank you for your constant encouragement and overwhelming generosity. My life in the UK would not have been easy without you (and of course your MacBook Pro as my birthday gift).

I am sincerely thankful to my family, Dad, Mum, my younger brother *Pin-Hung*, for their support and love. Dad, thank you for supporting me to chase my dream of studying abroad and backing me up when I decided to resign from the Taiwanese police force. 小郭, thank you for being my brother for over 30 years and taking care of dad and mum when I am far away from Taiwan. Best wishes to you that you are about to finish your PhD at the National Taiwan University soon.

My most profound gratitude is to my Mum, who raised me up with love and integrity. Thank you for being a loving and supportive mother and leaving me with beautiful memories. Perhaps I did not lose you but you just come round to me in another form. This thesis is dedicated to you.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviations	Meaning
AIM	Augmented intermediate model
BCS	British Crime Survey
BPR	Bayesian Profile Regression
CATI	Computer-assisted telephone interviewing
CIM	Constrained intermediate model
CSEW	Crime Survey for England and Wales
CSA	Child sexual abuse
DOSIH	Digital Opportunity Survey for Individuals and Households
DV	Dependent variable
EC	Environmental criminology
ICVS	International Crime Victims Survey
IV	Independent variable
LCA	Latent class analysis
LISA	Local indicator of spatial autocorrelation
LR	Likelihood ratio
LRAA	Lifestyle-routine activity approach
LRT	Likelihood ratio test
MLM	Multilevel logistic model
NCVS	National Crime Victimization Survey
NPA	National Police Agency
NRV	Near repeat victimisation
OR	Odds ratio
RAA	Routine activity approach
RV	Repeat victimisation
SCP	Situational crime prevention
SDT	Social disorganisation theory
TAVS	Taiwan Area Victimisation Survey
TYPD	Taoyuan Police Department
VIF	Variance inflation factor

Chapter 1 Introduction

This short introductory chapter provides an overview of what is to follow in this thesis. It begins by describing the main aims of the thesis. I then briefly introduce the research setting for the thesis – Taiwan – and, to help orient readers who may unfamiliar with Taiwan, provide information about key indicators and crime trends. This is followed by a discussion about why research on crime in Taiwan is important, particularly that which takes an environmental criminology (hereafter EC) perspective, as I do here. The last part of this chapter discusses the expected contribution of the thesis both to the research literature and crime prevention policy and practice, and summarises what the thesis will cover in the following chapters.

1.1 Main aims

This thesis is primarily focused on identifying and understanding the patterns of criminal victimisation in Taiwan. The main aim of the thesis is to examine patterns of crime, both offline and online, to determine if they are consistent with what would be expected following the opportunity framework that underpins EC. In doing so, this thesis explores the extent to which an EC framework is applicable to the Taiwanese context. Moreover, informed by EC, the thesis also seeks to identify the individual and area-level risk factors that explain the observed prevalence and concentration of crime, and in doing so provide practical crime prevention advice in Taiwan.

Criminology has traditionally focussed on explaining criminality rather than crime. It did so by focussing on so-called distal factors such as upbringing and poverty. EC marked a shift in the orientation of criminological research (Wortley & Townsley, 2016). It cast opportunity as a causal factor in crime and paid greater attention to the causal role played by factors existing in the immediate environment in which crime takes place (both people and objects). This shift in emphasis brought with it a need to better understand the environments in which crime does or does not occur, in order to investigate, control and prevent crime more effectively. The routine activity approach (RAA), which forms a major part of this thesis, is one of three theoretical perspectives that underpin EC (Wortley & Townsley, 2016), the other two being crime pattern theory (P. J. Brantingham & Brantingham, 1981) and the rational choice perspective (Clarke & Cornish, 1983; Cornish & Clarke, 2014).

The lifestyle theory proposed by Hindelang et al. (1978) is often combined with the RAA to produce a broader 'opportunity' framework for explaining crime patterns (Miethe et al., 1990). Briefly, the combined lifestyle-routine perspective typically focuses on the risk factors associated with criminal victimisation, namely exposure, lack of guardianship, proximity to potential offenders, attractiveness of potential targets, and specific crimes featuring specific characteristics (Cohen et al., 1981). The lifestyle-routine activity approach (LRAA) provides the theoretical background to much of the analysis reported in this thesis and is discussed in more detail in Chapter 2.

There is a large body of research concerned with the application of an opportunity framework (i.e. LRAA) to explain patterns of victimisation (Bowers et al., 2005; Cohen et al., 1981; Miethe et al., 1990; Miethe & McDowall, 1993; Tseloni et al., 2004). It is however noteworthy that most of this research has focused (a) on crime in western contexts and (b) on that we might call traditional crime types such as robbery and burglary. Discussing each point in turn.

Previous research has noted the lack of environmental criminological research in non-Western settings (see Sidebottom, 2013). In this vein, it is noted that little research attention has been paid to the applicability of the LRAA to Asian settings in particular. Proposed reasons for this lack of research in Asia include the lack of relevant crime data and the authorities' rigid control of data publication. It is widely accepted that due to the 'dark figure' of unreported crime (van Dijk, 2008; van Kesteren et al., 2014), research on victimisation patterns relies heavily on victimisation surveys more so than official police data. Nevertheless, access to such survey data is relatively limited in Asian contexts. Unlike their Western counterparts, few Asian countries conduct national victimisation surveys on a regular basis. Taiwan is an exception and has conducted a national victimisation survey every five years starting in 2005. Beyond national crime victim surveys, 12 Asian countries/cities have taken part in the International Crime Victim Survey (ICVS) between 1989 and 2005. In the 2005 sweep, for example, just Japan and Hong Kong were involved (International Crime Victims Survey (ICVS), 2021). For data that are available, Asian authorities are also arguably more reluctant to make data publicly accessible. For example, in Taiwan, police recorded crime data are not made available to the public in the way it is in England and Wales with the police.uk[1]. The same is true of Japan and South Korea, where most police recorded crime data is available only in aggregate form through periodic government reports.

Regarding the focus of environmental criminological research, in recent years it has been observed that there is a growing interest in applying the LRAA to examine patterns of online victimisation (e.g. Holt & Bossler, 2013; Maimon et al., 2013; Pratt et al., 2010; Reyns, 2013; Reyns et al., 2011; Reyns & Henson, 2016), in part because of a growing recognition that rates of cybercrime are increasingly internationally (at a time when many forms of traditional crime types have seen marked year-on-year reductions) (see e.g. Office for National Statistics, 2020). Nevertheless, despite this trend, knowledge about the determinants and patterns of cyber victimisation, particularly in atypical research settings such as Taiwan, is still underdeveloped compared to research on the patterns of direct-contact victimisation.

In light of these research gaps, this thesis aims to draw on the LRAA to better understand victimisation patterns for selected crime types in Taiwan, with the use of a variety of data sources including both police recorded data and victim surveys.

[1] The national website for policing in England, Wales and North Ireland. Police recorded crime data can be retrieved from https://www.police.uk/

Two broad categories of offences are explored in this thesis: traditional crime and cybercrime. For our so-called traditional crime, residential burglary was chosen as the crime of interest. The decision was made based on the fact that burglary is an extensively explored crime type in the West, having generated a large body of relevant research, and yet it remains comparatively underexplored in Asian settings such as Taiwan, particularly from an EC perspective. The existing research from Western settings therefore provides a useful benchmark against which to compare the findings of this research. Data collected as part of the 2015 Taiwan Area Victimisation Survey (TAVS) are used for the burglary research in this thesis. To complement the TAVS, local police recorded crime data from one region of Taiwan is analysed in this thesis, allowing an examination of repeat and near repeat burglary victimisation that is not possible using the TAVS data. In the case of cybercrime, data collected as part of the Digital Opportunity Survey for Individuals and Households (DOSIH) will be drawn upon. Whist sweeps of the DOSIH (2015-2017) provide an overview of the trends of cybercrime victimisation in Taiwan, the 2017 sweep is used in the empirical chapters here in a bid to better understand patterns of cybercrime from the perspective of LRAA. To the author's knowledge, the data collected as part of the DOSIH has hitherto not been analysed from an EC perspective.

To recap, drawing on an opportunity framework and, in particular, the LRAA, this thesis aims to examine the patterns of burglary and cyber victimisation in Taiwan, and to identify risk factors and mechanisms that can explain the observed patterns of victimisation. To achieve this, I take a quantitative approach drawing on multiple sources of data, namely the TAVS, DOSIH and local police recorded crime data. This study is the first of its kind to integrate these datasets in an effort to better understand crime patterns in Taiwan.

1.2 Why crime research in Taiwan?

Because readers outside of Asia may be unfamiliar with Taiwan, this section provides a brief introduction to the research setting and outlines what is known about crime trends in Taiwan. Comparisons of key indicators between Taiwan, the UK and the US are also provided, in order to set crime and crime research in Taiwan in an international context. Following this short overview of Taiwan as the research setting, I will then explain why it is important to conduct crime research in Taiwan.

1.2.1 Taiwan as the research setting

Taiwan is an Asian country with a population of around 23 million, where Han Chinese dominates. Taiwan is recognised as a developed country, for which the recent Human Development Index (HDI) is 0.907 (National Statistics, 2018)[2]. By comparison, the United Kingdom is 0.922, Japan 0.909 and Luxembourg 0.904 (United Nations Development Programme, 2018).

Table 1.1 shows several key indicators in Taiwan compared to the UK and the US. Taiwan is widely accepted as a socially stable society, with comparatively low crime rates. For example, Figure 1.1 shows general crime rates in Taiwan using police recorded crime data for the past two decades, with a rate of around 1,101 cases per 100,000 population observed in 2020. As a point of reference, the total police recorded crime rate in England and Wales over the same period was considerably higher at about 9,397 cases per 100,000 population (Office for National Statistics, 2021b).

[2] HDI is a criterion created by the United Nations Development Programme (UNDP) to assess the development of a country.

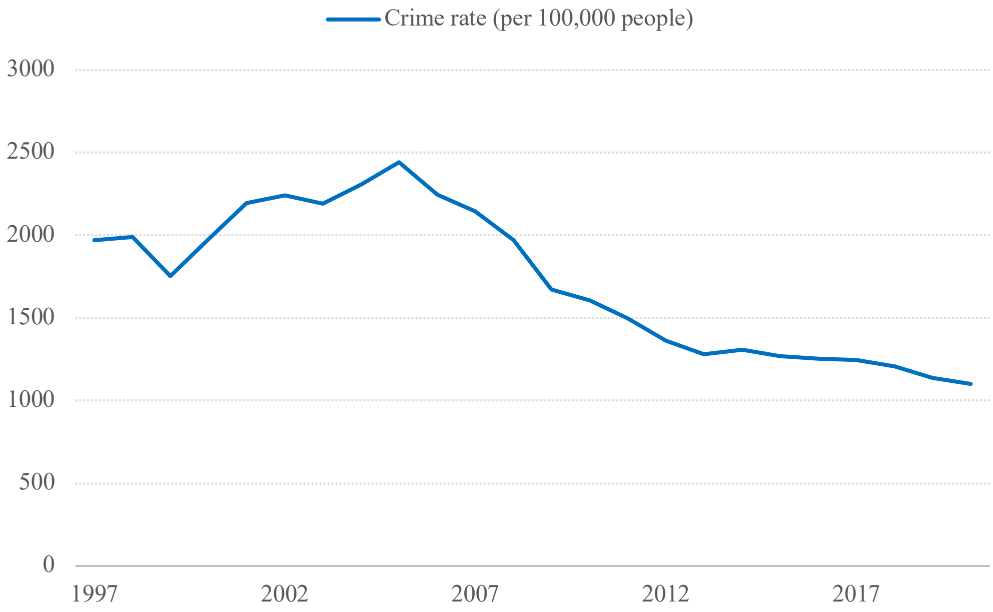
Table 1.1 Comparison of key indicators between Taiwan, UK and US

	Taiwan	UK	US
Surface area (km^2) (thousands)	36.2	243.6	9,831.5
Population (millions)	23.5	66.0	325.7
Urban population (% of total population)	61	82	81
Population density (persons per km^2)	649.0	272.9	35.6
Official language	Mandarin	English	English
HDI value	0.907	0.922	0.924
Life expectancy at birth (years)	80.4	81.7	79.5
Mean years of schooling	12.1	12.9	13.4
GNI per capita (PPP US$)	47,144	39,116	54,941
% population below poverty line	-[†]	0.2	1.2
Infant mortality rate (per 1,000 live births)	4.0	3.7	5.7

Source: United Nations Development Programme; The World Bank; Asian Development Bank; National Statistics, Republic of China (Taiwan)

[†] As Taiwan is not a member of The World Bank, this figure is missing. According to Taiwan national statistics, about 1.35 percent of the Taiwan population were below the national poverty line in 2017 (Directorate-General of Budget, Accounting and Statistics, Executive Yuan, R.O.C (Taiwan), 2020). A corresponding 16% of the UK population were in relative low income before housing costs were deducted and 22% once accounting for housing cost in 2016/2017 (McGuinness, 2018).

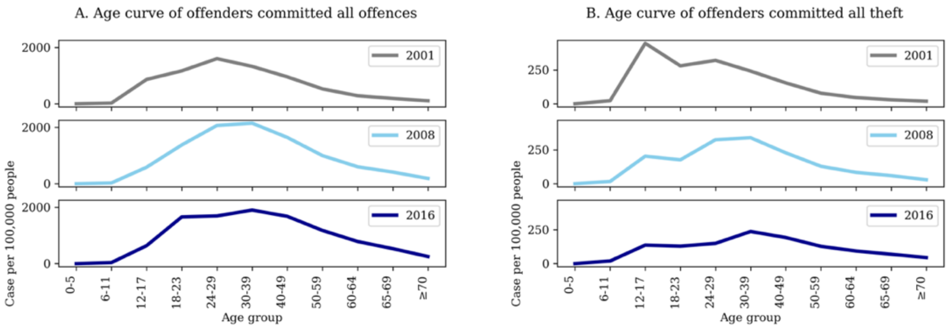
It is important to note that Taiwan, like many countries, has also experienced a substantial decline in crime over the past two decades, albeit starting somewhat later than the falls observed in the UK and US (Sidebottom, Kuo, et al., 2018). Internationally, the observed reductions in crime over time – the so-called international crime drop – have been linked to a variety of explanations including improved security, lower rates of offending amongst young people and an accompanying flattening of the age-crime curve (Blumstein et al., 2000; Farrell et al., 2014; Kim et al., 2016; Matthews & Minton, 2018).



Source: Criminal Investigation Bureau, Taiwan

Figure 1.1 General crime rates by year, Taiwan 1997-2020

Figure 1.2 displays the age-crime curves for a) all offences and b) theft in Taiwan in 2001, 2008, 2016, produced specifically for this thesis. The figure shows a general flattening over time for all offences as well as theft, a trend that is in line with that observed in other (Western) settings such as Denmark (Andersen et al., 2016), England and Wales (Morgan, 2014) and Scotland (Matthews & Minton, 2018). According to Figure 1.2, the Taiwanese offenders' age distribution of crime seems to peak at 30s while many western studies often find a right-skewed distribution with sharp adolescent peaks (aka inverted J-shape) (Farrington, 1986; Hirschi & Gottfredson, 1983; Matthews & Minton, 2017; Steffensmeier et al., 2017). Steffensmeier et al.'s (2017) comparative study supported the inconsistency in age crime curve between Taiwan and the US and called for researchers in Taiwan to give further attention to this.



Source: Criminal Investigation Bureau, Taiwan

Figure 1.2 Age curve of offenders committed crime 2001/2008/2016, Taiwan

However, research on crime should not centre merely on offenders' life-course but should also consider the trend more broadly from the EC perspective. Indeed, one of the major explanations for the international crime drop concerns changes not to offenders but to the opportunity structures which do or do not allow crime to take place, the so-called security hypothesis (Farrell et al., 2014). In this vein, it is important to understand victimisation patterns in Taiwan in more detail before we can more fully explain such crime drops. This further highlights the importance of the thesis as an exploratory study to understand victimisation patterns in Taiwan.

1.2.2 The importance of studying crime in Taiwan

There are two reasons why crime studies in Taiwan are important. First, and as mentioned previously, Taiwan has been the subject of relatively little criminological research to date. This might partly be due to the fact that crime rates in Taiwan are relatively low so that researchers find themselves with not enough data available for reliable analyses. However, research in a low-crime setting is of great importance as it could still inform the cross-contextual applicability of theories. Additionally, Taiwan also shows a consistent reduction in crime similar to that in the West (Sidebottom, Kuo, et al., 2018). It is therefore important to examine if patterns found in industrialised contexts apply to a developed non-western society where crime follows a similar trend yet has a contextual difference in prevalence.

Second, crime research in Taiwan has tended to focus on the issue of criminality, with a particular interest in juvenile delinquency (Hebenton & Jou, 2005; K.-L. Lin & Shen, 2016; W.-H. Lin & Mieczkowski, 2011; Sheu et al., 2018; S.-N. Wang & Jensen, 2011). Research in the tradition of EC taking place in Taiwan is limited, either in terms of online or offline contexts. Furthermore, as a former Taiwanese police officer, I recognise that drawing on research evidence to inform crime prevention and policing is seldom done in Taiwan. There is not an established evidence-based policing movement nor tradition of researchers working closely with practitioners. Mindful of these barriers, the findings reported in this thesis might bear relevance to crime prevention in Taiwan. I therefore expect my research on crime patterns in Taiwan to provide evidence-based implications for academia and crime prevention particularly from the perspective of EC.

Briefly, then, Taiwan was chosen as the study site for this thesis because of the identified gaps in research and the marked differences in trends and prevalence of crime from the Western countries where the bulk of comparable research has been undertaken.

1.3 Expected contribution to the literature and practice

Based on the research gaps described above, this thesis is expected to add to the research literature and inform crime prevention practice in four main ways.

Firstly, the thesis helps assess the generalisability of EC theories to atypical understudied settings, in this case Taiwan. Empirical research on crime victimisation in such settings can help better understand the mechanisms giving rise to crime (patterns), help refine the theories and generate knowledge to inform crime prevention. Furthermore, through studying cybercrime patterns from an opportunity perspective, the thesis also contributes to the growing literature on the applicability of LRAA beyond offline victimisation to online victimisation. Put simply, this thesis adds knowledge to the generalisability of EC across contexts (i.e. non-western or online contexts).

Second, the thesis contributes to the literature on repeat victimisation and the less-discussed field of poly-victimisation. Briefly, repeat victimisation (RV) refers to the same victim/target experiencing the *same* type of crime incident within a specific period of time – normally a year (Weisel, 2005). On the other hand, poly-victimisation refers to a target experiencing *different* types of criminal victimisation over a given time period (Finkelhor et al., 2007a). This thesis analyses both RV and poly-victimisation in Taiwan. Observed (in)consistencies would contribute to the literature and the practice of crime prevention. For example, consistent patterns would suggest that the mechanisms in operation in the western and non-western settings are alike. By contrast, inconsistent patterns would however invoke a rethinking of what explains the patterns observed in Taiwan, with obvious implications for prevention. Furthermore, by providing one of the first studies to explore online poly-victimisation in Taiwan, this thesis can help policy makers and practitioners develop protective strategies that deal with not only one specific type of cybercrime but online victimisation more generally.

Third, the thesis uses innovative quantitative approaches to identify crime patterns in Taiwan – in particular Bayesian models borrowed from medical research. Bayesian Profile Regression (BPR) is used here to model cybercrime victimisation because it avoids potentially biased inferences which occur in analyses that contain categorical dependent variables and inter-related independent variables, as is commonly observed in survey datasets (Molitor et al., 2010). To my awareness, Vakhitova et al.'s (2019) study was the first attempt to apply BPR to crime research, yet it was concerned with cyber abuse (defined by researchers as receiving abusive messages or comments online) alone. This thesis is hence the first piece of empirical research that uses BPR to model a wider range of cybercrime victimisation.

Lastly, the research contributes to crime research in Taiwan. As stated earlier, crime research in Taiwan has overwhelmingly focussed on criminality and young people's delinquency. Therefore, this thesis marks a shift in crime research in Taiwan from the perspective of distant causes of crime to the immediate environment in which crime occurs. Furthermore, should the thesis identify patterns and risk factors of cybercrime victimisation in Taiwan, it bridges the literature gap in which previous Taiwanese research used to focus on the manifestation of cybercrime. By adding knowledge to crime research in Taiwan, the thesis would inform practical crime prevention strategies.

1.4 Summary of the thesis

The text above provides a background to this thesis and outlines what I aim to achieve in the research reported here. The structure of the remainder of this thesis is as follows. Chapter 2 introduces the theoretical foundations supporting the thesis. It begins with a review of the literature on EC and the LRAA in particular, followed by its application to burglary and cybercrime victimisation, the two categories of crime which are focussed on here. Then, the literature on repeat victimisation and poly-victimisation is briefly reviewed. Lastly, based on the presented literature review, the research questions to be addressed in this thesis are outlined.

Chapter 3 provides an overview of the data sources used in this thesis. It begins with an overview of different measures of crime and explains why victim surveys are suitable for measuring victimisation. The chapter then describes the two main data sources used in the thesis – the TAVS and DOSIH – and identifies their limitations .

Chapters 4 to 7 contain the empirical contributions of this thesis. Each chapter addresses specific questions regarding crime patterns in Taiwan. All studies begin with descriptions of the specific issue of interest, along with a short review of the relevant literature, building on that covered in Chapter 2.

Then each study is structured around the hypotheses to be tested, features of the data to be used, measures and analytical strategies to be employed, findings and finally a discussion of the results, their implications and limitations.

Chapter 4 examines the patterns of burglary victimisation in Taiwan using data from the TAVS. The study uses Chi-square analysis, latent class analysis and single-level logistic regression to examine, amongst other things, how a household's security practices are associated with reported experiences of burglary victimisation. Multilevel logistic regressions are also conducted to examine the effect of individual- and area-level characteristics on burglary victimisation, informed by the theories discussed in Chapter 2.

Chapter 5 continues the analysis of burglary, but whereas Chapter 4 looks at the prevalence of burglary, Chapter 5 explores the concentration – both RV and near RV – of burglary in Taiwan, .drawing on both crime victim survey and local police data..

Chapter 6 marks the shift from offline victimisation to online victimisation. It is concerned with four types of cybercrime victimisation in Taiwan, as defined and measured by the DOSIH: verbal abuse, identity theft, fraud and virus. Using data from the DOSIH, this study employs multiple logistic regression models to examine and compare the observed patterns of these four types of cybercrime victimisation.

Building on Chapter 6, Chapter 7 examines poly-victimisation among victims of cybercrime. To this end, BPR models are used to build a profile of cyber poly-victims as compared to victims experiencing only one type of cybercrime.

Lastly, Chapter 8 brings together what has been found in this thesis and what it means for research and practice. It first reiterates the main aims of the thesis. It then summarises the main findings of each empirical study as they relate to the stated research questions. Following that, the theoretical and practical implications of the findings are discussed. I then review the limitations of the research and suggest avenues for future research. The last section draws out what I consider to be the main conclusions from this thesis.

Chapter 2 Literature Review

This chapter reviews the literature on crime patterns and trends, with a particular focus on the two main types of offences covered in this thesis: burglary and cybercrime. It begins by outlining the theoretical foundations of environmental criminology, the routine activity approach and the lifestyle perspective. It then discusses how these crime opportunity theories can be applied to both explain and prevent criminal victimisation, focussing mainly on burglary and cybercrime. The bulk of this discussion relates to criminal victimisation per se. However, towards the end of this chapter the literature is also reviewed on the concept of repeat victimisation and poly-victimisation, both of which are investigated in later chapters of this thesis. The chapter concludes by setting out the research questions that will be addressed in the thesis.

2.1 Environmental criminology

The term environmental criminology was first mentioned by Jeffery's (1971) in his seminal book *Crime Prevention Through Environmental Design*, in which he discussed ideas for designing out crime by reviewing the role of architecture and town planning (Wortley & Townsley, 2016). The term has developed and expanded significantly since Jeffreys. Nowadays, EC refers to a family of theories with a shared focus on crime events and the immediate environment in which crime occurs. Currently EC is said to comprise three main pillars – rational choice perspective (Clarke & Cornish, 1983; Cornish & Clarke, 2016), crime pattern theory (P. J. Brantingham et al., 2016; P. L. Brantingham & Brantingham, 1993), and routine activity approach (Cohen & Felson, 1979; Felson, 2016). In the interests of completeness, the next two sections provide a brief overview of rational choice and crime pattern theory. This is then followed by a more detailed discussion of RAA, since this is the theoretical perspective which informs much of the empirical analyses reported in later chapters.

The rational choice perspective was proposed by Clarke and Cornish (1983). It provides an important insight into recognising the influence of the immediate environment on decision-making and, by extension, behaviour. Rational choice perspective suggests that criminal behaviour is purposive and rational. Offenders are thought to take actions to achieve goals (e.g. desires for excitement, admiration, revenge, resources). Considering their motives and goals, rational choice perspective argues that offenders try to select the best actions to achieve their goals. Put differently, offenders make decisions about their engagement in specific crimes. Crime commission is driven by offenders' specific motives, goals and benefits. In this sense, criminal behaviour is considered rational and the criminal decision-making is crime-specific. Rational choice perspective is not a falsifiable theory. Nor does it claim to be a full and complete account of the offender decision-making process. Rather, the rational choice perspective was proposed to provide a heuristic to help analyse the situations that influence crime events and better understanding those situations and inform the development and implementation of strategies designed to prevent or disrupt criminal activities (Cornish & Clarke, 2016).

Crime pattern theory focuses on why crime tends to concentrate. It proposes that the clustering of crime is shaped by human activities. These activities involve "*where people live within a city, how and why they travel or move about a city, and how networks of people who know each other spend their time"* (P. J. Brantingham et al., 2016, p. 112), of which activity nodes (e.g. home, work, shopping and entertainment, etc.) are created. Crime pattern theory holds that criminals are more likely to commit crimes in and around their activity nodes and the paths that link them, around which the offenders' awareness spaces are formed. The reason that offenders prefer to commit crimes in their awareness spaces is because they are more likely to know the opportunities and risks in these spaces. Simply put, crime concentrates where the awareness space of offenders overlaps with the awareness space of victims (Felson & Clarke, 1998). Crimes are thus unevenly distributed in time and space near criminals'/victims' activity nodes and activity spaces. Crime pattern theory is to understand such concentration of crime and so that crime prevention can be informed.

The following section discusses the third theoretical perspective which is generally considered to be the final theoretical pillar of EC – RAA, and how it is often extended to form the lifestyle-exposure perspective (Cohen et al., 1981).

2.1.1 Routine activity approach

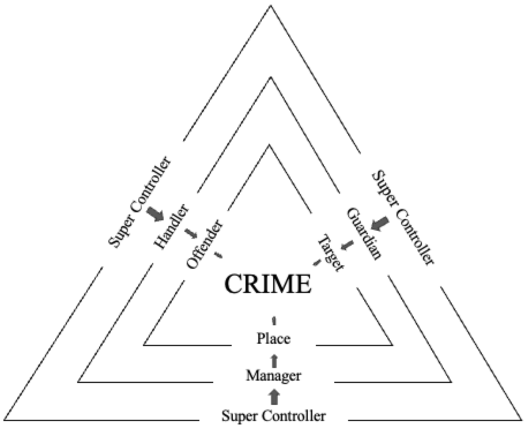
RAA was initially proposed to explain rising crime rates in the United States following WWII (Cohen & Felson, 1979). These crime rate trends were mainly attributed to structural changes in the routine activity patterns of the US population, such as increases in the number of single-adult households and greater participation in the workplace, especially among females (Felson & Cohen, 2011). In this sense, RAA demonstrated that ecological changes that are unrelated to crime can affect the likelihood that crime occurs and the way in which it is patterned. For example, an increased trend of people working in the daytime and hence leaving their houses unguarded was linked to an increased residential burglary rate during the day. Importantly, this pattern went against conventional wisdom (and prevailing theories in criminology) about the exclusive role of criminality in explaining crime and contributed to the development of opportunity-based crime theories.

RAA is both a macro- and micro-level theoretical perspective. At the macro level, the RAA shows how crime patterns can be explained by the supply, distribution and movement of victims, offenders and guardians, often as a result of everyday societal and economic developments that are not related to crime. At the micro level, RAA identifies those elements which need to come together for crime to occur. According to RAA, crime is dependent on the convergence of three elements: motivated offenders, suitable targets and the absence of capable guardians (Cohen & Felson, 1979).

Discussing each of these elements in turn. A motivated offender refers to anyone with the inclination to commit crime. A suitable victim or target includes any person or thing that may evoke an individual's disposition to offend and is vulnerable to victimisation. A guardian is someone or something that serves a supervisory function against crime, and whose presence reduces the likelihood that crime will occur. According to RAA, the convergence of these three elements might not definitely lead to crimes, but the absence of any of these elements will generally make crime not possible. Simply put, crime events occur when motivated offenders meet suitable targets in time and space without the presence of capable guardians (see e.g. Cohen & Felson, 1979; Felson & Boba, 2010; Maxfield, 1987; Robinson, 1999).

2.1.1.1 Crime triangle

The RAA is a theoretical framework. It provides a simple and highly influential account of why crime happens, and how crime can be affected by otherwise positive societal and technological developments (such as more women entering the job market). Inspired by the RAA, John Eck proposed the crime triangle in an effort to translate Felson's ideas into a tool to inform the analysis and response of crime problems (Eck, 2003). This is shown in Figure 2.1 (Eck, 2003; R. Sampson et al., 2010).



Source: Eck (2003); R. Sampson et al. (2010)

Figure 2.1 RAA's crime triangles

The crime triangle is actually made up of three separate triangles. The inner triangle contains the three necessary elements for a crime to occur as set out by the RAA, namely a motivated offender, a suitable target/victim and a place (lacking in guardianship). The outer triangle consists of the potential '*controllers*' (i.e. a collective term coined by Eck as guardians) who must be absent or ineffective for a crime to occur (Tillyer & Eck, 2011). To put it simply, a crime occurs when three sorts of controllers are missing, insufficient or ineffective: the handler absent from the offender; the guardian absent from the target/victim; and the place manager absent from the crime setting (i.e. place). There is also an outermost triangle comprising 'super controllers' – those who control the controllers (i.e. handlers, guardians and managers). Super controllers, as understood by Eck and colleagues, refer to people and organisations that provide incentives for controllers to act appropriately in the interests of prevent crime (R. Sampson et al., 2010). Table 2.1 summarises the types and examples of super controllers proposed by Sampson et al. (2010). Briefly, there are three categories of super controllers – formal, diffuse and personal super controllers. Formal super controllers depend upon formal authority to control the controllers. Diffuse super controllers are not single entities like formal super controllers but are collections of super controllers with the potential to influence controllers. Personal super controllers are individuals who, depending upon their personal and informal sets of social networks, can exert an influence on controllers.

To summarise, the RAA states that crime is likely to occur when motivated offenders meet suitable targets at places without the presence of effective guardians (Felson, 2016). In this sense, crime prevention can rely on altering these three elements to make crime less likely to occur. Crime triangles derive from the RAA and conceptualise guardians into three types of controllers. To explain why some controllers fail to take appropriate action to prevent crime, the crime triangles introduce the concept of super controllers. Super controllers provide incentives for controllers and influence them to be

Table 2.1 Types of super controllers

Category	Type	Examples
Formal	Organisational: influence controllers within the organisation	A nightclub chain replaces glass mugs with plastic ones to reduce injuries in bar fights (the bar managers have control over the bar and the chain has organisational control over them)
	Contractual: provide obligations among entities	Landlords set contractual agreements with property management companies to maintain the properties (the property managers have control over the property sites and property owners have contractual control over them; below such a relationship applies so the explanations are omitted)
	Financial: financial institutions control the controllers to prevent crime	An insurance company pressures a rental car company to prevent theft of vehicles or the insurance rates will be raised
	Regulatory: government agencies make controllers comply with the rules	Governments make security measures such as immobilisers compulsory in new cars to prevent vehicle theft
	Courts: civil and criminal courts influence controllers' behaviours	The use of nuisance abatement: property owners being taken to court when they fail to deal with problems on their property.
Diffuse	Political: provide incentives and disincentives for controllers to prevent crime	Political super controllers act especially when the government regulatory agencies do not have the powers to intervene. The legislations that ask store owners to restrict pseudoephedrine sales
	Markets: markets exert pressure on controllers, especially place managers	A list of 'certified' landlords released by universities as a market incentive to improve housing standards so that students may be protected from victimisation and drinking problems
	Media: publicity incite or steer controllers to prevent crime	Media attention may directly change controllers' behaviour, stimulate political/regulatory action, or trigger other super controllers
Personal	Groups: peer group pressure control controllers at either individual or organisational levels	Companies in the alcohol industry jointly created social responsibility standards for producing and selling alcoholic drinks
	Family: members of families influence other members' intervention with crime prevention	Typically, those who influence handlers, such as foster children's organisations that act as super controllers (both contractual and family) over foster parents.

Source: R. Sampson et al. (2010)

effective in crime prevention. For example, the bar managers as place managers have control over the bar and they are expected to intervene in preventing bar violence. But what if managers do not act appropriately? In this case, the company or organisation that has control over the manager can step in as a super controller to create incentives for the controller to take crime preventive actions (see examples in Table 2.1). Crime triangles thus have important implications for putting the RAA into practice in the service of crime prevention.

2.1.1.2 Clarification of routine activity approach – defining guardianship

Both RAA and crime triangles reinforce that the convergence of offenders, victims, absent capable guardians makes crime more likely to occur. Of these three key elements, offenders (people who choose to commit crime) and targets (people or things on which offenders choose to prey) are more self-evident than the concept of guardianship, which varies greatly in the literature (Hollis, 2013). The lack of a standard definition (and measurement) of guardianship means it is important to clarify the concept of guardianship being used in this thesis. This clarification is provided below.

To recap, guardianship in the RAA refers to the ability of persons and objects to prevent a crime from occurring (Cohen et al., 1981; Tseloni et al., 2004). Guardianship can take several forms, either by the presence of a guardian alone or by their direct or indirect action (Cohen et al., 1981). Therefore, it may comprise the broader classification as controllers in crime triangles – guardians protecting targets, handlers supervising offenders and managers maintaining places (Eck, 2003).

In prior research, guardianship has been measured in different ways and using different methods. Proxy measures are often centred on estimates of guardians' presence and indicators of security and personal/self-protection (Reynald, 2009; Reynald et al., 2018). In the case of burglary, for example, researchers have applied several measurements to evaluate the presence of guardians. Measurements may include household composition, marital and employment status, lifestyle indicators and whether occupants have neighbours who watch a dwelling when it is unoccupied (Tseloni et al., 2004). Indicators of security and personal/self-protection might be physical security devices, including burglar alarms or external lights (e.g. Coupe & Blake, 2006; Miethe & McDowall, 1993; Tewksbury & Mustaine, 2003; Tseloni et al., 2004).

This variation in how guardianship is operationalised suggests that guardianship, in RAA terms, is a rather vague concept which needs refining. To this end, Hollis et al. (2013) distinguished between the role of guardianship and target hardening in crime prevention. According to their clarification, target hardening is about decreasing the suitability of targets rather than increasing the availability of capable guardians. For instance, protective mechanisms such as extra locks make it harder for offenders to successfully complete burglary. Nevertheless, it does not involve human elements and hence it is regarded as an example target hardening rather than improved guardianship (Hollis et al., 2013; Hollis-Peel et al., 2011).

However, some researchers have a different opinion on human elements in defining guardianship. Felson and Boba (2010) suggested that not all human guards are in fact guardians. They argued that private guards as unlikely to be present when a crime occurs. Because those security guards do not deter or control untoward behaviours; they should not be considered as capable guardians. This conflicts with Hollis et al.'s (2013) guardianship construct, in which private guards, with human elements involved and an increased availability of capable guardians, should be considered as guardianship. In this vein, the disputes in defining guardianship also occur to physical security. Based on Felson and Boba's (2010) argument, physical security can in some cases be regarded as guardianship because they deter or control untoward crime behaviours. However, as mentioned, Hollis et al.'s (2013) guardianship construct classified physical security as target hardening techniques rather than capable guardians because physical security does not involve human elements.

The disputes above highlight some of the complexity involved in defining guardianship for research purposes and shows that presently there is no universally accepted measurement of guardianship. How it is measured will also vary by crime type. To avoid further dispute, for the purposes of this thesis, I take the broad definition of guardianship originally proposed by Cohen et al. (1981) as "*the effectiveness of persons (e.g. housewives, neighbours, pedestrians, private security guards, law enforcement officers) or objects (e.g. burglar alarms, locks, barred windows) in preventing violations from occurring, either by their presence alone or by some sort of direct or indirect action*" (p. 508). In this sense, guardianship refers to persons and objects who have the potential to prevent the occurrence of crime. Guardianship therefore might take on two forms: (a) physical guardianship, such as individual-level target hardening, place management, surveillance measures and neighbourhood-level target hardening; and (b) social (interpersonal) guardianship such as (in)formal social control and natural surveillance measures (Tseloni et al., 2004; Wilcox et al., 2007).

2.1.2 Lifestyle perspective

In addition to the RAA, the so-called lifestyle perspective is the other heavily researched theoretical perspective when speaking of victimisation patterns (Meier & Miethe, 1993; Pratt & Turanovic, 2016). Related to routine activity, researchers believe that personal victimisation is related to an individual's 'risky' lifestyle (Cohen & Felson, 1979; Hindelang et al., 1978; R. J. Sampson & Lauritsen, 1990). Hindelang et al. (1978) initially proposed the lifestyle-exposure perspective, suggesting that the amount of time individuals spend in public places, their interaction with others, and their demographic characteristics affect their suitability as and likelihood of being crime targets. More specifically, a person's exposure to "*high risk times, places and people*" makes them prone to experience victimisation (Hindelang et al., 1978, p. 245).

Researchers have further suggested that different background characteristics and daily activities affect the extent to which an individual's lifestyle is 'risky' from the perspective of criminal victimisation (e.g. Kennedy & Forde, 1990). For example, research finds that individuals with a higher level of exposure to deviant peers exhibit a higher level of risky lifestyle and thus are linked to a higher likelihood of dating violence victimisation (Vézina et al., 2011). Furthermore, males and adolescents are more likely to be victimised given their riskier lifestyles (e.g. exposure to the public, substance or alcohol use) compared to their female and older counterparts (Barrera, 2018; Mustaine & Tewksbury, 1998; Tewksbury & Mustaine, 2010). Such a perspective therefore suggests that victims and offenders share similar demographic or spatial profiles and thus lifestyle patterns influence individuals' exposure to risk of crime.

Lifestyle patterns correlate with individual-level proximity to crime and deviant behaviours (R. J. Sampson & Lauritsen, 1990). However, some researchers question whether the risk of victimisation might reflect demographic homogeneity in offense activity rather than a target's attractiveness or its proximity to motivated offenders. The correlation between crime victimisation and proximity might be a by-product of offenders' high probabilities of becoming targets rather than exposure to risks, especially in the case of violent crime. When controlling for the effect of living in a high crime area, Bottoms and Costello (2010) found that offenders themselves were very likely to suffer burglary (re)victimisation. This suggests that proximity to crime at the individual-level is not sufficient to draw an ecological inference (Jensen & Brownfield, 1986). Instead, it may require further examination on criminogenic factors at a neighbourhood level to see if the high risk of victimisation is derived from exposure to community-level factors or merely because the paths of offenders overlap with victims. To sum up, the lifestyle-exposure perspective accounts for variations in criminogenic exposure for differences in lifestyles, of which criminogenic exposure includes both direct exposure to criminogenic circumstances and exposure to individuals with similar criminogenic lifestyles (Engström, 2020).

2.1.3 Comparing routine activity approach and lifestyle perspectives

Both the lifestyle perspective and the RAA state that victimisation is related to the ‘lifestyle’ and ‘daily activities’ of individuals. Given their similarities, these two theoretical perspectives are often merged as part of empirical research into the so-called lifestyle-routine activity approach (which will be discussed later). However, despite this common tendency to combine the two approaches, there are in fact a few important differences between these two theoretical approaches which warrant mention here.

First of all, the lifestyle-exposure perspective focuses on ‘voluntary’ activities that might put individuals at greater risk of victimisation, whereas the RAA considers broader contexts which affect crime. It includes, for example, less discretionary activities, such as going to work, and how these activity patterns affect crime. The respective centres of focus of these two approaches are hence different. The lifestyle perspective is rooted in individual-level risky activities, while the RAA starts from structural changes in routine activity patterns to explain variation in crime at the macro level (though, as noted, later expanded to include individual-level analysis). The RAA further highlights the impact of “legitimate activities” (e.g. commute to and from work) on patterns of crime since such daily activity are unavoidable (Allen & Felson, 2012; Lemieux & Felson, 2012; Sidebottom, 2013). The occurrence of crime is seen to be more about the dispersion of legitimate activities rather than any ‘risky’ activities on the part of victims (Cohen & Felson, 1979; Messner & Blau, 1987).

Pratt and Turanovic (2016) have differentiated the lifestyle-exposure perspective from the RAA in a different way. They argue that the two theories perceive the ‘risk’ of victimisation very differently. The lifestyle perspective puts more emphasis on an individual’s exposure to ‘high risk elements’ and regards both risk and victimisation as a matter of ‘probability’. For example, individuals’ participation in risky behaviours, such as staying out late at night, does not make them inevitable victims but such involvement enhances their odds of being victimised. Compared to the lifestyle framework, which emphasises the effect of risky lifestyles on increasing personal victimisation, the RAA focuses on describing the victimisation event itself. It does not explore an individual's 'probability' of being victimised but emphasises the spatial and temporal convergence of motivated offenders, suitable targets, and the absence of capable guardians. From the perspective of RAA, if any of these three elements are absent, victimisation will not happen (i.e. the probability of victimisation is in fact zero). Therefore, it is of little importance for the RAA to discuss an event with 'zero probability' of victimisation. Conversely, the probability of victimisation dependent on individuals' exposure to risk elements remains important in lifestyle perspectives.

2.1.4 Combining routine activity approach and lifestyle perspectives – Lifestyle-routine activity approach

Despite noted differences in the routine activity and lifestyle perspectives (Maxfield, 1987; Pratt & Turanovic, 2016), both approaches mention personal exposure to risk as providing varying opportunities for victimisation. The LRAA is thus often referred to as an 'opportunity model', which focusses on five factors implicated in risk of criminal victimisation: *"exposure, guardianship, proximity to potential offenders, attractiveness of potential targets, and definitional properties of specific crimes themselves*[1] *"* (Cohen et al., 1981, p. 505).

The aforementioned opportunity model suggests that opportunity is dependent on the environment and varies across specific types of crime (i.e.

[1] Definitional properties of specific crimes by Cohen and the colleagues refer to the that specific crimes feature specific instrumental actions (or say lifestyle-routines and knowledge) by potential offenders. For example, compared to general larcenies, burglaries may require offenders' more awareness of victims' routine activities (e.g. about if the dwelling is occupied) and commands of techniques (e.g. ways to break in a dwelling).

‘the definitional properties of specific crimes’). Put simply, opportunities depend on the environment so that, for example, target attractiveness varies with offenders’ familiarity of surroundings. Opportunities vary across specific types of crime so that, for instance, compared to larceny offenders, burglars evaluate occupancy more than the potential target value in decision-making (Roth & Trecki, 2017). Overall, opportunity changes with the environment so risk of victimisation may vary by individual and environmental characteristics (R. J. Sampson & Wooldredge, 1987). The opportunity model highlights that both individual- and neighbourhood-level measures of risk factors are necessary for researchers because they allow examination on potential and actual criminogenic circumstances.

The reason for stressing the importance of opportunity in the environment is not only because opportunity plays an important role in crime but because opportunity differs for different forms of crime. The examination of criminogenic circumstances helps us understand patterns for specific types of crime. More importantly, as outlined later in this chapter (2.2.3), understanding opportunity structures is crucial for the implementation of situational crime prevention (Clarke, 1995, 2016).

Overall, inspired by such crime-specific opportunity perspectives, the following sections focus on their application to offline and online contexts, both of which are featured in the empirical analyses reported in later chapters of this thesis.

2.2 Explaining patterns of victimisation: an opportunity perspective

Many studies have applied the aforementioned opportunity framework to explain patterns of criminal victimisation. The following sections provide an overview of this research, demonstrating how the LRAA has (and can) been applied to both traditional offline context and to cyberspace.

2.2.1 Opportunity in traditional offline contexts (with a focus on burglary)

Since the foundation of EC in the 1970s (see Wortley & Townsley, 2016), the influence of opportunity in the environment has been gradually and heavily used to explain a variety of crimes in an offline context, including predatory crime such as larceny (Mustaine & Tewksbury, 1998), motor vehicle theft (Copes, 1999), arson (Pooley & Ferguson, 2017), child abuse (Khade et al., 2018), homicide (Beauregard & Martineau, 2015) and organised crime (Kleemans & Van de Bunt, 2008). In light of the focus of this thesis, the following sections discuss burglary research from an opportunity perspective, drawing on both the dominant Western literature as well as the smaller (but growing) Asian literature.

2.2.1.1 Burglary research in western literature

Residential burglary accounts for arguably the greatest amount of research from an opportunity perspective. Opportunities for this crime type can be thought of in main ways: individual (or household) and neighbourhood levels. At the individual level, the property itself offers opportunities for burglary in three main ways: target attractiveness, accessibility, and guardianship. Target attractiveness, often measured by family income, has been shown to be positively associated with the risk of burglary victimisation (Miethe & McDowall, 1993; Miethe & Meier, 1990). The inference is that people with higher incomes will live in more expensive properties and in affluent areas, and that their houses will, on average, contain more attractive items to steal. Accessibility of the property refers to how easy it is for the potential burglar to gain entry to the property. For example, burglaries have been found to disproportionately concentrate on the ground-floor units of a dwelling, as opposed to those higher up which, all things being equal, are likely to be less accessible (Robinson & Robinson, 1997). Lastly, guardianship refers to how protected the property is perceived to be. A simple example might be signs of occupancy that deter burglars from breaking into the house (Maguire et al., 2010).

With regard to opportunities for burglary victimisation at a neighbourhood level, several neighbourhood characteristics have been identified in prior research. These include (in)direct measures of proximity to potential offenders and (social) guardianship. The former might be exposure and proximity to crime or disorder while examples of the latter include population density (Battin & Crowl, 2017), neighbourhood poverty (Sharkey et al., 2017) and so on.

A place exposed to crime and disorder is more likely to attract a pool of potential offenders (R. J. Sampson & Raudenbush, 1999) than a place without such an exposure. This is because offenders' journey to crime are often short (Townsley et al., 2015; Townsley & Sidebottom, 2010) and are consistent with their routine activities. Offenders are also more likely to commit crimes in areas with which they are familiar (P. L. Brantingham & Brantingham, 1993; Eck, 1993). In terms of burglary, offenders' familiarity with an area has been shown to be a significant predictor of offenders' location selection (Frith et al., 2017). Hence, the places with closer proximity to crime or disorder cast opportunities for crime due to its close proximity to a pool of potential offenders. To avoid repetition and facilitate a smooth flow of this chapter, the measure of such an exposure to crime and its effect on burglary victimisation as an environmental factor will be detailed in Chapter 4 (Section 4.1.1.3).

Furthermore, population density may be an indirect measure of guardianship on the assumption that there are more potential guardians present around a dwelling that is located in a highly populated area. The logic linking neighbourhood poverty to guardianship is less straightforward. It is suggested that houses located in disadvantaged neighbourhoods might be exposed to a decreased level of capable guardianship due to a lack of (in)formal social control and limited access to crime prevention-related public resources (e.g. formal surveillance) (Battin & Crowl, 2017; Hipp & Roussell, 2013). This weakened function of guardianship is linked to social disorganisation theory (SDT) – in deprived environments (in)formal social control is typically in short supply, resulting in weakened guardianship against crime, including burglaries. Again, the impact and measurement of social (dis)organisation on burglary will be provided in Chapter 4 (Section 4.1.1.2).

A great body of Western literature has applied the opportunity perspective to examine burglary victimisation. Compared to that, burglary research has received less attention in Asian settings. Below I discuss the limited findings observed in Asia. To avoid overgeneralisation, it is noted that, unless specified, the Asian setting referred in this thesis is limited to (south)east Asia, of which region Taiwan makes a part.

2.2.1.2 Burglary research in Asia

There is a small body of literature dealing with burglary victimisation in Asia. Table 2.2 summarises the main research on burglary victimisation in Asia, predominantly in (south)east Asia as defined earlier. There are 12 studies identified, among which four explore burglary victimisation and eight focus on (near) repeat burglary victimisation (I will return to repeat victimisation in Section 2.3).

Across the four studies on single burglary victimisation, the range of reported victimisation is extreme, from about four percent in China (L. Zhang et al., 2007) and Taiwan (H. C. Wang, 2015) to 29 percent in South Korea (Roh et al., 2010). It is noted that burglary victimisation reported in China contains victims' experience of victimisation within the past *five* years; one year is more common for victim surveys. The lower burglary rate observed in the studies from China and Taiwan may demonstrate a lower rate of

Table 2.2 Summary of research into burglary and repeat burglary victimisation in Asia

Author(s)	Date of publication	Location	Data	Sample size	Time frame	Focus	Key findings relevant to burglary victimisation
Chiew et al.	2020	Malaysia	Police recorded crime data & official socioeconomic data	648 burglaries	2011 - 2016	Spatial analysis of burglary victimisation	• No information about the extent of victimisation • Burglaries were affected by fundamental socio-demographic variables and burglars' behaviours • Factors related to burglary risk include: a) Property's building types: Bungalow and flat experienced more burglary incidents b) Physical security level (dogs, alarms, locks amount, and the fence types of the building): negative relationship with burglary risk c) Education level of the residents: neighbourhoods with wealthy status and financial resources of highly educated residents experienced a higher density of burglaries d) Neighbourhood's working group density: burglaries were centralized in neighbourhoods with a high density of working group residents e) Immigrant Factors: burglaries were positively related to neighbourhoods' immigrant levels f) Old resident Factors: burglaries were positively related to neighbourhoods' old-resident levels (people aged 55 yrs.)
Hino & Amemiya	2019	Japan	Police recorded crime data	8,845 burglaries	Jan 2005 - Dec 2014	RV&NRV	• 31% of all burglary incidents occurred in once-burgled multifamily buildings; 8.4% of all burglaries occurred in once-burgled dwelling units • Risk of RV of a unit significantly communicated within 160 days from the originator incident • Burglaries were spatially and temporally concentrated in burgled buildings' neighbourhoods. The risk communicated 60 days within 200 metres of an offended place • The risk of NRV did not decay uniformly by temporal and spatial proximity to the offended place, with several peaks being observed within the defined range

(Continued)

Table 2.2 *(Continued)*

Author(s)	Date of publication	Location	Data source	Sample size	Time frame	Focus	Key findings relevant to burglary victimisation
Z. Wang & Liu	2017	China	Police recorded crime data	4,226 burglaries	1 Jan - 30 Dec 2013	NRV	• Demonstrated the existence of hot spots in a Chinese city • Regions in the vicinity of hot spots shared a similarly high risk • The risk of NRV could expand for 42 days and 1 km
S. -Y. Kuo	2015	Taiwan	2000 Taiwanese victim survey	10,354 survey respondents	Jan - Dec 1999	RV	• Opportunity model applied • 1.5% HHs experience RV (401 incidents or say 47.2%)
H.C. Wang (Chinese)	2015	Taiwan	2000 Taiwanese victim survey	10,354 survey respondents	Jan - Dec 1999	Single-level logistic regression of burglary victimisation	• 3.78% households experienced burglary in the past year. • Factors related to burglary risk include: a) Positive relationship: 1) the social disorganisation phenomenon of a dwelling's neighbourhood; 2) living in a family of three-generation family, or grandparent-grandchildren family; 3) households with more motor vehicles; 4) detached houses and low-rise buildings; 5) longer period of residence; 6) located in eastern and southern Taiwan; 7) owners' unemployment status b) Negative relationship: the level of security (including private security guards, police connection system, CCTV camera, burglar alarms, security chains, iron-barred windows, dogs, timer, light sensors)
Wu et al.	2015	China	Police recorded crime data	10,548 residential burglaries	2013	NRV	• Risk of the same location experiencing a second burglary within the next 7 days from the initial incident is over 600% greater than the city's average risk level • Should the crime prevention measures focus on targets within 120 metres of any burglarised location within 14 days after an initial event, 16% of the city's burglaries could be prevented
Ye et al.	2015	China	Police recorded crime data	882 residential burglaries	Jan - Jun 2013	NRV	Within 100 metres and 7 days after a residential burglary happens, the risk of victimisation is 55% more than the average

(Continued)

Table 2.2 *(Continued)*

Author(s)	Date of publication	Location	Data source	Sample size	Time frame	Focus	Key findings relevant to burglary victimisation
Tseng (Chinese)	2014	Taiwan	Interviews	31 serial burglars	N/A	NRV	80% chance that a serial burglar in Taipei would commit a subsequent offence within a 2.4-km radius of the former event
P. Chen et al.	2013	China	Police data	1,533 recorded burglaries	May - Oct 2007	NRV	Burglary risk communicated at least 3 weeks within 200 metres of an offended place
Huang (Chinese)	2011	Taiwan	Individual victim survey	472 HHs (12 NBs)	N/A	RV	8.26% of households victimised more than once, around 64% of cases were RV
Roh et al.	2010	South Korea	Individual victim survey	620 survey respondents (25 districts)	2003	Multilevel generalised linear regression of burglary victimisation	• About 29% respondents experienced residential burglary or residential robbery • An identified issue of time order about security measures • In line with the broken window perspective and the community decay perspective: a greater likelihood of residential crime victimisation found in neighbourhoods with more community disorder • Contradictory findings with literature regarding opportunity perspectives: a) Target hardening efforts (an intrusion detection sensor, CCTV, a door video phone, and a burglar alarm) were associated with greater odds of victimisation b) Poverty and community cohesion were positively associated with residential burglary at community level c) Residential mobility was not significantly associated with burglary victimisation d) The percentage of teenage population was negatively associated with residential crime victimisation

(Continued)

Table 2.2 *(Continued)*

Author(s)	Date of publication	Location	Data source	Sample size	Time frame	Focus	Key findings relevant to burglary victimisation
L. Zhang et al.	2007	China	Individual victim survey (random/ purposive sampling)	2,474 survey respondents	2004 (victimisation in the past 5 yrs.)	Multilevel logistic regression of burglary victimisation	• About 4% respondents reported a burglary victimisation in the past 5 yrs. • Target attractiveness (household income), guardianship (length of residence and 'somebody home' as occupancy) were in line with the literature, so as collective efficacy and public control • Some neighbourhood structural factors such as residential stability had conflicting findings with the West. A residential stable neighbourhood was found a risk factor for burglary at a neighbourhood level

Note. RV = repeat victimisation; NRV = near repeat victimisation; min Park's (2015) study was not included in this table as it examined eight types of victimisation (ranging from robbery to automobile theft) as a sum rather than burglary alone.

burglary victimisation being observed in greater China[2] than other Asian settings. It is also noted that most studies on Taiwan in Table 2.2 tend to be Chinese publications (n=3). Among these three studies, merely one study provided information on the prevalence of burglary in Taiwan (H. C. Wang, 2015), leaving it challenging for international researchers to conduct comparative studies.

Two additional points are considered noteworthy. First, among the limited Asian studies on single burglary victimisation (n=4), it is suggested that the opportunity framework can be applied in the Asian context to some extent. For example, security measures (e.g. dogs, alarms, etc.) are found to be effective protections against burglary victimisation in Malaysia (Chiew et al., 2020) and Taiwan (H. C. Wang, 2015), though they are not in South Korea due to a possible issue of time order between security installation and burglary incident (Roh et al., 2010). However, only two Asian studies have systematically applied an opportunity framework to explore burglary victimisation: one in South Korea (Roh et al., 2010) and the other in China (L. Zhang et al., 2007). Both studies have examined criminological opportunities from individual- and neighbourhood-levels. Taiwan contains no systematic research applying such a multilevel-opportunity framework to single burglary victimisation. Furthermore, the two studies on opportunities date back to a decade ago. The lack of contemporary and systematic research raises concerns about generalising the opportunity framework to an Asian context.

Second, evidence on some neighbourhood factors within the opportunity framework is not consistent with the Western literature. For example, in the Chinese study a residentially stable neighbourhood (defined in the study as

[2] Greater China refers to a geographic concept that contains the People's Republic of China (sometimes referred as PRC or mainland China), the Republic of China (ROC, in the current thesis referred as Taiwan), the Hong Kong Special Administrative Region of the PRC (commonly known as Hong Kong) and the Macau Special Administrative Region of the PRC, where ethnic Chinese constitute the majority of the population (Lo, 2016).

residents' lengthy residence in neighbourhoods) was found to be a risk factor for burglary at the neighbourhood level (L. Zhang et al., 2007), whilst residential stability was suggested to be a protective factor against crime and disorder within a neighbourhood in some Western studies (R. J. Sampson et al., 1997; R. J. Sampson & Raudenbush, 1999). The inconsistency suggests a necessity of further evidence. More discussions about Asian research on burglary will be provided in Chapter 4 (Section 4.1.2). Additionally, the following sections discuss crime victimisation from an offline context (burglary) to an online context (cybercrime).

2.2.2 Opportunity in an online context – cybercrime

Over the past two decades, there has been an emerging body of literature dealing with criminal victimisation in an online context. Despite this, it is widely acknowledged that there is no consistent definition of what constitutes a cybercrime. Broadly speaking, online victimisation may include offences that "*involve and depend on the use of new communication technologies for their commission*" (Leukfeldt & Yar, 2016, p. 263). These offences can be 'old' crime forms like fraud, stalking, bullying or pornography, albeit utilising new online venues ('computer-assisted crimes'). Or these offences can take on new forms of crime like computer hacking and the distribution of malicious software ('computer-focused crimes'). This distinction between computer-assisted and computer-focused crimes is also a common approach to classify cybercrime. Computer-assisted crimes refer to crimes that pre-date the internet but take on new forms of modus operandi in an online context whilst computer-focused crimes refer to crimes that have emerged only with the internet and could not be committed without the use of the internet (Yar & Steinmetz, 2019).

Notably, these new forms of cybercrime sometimes act in a similar fashion to traditional crime. Malware, for example, has many similarities with burglary, in the sense that malware infects and compromises computer systems similarly to how burglars illegally enter a dwelling (Bossler & Holt, 2009). In this sense, the aforementioned classification between computer-focused crimes and computer-assisted crimes may limit the scope of criminological research given its exclusive focus on the technology rather than the relationship between offenders and victims/targets (Yar & Steinmetz, 2019).

Yar and Steinmetz (2019) alternatively proposed a classification of cybercrime using existing legal frameworks: crime against property, against morality, against the person and against the state. Briefly speaking, crime against property includes stealing physical or intellectual property or trespassing into other individuals' property and/or causing damage. Examples would be credit card fraud, piracy, hacking or virus attacks. Crime against morality is about breaching laws to do with obscenity and decency. An example here would be cyber-pornography. Crime against the person refers to illicit behaviours that cause psychological harm to or encourage physical harm against other people. Examples are hate speech, stalking or bullying. Lastly, crime against the state refers to activities that endanger the nation or its infrastructure, including terrorism, leakages of official confidential information, and so on. Such a classification aids in explaining the relationship between offenders and victims, by utilising the opportunity framework (Yar & Steinmetz, 2019).

First posited by Marcum (2008) and reassessed by Mesch (2009), the RAA and LRAA have gained substantial attention in terms of cybercrime, though with a particular focus on cyberbullying (Bossler & Holt, 2009; Navarro & Jasinski, 2012; Reyns et al., 2011). To recap, the aforementioned opportunity model (including LRAA) involves five elements: attractiveness, exposure, proximity to potential offenders, absence of guardianship and specific properties of specific crimes (Cohen et al., 1981). In applying the LRAA, it is recognised that the elements involved do not have to be present in the exact same moment and in the same physical location. These elements could conceivably converge in a virtual network and the contact between victims and offenders can be delayed due to the fluidity of virtual spaces (Reyns, 2017). In this sense, it is argued that the LRAA is applicable to cybercrimes.

Below I provide a short review of the opportunity elements described above discussed in the context of cybercrime. To avoid repetition, I will delay discussing the properties of specific cybercrimes until Chapter 6, which deals with this issue.

2.2.2.1 Target attractiveness/vulnerability in an online context

Previous research identifies three common characteristics of target suitability for cybercrime: gender, disability and public Wi-Fi use (see e.g. Kalia & Aleem, 2017; NortonLifeLock Inc., 2020; Rose et al., 2015). Gender is one of the most extensively researched demographic characteristics for online crime risks, but there is conflicting evidence for which gender is more vulnerable. Take cyberbullying, for example. Some researchers have found that males are at a higher risk of being cyberbullied as they are more prone to engage in risky online activities than are females (Henson et al., 2013; X. Li et al., 2006). Conversely, a more recent study suggested that females were more susceptible to cyberbullying as they might be perceived by offenders as ‘softer’ targets who are less likely to report victimisation due to fear of reprisal (Kalia & Aleem, 2017).

Disability is another well-studied characteristic related to online target attractiveness. Under the UK Equality Act 2010 (Government Equalities Office, 2013), disability is defined as a “*physical or mental impairment and the impairment has a substantial and long-term adverse effect on his or her ability to carry out normal day-to-day activities*” (Government Equalities Office, 2013, p. 7). However, evidence on the link(s) between (cyber)victimisation and disability may draw on a wider definition covering both chronic conditions and disabilities (Alhaboby et al., 2019). Such evidence includes many forms of physical impairments (Mueller-Johnson et al., 2014), a range of mental/psychiatric problems (Sourander et al., 2010) and neurodevelopmental disorders such as Autism Spectrum Disorders

(Schroeder et al., 2014), intellectual disabilities (Didden et al., 2009), learning disabilities (Barringer-Brown, 2015), or other health care issues.

It is argued that individuals with disabilities may be more suitable targets for cybercrime as they are often marginalised by peers, lack social support, have difficulties participating in social interactions, or even understanding their victimisation. These vulnerabilities thus place them at higher risk of online victimisation, and cyberbullying in particular (Rose et al., 2011, 2015; Schroeder et al., 2014). More systematic evidence can be drawn from a recent review of eight studies conducted in Europe, North America, the Middle East, and Australia, suggesting that students with neurodevelopmental disorder are more likely to experience cyberbullying compared to students without any neurodevelopment conditions (Beckman et al., 2020).

The last identified risk factor with regard to target attractiveness is the use of public Wi-Fi. This is considered to be a risk factor for victimisation because an offender is able to get in between data transmissions from point A (device) to point B (service/website) and read these data when a device makes connection to the internet. This vulnerability arises when connecting to a poorly secured Wi-Fi network that hackers and their malware may target. Users fall prey to cybercriminals who access their information, which enables them to steal personal information, gain access to their devices, or install malware. Modus operandi may vary, however. For example, it is possible for cybercriminals to steal a users' identity or infect the computer with viruses. Several anti-virus companies, including Norton and Kaspersky, warn of the risks of using public Wi-Fi about malware infection, account hijacking and credential leakage (AO Kaspersky Lab, 2020; NortonLifeLock Inc., 2020). A Home Office report has further found a greater proportion of public wi-fi users experiencing more security breaches compared with those using home connections (53% versus 35%, see McGuire & Dowling, 2013). However, vulnerabilities among public Wi-Fi users warrant more empirical evidence.

It is, however, challenging to classify the use of public Wi-Fi as a measure of target attractiveness or exposure to risk. Potential offenders may consider these users as easy targets who are less aware of cyber security, thus more attractive and vulnerable to the offenders. Noticeably, the use of public Wi-Fi might also expose the users to potential offenders at the same time. Nevertheless, the thesis would conceptualise Wi-Fi use as target attractiveness rather than exposure to risk (I will return to the conceptualisation issue in Section 6.3.2.4).

2.2.2.2 Exposure and proximity in an online context

The second and third elements drawn from the opportunity framework are exposure to risk and proximity to potential offenders, discussed here in an online context. The two elements overlap and are not easy to separate. The main difference between these two elements is suggested to be "*whether the individual performs online activities on his or her own online "turf" (i.e. exposure to cyber risk) or whether they enter someone else's domain (i.e. proximity to cyber offenders)*" (Vakhitova et al., 2019, p. 229). Nevertheless, it is often difficult to classify the domain where an online activity is performed due to the fluidity of cyberspace. For example, an individual's activity of searching information online seems to start by performing the act on his or her own turf, but the following click on the resultant page will redirect them to someone else's domain. Arguably, it is more important to understand the risk associated with an individuals' online behaviours than to distinguish between the domains where those behaviours take place. Hence, it is more practical to discuss these two elements together as "exposure/proximity to potential offenders". An online activity can be viewed as a virtual avenue where potential targets might meet potential offenders online[3]. Different activities thus create different levels of risk.

Several studies have provided evidence on the effect of individuals' online activities in explaining the variation in cybercrime victimisation and have suggested that different activities are related to different types (and levels) of victimisation. For example, online purchasing has been found to be a reliable

[3] Though the contact between victims and offenders can be 'delayed' (see Reyns, 2017).

risk factor for internet fraud victimisation, while behaviours like e-banking, online shopping, emailing, downloading, and selling on online auction sites are shown to predict an individual's risk of online identity theft (Pratt et al., 2010; van Wilsem, 2013a; M. L. Williams, 2016). Furthermore, behaviours such as communicating with others online (e.g. in online chatrooms or forums) or sharing personal information (e.g. active social networking, or frequent site profile updating) are positively related to an individuals' risk of experiencing online bullying or harassment (Bossler & Holt, 2009; Hinduja & Patchin, 2008; Marcum, 2008; Marcum et al., 2010; Mesch, 2009; Navarro & Jasinski, 2012; Reyns et al., 2011). To summarise, consistent with the RAA approach in particular and EC more generally, the emerging evidence on cybercrime further highlights the importance of being crime specific. More online activities judged to be risk factors for cybercrime victimisation will be detailed in Chapter 6 (Section 6.1.2).

2.2.2.3 Guardianship in an online context

The last element to be discussed here is guardianship. Guardianship in cyberspace can be refer to both persons (e.g. law enforcement officers, parents or family members) or objects (e.g. anti-virus software, firewall software, family safety tool services and apps) (Yucedal, 2010). Specifically, in line with the conceptualisation of guardianship discussed in Section 2.1.1.2, in this thesis physical guardianship in cyberspace refers to the use of tools and target hardening techniques (e.g. self-protection measures such as anti-virus and firewall software) whilst social (interpersonal) guardianship involves the presence of various human elements which serve to reduce the likelihood of a cybercrime occurring (e.g. formal and informal social control and surveillance measures such as parents, friends, peer, police or network administrators).

The operationalisation of capable guardianship in cyberspace covers a range of measures. The proxies used for measuring guardianship in previous studies on online victimisation include: (a) the use of self-protection measures such as anti-virus software, spyware, or firewall software (Leukfeldt, 2014; Lwin et al., 2012; Marcum et al., 2010; Ngo & Paternoster, 2011); (b) digital awareness such as having computer skills and education on cybercrime (Ngo & Paternoster, 2011); (c) social/interpersonal guardianship such as peer deviance (Bossler et al., 2012; Reyns et al., 2011) or parental support and friendship in an offline environment (J. Wang et al., 2009); and (d) the presence of parent/teachers/others accompanying internet users or monitoring the use of a computer (Marcum et al., 2010). While one study found a negative association between parental support and adolescents' involvement of cyberbullying (J. Wang et al., 2009), most studies have found little empirical support for guardianship in explaining patterns of online victimisation (for summary of relevant research see Leukfeldt & Yar, 2016; Vakhitova et al., 2016). These findings clearly go against the RAA. A possible explanation might be the fact that the concept of guardianship functions differently online. The measures used in the aforementioned studies do not truly reflect the way guardians supervise targets online. The operationalisation of capable guardians might thus be tailored in an online context, which is considered by researchers as more challenging than other concepts such as exposure and proximity in the context of online victimisation (Leukfeldt & Yar, 2016).

However, situating capable guardianship in cyberspace remains a challenge for researchers. Firstly, it is difficult to quantify online interpersonal interactions as they might be influenced by offline interactions. The inclusion of both online and offline information might require the use of a lengthy questionnaire that is not welcomed by participants. Second, capable guardians may change dramatically from one type of cybercrime to the next. For example, up-to-date anti-virus software might be effective against malware. However, banks may act as a more competent guardian in terms of phishing attacks that 'resulted in financial damage' (Leukfeldt, 2014).

Additionally, evaluating the timing of installing self-protection measures before/after online victimisation may not be as easy as when done offline (for example, burglar alarms against burglary). Due to the diversity and complexity of online victimisation, it is difficult to clarify the event order. For example, an individual might encounter a virus attack, turn to installing anti-virus and anti-intrusion software and then encounter another attempt of identity theft. Therefore, it is sometimes difficult to define if the installation of security measures occurred before or after criminal victimisation, particularly in the case of repeat victimisation.

A sequence of events further challenges the identification of causal relations between installation of security measures and cybercrime victimisation. Without knowledge about antecedents of all other types of victimisations, we might find a positive relationship between self-protection software and one type of victimisation. That is to say, a false positive relationship between anti-virus software and identity theft is likely to be observed in the example given above. To put it differently, it is difficult to evaluate the timing of installation of each security measure against a range of victimisation within merely one single study. Overall, the difficulty in quantifying online interpersonal interactions, the diversity in capable guardians across types of cybercrime, and the complexity in evaluating the timing of security installation make the operationalisation of guardianship in the cyberspace challenging.

2.2.3 Situational crime prevention

Opportunity structures differ from one crime to the next. The examination of criminogenic circumstances helps us understand patterns and causes of specific types of crime. Understanding specific opportunity structures is crucial for the implementation of situational crime prevention (hereafter SCP) (Clarke, 1995). SCP attempts to make crime less likely to happen by changing the immediate circumstances where crime is carried out, rather than (attempting to) changing the disposition of offenders. SCP thus seeks to introduce measures into an environment to reduce the likelihood that opportunities are seized (Clarke, 1997). This is the underpinning logic of EC as mentioned above.

SCP reinforces the importance of understanding how crime is committed and distinguishes *motivation* from *motive*. Motivation refers to a criminal motivation, or say a long-term disposition to engage in crime, whilst motive is an immediate driver of behaviour (Clarke, 2016). It is thus more important, according to advocates of SCP, to understand offenders' motive than motivation, by which criminal behaviours could be intervened and crime could be prevented. This practical initiative complies with EC, which, for the purposes of crime prevention, tends to place higher value on the nearer (situational) causes of crime more than the distant causes (dispositions). This does not mean that altering distant causes is not important, but that changing dispositions is a difficult and long-term proposition. Reducing opportunities can produce immediate reductions in crime in the here and now.

To date, 25 techniques have been proposed for SCP, grouped under five main headings or mechanisms: increase the effort, increase the risks, reduce the rewards, reduce provocations, and remove excuses. These five mechanisms incorporate several different theoretical perspectives: the first three derive from rational choice perspective to increase the effort needed for crime commission, increase the risks of detection or apprehension and reduce the rewards earned by offenders (Cornish & Clarke, 2016); reducing provocations derives from social and environmental psychological theory to reduce provocations that precipitate criminal acts (Wortley, 2001); and removing excuses derives from Sykes and Matza's (1957) social deviance theory of "techniques of neutralisation" and Bandura's (1976) social learning theory of violence to remove offenders' justification for crime commission as an act of 'everyone doing it' (see Homel & Clarke, 1997).

There is a large number of specific interventions that might activate these crime prevention mechanisms. Target hardening (*increase the effort*), formal surveillance strengthening (*increase the risks*), target removal (*reduce the rewards*), dispute avoidance (*reduce provocations)* and rule setting (*remove excuses*) are all examples of SCP techniques which relate to different preventive mechanisms (see Clarke, 2016; Clarke & Eck, 2005). As each type of crime relates to different opportunity structures, those techniques are crime-specific. For example, target hardening describes a technique that increases the security of a victim/target, making it more difficult to be victimised, thereby increasing the effort needed by the offenders to succeed. In this sense, target hardening might be the installation of an immobiliser against auto theft and the installation of anti-virus software against malware.

It is, however, noted that there is some overlap among these classifications. For example, a technique to strengthen formal surveillance (e.g. the assignment of security guards in shops) would increase offenders' risk of apprehension for committing theft and thus increase offenders' effort to make a crime succeed. This means that there is sometimes difficulty in classifying measures by the five main headings and therefore some measures can be classified under more than one (Clarke, 1997). Yet the principle embedded in SCP is the same: to manipulate the opportunity in environment to make crime less likely to succeed.

Despite gaining a gradual acceptance within crime research, SCP is sometimes criticised for two main aspects: (1) theoretical and conceptual inadequacy and (2) ethical foundations and social outcomes (Wortley, 2010). Table 2.3 summarises Wortley's (2010) work on the main criticisms against SCP and the responses to each criticism. Criticisms are that SCP: (1) simplifies responses to a complex social problem; (2) ignores the root causes of crime; (3) will only displace crime but not prevent it; (4) does not work for 'irrational' crime; (5) uncritically supports the status quo (e.g. focusing on the crimes of the poor and disadvantaged); (6) can only be afforded by the rich as governments withdraw from law enforcement; (7) blames the victims and revokes government's role in law enforcement; (8) invades and restricts personal freedoms by increased surveillance; and (9) creates an isolated society by forms of obtrusive security (e.g. locks, bars, guards, etc.).

Table 2.3 Criticisms and responses of situational crime prevention (SCP), as proposed by Wortley (2010)

Sorts of criticisms	Criticisms	Responses
Theoretical & conceptual	Simplifying responses to a complex social problem	Target-hardening is just one of 25 major techniques of SCP. The choice of appropriate intervention requires a tailored scheme into the crime problem of interest.
	Ignorance of the root causes of crime	Situations are also one cause of behaviour. It is sometimes difficult to alter the distal causes of crime (e.g. criminal dispositions) but relatively easy to make the near environment unfavourable for crime commission.
	Crime displacement rather than prevention	Empirical evidence has shown little chance of displacement and often observed a diffusion of benefits (i.e. preventative effects beyond the original target). Even if displacement occurs, the amount of crime is often reduced.
	Inappropriate for 'irrational' crime	Recent evidence supports that, by altering situational factors that provoke crime, SCP can be applied in a range of 'pathological' behaviours including suicide, child sexual abuse, serial murder, and drug addiction.
Social & ethical	Uncritical support of the status quo (e.g. ignoring crimes of the affluent and crimes against women and minorities)	SCP is pragmatic and targets both offenders and victims. It also applies in crimes of the affluent and crimes against women and minorities, including computer fraud, assault, and rape.
	Privileged access by the rich due to governments' withdrawal from law enforcement	There is little evidence that governments are withdrawing from law enforcement.
	Victim blaming	SCP assists citizens with advice on what routine security precautions are most effective. Governments should not take full responsibility in public safety and in some circumstances where irresponsible victims generating crime problems should be blamed.
	Invasive and oppressive intervention due to increased surveillance	Personal freedoms can be ensured by checks and balances in democratic societies. Increased surveillance should be justified if benefits outweigh the costs, e.g. airport screening procedures against the threat of terrorism
	Creation of a fearful and distrustful society divided by forms of obtrusive security	Target-hardening is just one of 25 major techniques of SCP, many of which involve 'softening' the environment, increasing community interaction, or reducing fear of crime.

Source: Wortley (2010)

Responses to those criticisms can also be seen in Table 2.3. An example response to the criticism that SCP merely applies in tackling property crime is that by altering the situational factors that provoke crime to occur, SCP can also work for so called 'irrational' or predatory crimes. These may include homicide (Tillyer & Kennedy, 2008), child sexual abuse (Terry & Ackerman, 2008; Wortley & Smallbone, 2006), or organised crime (Bullock et al., 2010).

The thesis however has an exclusive focus on two categories of offence, burglary and cybercrime, on which the following discussion on SCP would be centred.

2.2.3.1 Situational crime prevention and burglary

Burglary is one of the most targeted offences to which SCP has been applied to manipulate the immediate environment, making it less favourable for offenders. Table 2.4 shows examples of burglary prevention strategies that draw on SCP. Examples include target hardening (e.g. installing security alarms) or natural surveillance assistance (e.g. implementing neighbourhood watch schemes) to increase the effort/risks and target concealment (e.g. keeping curtains down or hiding valuables) to reduce the rewards perceived by burglars.

Specifically, a typical form of SCP that aims to reduce the opportunity for domestic burglary is alley gating (Johnson & Loxley, 2001) – the installation of security gates across footpath and alleyways that can control potential offenders' access to potential crime targets (i.e. increasing the effort). A recent synthesis of evidence has further suggested alley gating a modest but significant effect of burglary reduction, with little evidence of spatial displacement (Sidebottom, Tompson, et al., 2018).

In regard to the comprehensive effectiveness of SCP against burglary, Bowers and Johnson (2003) evaluated 21 burglary reduction projects located in the North of England. They found location-specific SCP and stakeholder interventions were the most successful at reducing burglary. The former involved interventions such as target hardening of individual households and household surveillance. Overall, evidence supported the effectiveness of SCP for burglary prevention (see Bowers & Johnson, 2003).

Table 2.4 Examples of SCP techniques against domestic burglary

Increase the effort	Increase the risks	Reduce the rewards
• Target harden: double glazing windows, locks, security alarms • Control access to facilities: alley-gating, defensible space designs for housing	• Extend guardianship: 'cocoon' neighbourhood watch[4], leaving signs of occupancy when away from the house • Assist natural surveillance: improved street lighting, neighbourhood watch, windows overlooking gardens and clear sightlines with no high walls • Reduce anonymity: guest registration • Use place managers: apartment complexes with doormen • Strengthen formal surveillance: burglar alarms, video cameras	• Conceal targets: hiding valuables, keeping curtains down • Remove targets: cash reduction at home • Identify property: property marking (e.g. SmartWater technology[5]) • Disrupt market: monitor pawn shop • Deny benefits: ink tags, "National Mobile Property Register" for valuable devices

Sources: Adapted from Clarke (2016); Clarke and Eck (2005)

2.2.3.2 Situational crime prevention and cybercrime

As mentioned, there is an emerging trend to examine cybercrime victimisation using an opportunity framework (e.g. Choi, 2008; Leukfeldt & Yar, 2016; van Wilsem, 2011). Meanwhile, researchers have utilised SCP to cybercrime prevention, by changing the conditions and circumstances of risk factors online. SCP has been expanded to a range of cybercrime from crime against property (e.g. malware attack see Leukfeldt, 2015), crime against the

[4] Close groupings of dwellings share information and support each other.

[5] A technology that uses 'traceable liquids' and forensic asset marking system that can be applied onto the values to identify thieves (SmartWater Group, 2021) and deter theft by reducing the rewards and increasing the risks of detection.

person (e.g. cyberstalking see Reyns, 2010), crime against morality (e.g. online pornography see Me & Spagnoletti, 2005), and further to crime against the state (e.g. organisational information security see Beebe & Rao, 2010).

Table 2.5 shows 16 cyber-related SCP techniques summarised by Back and LaPrade (2020). Their work drew upon the original SCP research (Clarke, 1995; Cornish & Clarke, 2003) and incorporated some cyber-SCP research (Beebe & Rao, 2005; Hinduja & Kooi, 2013). There were 46 cybercrime measures included under the four categories: increase the effort, increase the risks, reduce the rewards, and remove the excuses. Generally speaking, Back and LaPrade's (2020) study identified the three most commonly used cyber-SCP techniques: target hardening, entry/exist screening and reducing temptation. It further provided empirical evidence supporting the use of these three techniques to effectively prevent crime in an online setting.

It is noted that Back and LaPrade's (2020) summary of cyber-SCP techniques focused extensively on information security. Furthermore, their work did not include the category of reducing provocations which is considered critical to the current cyber-SCP researchers (e.g. Leukfeldt & Kleemans, 2020). Specifically in terms of phishing or banking malware, money mules are recruited in the criminal network to assist offenders' money withdrawal. Some money mules believe that they are conducting a legitimate transaction or that there are no victims (or that the victims are to be blamed as they have exposed themselves to the risks of cybercrime). Despite the neutralisation techniques that remove money mules' excuses, reducing provocations such as reducing peer pressure and imitation might also work to make the recruitment of money mules more difficult, thus preventing financial cybercrime (Leukfeldt & Kleemans, 2020).

Table 2.5 Back and LaPrade's (2020) cyber-situational crime prevention techniques

Opportunity-Reducing Strategies	Cyber-SCP Techniques	Cybercrime Prevention Measures
Increase Efforts	1.Target harden	a) Firewall: perimeter, b) firewall: interior, c) internal firewall, d) patch computers
	2.Access control	a) Digital signatures, b) password management, c) single sign-on, d) access control list
	3. Deflecting offenders	a) Honeypot (i.e., identifying malicious hackers), b) honeynet (i.e., identifying bots/zombies)
	4. Controlling facilitators	a) Reference check, b) criminal background check, c) identity management, d) role-based access control
Increase Risks	5. Entry/exit screening	a) intrusion detection system, b) intrusion prevention system, c) anti-virus, d) anti-spyware, e) use content filtering, f) email content filtering, g) spam filtering, h) web content filtering
	6. Formal surveillance	a) bot monitoring, b) monitor activity, c) monitor for rogue devices
	7. Surveillance by employees	a) employees mandatory training, b) full-time IT officer
	8. Natural surveillance	a) peer-to-peer technology: monitor bandwidth, b) peer-to-peer technology: shape bandwidth
Reduce Rewards	9. Target removal	a) encryption data on hard drive, b) encryption backup data for off-site storage, c) monitor use of backup media (e.g., USB drives)
	10. Identifying property	a) information asset classification
	11. Reducing temptation	a) level of sensitive information sharing, b) physical separation
	12. Denying benefits	a) encryption (e.g., WEP, WPA), b) encryption data in transit (PKI, SSL, HTTPS), c) encryption data on network or computers
Remove Excuses	13. Rule setting	a) user agreement, b) acceptable use policy/laws
	14. Stimulating conscience	a) warning banners on website, b) codes of ethics
	15. Controlling disinhibitions	a) warning violators, b) suspension, c) dismissal, d) restricted access to network
	16. Facilitating compliance	a) cybersecurity education for staff, faculty, and student

Sources: Back and LaPrade (2020); adapted from: Beebe and Rao (2005); Clarke (1995); Cornish and Clarke (2003); Hinduja and Kooi (2013)

However, the aforementioned gap observed in Back and LaPrade's (2020) work also reinforces SCP as a crime-specific approach to crime prevention. Techniques may thus perform better in particular types of cybercrime. For example, the use of target hardening techniques (e.g. enhanced and up-to-date computer security) and improving access control (e.g. via frequent password changes and multifactor authentication[6] to access devices) might make cybercriminals more difficult to access potential victims (i.e. increasing the effort). The techniques are thus expected to tackle hacking or identity theft in particular (Anandarajan & Malik, 2018; Choi, 2008). Additionally, abnormality detection, log data gathering, or periodic audits, which increase offenders' perception of the risks involved in committing crime, would work in dealing with insider threat such as hacking (Stockman, 2014) and employee fraud (Willison & Siponen, 2009). With regard to financial cybercrimes as mentioned above, it is suggested that SCP could target money mules through awareness campaigns to interrupt the criminal network: (a) to reduce provocations (e.g. peer pressure) that incite criminal behaviours; (b) to remove excuses by making potential money mules aware of their participation in the criminal network. In this way, the recruitment of money mules becomes more difficult, stolen money is less likely to be transferred, and some financial cybercrime is disrupted (Leukfeldt & Kleemans, 2020).

Notably, some researchers further argue that SCP needs to be adapted when being applied online. Specifically, it is argued that cyber-SCP will have to focus more on the role of other stakeholders than just the users themselves (Jansen & Leukfeldt, 2016). Such an argument is based on evidence suggesting that online victimisation is often related to users' legitimate routines and that there is a limited effect of anti-virus software on averting victimisations such as phishing attacks or malware infection (Bossler & Holt, 2009; Jansen & Leukfeldt, 2016; Leukfeldt, 2014, 2015). In the example of malware infection, the role for owners of (popular) websites becomes crucial in curtailing victimisation as potential offenders might lurk in these online

[6] Examples are biological scans and one-time passwords sent as text messages to cell phones.

places and the owners of these places have responsibilities to protect their visitors from getting infected. Researchers therefore suggest that more responsibilities should be carried out by owners of each domain. However, this point of view does not distinguish cyber-SCP from offline settings. The responsibility of website owners and hosting companies to reduce online victimisation is similar to that of bar owners to deal with violence in the bars by interventions like live music elimination (R. Sampson & Scott, 1999) or the use of plastic cups and bottles (Merseyside Police, 2001).

Overall, SCP provides a viewpoint that crime prevention should never be the sole responsibility of a standalone stakeholder but responsibility should be shared by all those involved in providing opportunities for crime. The impact of specific stakeholders may vary across specific crimes. Yet evidence so far has supported SCP as an applicable approach in preventing both offline and online victimisation.

Sections above discuss the theoretical background of criminal victimisation and the aspects of prevention informed by theories – particularly with regard to burglary and cybercrime. The following sections would then cover the literature on specific types of victimisations – namely repeat victimisation and poly-victimisation that inform the remaining empirical studies in this thesis.

2.3 Repeat victimisation and poly-victimisation

In contrast to single victimisation, repeat victimisation refers to the situation in which a crime target (a person, object, or household) suffers crime on multiple occasions over a given time period (a calendar year for instance) (Grove & Farrell, 2012). RV derives from one of the most consistent findings in crime research, that crime incidents are not equally distributed over places (Favarin, 2018; Lee et al., 2017) and victims (O et al., 2017). RV describes the concentration of crime incidents on the same target (crimes per victim), compared to the prevalence of crime over the whole population of targets (victims per head) and the incidence of crime, which denotes the average number of crimes per 100 (or some other denominator) of the population at risk (crimes per head) (Farrell, 1995).

Distinctive from RV, which refers to an individual's victimisation of the *same* form of offence, the concept of 'multiple victimisation' describes individuals' experiences of one or more incidents of *different* forms of offences over a given period (Tseloni & Pease, 2005). An example of multiple victimisations is when an individual has experienced a burglary, an auto theft, and a fraudulent incident in the past year. Confusingly, some early studies also used 'multiple victimisation' to describe incidents in which multiple offenders commit a crime or in which more than one victim is affected in a single incident (e.g. Sparks, 1981). To avoid uncertainty, 'poly-victimisation' will be used in this thesis to describe individuals' experience of multiple forms of criminal victimisation over a given time period (Finkelhor et al., 2009; Le et al., 2016; Turner et al., 2017).

Below I introduce the literature on RV and poly-victimisation.

2.3.1 Theoretical background and mechanisms of repeat victimisation

The literature on RV dates back to the 1970s in the US and the phenomenon has now been researched and identified in many countries and across many crime types (Farrell & Pease, 2014). Four recurrent findings are identified: (1) a small number of repeat victims typically account for a sizable proportion of all victimisations; (2) repeat victimisation occurs quickly in the wake of an initial victimisation; (3) repeats are highly prevalent in high crime areas; and (4) prior victimisation tends to be a reliable predictor of future victimisation (see e.g. Farrell et al., 1995; Farrell & Pease, 2017; Townsley et al., 2000). Discussing each finding in turn.

Firstly, a considerable volume of crime is repeat victimisation against the same targets. Generally speaking, crime victimisation surveys in industrialised countries find that an average of 40% of crimes that have been committed against individuals and households are repeats against targets with prior victimisation in the same year (Farrell & Bouloukos, 2001). In England and Wales, for example, about half of property crime and two-thirds of personal crimes (including violent crime) are repeats against the same targets/individuals in the same survey period. Research on 'super targets' (also known as chronic victims) indicates that they accumulate a disproportionate volume of crime: 2% of the super targets account for 44% of property crime and 1% of them account for 59% of personal crime (Farrell & Pease, 2017).

The second consistent finding is that when RV occurs, it tends to happen quickly (Polvi et al., 1991). For example, in their research analysing repeat burglaries , Polvi et al. (1990) found that half of the second repeat burglary occurs within seven days following the initial incident. A possible explanation why RV happens so quickly is that offenders attempt to minimise the changes that could be made (e.g. removal of values, strengthened security) after their previous offence (Grove & Farrell, 2012). Burglars are found returning quickly to the dwelling if they are aware of values left behind and the layout, though some may delay their return for a few weeks so that insurance payments would replace stolen items (Clarke et al., 2001). The third consistent finding is that repeats are highly prevalent in high crime areas. This is based on two possible mechanisms. On the one hand, targets (persons, households or places) in high crime areas encounter a greater risk of initial victimisation for many crimes, and they often lack the resources to curtail a subsequent offence by quickly improving security measures (Weisel, 2005). On the other hand, an area with high crime prevalence and incidence rates tends to have a shorter time course of revictimisation than a low-crime area, though the time course may vary by crime type and local circumstance (Farrell, 1995). A shorter time course of revictimisation observed in high-crime areas might be attributed to a larger pool of chronic victims shortening the time-course of revictimisation (Townsley et al., 2000) or chronic offenders having shorter between-times of commission by virtue of familiarity with the targets. These make repeats more likely to be observed in high crime areas.

Lastly, prior victimisation tends to be a good predictor of future victimisation. This embodies two theoretical processes that have been proposed to explain RV: risk heterogeneity (*flag accounts*) and event dependence (*boost accounts*) (Johnson & Bowers, 2004b; Pease & Tseloni, 2014; Townsley et al., 2003). The former states that there are certain characteristics that make some targets more susceptible to victimisation than others, independent of their victimisation history. These characteristics '*flag*' their target suitability to potential offenders (Pease, 1998). In this process, prior victimisation, as a sign of vulnerability, may predict future victimisation. In the context of residential burglary where this thesis concerns, such flags include easy accessibility, poor security and signs of inoccupancy (Bowers et al., 2005; Johnson, 2008), providing clues for rational offenders to judge the perceived risks and efforts associated with burgling a household.

The second mechanism – event dependence – suggests that an initial successful victimisation '*boosts*' the likelihood of further victimisation in the future. Because of their increased familiarity with the targets and surrounding areas following the initial offence, the offenders are boosted to revisit the previously victimised targets (see e.g. Chainey & da Silva, 2016). To put it differently, success breeds repeats. This applies especially in the context of burglary. Burglars are more likely to return to the same property once they have successfully burgled it and have learned that the target is worth revisiting. This may be because of their increased familiarity with the layout and (the lack of) security measures in the property, or because they are returning for those goods they couldn't take on the first occasion (M. Shaw & Pease, 2000). This mechanism relates to the rational choice perspective (Clarke & Cornish, 1985), in which the perceived risk of subsequent burglaries by offenders against the same property is reduced by increased awareness and familiarity following the successful completion of the initial offence.

Both mechanisms are widely used to explain why repeats occurs. Two main differences in terms of causality are raised: who commits repeats and the time interval between repeats (Chainey & da Silva, 2016). First, as success breeds repeats, the boost account implies that repeats are likely to be committed by the same offender[7]. In fact, it was found that within a 15-day timespan, 95 percent of repeat burglaries were committed by the same offender. When the timespan was extended to less than 3 months, the proportion slightly declined yet 91 percent of repeats still involved the same offender (Bernasco, 2008). Conversely, the flag account does not suggest this causality as repeats are independent of prior victimisation. A repeat offence can be committed by a different offender than who committed the initial offence. Second, the boost account suggests a temporal causality so that a repeat would follow swiftly after an initial incident. Instead, the flag account might suggest that the time interval between an initial offence and a repeat is more likely to be random. In practice, both mechanisms are combined to explain RV. That is, the flag characteristics may initially attract an offender because the target is recognised as an easier one, with the risk of future victimisation being boosted following an initial incident.

2.3.1.1 Extension of repeat victimisation – Near Repeat Victimisation

An extension of RV is known as near repeat victimisation (NRV), for which victimisation is linked to previous victimisation but not necessarily against the same targets (Farrell & Pease, 2014). NRV refers to the phenomenon in which crime clusters in space and time and follows a contagion-like process, whereby targets located close to a prior incident of victimisation show an elevated risk of victimisation in the short term (Farrell & Pease, 2017; Johnson et al., 2007; Townsley, 2008; Townsley et al., 2003). Like RV,

[7] Researchers otherwise also argue that repeats do not have to be committed by the same offenders. The boost mechanism can also occur through other means than offenders' actual success of burglary in a location, say like through information flow via offender ties and social networks (Hearnden & Magill, 2004; Lantz & Ruback, 2017; Polvi et al., 1991).

patterns of NRV have been identified for a variety of crime types, including gun-shootings (J. Ratcliffe & Rengert, 2008), sex crimes (Amemiya et al., 2020) and the most researched field of burglary (Clark, 2018; Johnson et al., 2007; Johnson & Bowers, 2004a, 2004b; Townsley, 2008; Townsley et al., 2003).

The aforementioned two mechanisms – flag and boost – also apply to explaining NRV. Recall that the flag account highlights the high level of vulnerability of targets to potential offenders while the boost account suggests the prior victimisation breeds future victimisation. To explain NRV, the flag applies because targets close to the initial victimisation are likely to be similar in terms of risk heterogeneity. Boost applies because offenders may anticipate a similar success in targets within a neighbouring area following the initial success, with their familiarity with the nearby area. Additionally, the layout of the neighbouring properties might be more similar and the neighbours might be as attractive and vulnerable as those victimised initially. Hence, the offenders are boosted to return to the neighbouring targets (Grove & Farrell, 2012).

Furthermore, the optimal foraging theory is also introduced to explain NRV (Bernasco, 2009; Johnson, 2014; Johnson et al., 2009; Vandeviver et al., 2021). According to this theory, offenders target whole neighbourhoods rather than one property in order to minimise their effort and maximise their potential rewards for crime commission (Bowers & Johnson, 2004; Stokes & Clare, 2019). This account of minimising effort and maximising rewards accords with the rational choice perspective (Clarke & Cornish, 1985) and the offenders are thus likely to 'forage' in areas where they have a successful commission of crime (Bernasco et al., 2015). The foragers will not move on to other locations until the rewards deteriorate sharply in the current 'optimal' neighbourhood (Chainey & da Silva, 2016; Vandeviver et al., 2021).

In combination with the aforementioned three mechanisms – the boost and flag accounts and optimal foraging theory – the risk of repeat and near repeat victimisation occurs because offenders: forage in areas where they are familiar with; make rational decisions to prey on suitable targets (‘flags’) or targets with prior success of offence (‘boosts’); and then search for targets nearby for optimal foraging (Chainey & da Silva, 2016). Applying this process to burglary, the flag characteristics of a property make it perceived as an easier target and initially attractive to a potential offender. Then, the risk of future burglary is boosted following an initial incident of victimisation. The elevated risk also exists for nearby locations for a short period as offenders return to carry out a series of further offences after an initial offence.

The key finding drawn from research into near repeat burglary is that the burglary risk of properties close to a recently burgled counterpart is significantly higher than the risk to those further away. In a UK study, burglary was found to be more likely to occur within 300-400 metres from the location, and within 1-2 months from the time, of the initial event (Johnson & Bowers, 2004a, 2004b). Similar patterns have been found across countries such as Australia (Townsley et al., 2003), the Netherlands, the United States (Johnson et al., 2007), South Africa (Clark, 2018), Brazil (Chainey & da Silva, 2016), and China (P. Chen et al., 2013).

The risk of burglary to these neighbouring properties decays over time and distance from the initial incident, a feature known as the decay function (Chainey & da Silva, 2016; Hammond & Youngs, 2011; Johnson et al., 2007). Risk of victimisation not only decays gradually by the proximity to the initial incident but further, one can see a dramatic decline in risk beyond a specific temporal and spatial distance to the initial incident. For example, research in a Chinese city has found that after three weeks and beyond 200 metres of the initial incident, the risk of burglary drops dramatically and to a non-significant level ($p > .05$) (P. Chen et al., 2013). A cross-national study drawing on data from Australia, Netherlands, New Zealand, UK and US found an average range of 200 metres and 14 days over which burglary risk decays (Johnson et al., 2007), though the exact time and distance range varied across countries. This highlights the necessity of further research in more countries, especially a non-western setting, to examine if the patterns observed in the literature can be generalised across context.

2.3.1.2 Burglary research on repeat and near repeat victimisation in Asia

There is now an extensive body of research on RV covering a wide range of settings and crime types (see e.g. Farrell & Bouloukos, 2001; Farrell & Pease, 2017; O et al., 2017). Burglary is the most researched type of victimisation and research into repeat and near repeat burglary has been conducted in many western countries, including Europe (Johnson et al., 2007), Australia (Townsley et al., 2003), and the US (Y. Zhang et al., 2015). Yet, as has been noted, the body of Asian research remains sparse.

To the best of my knowledge, there are only eight published studies that focus specifically on repeat and/or near repeat burglary victimisation using data from Asian settings (see Table 2.2). In addition to research into the prevalence of burglary, Table 2.2 also summarises the key findings drawn from these eight studies, two of which are published in Chinese.

Two general patterns can be observed in the studies on (N)RV in Asian settings. First, repeat burglary is also observed in Asian settings despite levels of concentration varying across studies. About one tenth of the burglary cases are suggested to be RV in Japan (Hino & Amemiya, 2019) while RV is estimated to account for nearly half of burglary cases in Taiwan (S.-Y. Kuo, 2015). Second, near repeat burglary also occurs and is not randomly distributed across victims. Targets with spatial and temporal proximity to the originator incident tend to experience significantly higher risks of burglary than those properties located further away. However, due to the sparsity in literature, it is difficult to identify a uniform spatiotemporal range in which the risk would significantly communicate across Asian countries. In mainland China where studies on NRV are more common, it is suggested that the risk of near-repeat burglary could expand for 56 days and one kilometre from the initial burglary (Ye et al., 2015). However, another study suggested a shorter spatiotemporal range, of which the risk after three weeks and beyond 200 metres to the initial burglary became non-significant (P. Chen et al., 2013).

Across the eight studies on (N)RV in Table 2.2, there are three additional points which are considered noteworthy. First, the majority of studies (n =4) use data from mainland China. Second, most studies use official police recorded crime data (n = 5), with two studies drawing on victim surveys and one on interviews with burglars. No studies have applied multiple sources of data on burglary information. As police data and victim surveys have their own (dis)advantages (which will be discussed in Chapter 3), the utilisation of multiple sources may convey a more comprehensive picture of (N)RV patterns. Third, despite the extent of burglary concentration being reported in some studies, only Chinese studies report the decay function for which the risk of burglary depends on the temporal and spatial proximity to the originator incident. Consequently, the generalisation of such a decay function remains less evident due to the lack of analytical approaches into spatial and temporal patterns of near repeat burglary in other Asian countries.

2.3.2 Theoretical background and mechanisms of poly-victimisation

Studies have shown that poly-victims tend to exhibit more mental health problems than individuals with single victimisation (Hamby et al., 2018) or than victims with the repeated experience of the same form of victimisation (Turner et al., 2017). Poly-victimisation is often accompanied by serious consequences, such as mental health issues (Álvarez-Lister et al., 2017; Schaefer et al., 2018), self-harm (Baldwin et al., 2019), suicidal thoughts/plans (Le et al., 2016), or distress symptoms (Finkelhor, Shattuck, et al., 2011). This makes research on poly-victimisation of great importance.

As previously discussed, research on poly-victimisation can be dated back to 1980s in the US, though the term ‘multiple victimisation’ was often used rather than the current ‘poly-victimisation’. Using data drawn from the 1972-1975 National Crime Survey, Reiss (1980) observed the occurrence of poly-victimisation and found it more frequent than chance alone for the same targets (either households or house members). By displaying a ‘crime-switch matrix' to cross-tabulate multiple crime victimisation, he then concluded that, together, personal larceny and attempted assault was the most frequent combination to be observed in the data, which included victimisation experienced by the same individuals for rape, assault, robbery, larceny, and burglary (Reiss, 1980). A similar clustering of victimisation over the same targets was also observed in later studies. This was especially so for violence; for example, it was found that children who had been physically assaulted were more likely to also experience sexual assault than those without being physical assaulted, either during the survey period (Finkelhor, Turner, et al., 2011) or over his or her lifetime (Finkelhor et al., 2009).

To date, it is noted that most research on poly-victimisation has been concerned with children and (or) young people. In some high-income countries[8], for example, the prevalence of poly-victimisation among children and adolescents in the US (Finkelhor et al., 2007a) was reported to be 10 percent, comparable to 10 percent among adolescents aged 14-18 years old in Spain (Soler et al., 2012). Diversity in the items used to measure poly-victimisation in the two studies is noted. The US study measured: (1) violent and property crimes (e.g., assault, sexual assault, theft, burglary); (2) child welfare violations (child abuse, family abduction); (3) the violence of warfare and civil disturbances; and (4) bullying victimisation (see Finkelhor et al., 2007a), whilst the Spanish study measured: (1) conventional crime (robbery, personal theft, vandalism, assault with and without weapons, attempted assault, kidnapping, and bias attack); (2) child maltreatment; (3) peer and sibling victimisation (gang or group assault, peer or sibling assault, non-sexual genital assault, bullying, emotional bullying, and dating violence); (4) sexual victimisation; and (5) witnessing and indirect victimisation (e.g.

[8] According to the World Bank website, low-income countries are defined as those with a GNI per capita of $1,035 or less in 2019; lower middle-income countries are those with a GNI per capita between $1,036 and $4,045; upper middle-income countries are those with a GNI per capita between $4,046 and $12,535; high-income countries are those with a GNI per capita of $12,536 or more.

burglary of family household or exposure to random shooting)[9] (see Soler et al., 2012).

Based on the evidence mentioned above, disadvantaged settings tend to see a greater level of poly-victimisation among children and adolescents. A systematic review synthesising evidence on the prevalence rates of poly-victimisation of children and adolescents in countries with low/lower-middle income found an overall prevalence rate of 38.1 percent (95% CI [18.3%, 57.8%]) (Le et al., 2018). The disadvantaged countries comprised eight from Africa (e.g., Egypt, Kenya, etc.), four from South Asia (e.g., India), two from East Asia and Pacific region (Vietnam and Cambodia), one from South America (Bolivia), and one from Central America (El Salvador). Noticeably, the forms of victimisation included in the systematic review involved individuals' experiences of (1) physical, verbal/emotional, or sexual violence; (2) neglect; (3) witnessing of violent acts in the family or in the community; (4) property vandalism; (5) abduction; (6) displacement; (7) being threatened; or (8) robbed (see Le et al., 2018). That is to say, given a wide range of forms of poly-victimisation across studies, the slightly high prevalence rate of poly-victimisation observed in disadvantaged settings needs to be taken with caution.

Notably, using "poly AND victim" as keyword searches in Google scholar returned 9,430 results since 2016 (around one fourth to the 35,300 results for "repeat AND victim")[10]. Suggested reasons for this disparity might be because poly-victimisation is more difficult to identify, estimate and analyse, or slightly because the term repeat victimisation or multiple victimisations is used interchangeably with poly-victimisation. For example, min Park (2015) reported that around one fifth of victimised households in South Korea had experienced *poly-victimisations* in the past year, though the experience of two or more different types of victimisations was described as repeat victimisation

[9] Witnessing and indirect victimisation included being a witness to domestic violence, a witness to parent assault of a sibling, a witness to assault with and without weapons, burglary of family household, homicide of a family member or friend, witness to homicide, exposure to random shootings, terrorism or riots, and exposure to war or ethnic conflicts.

[10] The search was conducted on 16th August 2020.

in his research[11]. The latter reason indeed makes it challenging to identify relevant literature on ‘poly-victimisation’.

Nevertheless, studies retrieved from this search strategy reinforce the point that research on poly-victimisation has an exclusive focus on childhood/adolescent violence (Almeida et al., 2020; Kretschmar et al., 2017; Leoschut & Kafaar, 2017) and their relationship with mental health (Álvarez-Lister et al., 2017; Haahr-Pedersen et al., 2020; Lätsch et al., 2017), for which victimisation against adults and in online contexts are less explored. Meanwhile, it is also noted that few studies have applied an ecological approach to explore poly-victimisation.

Among the few studies applying a LRAA to explore poly-victimisation, a number of risk factors have been identified: lack of guardianship, exposure and proximity to crime, disorder and potential offenders and target attractiveness/suitability (e.g. disability). The most evident example demonstrating the impact of individuals’ lifestyle-routines on the risk of poly-victimisation can be seen in a Finnish study (Ellonen & Salmi, 2011). There were nine categories of victimisation involved in defining poly-victimisation, including physical or mental violence from family, peer or teacher and electronic bullying. A significant correlation was found between poly-victimisation and personal/family backgrounds among pupils aged 12-16 years. The correlation between pupil’s experience of poly-victimisation and their backgrounds, however, depended on their lifestyle-routines. Poly victims tended to spend most of their free time alone and spend a lot of time in public spaces (i.e. the absence of capable guardianship). Conversely, individuals with the least poly-victimisation being reported tended to spend most of their free time with their family.

[11] Types of victimisations included in the study are: (1) robbery through criminal trespassing, (2) burglary, (3) criminal trespassing, (4) other trespassing, (5) property damage, (6) property damage through criminal trespassing, (7) automobile theft, and (8) automobile damage.

Ellonen and Salmi’s (2011) research further suggested correlations between pupils’ poly-victimisation and their living situations. Living situations included a poor family financial situation, frequent parental fighting, seeing parents intoxicated, and poor family communication (e.g. not having dinner together, or parents not knowing with whom their children spent free time), for which the absence of capable guardianship underpinning the opportunity framework could also be linked (Ellonen & Salmi, 2011).

Otherwise, with regard to exposure and proximity to crime, disorder and potential offenders, a deviant lifestyle might be considered. A deviant lifestyle, including alcohol consumption, drug use, smoking, and delinquency, has also been found to be positively associated with young people’s self-reported experience of poly-victimisation in Ellonen and Salmi's (2011) research. Other evidence on target attractiveness/suitability as identified risk factors embedded in LRAA includes personal vulnerability such as a chronic disease, disability, mental issues or cognitive/psychological issue (i.e., self-control) that make young people prone to risky behaviours or less self-protected and fall prey to poly-victimisation (i.e. suitable target) (Finkelhor et al., 2009; Le et al., 2016; Tanksley et al., 2020).

Again, it is noteworthy that the studies to date on poly-victimisation, though with the application of LRAA, are limited to childhood/adolescent research on violence. More research such as poly-victimisation against adults and in online contexts is thus needed.

2.3.3 Implications of (near) repeat victimisation and poly-victimisation research

Research on repeat and near repeat victimisation, along with poly-victimisation has important implications for crime prevention. Presuming that crime concentrates on a small number of repeatedly victimised targets – so-called super targets – then it makes sense to devote prevention resources to those super targets. There is strong evidence to support this approach to crime prevention, particularly in relation to residential burglary (see Grove et al., 2012). The logic similarly applies to prevention against poly-victimisation, though this aspect requires more research. Likewise, research on near repeats means that time-limited predictions can be made about where crime is most likely to occur so that preventive resources can be deployed accordingly. Again, there are numerous studies demonstrating the effectiveness of this approach in reducing residential burglary (Fielding & Jones, 2012; Stokes & Clare, 2019).

Despite the evidence on which patterns of (N)RV are observed, and their importance for crime prevention, research into the extent, patterns and prevention of (N)RV in Asia is limited. Not to mention little research attention being paid to poly-victimisation in Asian contexts. This lack of research hinders communication between research and practical prevention against crime in Asia. This thesis therefore aims to contribute to the limited evidence base on (near) repeat victimisation and poly-victimisation in Asia, with a specific focus on Taiwan.

2.4 Research questions

Based on the literature review above, three main gaps and points of contention are highlighted: (1) there are presently no systematic studies on either burglary or cybercrime victimisation patterns in Taiwan using an opportunity framework; consequently it is unknown whether the much-used LRAA is generalisable to the (low-crime) Taiwanese context; (2) there remains much uncertainty about the extent, patterns, and temporal and spatial range of (near) repeat victimisation in Taiwan; and (3) little is known about the extent and patterns of poly-victimisation in Taiwan, particularly that which relates to cybercrime.

In light of the above research gaps, this thesis aims to answer six research questions that relate to four crime issues in Taiwan: burglary and repeat burglary victimisation, online victimisation and poly-victimisation. The specific research questions addressed in this thesis are:

Question 1: Does a lifestyle-routine activity approach adequately explain burglary victimisation patterns in Taiwan?

Question 2: Is there evidence of (near) repeat burglary victimisation in Taiwan?

Question 3-a: Does the LRAA adequately explain patterns of online victimisation in Taiwan?

Question 3-b: Do victimisation patterns vary across different types of online victimisation in Taiwan?

Question 4-a: Is there evidence of online poly-victimisation in Taiwan?

Question 4-b: Do victimisation patterns vary between single and poly-victimisation online?

Chapter 3 Measuring and analysing crime in Taiwan

This chapter describes the data sources used in this thesis. It begins by introducing the methods that are generally used to measure crime – administrative crime statistics and victim surveys – and discusses their respective strengths and weaknesses. It then presents an overview of crime statistics in Taiwan, including the official statistics and survey data which are drawn on in this thesis. Lastly, general limitations of the datasets used in this thesis are discussed.

3.1 Measuring crime

There are two main sources of data with which to measure the extent of crime: official crime statistics and victimisation surveys. Official statistics, also known as administrative crime statistics, comprise the counts of crime reported to and recorded by the police (Mosher et al., 2011). By contrast, victimisation surveys measure self-reported experience of (certain) crime types among a sample of people over a given period, most often the past year. In the section that follows I describe each kind of data source and discuss their strengths and weaknesses.

3.1.1 Official crime statistics

'Official crime statistics' is a broad term that applies to any set of administrative statistics drawn from the criminal justice system. In practice, however, this term usually refers to statistics taken from police or court records (Loftin & McDowall, 2010).

There are three main strengths of official crime statistics. First, they provide a good measure of the patterns and trends in well-reported crimes, most notably serious violence (especially that involving a weapon) and those crimes which typically trigger insurance claims, such as car theft (Maguire & McVie, 2017). Second, official crime statistics are important indicators of the criminal justice system (CJS) workload. Third, official crime statistics generally contain data for small geographic areas which can be utilised for local crime pattern analysis. For example, police data often includes point-level information on where crime takes place, which can be utilised for, amongst other things, crime hot spot analysis.

However, official crime statistics often receive criticisms on two main fronts: one, they are dependent on victims' reporting practices; and two, they might be affected by the recording practices of the CJS, particularly the police (Lauritsen et al., 2016). I will discuss each in turn. Victims' underreporting of crime is believed to undermine the completeness of official crime statistics. For example, Langton et al. (2012) suggested that there were 58% of all victimisations not reported to the police during the period from 2006 to 2010 in the US. Breaking down this figure in more detail: 60% of all household thefts and 52% of all violent victimisations were estimated to not be reported to the police[1]. Victims' crime reporting to the CJS is known to be dependent on a range of variables such as the nature and seriousness of victimisation, victim-offender relationships, trust and confidence in police, (in)convenience of crime reporting to police, or even insurance requirements that can influence a victim's willingness to report victimisation (Junger-Tas & Marshall, 1999; Murphy & Barkworth, 2014). Hence, whilst homicide and vehicle theft are known to be well-reported crimes, violence – especially sexual assault – is often under-reported to the CJS (Langton et al., 2012).

Just as victim reporting practices are influenced by multiple variables, so can the recording practices of the CJS be influenced by various factors. First, official crime statistics might vary due to inconsistencies in recording practices across different administrative areas (Warner, 1997). Put differently,

[1] For serious violent victimisations: 65% of all rapes/sexual assaults, 44% of all aggravated assaults, 41% of all robberies were not reported to the police. For household theft: 67% of all theft and 45% of all burglaries and 17% of all motor vehicle theft were not reported to the police.

official statistics may vary either due to revisions in legislation within a country or variance in legislation across countries. The official crime statistics are dependent on what sorts of criminal activities they cover and how they are recorded by the administrative system (Maguire & McVie, 2017). Second, crime statistics vary by case attrition at each stage of the CJS, from police investigation to conviction. For example, it was found in England and Wales that during the police investigation stage, 67% of rape allegations were withdrawn by the victim[2]. Among these non-withdrawn rape cases, 19% of case attrition were made by police decision as 'no-crime' and 67% of attrition as 'no further action' whilst Crown Prosecution Service decisions to take no further action accounted for 14% of the observed attrition[3] (Hohl & Stanko, 2015).

The attrition issue discussed above raises a further concern with how crime can be recorded. That is to say, as CJS actors – the police in particular – make discretionary decisions, crime statistics are likely to be affected by recording practices by the police (Nickels, 2007; Varano et al., 2009). Specifically, research has indicated that the under-recording of crime by the police is an endemic feature of policing around the world (Maxfield et al., 1980; Warner & Pierce, 1993). In England and Wales, for example, it is estimated that around 19 percent of cases reported to the police each year are not recorded as crimes (i.e. over 800,000 crimes unrecorded by police; HMIC, 2014). Similarly in the Netherlands it is estimated that around one third of all crime reports are not recorded as crimes (van Dijk, 2008). By offence type, violence against the person (33%) and sexual offences (26%) are found to be affected most by under-recording in England and Wales (HMIC, 2014). There are several proposed reasons for variations in rates of under-recording by offence types. These include the nature and seriousness of the offence, the probability

[2] Victim withdrawal accounted for 48% of attrition in the sample when those allegations awaiting trial were taken into account.

[3] Among these non-withdrawn rape cases, 11% of case outcomes were made as 'no-crime' and 39% of case outcomes as 'no further action' by police decision and merely 15% of case outcomes ended up with a charge by Crown Prosecution Service.

of case clearance, and definitional issues of offence qualification perceived by the police (Junger-Tas & Marshall, 1999; Yu & Zhang, 1999).

Furthermore, police recording practices are influenced by institutional issues like organisational goals or task prioritisation, leading to slumps or spikes in some crimes (van Dijk, 2008). For example, the rate of recorded child sexual abuse (CSA) in England and Wales has more than doubled since 2013 while the actual rates of CSA are suggested to have remained relatively stable. Researchers have attributed the rise in recorded CSA to improvements in the quality of crime recording and successes in the identification of CSA offenders by the police and local police priorities particularly with regard to image offences, rather than an actual increase in crime rates of CSA (see e.g. Kelly & Karsna, 2018).

To summarise, official crime statistics are those recorded by the CJS. Their main strengths are that they are generally a good measure of trends in well-reported crimes and the CJS workload, and could provide sufficient information to enable geographic patterns of crimes to be analysed. As mentioned, official crime statistics underestimate actual crime rates when criminal cases are not reported by victims or not recorded by the police. Those crimes are termed the ‘dark figures’. With the awareness of the existence of the ‘dark figures’ of unreported or unrecorded crime, new ways of measuring crime have been developed from the 1960s onwards (Coleman & Moynihan, 1996). Victimisation surveys have since been the prevailing alternative measure of crime, designed to complement (and supplement) police crime statistics. Victimisation surveys are generally considered to provide a more reliable portrait of (some) crimes than do police figures. The next section describes victimisation surveys and then discusses the strengths and weaknesses of them.

3.1.2 Victimisation surveys

A victimisation survey measures the experience of criminal victimisation from the perspective of victims themselves. Victimisation surveys were introduced from the late 1960s onwards primarily as a way of overcoming the observed bias in administrative crime statistics, most notably the problem of the dark figure of crime (Block & Block, 1984; Sparks, 1981; Thornberry & Krohn, 2000; Wetzels et al., 1994). Victimisation surveys can involve either (a) self-administered surveys asking participants' their self-reported experience of certain types of criminal victimisation such as violent victimisation (Khade et al., 2018) or cybercrime (e.g. Vakhitova et al., 2016), etc., or (b) on a nation-wide scale, measuring a variety of variables related to crime problems including citizens' experience of victimisation as well as related measures such as fear of crime or perceptions of the CJS. Nationwide surveys using a representative sample also allow for estimates to be computed of prevalence and incidence rates of crime and delinquency of specific populations and are believed to have higher validity of estimates than do official measures (Junger-Tas & Marshall, 1999).

Nowadays, national victimisation surveys are carried out in many countries including the US, Finland, the Netherlands, Italy, Switzerland, Canada, Australia, the UK and so on. With regard to comparative surveys between countries, the International Crime Victim Survey (ICVS) is one of the largest, with around 80 different countries having participated in at least one sweep of ICVS over the past 20 years (Maguire & McVie, 2017; Mayhew & van Dijk, 2011).

Victim surveys have several noted strengths, including: (1) giving a more complete estimate of the scale of crime and risk (should a representative sample be recruited); (2) providing data on unreported and unrecorded crime (the so called 'dark figure'); and (3) enabling research into the causes and impact of crime through valid and reliable measures of victimisation and characteristics related to victimisations (Boslaugh, 2015; Junger-Tas & Marshall, 1999). Put simply, victim surveys often utilise high standard sampling plans and complex weighing strategies, giving rise to highly reliable and representative datasets that overcome the problem of the dark figure of crime. The scope of victimisation surveys thus allows for a more comprehensive estimate of crime and risk than that of police data.

Furthermore, these surveys collect lots of information which can be used to better understand the characteristics and lifestyle of respondents and which can be used to explore differences in, say, experience of crime (Aromaa & Heiskanen, 2008). This additional information is of great value to researchers interested in determining the correlates of crime and testing theories on crime.

There are, however, several limitations in regard to victimisation surveys, including: 1) a potential bias resulting from self-selected samples, particularly with regard to surveys with low response rates (Di Gennaro & La Spina, 2016); and (2) memory effects (Junger-Tas & Marshall, 1999; Sparks, 1981), sometime referred as recall bias (Althubaiti, 2016). Memory effects derive from the retrospective nature of victimisation reporting. They include cases in which participants forget events entirely or misplace events in time (i.e. telescoping). An incident may be recalled as having occurred more recently than it actually did (forward telescoping), or it may be recalled as having occurred earlier than it actually did (backward) (Gottfredson & Hindelang, 1977). Telescoping is common (Averdijk & Elffers, 2012; Skogan, 1975). For example, Averdijk and Elffers (2012) found that forward telescoping occurred in 28% of cases reported in the Dutch victimisation surveys, based on comparisons with police recorded crime. Issues can also arise with reliability issues resulted from over-reporting or under-reporting of victimisation by respondents or further the adjustment issue (Ellonen & Pösö, 2011). The adjustment issue refers to the case that respondents, probably being affected by social desirability pressures, adjust their answers in order for them to appear more socially acceptable (see Althubaiti, 2016; Junger-Tas & Marshall, 1999; Yar & Steinmetz, 2019) .

Fortunately, many approaches have been proposed to ensure the validity and reliability of self-reporting surveys. These may include: (1) the choice of appropriate recall period; (2) validation of the survey instrument before implementation and (3) careful examinations into reasonable entries of data (Ellonen & Pösö, 2011; Harrison & Hughes, 1997; Junger-Tas & Marshall, 1999; Magura & Kang, 1996; van de Mortel, 2008). By adopting such strategies, many of the aforementioned limitations have been addressed in contemporary victim surveys. However, to ensure the validity and reliability, it is noted that victim surveys may implement a counting convention to limit the maximum number of victimisations that can be recorded. This capping convention is to avoid extreme figures inflating overall crime rates (Budd & Mattinson, 2000); however, it also imposes a risk of underestimating crime, particularly with regard to RV or say the super targets (I will cover the issue of capping later in Section 3.2.2.1).

There are some other limitations with the nature of victim surveys themselves. Given that victim surveys measure victimisation from the perspective of victims, it is noted that not all crimes are included in victim surveys. Obvious examples include homicide, in which victims are dead and cannot be recruited as a respondent in a survey. Some types of crime, such as drug abuse and smuggling of migrants, are also not measured by victim surveys as they are often considered 'victimless' crimes (Heiskanen & Laaksonen, 2021). Furthermore, not all people are included in the sampling frame of a victim survey. For example, victim surveys that utilise landlines to recruit respondents would exclude those who do not have access to a landline (e.g. homeless) and those that use an online instrument would recruit exclusive samples with such access.

To sum up, victim surveys measure crime from the perspective of victims themselves. Hence, victim surveys with a representative data can provide a more complete estimate of crime without the impact of unreported and unrecorded incidents. Researchers can also use victim surveys to understand the causes and impact of crime should individual victimisations, characteristics, or lifestyles be measured. Whilst the validity and reliability of victim surveys can be assured by approaches mentioned above, super targets with extreme victimisations, some types of crime and certain samples would (inevitably) be excluded from victim surveys, thereby giving rise to skewed results.

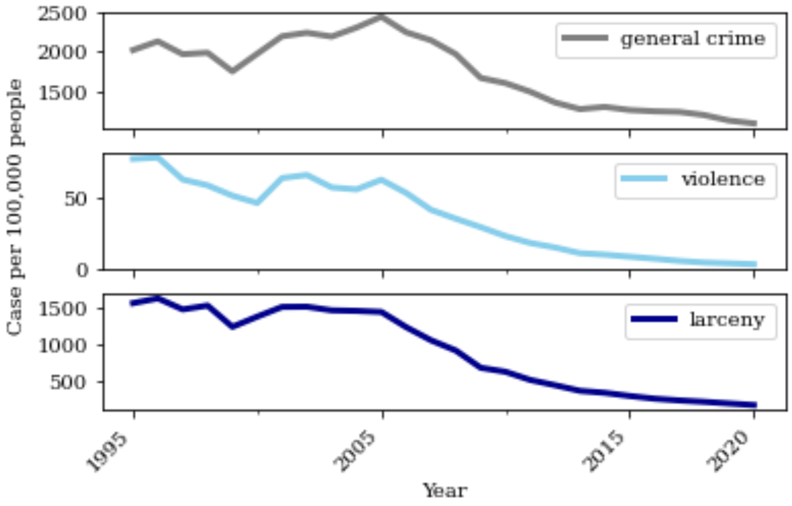
The following sections present crime statistics in Taiwan, drawing data from both official statistics and victim surveys.

3.2 Taiwan crime statistics

Police recorded crime data and victim surveys are both available in Taiwan, though they are not freely available and might be difficult to access. It is noted that Taiwan does not participate in the ICVS. It does however conduct a national victimisation survey – the TAVS. Below I discuss Taiwanese police recorded crime statistics and the TAVS data, respectively.

3.2.1 Taiwan police recorded crime data

In the case of police recorded crime in Taiwan, crime can be reported through a variety of means, including the 110 police hotline, online reporting, cloud video, at the scene, or at the front counter of police stations. More recently, the smartphone application 'Police Service App' has been developed to allow citizens to file a crime report via texting or instant image sharing. For every report made at a duty counter, citizens will be issued with a formal receipt (*baoan sanliandan*), by which they can track the progress of their cases. The 'One-stop Window' policy allows citizens in Taiwan to report and have cases recorded at any duty counter regardless of jurisdiction. The National Police Agency (NPA), under the Ministry of the Interior, oversees all police forces in Taiwan, including central police organisations and local police departments. Given this, the NPA is responsible for publishing official crime statistics to the public, through monthly, seasonal or annual reports. However, it is noted that the official statistics released to the public do not draw from the aforementioned formal receipts, but from modified statistics of the police internal recording system. Hence, there might be inconsistency in crime statistics across the formal receipt system, police internal records and publicly accessed data (see T.-L. Kuo, 2017).



Source: National Police Agency, Taiwan

Figure 3.1 Police recorded crime rates by offence type, Taiwan 1995-2020

However, as mentioned above, one benefit of official crime statistics is that they provide a picture of crime trends over time (for those crimes which tend to be reported and recorded). With this in mind, Figure 3.1 displays crime rates per 100,000 population according to police records in Taiwan by offence type between 1995 and 2020. It can be seen that in the past few decades, official records of general crime rates in Taiwan peaked at about 2,442 cases per 100,000 population in 2005 and declined to roughly 1,101 cases per 100,000 population in 2020 (also see Section 1.2.1). These general reductions in crime are akin to the general reductions observed in many countries – the so-called international crime drop (Farrell, 2013; Sidebottom, Kuo, et al., 2018; van Dijk et al., 2012). Two subcategories of crime are considered noteworthy here: violence and larceny. According to the Taiwanese police categorisation, the former contains offences of intimidation or extortion, kidnapping, robbery and forceful taking, serious injury and wilful manslaughter, and rape. The latter otherwise includes serious larceny[4], general larceny, motor vehicle theft and motorcycle theft (National Police

[4] Serious larceny is defined by a crime report of loss over one million New Taiwan dollars since 24 March 2016 (before then as NT$500,000). One million New Taiwan dollars are about GBP£25,740.

Agency, 2019a). Violence and larceny have both followed a similar downward trend over time; in 2005, violence had a rate of about 63 cases per 100,000 population and larceny about 1444 cases per 100,000 population. In 2020, the rates have plummeted to around 3 cases per 100,000 population for violence and 157 cases per 100,000 population for larceny. Considering the focus of this thesis, the sections below focus on what official police statistics indicate with respect to burglaries and cybercrimes in Taiwan.

3.2.1.1 Defining burglary and cybercrime in Taiwan official statistics

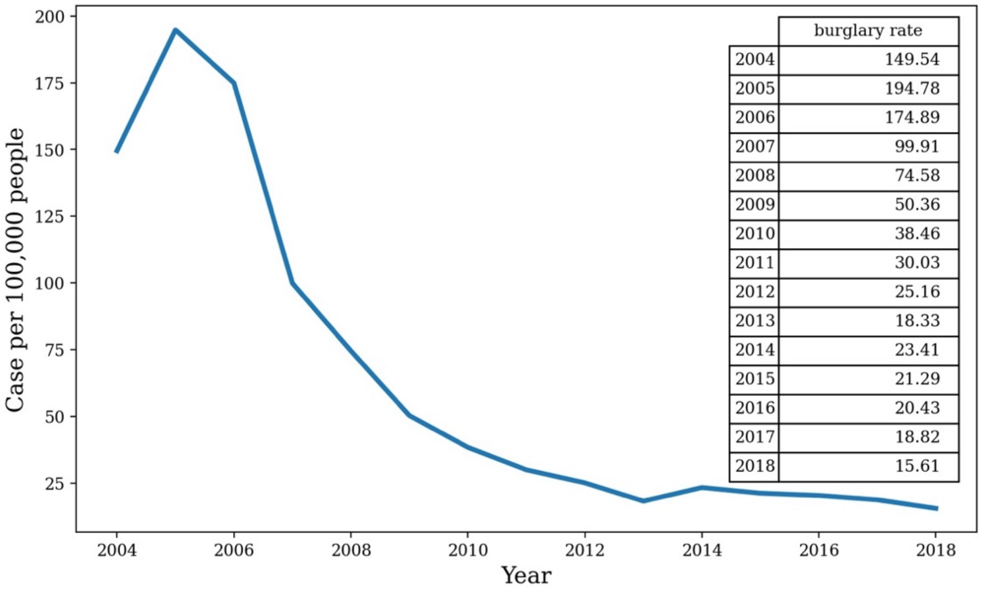
According to the 'Criminal Code of the Republic of China' (below as Criminal Code), Chapter 29, Article 321, residential burglary refers to "*…intruding a dwelling house, a structure used as a dwelling house, or a vessel, or concealing himself therein…*" and *"...damaging and breaking into a window, a door, a wall, or other protective features…*", either carrying a dangerous weapon, involving groups of offenders, or taking advantage of any disasters.

According to Criminal Code Article 339-3, cybercrime refers to cases where "*A person who for purpose to exercise unlawful control over other's property for himself or for a third person takes property of another by entering false data or wrongful directives into a computer or relating equipment to create the records of acquisition, loss or alteration of property ownership*". A person who "*takes an illegal benefit in property*" by those methods are also regarded as a commission of cybercrime.

Presented below are the official crime statistics for burglary and cybercrime, as defined above, drawing on official Taiwanese police recorded crime data.

3.2.1.2 Police recorded burglary

Burglary is counted as a larceny offence and is not specifically disclosed in official statistics in Taiwan. Yet it is published in some announcements by the NPA on an irregular basis (National Police Agency, 2020). Figure 3.2 displays the trend in burglary rates in Taiwan between 2004 and 2018. Similar to that observed in Figure 1.1 for general crime in Taiwan, Figure 3.2 shows a downward trend in burglary since 2005. Over this time period (2004-2018), burglary rates in Taiwan are found to have peaked in 2005 at around 195 cases per 100,000 population and then experience a consistent downward trend, falling to 16 burglaries per 100,000 population in 2018. These falls are dramatic. The reason for these falls in Taiwan is unclear, though improved household security might be a key driver in the declines in burglary as the Western literature suggested (Farrell et al., 2014; Tilley et al., 2015; Tseloni et al., 2017). However, more research is needed to support whether improvements in household security can account for these falls in Taiwan (Sidebottom, Kuo, et al., 2018).



	burglary rate
2004	149.54
2005	194.78
2006	174.89
2007	99.91
2008	74.58
2009	50.36
2010	38.46
2011	30.03
2012	25.16
2013	18.33
2014	23.41
2015	21.29
2016	20.43
2017	18.82
2018	15.61

Source: National Police Agency, Taiwan

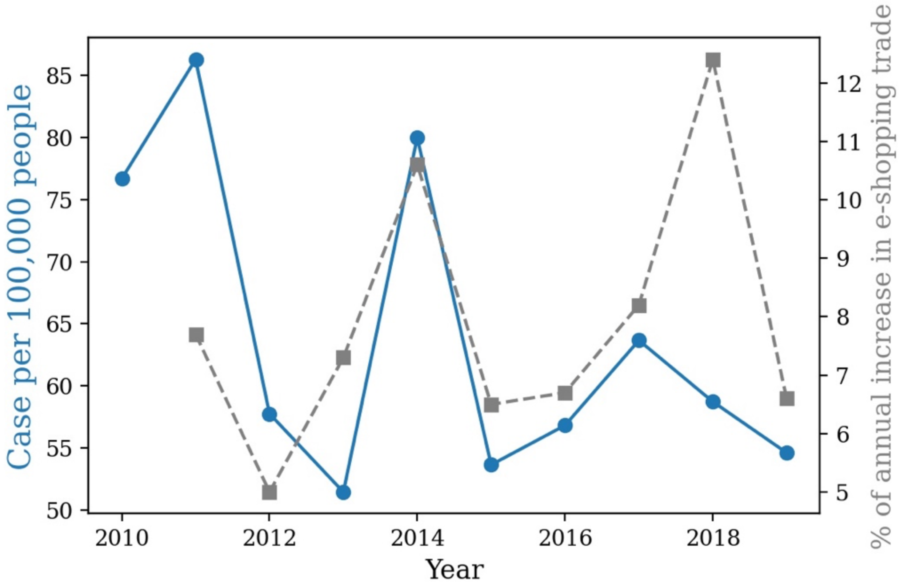
Figure 3.2 Police recorded burglary rates by year, Taiwan 2004-2018

It is noteworthy here that other than the NPA, a few local police departments in Taiwan also publish their own burglary data to the public. The datasets often comprise merely burglary statistics at a city/country level (or further at a district-level). An exception is those released by the Taoyuan Police Department (TYPD), of which data the geographical information of burglary incidents is disclosed. In Chapter 5, I use police data made available by the TYPD. Further details are provided in Section 5.3.1.

According to the profiling of burglary offences during the year of 2019 performed by the NPA, offenders tend to be male (nearly 90 percent), aged 30-49 years old, unemployed, and the offences take places in working hours (9 am to 6pm) (National Police Agency, 2019b). The most common modus operandi is breaking into a house when it is vacant and without the use of force. The most common entry points for burglary in Taiwan are by doors and windows (Ho, 2013; National Police Agency, 2019b). No evidence is presented on which type of property in Taiwan experience higher rates of burglary.

3.2.1.3 Police recorded cybercrime

Official statistics on cybercrime can be found in the annual publication of crime statistics by the Criminal Investigation Bureau (CIB) of the NPA (see e.g. Criminal Investigation Bureau, 2020). Figure 3.3 displays the trend of cybercrime rates for the past decade in Taiwan (marked in blue), with the percentage of the annual increase in the electronic shopping trades given as a complementary line (marked in grey).



Source: National Police Agency; Department of Statistics, Ministry of Economic Affairs, Taiwan

Figure 3.3 Rate of police recorded cybercrime and changes in trades of electronic shopping by year, Taiwan 2010-2019. The blue line represents the trend of cybercrime rates. The grey dashed line reflects the percentage of the annual increase in the electronic shopping trades.

Compared to the rates of general crime and burglary presented above, cybercrime rates, as measured by official crime statistics, exhibit a much greater level of fluctuation, although an overall reduction in cybercrime can be observed over the ten-year time period covered in Figure 3.3. The rate seemed to peak at over 80 cases per 100,000 population in 2011 and then again in 2014. A third peak can be seen in 2017, of which point around 64 cases of cybercrime per 100,000 population was recorded. The rate then declined gradually to around 55 cases per 100,000 population in 2019. To my best awareness, there were no noticeable changes in reporting and recording practices that may contribute to those peaks and slumps. An explanatory factor might be sharp increases identified in the level of electronic shopping in certain years (see Figure 3.3 the grey line), of which points there might be a boost in the number of ecommerce platforms, thus providing more opportunities for cybercrime to occur. Yet further evidence is required to support such correlations between increased trades, platforms and cybercrime rates. More research is needed.

The annual publication on crime statistics by the CIB provides little additional information about cybercrimes in Taiwan. According to the limited analysis of cybercrime committed in 2019, cyber offenders in Taiwan tend to be male (nearly 70 percent) while cyber victims tend to be slightly dominated by male as well (about 60 percent). Half of the cases took place in the daytime (between 9am and 7pm) (National Police Agency, 2019b). There are no sub-categories of cybercrime provided in the official report, in which we do not know which type of cybercrime or modus operandi are the most common.

The aforementioned discussions about cybercrime patterns bring up a question that whether official crime statistics are a decent measure of cybercrime victimisation. Firstly, many victims may not report to the police but instead report to, say the banks. Second, unlike burglary, the category of cybercrime refers to a wide range of different offences whose individual patterns might be masked by this overall category. These points inform the following sections to discuss victim surveys in Taiwan, with respect to both conventional crime and cybercrime.

3.2.2 Victim surveys in Taiwan

Currently, the national estimate of victimisation in Taiwan mainly draws on the TAVS, which began in 2000. However, it is noteworthy that the TAVS does not contain information on cybercrime. For a reference point, the Crime Survey for England and Wales (CSEW) included fraud and computer misuse from October 2015 and the first estimate of CSEW on fraud and computer misuse was published in July 2016 (Office for National Statistics, 2018). Hence, one may foresee cybercrime-related questions being included in future TAVSs. Nevertheless, this thesis utilises another series of national surveys on citizens' access to the internet – the DOSIH that contains several questions related to cybercrime, but which hitherto has not been analysed from a crime science perspective. This thesis is, thus, the first to do so. It should be noted, however, that the DOSIH was not designed for the purpose of better understanding cybercrime in Taiwan; it was conceived mainly to understand how Taiwanese citizens spend their time online (I will return to this point in Section 3.2.2.2). Below I describe the two main survey datasets that used in the thesis: the TAVS and DOSIH.

3.2.2.1 Taiwan Area Victimisation Survey

The studies reported in the following chapters will use data collected as part of the 2015 TAVS. As a general rule in Taiwan, victimisation surveys are funded by the NPA which, as described above, oversees all national and local police forces in Taiwan. The NPA has been outsourcing victimisation surveys to selected university researchers in Taiwan since 2000. Unlike most western countries that carry out national-level crime victimisation survey on a frequent basis (say quarterly like CSEW), Taiwan conducts their victim survey every five years. The first TAVS took place in 2000 and there have been three subsequent sweeps[5]. The 2015 TAVS is used here as that was the most recently available data at the time of writing.

The 2015 TAVS used stratified random sampling, with the assistance of Computer Assisted Telephone Interview (CATI). Participants were nested in 20 of the 22 cities/counties[6] in Taiwan and all registered nationals aged 12 or older were eligible for inclusion. Also, because the sampling for the TAVS required a registered landline, a general limitation is that some population groups might be excluded from the TAVS – most obviously young people (who only have mobile phones), the homeless and immigrants. However, the

[5] The most recent sweep is expected to be administered in 2020 but the project might be delayed due to the Covid pandemic in Taiwan. Until I am writing up this thesis, there is no further information released by the NPA about which unit would be in charge of the new TAVS.

[6] Due to the political controversy with mainland China, the survey area of TAVS tend to focus on the 'Taiwan area' (officially referred as the 'Province of Taiwan'), excluding the two counties: Matsu and Kinmen. The two counties are located in provinces that are dominantly governed by mainland China and outside the province of Taiwan.

TAVS researchers suggested that the survey be considered a nationally representative sample of Taiwan population with respect to regions, age and gender (at a significance level of 0.05) (Central Police University, 2015). Phone calls were made between 5 May and 20 July 2015 and 13,016 interviews were marked as completed, reaching a response rate of 30.76 percent[7]. The big attrition rate was attributed to a high volume of refusals (nearly 50%) made at the time of phone contacts. For a reference point, the original response rates for the CSEW were 70% for year ending March 2019 and 64% for year ending March 2020 (Office for National Statistics, 2021a). Researchers have found that the response rates for the CSEW tend to be lower in areas that report higher crime, though the impact of non-response on the crime estimates is small (Hopper, 2015). Because the TAVS did not disclose such information about patterns of non-response/attrition, it is difficult to explain why there were a such big difference in response rates between the TAVS and CSEW.

Nevertheless, the TAVS participants were asked about eight types of criminal victimisation experienced in the previous year (1 January to 31 December 2014), namely residential burglary, motorcycle theft, car theft, fraud, robbery, forceful taking, injury and general larceny. The questionnaires were delivered in Chinese. The question asking participants about the experience of residential burglary was: "*In the past year, did anyone steal belongings from your residence (including residential and office mixed use buildings)?*".

To provide some context to the reader, Table 3.1 compares some of the key attributes and findings from the national crime victim surveys in Taiwan, the US and England and Wales for a comparable survey period (roughly 2014/2015). Note that Taiwan includes respondents as young as 12-year-olds; the CSEW has been criticised for setting the minimum age at 16 years and thus missing a sizable portion of crime. In response to this criticism, the

[7] The response rate refers to the percentage of interviews completed out of the total number of individuals who could be contacted in the sample.

CSEW has extended to include children aged 10 to 15 years and reported the data as a separate annex (Office for National Statistics, 2021a).

Table 3.1 Comparison of victim surveys in Taiwan, UK and US, 2014/2015

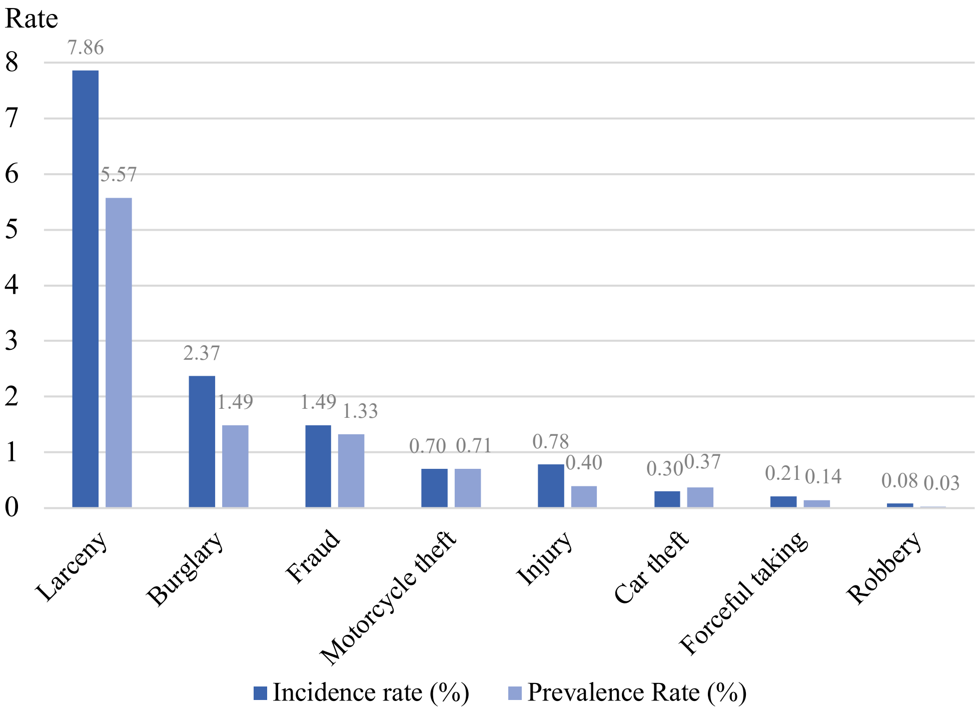
	TAVS(Taiwan)	CSEW(UK)	NCVS(US)
Sample size	13,016	35,248	90,380
Minimum respondents' age	12	16 (10)*	12
Originated in	2000	1981	1973
Frequency of survey	5 yrs.	Quarterly	2 per yr.
Public access to data	N	Y	Y
Agency in charge	NPA	ONS	BJS
Multiple victimisations counting cap	6	5 (98th %)ǂ	10 (since 2010)
Prevalence rate of burglary	1.49	2.29	1.67
Prevalence rate of theft	5.57	10.61	6.41
Prevalence rate of robbery	0.03	0.28	0.16
Incidence rate of burglary (per 100 HHs)	2.37	2.89	2.31

Source: National Police Agency (NPA); Office for National Statistics (ONS); Bureau of Justice Statistics (BJS).

Note. TAVS = Taiwan Area Victimisation Survey ; CSEW = Crime Survey for England and Wales ; NCVS = National Crime Victimization Survey. *A sole child aged 10 to 15 is randomly selected to be interviewed in households that have participated in the main survey if applicable. ǂ CSEW used to apply a capping of victimisation at five. Yet according to a review commissioned by ONS (J. Williams, 2016) and its consultation response (Office for National Statistics, 2016), an approach of the 98th percentile of victim incident counts has been applied for the first time in the CSEW: year ending September 2018 (released on 24 January 2019). A possible 12 for violence and sexual offences, and 18 for threats was suggested using data for 2003 to 2015 (Office for National Statistics, 2019).

There are three main limitations with the TAVS that warrant mention: frequency of survey, public access to the data, and the capping issues. Due to the TAVS being carried out every five years, the first limitation results in the absence of a clear picture of crime trends over time. The second limitation of public access to the data constrains the capacity of research into victimisation in Taiwan. It is because external utilisation of data cannot be made unless external researchers have a connection with the selected university researchers who are in charge of the survey project. The third limitation, capping, refers to a recording practice in which a maximum number of victimisations can be recorded. The intention behind this decision is to avoid extreme figures unduly influencing overall crime rates (see Budd & Mattinson, 2000). Such counting conventions are common in national victim surveys. For example, the US National Crime Victimization Survey (NCVS) caps the number of victimisations a respondent can report at ten since 2010 (a cap of 6 before 2010) (Lauritsen et al., 2012) and the UK CSEW used to cap at five until the year ending September 2018 of CSEW (Office for National Statistics, 2019).

However, researchers have argued (and demonstrated) that such capping conventions underestimate the true count of crime and, in particular, the extent of repeat victimisation (Farrell & Pease, 2007a, 2007b). Studies using British Crime Survey (BCS) data revealed that estimates of violence were the most affected and that the actual burglary count is nearly one fifth (19.7%) higher than that shown in the (capped) survey data. Tseloni and Pease (2005) have also estimated that the entry of actual number rather than a cap of five to BCS would make the property and personal crime incidence increase by about 2 and 1.5 times, respectively (Tseloni & Pease, 2005). Responding to such criticism, ever since the year ending September 2018 (released on January 2019), the CSEW has applied a cap of 98th percentile of victim incident counts for each crime type (Office for National Statistics, 2019). Although not quantitively examined here, I expect the capping conventions of the TAVS will similarly undercount the extent of crime more generally and repeat victimisation in particular. Further details of this limitation will be discussed in Chapter 5 (Section 5.5.2) – the chapter examining repeat victimisation in Taiwan.



Source: 2015 TAVS; Central Police University (2015)

Figure 3.4 Rates of victimisation by offence, 2015 TAVS. Incidence rate = number of victimisations per 100 individuals/households; prevalence rate = % of victimised individuals/households by individual/household's exposure to victimisation risk

Despite the limitations mentioned above, the TAVS can still provide a good overview of crime victimisation in Taiwan, and one which usefully supplements that provided by official crime statistics. Figure 3.4 shows the incidence and prevalence rates for each offence type included in the 2015 TAVS. Incidence rates here refer to the number of victimisations per 100 individuals/households, taking multiple experiences of same types of victimisations into account. Prevalence rates, as defined by the 2015 TAVS, refers to the proportion of victimised individuals/households by individual/household's exposure to victimisation risk. Multiple experiences of victimisations were thus counted once. It is also noted that in the case of burglary, the denominator of incidence and prevalence – the number of sampled households – would be the same. Yet in some cases, the number of individuals/households exposed to victimisation risk sometimes does not comply with the sample number of individuals/households. For example, the households that do not have a car/motorcycle would not be exposed to car/motorcycle theft. They would count for the denominator of incidence rates but not for prevalence ones, as defined by the TAVS. Note that this definition is different from that by Farrell (1995) (see Section 2.3), of which the incidence denotes the average number of crimes per 100 (or other definite number) of the population at risk and prevalence relates to the whole population.

Briefly, the ratio of incidence to prevalence rates for each offence type indicates the extent of concentration over the sampled population. The incidence divided by prevalence indicates how certain types of crime are unevenly distributed over targets. Note again that the Taiwan survey capped the total number of victimisations that a victim could report to six. Experience of victimisation over six times were hence coded as six and over. That is to say, provided that this truncation was removed from the TAVS, incidence rates would be higher as the same number of victims would have the chance to experience more incidents, so that a higher extent of concentration would be expected.

In line with police statistics, Figure 3.4 shows that larceny was the most prevalent type of crime in Taiwan, with a prevalence rate of 5.57 and incidence rate of 7.86 in the 2015 TAVS. The least prevalent crime was robbery, with a prevalence rate of 0.03 and incidence rate of 0.08. However, robbery was the most concentrated crime over victims, with a concentration rate of 2.67. Car and motorcycle theft were less concentrated, with both having a rate less than 1.

It is also noted that the 2015 TAVS did not measure the victimisation of cybercrimes as other national victim survey did (say CSEW for example). This warrants alternative data source to be identified. Fortunately, another nation-wide survey – the DOSIH – includes such information to be drawn on estimating the extent of cybercrime victimisation in Taiwan. This is introduced below.

3.2.2.2 Digital Opportunity Survey for Individuals and Households

The second main dataset used in this thesis is the DOSIH. The survey is commissioned by the National Development Council, a policy-planning agency of the Executive Yuan of Taiwan, and often conducted by private polling organisations in Taiwan. The stated aim of this survey is to better understand generational and regional inequalities in accessing the internet and computer devices. The Taiwanese government has commissioned the DOSIH every year since 2001, though cybercrime victimisation was not measured until 2015. These surveys have focused on digital opportunities and risks raised by new ways of communication (such as internet technology) at a national scale.

Unlike the TAVS, for which the public has limited access, raw data from the DOSIH are accessible to researchers for academic use with permission from Survey Research Data Archive (SRDA). The 2017 sweep is used in this thesis, as it was the first sweep that additionally measured individuals' victimisation of virus infection beyond cyber abuse, fraud and identity theft in the 2015/2016 sweeps.

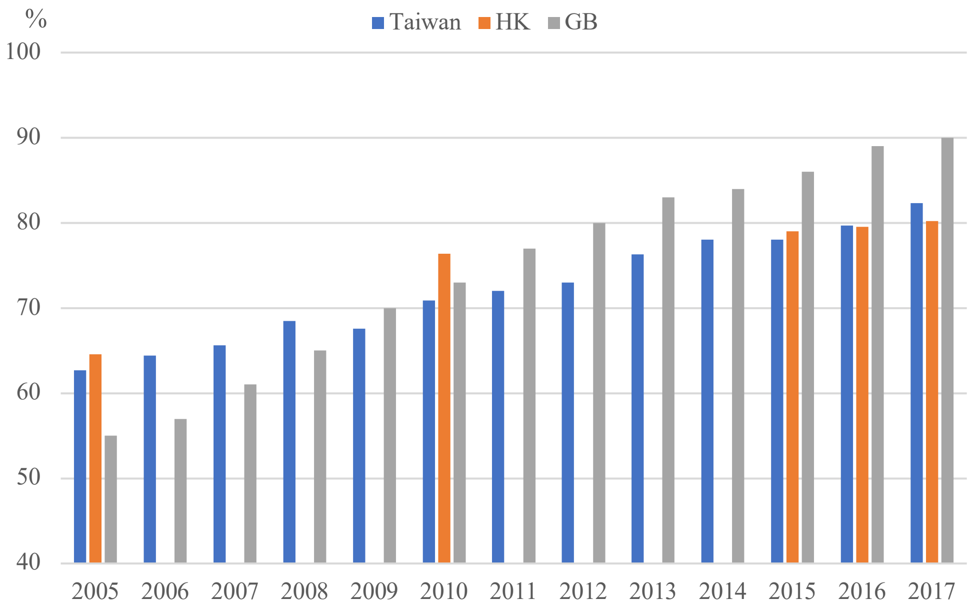
The 2017 DOSIH used stratified random sampling and the assistance of CATI, for which all registered nationals aged 12 or older and nested in all 22 cities/counties in Taiwan were eligible for inclusion. Like the TAVS, as the sampling required a registered landline, those young, affluent, homeless or immigrants might therefore be excluded from the survey. Phone calls were made between 22 August and 29 September 2017 and 9,337 cases were completed, reaching a response rate of about 67 percent.

As stated above, the DOSIH was primarily designed to understand generational and regional inequalities in accessing the internet and computer devices. Although it included a few items on the risks that people would encounter in the cyberworld, the questionnaire was not intended for cybercrime research. To my knowledge, no research has been done on cybercrime victimisation in Taiwan using such data. This thesis is hence the first study applying the DOSIH for criminological purposes.

Individuals' experiences of cybercrime victimisation were covered in four questions (translated from Chinese into English) as: (1) "*During the past year, have you suffered online verbal attack?*"; (2) "*During the past year, have you suffered personal information leakage (e.g. credit card/phone number) or account theft because of internet use?*"; (3) "*During the past year, have you suffered fraud because of internet use?*"; and (4) "*During the past year, have your PC or phone contaminated with virus because of internet use?*". Unlike the TAVS, which asked about multiple experiences of the same type of victimisation, the DOSIH merely recorded whether a respondent had experienced a certain type of cybercrime (i.e. yes or no). This means that the concentration of cybercrime victimisation in Taiwan cannot be computed using the DOSIH.

A main limitation of the DOSIH is noted here. To reiterate, the DOSIH survey was not designed for the purposes of understanding the extent or patterns of online victimisation in Taiwan. Hence, some key concepts in regard to cybercrime were not clearly stated or included. For example, the second question actually measured two types of cybercrime, namely information leakage and identity theft. The missing concepts otherwise may include a person's time spent online, their installation of security software, and so on. The limitations will be detailed in Chapter 6 (Section 6.6.4) and Chapter 7 (Section 7.6.3), which concern cybercrime victimisation in Taiwan.

Before presenting the trends of cybercrime victimisation in Taiwan, it would be helpful to provide some key indicators for readers to better understand internet access and use in Taiwan, with comparison to other regions. Figure 3.5 shows the trend of internet access in Taiwan, Hong Kong and Great Britain. In addition to the DOSIH, the statistics provided were drawn from official surveys (Census and Statistics Department, Hong Kong Special Administrative Region, 2020; Office for National Statistics, 2017). Figure 3.5 shows the rate of household internet access in 2017 was about 82% in Taiwan, while that in Hong Kong was around 80% and in the GB was 90%. For a reference point, the internet penetration rate (i.e. number of internet users divided by the population) is about 64% in Asia, 88.2% in Europe, 94% in North America, and an average of 66% across the globe (Miniwatts Marketing Group, 2021). The statistics suggest that Taiwan has a higher-than-average level of internet access in the Asian region; yet slightly lower than that in the European regions.



Source: DOSIH(Taiwan), Census and Statistics Department (HK), and ONS(GB).

Figure 3.5 Trends of internet penetration between Taiwan, Hong Kong (HK) and the Great Britain (GB), 2005-2017. Data on Hong Kong is only available every 5 year before 2015.

Figure 3.5 also indicates an upward trend in which a growing proportion of citizens aged 12 and older had access to the internet between 2005 and 2017 in Taiwan. Important implications drawn on this upward trend are that cyberworld has been growing in Taiwan, more problems might be brought out, and that more studies should be conducted to understand the risk factors of cybercrime.

Table 3.2 shows cybercrime victimisation in Taiwan drawn on the three sweeps of DOSIH between 2015 and 2017. Their sample sizes ranged from 9,408 to 23,465 participants. The table indicates personal information leakage (or known as data breach) and identity theft to be the most problematic – around one tenth of participants across sweeps had experiences of such victimisation in the past year. Virus infection was only available as an option in the 2017 sweep where it accounted for one tenth of cybercrime victimisation in Taiwan.

Table 3.2 Statistics of cyber victimisation, DOSIH 2015-2017

Types of victimisations	2017	2016	2015
	Count (% of n)	Count (% of n)	Count (% of n)
Online verbal abuse	218 (2.33)	528 (2.25)	224 (2.38)
Information leakage/ identity theft	715 (7.66)	2,196 (9.36)	1,018 (10.82)
Online fraud	309 (3.31)	880 (3.75)	369 (3.92)
PC/phone virus infection	946 (10.13)	-	-
Sample size (n)	9,337	23,465	9,408
Response rates (%)	67.01	65.45	67.31

For a reference point, Table 3.3 displays the prevalence of cybercrime victimisation by regions drawn on Kaakinen et al.'s (2018) comparative study. The study utilised online questionnaires and recruited youth and young adults aged 15-30 years old from the US (n = 1,033) and Finland (n = 555) in spring 2013, and the UK (n = 999) and Germany (n = 978) in spring 2014. Cybercrime victimisation was measured for the past 3 years. Two subcategories of cybercrime victimisation were recorded: offensive cybercrime and cyber-fraud. Offensive cybercrime included defamation, illegal threat, and sexual harassment while the cyber-fraud included identity theft and online fraud. The table shows offensive cybercrime was more prevalent than cyber-fraud across countries. Comparable types of victimisations were identity theft and online fraud, for which the prevalence rates were about five times and nearly two times greater (respectively) in Taiwan than for these four countries. This suggests that cybercrime victimisation is more prevalent in Taiwan than that in a western context.

Table 3.3 Prevalence rates of cybercrime victimisation (%) by countries drawn on Kaakinen et al.'s (2018) study

Type of victimisation	All countries	US	UK	Germany	Finland
Victim of cybercrime	6.42	6.10	7.41	6.03	5.95
Victim of offensive cybercrime	4.26	4.36	4.80	4.09	3.42
Defamation	2.61	2.90	2.50	2.76	1.98
Illegal threat	2.19	1.65	2.70	2.35	1.98
Sexual harassment	1.09	1.26	1.00	1.02	1.08
Victim of cyber-fraud	2.92	2.52	2.80	3.27	3.24
Identity theft	1.49	1.65	1.60	1.12	1.62
Fraud	1.77	1.16	1.60	2.35	2.16
Sample size	3,565	1,033	999	978	555

Source: Kaakinen et al. (2018)

3.2.3 General limitations of Taiwanese datasets used in this thesis

The limitations for the selected Taiwanese data sets used here are the same as the general limitations of using police recorded crime data and victim surveys. In addition, there are further limitations concerning the lack of input by the researcher into the design of the questionnaire. Using secondary data can present more difficulties in analyses than using primary data since researchers are unable to tailor the questions of interest by themselves (Jones, 2010). The variables provided in the secondary dataset are often not well defined in terms of the researchers' interests. For example, some responses may be collected in categories when the researchers need them to be exact figures, as is the case with cybercrime victimisation on the DOSIH.

To summarise, Taiwanese police data is limited in providing profiles of victims/targets, either in terms of burgled house or specific cybercrime. Furthermore, limitations of the TAVS are that: (a) the low frequency and limited access to surveys have an effect on the capacity of crime research; (b) the capping convention at six may underestimate the concentration of crime in Taiwan; and (c) there is no measures of cybercrime victimisation. Otherwise, the DOSIH, as an alternative data source of cybercrime victimisation, has three limitations noteworthy: (a) no entry of multiple experiences of cybercrime victimisations that limits an examination into the concentration of cybercrime over population and further patterns of repeat cybercrime victimisation; (b) an inappropriate question measuring victimisation that might bias the prevalence of identity theft; and (c) absence in measures with regard to cyber lifestyle and security. The main reason for raising aforementioned limitations is that the DOSIH is not originally designed for cybercrime victimisation. Therefore, some important items related to cyber security are absent from the questionnaire. Examples of key concepts are like items to measure individuals' time spent online or the presence of (updated) security software, which are not included in the DOSIH. More limitations about the police data, TAVS and DOSIH will be addressed in the following empirical chapters.

3.3 Summary of chapter

This chapter introduces the data sources used in this thesis. It acknowledges the strengths and weaknesses of both official crime data and victim surveys. On the one hand, official data has strengths in measuring longitudinal patterns and trends in well-reported crime and containing geographic information that can be used for local crime pattern analysis. Its weaknesses lie in the fact that the statistics are dependent on victims' reporting behaviours and the recording practices of the CJS and particularly the police. On the other hand, victim surveys provide a more complete estimate of crime and risk, overcoming the issues of unreported and unrecorded crime. They are also a valid and reliable measure that can be used to understand the causes and impact of crime. However, the reliability of victim surveys might be influenced by issues such as self-selected samples, recall bias, over-reporting or under-reporting of victimisation, or adjustment issues with social desirability. Each measure of crime has its strengths and limitations; and therefore the utilisation of both measures would provide a better estimate of crime patterns. This thesis would use both police recorded data and victim surveys.

Chapter 4 A Multilevel Assessment of Domestic Burglary Victimisation in Taiwan

This chapter presents the first empirical study of this thesis. It aims to answer the research question presented in Chapter 2 (Section 2.4), namely: Does a lifestyle-routine activity approach adequately explain burglary victimisation patterns observed in Taiwan, as measured by the TAVS? As mentioned previously, the LRAA has been applied extensively to examine victimisation patterns in various industrialised contexts, yet it is less evident whether the same approach is applicable to an Asian context, specifically burglary in Taiwan. Consequently, this study is the first in the criminological literature to use multilevel modelling to better understand if the LRAA applies to burglary victimisation patterns in Taiwan.

4.1 Background

As outlined in Chapter 2, the RAA suggests that the convergence of motivated offenders, suitable targets, and the absence of capable guardians constitutes a crime event (Cohen & Felson, 1979; Felson & Cohen, 2011). With the inclusion of a lifestyle-exposure perspective, the LRAA proposed by Cohen et al. (1981) is increasingly used by researchers to explain criminal victimisation patterns. According to the LRAA, an individual's risk of victimisation is related to his/her daily routine activities that comprise his/her lifestyle. The attractiveness of potential targets, absence of guardianship, exposure to risk, proximity to potential offenders, and the specific properties featured by specific crimes[1] are the five elements deemed crucial for

[1] Specific crimes feature specific instrumental actions (or say lifestyle-routines and knowledge) by potential offenders. For example, burglaries may require offenders' more awareness of victims' routine activities (e.g. about if the dwelling is occupied) and commands

explaining opportunities for crime (Cohen et al., 1981). The first four elements of the LRAA model provide opportunities for crime to occur, whilst the last element relates to variations in opportunity for different types of crime (also see Section 2.1.4).

Drawing on the LRAA, the following sections present what is known from previous (mainly Western) research about the patterns of residential burglary victimisation. This research literature is important because it acts as a guide for the variables used in the analysis reported in this chapter. This is followed by a summary of relevant Asian research (also see Section 2.2.1.2) before the presentation of the results of the multilevel analysis. The literature review provided below builds on that presented in Chapter 2.

4.1.1 Residential burglary victimisation from the perspective of lifestyle-routine activity approach

Several studies have examined patterns of residential burglary from a LRAA. This line of research has identified multiple factors associated with differing risk of victimisation. Table 4.1 summarises the key risk factors identified in previous research as they relate to both the household (i.e. the property itself) and neighbourhood level (i.e. the wider environment in which the property is located). These factors can be categorised according to three main theoretical concepts which lie at the heart of the LRAA – target attractiveness/suitability, guardianship and proximity/exposure to crime and disorder. Discussing each concept (and the associated research) in turn.

of techniques (e.g. ways to break in a dwelling), than that required by general larcenies. Also see Section 2.1.4.

Table 4.1 Lifestyle-routine factors related to burglary victimisation at household (HH) and neighbourhood (NB) levels

Concepts	Dimensions	Level	Related factors	Explanation & references	Relationship with burglary
Target attractiveness/ suitability	Attractiveness: the perceived rewards on offending	HH*	HH income	HHs with higher incomes would tend to live in more expensive properties in affluent areas and, crucially, be in possession of more expensive (attractive) items (Cohen et al., 1981)	Positive
			Availability of expensive items in a property	Such dwellings would have higher perceived rewards so that they may experience higher risk of burglary (Miethe & McDowall, 1993; Miethe & Meier, 1990)	Positive
			Layout of a dwelling	Living in a detached house might suggest the privileged economic status of inhabitants, though there was mixed evidence being found (Bowers et al., 2005)	Mixed
	Accessibility: the ease of entry and physical visibility	HH	Fences	Fences can be both a barrier to access the property and an obstacle obscuring dwellings from public view, and thus hindering the intervention of potential guardians (Hope, 1984)	Mixed
		HH	Permeability of dwelling	Mixed findings partly because of its interaction with physical visibility: a) dwellings on more accessible street segments (e.g. those located on major roads and connected street segments) suffered a higher risk of burglary than those on cul-de-sacs because they might be more visible and accessible to burglars (Johnson & Bowers, 2010); b) dwellings on cul-de-sacs suffered a greater risk of burglary than those on major roads because the former dwellings were less guarded by the public (Hillier, 2004)	Mixed
		HH	Types of dwellings	• The ground-floor units of a building suffered a higher risk of burglary because they were easier to be accessed by burglar (Robinson & Robinson, 1997); so as terraced houses and flats on the second floor and above were less likely to be burgled than detached or semi-detached houses (Ellingworth et al., 1995; Osborn & Tseloni, 1998) • Mixed finings observed in detached houses: a) having more entry points on the ground floor would attract more burglaries (Miethe & Meier, 1990); b) detached houses suffered the least burglary risk, compared to flats and semi-detached properties, when controlling dwellings' environmental factors (i.e. economic conditions by area) (Bowers et al., 2005)	Mixed

(Continued)

Table 4.1 *(Continued)*

Concepts	Dimensions	Level	Related factors	Explanation & references	Relationship with burglary
Guardianship [§]	Physical guardianship: self-protection measures	HH	Security measures against burglary (e.g. burglary alarm, locks, etc.)	HHs with security measures, considered as being guarded, would be less likely to experience burglary (see e.g. Budd, 2001; Miethe & McDowall, 1993; Miethe & Meier, 1990)	Negative
	Social guardianship	HH	House occupancy	A house without occupancy may lack guardianship and experience a higher risk of burglary than those being occupied. a) Residents' employment status: those at work or in education leave houses empty for several hours a day, and the time of leaving and returning home is quite predictable to potential offenders (Miethe et al., 1987); b) HH composition: houses are more likely to be occupied when the HH is composed of two or more adults. These houses were found to have a reduced risk of being burgled (Osborn & Tseloni, 1998).	Negative
		NB	NB watch schemes	When the dwelling is unoccupied, NB watch schemes would act as a guardianship against burglary. Hence, HHs with NB watch schemes were found to experience a reduced risk of burglary (Bennett et al., 2007; Hunter & Tseloni, 2016).	Negative
		NB	Population density	An indirect measurement of social guardianship. A high population density implies more potential guardians in presence, and thus HHs located in highly populated NBs would experience a lower risk of burglary (Battin & Crowl, 2017; Hipp & Roussell, 2013).	Negative

(Continued)

Table 4.1 *(Continued)*

Concepts	Dimensions	Level	Related factors	Explanation & references	Relationship with burglary
(Guardianship)	(Social guardianship)	NB	Informal social control (i.e. the extent to which the community intervenes in neighbourhood problem solving) drawn from social disorganisation theory (SDT)	These include several neighbourhood characteristics that influence the level of collective efficacy within a community and further to informal social control within that community to combat crime (Kubrin & Wo, 2016; R. J. Sampson et al., 1997; R. J. Sampson & Wikström, 2008). a) Objective and quantifiable qualities: e.g. poverty, population heterogeneity, or residential instability. For example, capable guardianship is less likely to be found in disadvantaged areas in which communities' access to public resources is generally more limited. Such resources refer to sources of informal social control and collective efficacy (i.e., sources of informal social control) $^{+}$. That is to say, in deprived, mix-resident, and resident-unstable environments (in)formal social control is typically in short supply, resulting in weakened controls against crime, including burglaries (Wilcox et al., 2007) b) Perceptual qualities: 1) signs of social disorder (e.g. graffiti, drug deals, peer gangs hanging out, decayed facilities, loitering, street prostitution, etc.): more signs are related to a weakened level of informal social control and to a higher level of crime risk within a community (R. J. Sampson & Raudenbush, 1999); 2) Organisational participation (e.g., items asking to what extent did the residents socialise with each other, feel belong to the neighbourhoods, or was willing to solve the problem within the neighbourhoods): the higher organisational participation within a community the higher level of informal social control; 3)social interaction and informal network (e.g. friendship and kinship ties within the community): the closer connection between residents a community has, a higher level of informal social control it has and the lower level of crime risk within the community (R. J. Sampson et al., 1997); 4)collective efficacy (i.e. a community's ability to maintain public order) (Cantillon et al., 2003; R. J. Sampson & Groves, 1989)	Mixed

(Continued)

Table 4.1 *(Continued)*

Concepts	Dimensions	Level	Related factors	Explanation & references	Relationship with burglary
Proximity/exposure to crime/disorder	Objective & quantifiable qualities	NB	e.g. neighbourhood crime rates, area unemployment rates, etc.	Studies have supported that offenders' journey to crime is often short (Rossmo, 1999; Townsley & Sidebottom, 2010). As a result of their routine activities, offenders are more likely to commit crimes in areas that they are familiar with (P. L. Brantingham & Brantingham, 1993; Eck, 1993). The cost of travel and offenders' familiarity and awareness of opportunities to succeed within those areas plays a role in attracting offenses, thus explaining why exposure and proximity to crime/disorder has an environmental implication of crime. Specifically in terms of burglary, offenders' familiarity was proved a significant predictor of offenders' location selection (Frith et al., 2017). Evidence otherwise suggested that neighbourhoods might suffer higher burglary rates if located close to affluent potential offenders (Mawby, 2001).	Positive
	Perceptual qualities	NB	e.g. signs of social disorder, individuals' perception of risks, etc.	Signs of disorder as a proximity/exposure element may overlap with the aforementioned SDT (R. J. Sampson & Raudenbush, 1999; Skogan, 2012) concept. Nevertheless, signs of disorder as a proximity/exposure element can also be drawn upon the "broken windows" theory (Kelling, 1997; Kelling & Coles, 1997) arguing that visual evidence of "incivilities" (or say anti-social behaviours) such as public gambling, drinking, or drug sales, etc. give potential offenders an impression of misbehaviour tolerance within the neighbourhoods and thus attract predatory crime (R. J. Sampson & Raudenbush, 1999). This perspective echoes the concept of proximity/exposure to crime embedded in LRAA.	Mixed

Note. [*]Target attractiveness is suggested to be related to both the perceived appearance of a property and an interaction between the property and wider environmental factors. Affluent properties located in poorer areas are shown to be at especially high risks of being burgled compared to affluent and poorer houses in affluent areas (Bowers et al., 2005). [§] Physical and social guardianship are classified according to Tseloni et al.'s (2004)[+] SDT causal model of crime would be like this: neighbourhood characteristics → collective efficacy → informal social control → crime (see e.g. Kubrin & Wo, 2016; R. J. Sampson et al., 1997; R. J. Sampson & Wikström, 2008)

4.1.1.1 Target suitability (attractiveness and accessibility) in the context of burglary

From the perspective of the LRAA, a property can be thought of as a burglary target. Previous research has therefore considered properties with regard to target suitability in two dimensions – attractiveness and accessibility (see Table 4.1).

Two aspects of attractiveness (i.e. household income and perceived availability of valuable goods inside the property) have been found to be positively related to burglary risk. (Cohen et al., 1981; Miethe & Meier, 1990), while mixed evidence has been found on the impact of dwelling type on burglary victimisation. For example, Miethe and Meier (1990) found that detached houses attract more burglaries while Bowers et al (2005) suggested that detached houses exhibit the least burglary risk, compared to flats and semi-detached properties, when economic conditions in dwellings' surroundings were controlled (see Table 4.1).

Likewise, accessibility has been shown to have an inconsistent relationship with burglary risk. Some studies have suggested that dwellings on more accessible street segments (e.g. those located on major roads and connected street segments) suffer a higher risk of burglary than those located on cul-de-sacs because, all things being equal, they are more visible and accessible to burglars (Johnson & Bowers, 2010). By contrast, other scholars have argued that dwellings located on cul-de-sacs suffer a *greater* risk of burglary victimisation because they are less guarded by the public (Hillier, 2004). It is also noted that target attractiveness can be related to the perceived appearance of a property and its interaction with the neighbourhood in which it is located. For example, using data from Merseyside (UK), the aforementioned Bowers et al.'s (2005) research found that detached houses located in poorer areas[2]

[2] There were 118 wards in Merseyside which were categorised into five levels of deprived/affluent areas using the ward-level *Index of Multiple Deprivation 2000.*

were shown to be at especially high risks of being burgled compared to detached houses located in more affluent areas (Bowers et al., 2005).

4.1.1.2 Guardianship in the context of burglary

The second class of factors found to be related to burglary victimisation is guardianship, which can be referred as both physical and social guardianship (see Section 2.1.1.2). Physical guardianship in the context of burglary mainly comprises self-protection measures (e.g. burglar alarm, locks, etc.) which affect the ease and risk with which an offender can gain access to a property (Tseloni et al., 2004)[3]. Factors related to social guardianship may range from signs of occupancy at the household level to levels of informal social control, drawing from SDT[4] at the neighbourhood level (see Table 4.1).

Briefly speaking of SDT, informal social control and collective efficacy are two key concepts at the heart of this popular criminological theory. Informal social control refers to the extent to which a community intervenes in resolving neighbourhood problems. Collective efficacy refers to a community's ability to maintain public order (R. J. Sampson et al., 1997). Put simply, a SDT causal model of crime looks like this: disorganised neighbourhood → weak collective efficacy → weak informal social control → more crime (Kubrin & Wo, 2016; R. J. Sampson et al., 1997; R. J. Sampson & Wikström, 2008). According to this model, in a socially disorganised neighbourhood where informal social control and collective efficacy is weak, residents are more isolated from one another and their social institutions. Neighbours are thus less likely to provide supervision over and intervene in forms of delinquency carried out within their neighbourhood

[3] Note that Tseloni et al. (2004) included participation in collective crime prevention enterprises such as neighbourhood watch programme might be confusing with social guardianship.

[4] Three elements – solidarity, cohesion, and integration – are considered essential in a socially organised neighbourhood. Residents within these neighbourhoods share similar perspectives about norms and values, have strong connections and established networks between each other (Kubrin & Wo, 2016). Conversely, these three elements are less likely to be observed in a socially disorganised neighbourhood. As a result, informal social control is weak in such neighbourhoods (C. R. Shaw & McKay, 1942).

(Cantillon et al., 2003). As potential guardians/controllers are less able to function in their neighbourhood, crime is considered more likely to occur. Examples of key SDT studies are referred to in Table 4.1 (see also R. Bursik, 1988; Jobes et al., 2004; R. J. Sampson & Raudenbush, 1999; C. R. Shaw & McKay, 1942).

The purpose of mentioning SDT here is to highlight how the presence and capability of potential guardians – a key feature of the LRAA model – is also influenced by neighbourhood level factors. However, one thing to note is that despite the impact of social disorganisation on crime, to date SDT research has mainly centred on violent crime and using data from the US. Further, among those few burglary-related studies which draw on SDT, inconsistent results emerge. For instance, a study using three waves of BCS data found that neighbourhood cohesion exerted an indirect effect on social disorder and burglary (Markowitz et al., 2001). Other early research indicated an effect on robbery rather than on burglary or homicide (R. J. Sampson & Raudenbush, 1999). Clearly, the effect of social (dis)organisation on burglary (in a relation to the presence of guardians in an area) requires more empirical attention.

4.1.1.3 Exposure/proximity to crime or disorder in the context of burglary

The third factor related to burglary victimisation is exposure and proximity to crime or disorder. Connections between disorder and crime draw from many theoretical perspectives, including: (a) "broken windows" theory (Kelling, 1997; Kelling & Coles, 1997), arguing that visual evidence of "incivilities" (or say anti-social behaviours) such as public gambling, drinking, or drug sales, etc. gives potential offenders an impression of misbehaviour tolerance within the neighbourhoods and thus attracts predatory crime (R. J. Sampson & Raudenbush, 1999); (b) SDT: disorder weakens neighbourhood stability, informal social control, and enhances fear of crime (Skogan, 2012); and (c) crime pattern theory: since motivated offenders will select targets in close proximity to their residences, closer proximity to motivated offenders will increase residents' likelihood of being victimised. Evidence suggests that neighbourhoods might suffer higher burglary rates if located close to more potential offenders (Mawby, 2001), about whom extensive evidence shows mostly undertaken journeys to crime are short (Rossmo, 1999; Townsley & Sidebottom, 2010). As a result of their routine activities, offenders are hence more likely to commit crimes in areas that they are familiar with (P. L. Brantingham & Brantingham, 1993; Eck, 1993).

It is noteworthy that most routine activity perspective-driven research applies indirect measures to examine the effects of proximity to crime. Such measures include objective measures such as neighbourhood crime rates and area unemployment rates as well as more subjective measures such as signs of social disorder and individuals' perception of risks (see Table 4.1).

As indicated above, Table 4.1 provides a summary of the research associated with those factors implicated in burglary victimisation, organised according to the key elements of the LRAA. However, it should be noted that these categories are not independent. Some factors linked to burglary risk relate to several theoretical concepts. An example might be the type of a dwelling, say a detached house. A property being detached may be considered as both an attractive burglary target (i.e. privileged economic status of house owners perceived by burglars) and an accessible burglary target (i.e. more entry points compared to, say, a top floor apartment). Likewise, signs of social disorder in a given area might indicate not only signs of less guardians but also provide evidence that there are more potential offenders operating within a neighbourhood. Table 4.1 is therefore intended to summarise the main findings regarding burglary risk factors using a LRAA framework, and should not be taken as a strict classification of the concepts.

We turn now to burglary research in an Asian context, and in particular the limitations with the existing research, some of which are addressed in this chapter.

4.1.2 Issues with burglary research in Asia

As described in Chapter 2, there is presently a small body of research on burglary in Asia using an opportunity perspective (recall the summary of key studies presented in Table 2.2). Focussing on Taiwan in particular, Wang (2015), using data from the 2010 TAVS, found through logistic regression analysis that properties that were detached, located on the ground floor, and in a socially disorganised area suffered higher risks of burglary. The analyses further suggested that individual security measures were associated with a reduced risk of burglary victimisation. Those security measures included security guards, burglar alarms, security bars on windows, the presence of dogs, light sensors, and the use of a police-connected security system[5] (H. C. Wang, 2015). Another study from Taiwan, using a sequential negative binomial regression with the same data produced a slightly different picture. It suggested that whilst security guards significantly lowered a dwelling's burglary risk, light sensors significantly *increased* the risk of burglary victimisation (S.-Y. Kuo, 2015).

In addition to the use of different analytical techniques, the mixed findings described above may be a consequence of using only single-level analyses rather than multilevel analyses, meaning that neither Wang's (2015) nor Kuo's (2015) study accounted for possible environmental/neighbourhood-level influences on burglary patterns in Taiwan. To be more specific, in Wang's (2015) study the measurement of social disorganisation related to individual household's responses toward questions about teenagers hanging around on the street, social disorder caused by recreational facilities, and violence in the community. However, considering that individuals' responses are not in fact independent and might be influenced by the community where

[5] Police-connected security system is a security system in which the installed burglar alarms are connected to the local police stations. Once an alarm is triggered, the station will receive a report of burglary immediately. However, the system is operated by a third-party security company rather than the police authority.

they live[6], this individual-level measurement may not fully (or accurately) capture social disorganisation at a community level. Ignoring the issue of nesting and non-independence might lead to a biased estimation of predictors' effects (Aarts et al., 2014). Therefore, a more appropriate approach is to aggregate those responses at a neighbourhood level. I will expand on this in the analysis section (Section 4.3.3.3).

Only a few Asian studies have examined multilevel factors of burglary risk. To my best knowledge, one is conducted in South Korea (Roh et al., 2010) and the other in China (L. Zhang et al., 2007). Both studies have found some individual- and neighbourhood-level characteristics consistent with theoretical expectations and consistent with what is routinely observed in Western societies. The characteristics include target attractiveness (e.g. household income), guardianship (e.g. occupancy at an individual level and collective efficacy and public control at a neighbourhood level) and community disorder (see Table 2.2).

Of those multilevel studies which have taken place in Asia, inconsistencies with Western research findings are also identified. For instance, in the South Korean study, the presence of household security measures[7] and community cohesion (relevant to the aforementioned SDT concepts) *enhanced* the risk of burglary and robbery (Roh et al., 2010). Likewise, Zhang et al.'s (2007) study also found that residential stability was *positively* related to burglary victimisation, which conflicts with the SDT literature (Wilcox et al., 2007).

Conflicting findings on SDT may be attributed to differences in measurement or cultural and contextual differences across studies (L. Zhang et al., 2007). However, an *increased* risk of burglary observed in Korean dwellings with security measures did not indeed conflict with all Western research findings. In a recent study, Tilley et al. (2015) also found a positive

[6] Those who live in a community tend to act more similarly than those who live elsewhere. More detail will be provided in the Method section.

[7] Roh et al.'s (2010) study conceptualised target hardening efforts as security measures implemented in residence, including an intrusion detection sensor, CCTV, a door video phone, and a burglar alarm.

association between the presence of burglar alarms and the risk of burglary when using multiple sweeps of the CSEW. Beyond coding and respondents' error, they proposed several possible explanations for this positive (and to some extent counter-intuitive) relationship: (1) *adaptive offenders* who learned how to avoid or distinguish the effective alarm system; (2) *flags for target suitability* in which burglar alarms informed burglars of valuable items in presence; (3) *drowned out effects* in which (false) alarms became so prevalent that its function of attention decayed and (4) *heterogeneity in systems and effects* (or say some alarms systems may be less effective than others). Lastly, they noted that the CSEW does not provide information about the quality or the actual functioning of an alarm system. The difficulties in controlling for the quality and functioning of an alarm system meant that such findings of ineffectiveness against burglary need to be taken with caution (Tilley et al., 2015).

In addition to the explanations offered by Tilley et al. (2015), *when* the security features were installed is a key consideration about their effectiveness against burglary. The aforementioned studies in Taiwan (S.-Y. Kuo, 2015; H. C. Wang, 2015), South Korea (Roh et al., 2010), and China (e.g. L. Zhang et al., 2007) did not give clear information about the time point of household security implementation. If the security measures were installed *after* residents' experiences of burglary, then a positive association is expected to be observed between those burgled and the number of security measures since burgled households would somehow take protections against future victimisation. Few Asian studies are able to distinguish between the time-ordering of security and victimisation.

The differential measurement of security devices, inconsistent conclusions, and problems with analytical methods raise questions about whether it is appropriate to apply Western research findings to a non-Western context such as Taiwan. Moreover, the noted shortage of multilevel studies makes it difficult to reliably examine the differences across contexts and to determine the extent to which observed patterns relate to household or neighbourhood level variables, and interactions between the two. This lack of research in Asia is to some extent understandable because such research often requires a large data sample in order to provide enough aggregated (higher-level) units beyond individuals in order to allow for multivariate statistical analysis. A lack of studies in Asia thus likely reflects the lack of suitable data, a point touched upon in Chapter 1 (see page 28-29). However, as mentioned previously in this thesis, the logic behind situational crime prevention is very crime specific (Section 2.2.3). Without the decent understanding of the specific contexts in which crime takes place, it is difficult to plot an effective prevention scheme. For these reasons, the current study targets Taiwan as a non-western context to revisit opportunity-based theories into burglary victimisation, drawing on a large nationally representative dataset.

4.2 The current study

The LRAA framework has gathered much research attention in the process of better understanding the risk of burglary victimisation. This framework considers the effect of target attractiveness/suitability, guardianship and exposure/proximity to potential offenders (see Table 4.1). Taken together, this framework emphasises the role of opportunity in crime and argues that the opportunity structure should be examined separately for different types of crime. Moreover, given that opportunity changes by environment, this framework brings out the need to understand risk factors of victimisation at not only a household level but also at an environmental/neighbourhood level, as well as explore interactions between the two.

Unfortunately, it is difficult to identify many Asian studies – especially in the context of Taiwan – applying this perspective to understand crime patterns. If we focus on the specific crime of burglary, the crime of interest in this chapter, the limited studies from Asia to date cannot provide consistent evidence to support whether what has been found in the Western literature is generalisable to the distinct (and different) settings of Asia. The most controversial inconsistency lies in the (in)effectiveness of household security measures (e.g. S.-Y. Kuo, 2015; Roh et al., 2010; H.C. Wang, 2015), and, as discussed above, this inconsistently may be attributed, in part, to the researchers' failure to record a household's timepoint for installing security measures. Research evidence relating to SDT in Asia, in which informal social control might be related to the concept of guardianship, has also produced conflicts with what is typically reported in the Western literature, most notably with respect to the effect of residential stability (L. Zhang et al., 2007) and community cohesion (Roh et al., 2010) on burglary risk.

Given the aforementioned sparsity of Asian victimisation research, this study aims to better understand burglary victimisation patterns in Taiwan, using a multilevel lifestyle-routine approach. As mentioned in Chapter 2 (Section 2.4), the research question for this study is "*Does a lifestyle-routine activity approach adequately explain burglary victimisation patterns in Taiwan?*" In response to the research question and inconsistent findings in previous Asian studies, a series of hypotheses will be examined here, the outcome of which will collectively help assess the applicability of an opportunity-based model (namely attractiveness of potential targets, guardianship and exposure/proximity to potential offenders) in the Taiwanese context.

Informed by relevant theory and previous research, below are the hypotheses to be tested in this study:

- H1.a: Households with less security measures are more likely to be burgled.

The first hypothesis is derived from the inconsistent findings on the effectiveness of security measures against burglary in Asia. Fortunately, the 2015 TAVS, which will be used in the following analyses, contained information on the installation of household security measures, specifically whether they were put in place before or after a burglary event, thereby overcoming the abovementioned time-ordering problem that affects many previous Asian studies. As a result, it is assumed in this study that if security measures are in place before a burglary incident, they will likely have a preventive function and be associated with lower risks of burglary. It is also assumed that more security measures will work more effectively, as has been found in previous research from the UK (see Tseloni et al., 2017).

- H1.b: Households without dogs are more likely to be burgled.

Another security measure considered here relates to the presence of dogs. This study is one of the first to empirically examine the effect of dogs on risk of burglary victimisation. Clearly the effectiveness of a dog against burglary may vary by types of dogs. A Chihuahua, the smallest breed of dog, is likely to be less aggressive or threatening to a potential burglar compared to a larger bread such as a Pit Bull. Regrettably, however, the data used here did not contain information on the breed or number of dog(s) in sampled households. Hence, the dog-security hypothesis tested here follows the conventional direction of security measures, in which dogs are considered to serve a preventive function against burglary. Simply put, it is predicted that the presence of a dog will be associated with lower risks of burglary as their presence is assumed to deter potential offenders by increasing the perceived risk of injury.

- H1.c: Households without security bars on windows are more likely to be burgled.

Findings on the effectiveness of individual security measures are inconsistent in Taiwanese studies (S.-Y. Kuo, 2015; H. C. Wang, 2015). Among those security measures considered, security bars on windows (or some called iron-barred windows) are quite prevalent in Taiwan yet remain neglected in previous Taiwanese research. This study thus examines the effect of iron-barred windows on burglary risk. It assumes that houses with barred windows will suffer a lower risk of burglary, since the presence of bars will, all things being equal, increase the effort involved in an offender gaining access to the property and/or increase the risk that an offender might be spotted trying to gain illegal access to said property.

In addition to the abovementioned role of individual household security measures, and inspired by the opportunity framework and SDT (using Table 4.1 as a reference), this study also investigates the effect of *target,* *guardianship, exposure/proximity,* and *social disorganisation* on burglary victimisation. The following hypotheses relate to these elements:

- H2.a: More attractive households, measured here as household income, are more likely to be burgled.

A positive relationship between household income and its burglary victimisation is suggested by both the western and Asian literature (see both Table 2.2 and Table 4.1). The rationale is that households with higher incomes would tend to live in more expensive properties in affluent areas and, crucially, be in possession of more expensive (attractive) items. The current study follows this statement and assumes a positive relationship between household income and burglary victimisation.

- H2.b: More accessible households, measured here as the presence of conspicuous security measures, the awareness of police anti-burglary consultancy and easy entry, are more likely to be burgled[8].

Likewise, studies have suggested that the accessibility of households relates to their burglary victimisation (Robinson & Robinson, 1997), though variations in measuring accessibility are observed (see Table 4.1). This study assumes that houses with accessibility will reduce the effort involved in an offender gaining access to the property and/or reduce the risk that an offender might be spotted trying to gain illegal access to said property. All things being equal, those properties will suffer a higher risk of burglary. The measures of accessibility will be detailed later in Section 4.3.2.

- H3: Households with fewer guardians present are more likely to be burgled.

As mentioned, guardianship is a key concept underpinning the LRAA. The study assumes that households with fewer guardians in place will reduce the risk that offenders might be detected when they try to gain illegal access to

[8] Conspicuous security measures in this thesis refer to two security measures (i.e. security door chains and iron-barred windows) that hinder potential offenders' access to a dwelling. Also, I would discuss how I measured household attractiveness and accessibility in the Data section (Section 4.3.2).

said property. All things being equal, households with fewer guardians will be more likely to be burgled.

- H4: Households with greater exposure and proximity to crime/potential offenders are more likely to be burgled.

Offenders' familiarity has been found a significant predictor of offenders' location selection (Frith et al., 2017). Evidence otherwise has suggested that neighbourhoods might suffer higher burglary rates if located close to a greater number of motivated offenders (Mawby, 2001). This study thus assumes that households with greater exposure and proximity to crime/potential offenders are more likely to be burgled. Again, measures of exposure and proximity will be detailed later in Section 4.3.2.

- H5: Households located in 'socially disorganised' neighbourhoods are more likely to be burgled.

Guardianships, or say (in)formal social control, are typically weak in a 'socially disorganised' neighbourhood (see Table 4.1). All things being equal, households located in such neighbourhoods are less likely to have guardians nearby. This study thus assumes that households located in 'socially disorganised' neighbourhoods are more likely to be burgled. Measures of 'socially disorganised' neighbourhoods will also be covered in Section 4.3.2.

4.3 Data and Method

The following sections describe the data, variables and analytical strategies used in this study. I then explain why this study uses a reduced sample of TAVS data in order to avoid biases and the drawing of incorrect statistical inferences.

4.3.1 Data

This study used data collected as part of the 2015 TAVS. The details of the data were given in Chapter 3 (see Section 3.2.2.1). To reiterate, unlike most Western countries which carry out a national crime victimisation survey on a frequent (typically annual) basis (say like England and Wales, US), Taiwan conducts its victim survey every five years. Hence, the 2015 version is the most recently available data at the time of writing.

The 2015 TAVS used stratified random sampling, with the assistance of CATI. Participants (n = 13,016) were nested in 20 out of the 22 cities/counties and 350 districts that make up parts of Taiwan. All registered citizens aged 12 or older were eligible for inclusion. Participants were asked about the experience of eight types of criminal victimisation in the previous year (1 January to 31 December 2014): residential burglary, motorcycle theft, car theft, fraud, robbery, forceful taking, injury, and general larceny.

This study is concerned only with residential burglary, and so used the following question as the dependent variable: "*In the past year, did anyone steal belongings from your residence (including residential and office mixed-use buildings)?*"[9]. One hundred and ninety-four respondents indicated that they had been the victim of burglary over the past year, accounting for 1.49% of surveyed households. For the purposes of comparison, over the same time period 2.29% of respondents in the CSEW reported experiencing burglary in the past year (see Table 3.1).

4.3.2 Variables

Table 4.2 describes the variables used in this study and their expected relationship with burglary victimisation in Taiwan, informed by relevant theory and research. Put simply, the variables used here exist at two levels – household-level variables and community/neighbourhood-level variables.

[9] It is noted that this question did not specify illegal entry as an important component of burglary from a legal standpoint. By virtue of the wording, the responses might include cases where "larceny-theft" victims were victimised by offenders who were legally allowed or invited into a residence. However, this description is in line with the police statistics, of which burglary is specified as one form of "larceny" taking place in a "residence", regardless of (il)legal entry.

Table 4.2 Framework of independent variables used in burglary research in Taiwan

Aspects	Variables	Measures/items	Expected relationship with burglary victimisation
Household-level variables			
Target attractiveness	Family income (ordinal)	*"What is your family income per month?"* (11-item ordinal scale ranging from less than NT$20,000 to 120,000 or more; NT$1 ≈ £GBP 0.025)	The higher the family income is, the more likely the house would be burgled (Cohen et al., 1981) (also see Table 4.1).
Accessibility	Conspicuous security measures (1= yes = security door chain or iron-barred window)	*"During 2014, did your residence take any security measures [before burglary]?"*	The dwellings with conspicuous security measures would be less likely to be accessed, and thus less likely to experience burglary (Miethe & Meier, 1990).
	Awareness of anti-burglary consultancy (1=yes)	*"Are you aware of the following crime prevention measures [anti-burglary consultants] conducted by the police?"*	• Anti-burglary consultancy is a special service provided by Taiwan police, in which security surveys of individual properties are conducted to help residents detect potential vulnerabilities in their houses and surroundings in terms of burglary. • Those householders who were aware of this service were therefore assumed to have had their house strengthened in response to the advice of the police, and hence be less suitable targets for burglary and thus less likely to fall prey to burglars. • Note: this variable might not truly reflect the protective level of a dwelling since the question asked the participants if they were '*aware of*' this police service rather than if they actually used it or acted in accordance with police advice. Individuals' awareness might not accurately represent their application of anti-burglary measures.
	Easy access (1= yes = detached, 2nd floor and below§)	*"What is your house type (and at which floor is it located)?"*	The easier the dwellings can be accessed, the higher risk of burglary victimisation they would experience (Miethe & Meier, 1990).
Guardianship	Number of security measures (ordinal)	*"During 2014, did your residence take any security measures [before burglary]?"* (Security measures include: dogs, CCTV cameras, light sensors, door/window, anti-theft alarms, police connection security system, private security guards, timers)	• Given that research suggested that combined security devices worked better than a specific individual one (Tseloni et al., 2017), security measures were coded into integers (i.e. the number of security measures). The more security measures a dwelling had, the less likely it would be burgled. • Note: The rationale behind this coding was to verify if more security measures function better against burglary as the opportunity-based theory predicts rather than identifying the most effective measure.

(Continued)

Table 4.2 *(Continued)*

Aspects	Variables	Measures/items	Expected relationship with burglary victimisation
(Guardianship)	Daytime Occupancy (1 = yes)	Occupation: housewife/househusband or unemployed	• Daytime occupancy was coded according to participants' employment status (see e.g. Miethe et al., 1987). A dwelling with daytime occupancy were expected to experience a lower level of burglary risk. • Note: (un)employment does not exactly confirm whether guardianship was actually present at the time of the incident. A better measure of guardianship would be more like "*Were you or any other member of this household present when this incident occurred?*" (see Hollis et al., 2013). However, survey responses regarding occupiers' presence were only available for those burgled, which does not provide enough information to distinguish occupancy patterns between victims and non-victims.
	Night-time occupancy (1 =yes)	*"How often do you go out at night in a typical week?"*	Participants who went out at night less than twice in a typical week were believed to be more likely to guard their dwellings at night, and their dwellings were thus less likely to experience burglary.
	Lone guardian (1 = yes)	*"How many family members (including yourself) aged 12 years old live together? _______ people"*	A household with merely one adult was regarded as lone-guardian since the resident was less likely to provide control function over the property for longer periods of time, and thus the household would be expected to experience a higher level of burglary risk.
	Number of male adults (ordinal)	*"How many male family members (including yourself) aged 18 years old live together? ______male."*	Male adults often exert more protective power against burglary (Sidebottom, 2013). The number of male adults in a household was included under the concept of guardianship to examine whether it was negatively associated with burglary victimisation.
	Family size (ordinal)	*"How many family members (including yourself) aged 12 years old live together? _______ people"*	More occupiers were assumed to provide stronger guardianship as a function of higher chance of occupancy, and thus a dwelling with a bigger family size would be expected to experience a lower level of burglary risk (see Miethe et al., 1990).

(Continued)

Table 4.2 *(Continued)*

Theoretical concept	Variables	Measures/items	Expected relationship with burglary victimisation
Community-level variables (aggregated and divided by the number of households per district)			
Guardianship	Population density by district (person/10,000km^2)	Alternatively utilising Taiwan official data in 2014 (Department of Household Registration, M.O.I., 2020) instead of TAVS	In a more crowded district, it is more likely that a house will be under the surveillance of neighbours (i.e. potential guardians) even though the occupiers are absent (Battin & Crowl, 2017; Hipp & Roussell, 2013). A dwelling located within a higher populated district would hence be less likely to be burgled.
	Proportion of volunteer patrol team by district	*"Is there any volunteer community patrol team in your residential area?"* (Responses as "yes" were coded as 1 and aggregated to a district level)	• Volunteer community patrol team was termed as a "Civil Patrol Team" by Martin (2011). This institution consists of neighbourhood members on a voluntary basis and is partially sponsored by the local police authority. It could be understood as some neighbourhood watch-alike programmes in the West. • Dwellings located in neighbourhoods with a higher level of volunteer patrolling would have a higher level of social guardianship in presence , and thus experience a lower level of burglary risk.
	Neighbourhood poverty: proportion of poor households per district*	The number of poor households was divided by the number of total households per district. The number of poor households was retrieved from the Ministry of Health and Welfare (Department of Statistics, 2017) while the number of total households per district was retrieved from the Department of Household Registration (Department of Household Registration, M.O.I., 2020). Both represented conditions in the corresponding survey year of 2015 TAVS, say 2014.	• Three explanations for the link between neighbourhood poverty and crime: a) poverty generates greater incentives for individuals to commit crimes for economic benefits. Neighbourhood poverty may be signs of more motivated offenders in a community; b) community poverty may indicate an environment where informal social controls are weakened and thus there is a general failure to intervene in antisocial and criminal behaviours in public space (R. J. Sampson et al., 2002); c) neighbourhood poverty is a sign of homogeneity of poorly secured properties in neighbourhoods and a situational factor related to the greater vulnerability of victims (e.g. deficiencies in security measures) (Sharkey et al., 2017). • This thesis initially regarded neighbourhood poverty as signs of deficiencies in security measures and weakened social guardianship within neighbourhoods. It was thus conceptualised as a guardianship-related variable. Dwellings located in neighbourhoods with a higher level of poverty would experience a higher level of burglary risk. • Further, this variable was included to examine if there was an interaction between target attractiveness (i.e. family income) and surroundings (Bowers et al., 2005). In line with the literature, this thesis expected a similar interaction in which affluent properties located in poorer areas would have a higher risk of being burgled than poorer houses in affluent areas in Taiwan.

(Continued)

Table 4.2 *(Continued)*

Theoretical concept	Variables	Measures/items	Expected relationship with burglary victimisation
(Guardianship)	Residential stability: mean of years living in the residence by district*	*"How many years have you been living in this property?"* (Ordinal responses were recoded into their mean of years (i.e. 1, 2, 4, 7.5, 15, 20 years) and aggregated to a district level)	A district with a greater number represented a higher level of stability. A dwelling located in such a district was expected to suffer a lower risk of burglary victimisation (Markowitz et al., 2001).
	Proportion of neighbourhood problem solving by district*	*"If the problems mentioned above [juvenile hanging around on the street, violent crime such as fight and brawls, social disorder caused by places of entertainment such as internet café, pool, or karaoke room] occurs near your residential area, will you or your neighbours go approaching?"* (Responses as "often" and "sometimes" to deal with neighbourhood problems were coded as 1 and aggregated to a district level)	Neighbourhoods with a higher level of problem-solving would have a higher level of collective efficacy (or say neighbourhood cohesion), within which neighbourhood the dwellings would experience a lower level of burglary risk (R. J. Bursik, 2000; R. J. Sampson & Raudenbush, 1999).
	Trust in police: proportion of trust in the police by district*	*"Does the local police enforce the law fairly?"; "Does the local police respect citizens?"; "Does the local police have a good communication with citizens?"* (Responses as "strongly agree" or" slightly agree" to either two of these three questions were marked as showing trust toward police and aggregated to a district level)	• As a confounding factor in predicting burglary victimisation based on two reasons: a) police function is tied up with social control of deviance within a community (Bradford & Jackson, 2016). b) extensive research, although slightly inconsistent about its effect power, has found a relationship between public trust in the police and public willingness to cooperate with officers to combat crime (Bradford & Jackson, 2010; Reisig et al., 2012; Sunshine & Tyler, 2003; Tankebe, 2013; Tyler & Fagan, 2008). Missing the role of police in the community may overestimate the effect of social cohesion or collective efficacy on burglary victimisation. • Note: unlike research in a western context on measures of public confidence in the police (Jackson & Bradford, 2010), this construct has not been standardised in the Taiwanese literature. To avoid confusion, I used "trust" rather than a more comprehensive concept of "confidence". Further, considering that those questions

(Continued)

Table 4.2 *(Continued)*

Theoretical concept	Variables	Measures/items	Expected relationship with burglary victimisation
(Guardianship)	(Trust in police)		allowed blank responses such as “refuse to answer” and “no comment”, it is not appropriate to either neutralise “disagree” with “agree” responses or to use single confidence measure. Items were not weighted because little research can be borrowed from such operation. The weighted operation required further literature.
	Area type: urban (1=yes)*	*“Where do you live? ___City/County; ___District”* (According to (Fu, 2015) 7-level stratification of urbanisation in Taiwan, dwellings located at the two most urbanised levels were recoded as being located in urban areas)	Neighbourhoods situated in an urban setting demonstrated lower levels of collective efficacy and informal social control) (Twigg et al., 2010), and thus dwellings located in urbanised neighbourhoods would be expected to experience a higher level of burglary risk (Markowitz et al., 2001).
Exposure/proximity to crime	District burglary rates	The number of burgled dwellings was divided by the number of total households per district	Neighbourhoods with higher burglary rates suggested more exposure to an environment with a pool of potential offenders, within which neighbourhood dwellings would be expected to have a higher risk of burglary.
	Proportion of neighbourhood disorder by district	*“Within 200 metres from your residence: a) How serious is the problem of juvenile hanging around? b) How serious is violent crime such as fight and brawls? c) How serious is the social disorder caused by recreation such as internet café, pool, karaoke room?”* (Neighbourhood disorder was coded as 1 when at least one of three problems sometimes/often occurred nearby. Neighbourhood disorder referred to an aggregated count of neighbourhood disorder divided by the number of participants by district)	The higher proportion implied a higher possibility of contacts between residents and potential offenders, thereby a higher risk of burglary victimisation.

(Continued)

Table 4.2 *(Continued)*

Theoretical concept	Variables	Measures/items	Expected relationship with burglary victimisation
(Exposure/proximity to crime)	Proportion of young people by district	The number of respondents aged 35s and younger was divided by the number of households per district	• The choice of 35 as a reference line was based on research suggesting that the age of offending for property crime peaks in the 30s and then tails off in Taiwan (Steffensmeier et al., 2017). • A higher proportion implied a higher possibility of contacts between residents and potential offenders and thus a higher risk of burglary victimisation within that district.
	Proportion of public security dissatisfaction by district	*"Are you satisfied with the public security near your residential area?"* (Responses as "dissatisfied" and "very dissatisfied" were coded as 1 and aggregated to a district level)	A higher proportion implied a higher level of exposure/proximity to crime/disorder and thus a higher risk of burglary victimisation within that district (for logic see e.g. Markowitz et al., 2001).
	Proportion of fear of crime by district	*"Generally speaking, are you worried about being a victim of crime?"* (Responses as "very worried" and "somewhat worried" were coded as 1 and aggregated to a district level)	A higher proportion implied a higher level of exposure/proximity to crime/disorder and thus a higher risk of burglary victimisation within that district (for logic see e.g. Markowitz et al., 2001).
	Proportion of drug exposure by district	*"Did you have any following experience [witnessing or having actual contact with new drug (ketamine, FM2, Nimetazepam/Erimine, laughing gas, etc.)] during the past year?"* (Positive responses were coded as 1 and aggregated to a district level)	The higher proportion implied a higher possibility of contacts between residents and potential offenders and a thus higher risk of burglary victimisation.

Note. * Variables drawn upon SDT. § 2nd floor in Taiwan refers to 1st floor in the UK.

An opportunity framework argues that households with greater security will, all things being equal, experience lower levels of residential burglary. This was examined here using ten household-level variables that speak to issues of target suitability and levels of guardianship: family income, conspicuous security measures (defined in this study as iron-barred windows and door chains that block burglars from entering the dwelling), awareness of anti-burglary consultants, easier entry (defined in this study as lower-level dwellings and detached houses with more entry points on the ground), the number of security measures, daytime occupancy, night-time occupancy, lone guardian, number of male adults and family size (see Table 4.2).

As mentioned previously, there is sparse research on burglary in Asia which has examined empirically the role of community-level variables. Multilevel analysis is rare. To complement the flaw of merely examining social disorganisation at the individual level mentioned above (H. C. Wang, 2015), the current study examined the effect of environmental factors on household burglary risk and aggregated relevant variables at a district-level (see Table 4.2). In this sense, the neighbourhood, community, area and environmental level may be used interchangeably to describe level-two variables in this chapter. Community-level variables were composed of two aspects – guardianship and exposure/proximity to crime, with seven and six variables underpinning them respectively. Briefly, the community-level guardianship aspect included population density and volunteer patrol team and other variables drawn upon SDT: neighbourhood poverty, residential stability, neighbourhood problem-solving, trust in police and area type. The exposure/proximity aspect contained variables related to district burglary rates, neighbourhood disorder, young population, public dissatisfaction toward security, fear of crime, and drug exposure. Their explanations and expected relationships with burglary victimisation were also given in Table 4.2.

4.3.3 Analytical strategy

There were three sets of analytical strategies used in this study. A Chi-square analysis and a latent class analysis were applied to preliminarily examine hypothesis 1 concerned with the effectiveness of individual security measures. A more sophisticated approach (i.e. multilevel logistic regression) was then used to test the remaining hypotheses.

4.3.3.1 Chi-square analysis

The Chi-square analysis was first used to provide evidence relating to hypothesis 1. In a situation where variables are categorical (in the case of the first hypothesis, say, the application of security measures and burglary victimisation), it is meaningless to compare means or similar statistics because they are not measured continuously. The researcher should compare the observed frequencies in certain categories with the frequencies that would be expected on the basis of chance (Field, 2009). In this situation, the Pearson's chi-square test was utilised.

Despite a Chi-square analysis being appropriate for analysing categorical variables, one drawback is that it fails to control for other confounding factors. This approach could give researchers a basic idea about the relationship between certain variables, but one should bear in mind that the result needs to be taken with caution. Otherwise, the examination of security measures as a whole (the number of security measures) can be examined in a more sophisticated method, such as multilevel logistic regression (as detailed in later Section 4.3.3.3).

4.3.3.2 Latent Class Analysis

To identify unobserved constructs underlying observed responses, factor analysis is the most popular analytical technique. However, a factor analysis is designed for use on continuous data and usually normally distributed latent variables. In the case of binary or categorical variables, problems might occur regardless of the transformation of variables. Alternatively, latent class analysis (LCA) has gradually been used to cluster or construct typologies (Denson & Ing, 2014; Vermunt, 2003). That is, LCA permits researchers to classify latent variables and improve the analysis value of the class variables. Briefly, by maximising the between-cluster differences and minimising the within-cluster differences, LCA classifies observed variables into latent variables. By allowing several statistical models to be compared and the residuals between items to be examined statistically, LCA can improve the analysis value of the class variables and helps researchers to adopt a model (Schreiber, 2017). In this way, the latent impact factors of the class variables can be retrieved through probability (Liu et al., 2017).

A simple example using LCA is: presuming that we had three questions asking people if they like alcohol, fizzy drinks, and bubble tea, we may end up identifying a few groups. These groups may be people who like them all ('unhealthy drinker'), people who like them none ('healthy drinker'), people who like merely fizzy drinks and bubble tea ('sweet tooth drinker'), and people who like merely alcohol ('boozer'), and so on. Or we may just find the first two groups covering everyone in the survey. This is the time that LCA can help us *statistically* decide how many groups to be used in our model.

LCA was used here in the classification of security measures among households against burglary. That is, security measures applied in households were analysed to fit a latent class model, ending up with three unobserved security behaviour classes. After running LCA, the observed values could be assigned to the appropriate latent classes. The posterior classification properties of the observed value would enable me to analyse the relationship between clustered classes of security measures and burglary victimisation, with further application of simple logistic regression.

4.3.3.3 (Multilevel) Logistic Regression

A simple logistic regression was used to verify the effect of security measures on burglary, with posterior classification derived from LCA. However, to understand whether security measures have an impact on preventing burglary, the aforementioned approaches might be inaccurate as there are likely to be interactions between household opportunities for crime and neighbourhood-level effects (R. J. Sampson & Wooldredge, 1987). A multilevel approach, including both individual- and neighbourhood-level variables, is often used to estimate the effect of environmental variables (e.g. Miethe & McDowall, 1993; Rountree et al., 1994; Sampson & Wooldredge, 1987; Tseloni, 2006; Wilcox et al., 2007). Hence, a multilevel approach was used in this study, as a complement to hypothesis 1 and more importantly, other hypotheses about lifestyle-routines and SDT. Besides, as my data contained a dichotomous response toward burglary victimisation and large-scale participants, the multilevel logistic model (MLM) is more appropriate than a simple logistic regression since the former MLM allows for the identification of risk factors among certain areas/environments. That is to say, failing to distinguish the features of particular areas that are associated with a greater risk of burglary may risk missing the mechanism(s) behind victimisation patterns, resulting in a bias for verifying the hypotheses about the lifestyle-routine framework and SDT.

Another reason to run a multilevel model instead of a standard logistic regression is because the nested data structure violates the assumption of independence of the residuals in the linear model (Sommet & Davide, 2017). Nested data refers to data that is organised at hierarchical or multiple levels such as various neuron samples collected from one animal. In the social science field, students grouped into classes, and further in schools is a typical example of nested structure. In the 2015 TAVS, the households were sampled based on a stratified random selection, in which districts and cities were used as stratification. This meant not only that the district where the respondents lived might be influential, but that individuals' responses should not be considered as independent. That is, participants nested in the same cluster (i.e. district) tend to respond in a more similar way than those nested in different clusters. Ignoring this dependency will result in an incorrect estimation of predictors' effects, especially their statistical significance or say an inflated type I error rate (Aarts et al., 2014).

The original TAVS data consisted of 13,016 participants nested in 350 districts; however, the analysis reported here used a reduced sample to avoid concerns of biases and incorrect statistical inferences. Concerns and reasons for this approach are discussed shortly in the following section (i.e. Section 4.3.4). Put simply, with a reduced sample of 6,158 participants (level-one units) nested in 121 clusters (level-two units), the multilevel modelling can extricate within-cluster effects (the extent to which some household characteristics are associated with the odds of burglary victimisation) from the between-cluster effects (the extent to which some district characteristics are associated with the odds of burglary victimisation). In this sense, this study used a multilevel logistic regression to analyse patterns of burglary victimisation in Taiwan.

Statistical analysis reported in this chapter followed the steps proposed by Sommet and Morselli (2017). First, an intercept-only (unconditional) model with no predictor variables was performed (model 1)[10]. This model indicates whether there is any variation in the risk of residential burglary between clusters (i.e. Taiwanese districts). Second, the ten household-level variables were added to explain variations in burglary risk (model 2). Third, community-level variables were added to assess the influence of district-aggregated characteristics on burglary risk. To construct this model, two intermediate models were built. First was the constrained intermediate model (CIM) which contained all household-level variables, all community-level variables, and possibly all intra-level interactions if needed. CIM is used to estimate the unexplained variation of lower-level (i.e. household-level) effects. The CIM equation is shown below:

[10] Equation: $Y_i = B_{00} +_{0j}$

$$Y_i = B_{00} + B_{10} \times X_{ij} + B_{01} \times X_j + U_{0j} \tag{4.1}$$

where B_{10} is the fixed slope of X_{ij} (the overall effect of household-level variables) and B_{01} is the (necessarily fixed) slope of X_j (the overall effect of district-level variables).

Then the augmented intermediate model (AIM), with each lower-level variable was built respectively to compare with the CIM. The AIM includes the residual term associated with the relevant level-one variable, allowing estimating the random slope variance. The random slope variance refers to the extent of the variation of the effect of the lower-level variable from one cluster to another (i.e. the extent of the variation in household-level variables from one district to another). The AIM equation is shown below:

$$Y_i = B_{00} + (B_{10} + U_{ij}) \times X_{ij} + B_{01} \times X_j + U_{0j} \tag{4.2}$$

where U_{ij} is the deviation of the cluster-specific slope (i.e. the specific effect of a household-level variable on burglary victimisation within a given district) from the fixed slope (i.e. the average effect of household-level variables regardless of districts).

A likelihood-ratio (LR) test was then performed to determine whether considering the cluster-based variation of the effect of the household-level variables improves the model. The LR test formula is as below:

$$LR\ \mathcal{X}^2\ (1) = deviance\ (CIM) - deviance\ (AIM) \tag{4.3}$$

where deviance (CIM) is the deviance of the constrained intermediate model, whereas deviance (AIM) is the deviance of the augmented intermediate model.

“(1)” corresponds to the number of degrees of freedom. The deviance is a quality-of-(mis)fit index: the smaller the deviance, the better the fit. Since the model has ten household-level variables, the test needed to be performed ten times in total. The LR tests showed that the AIM was not significantly different from the CIM. Hence, this study presented only the CIM, representing a random intercept model including fixed effects of individual-level and district/city-level variables varying within groups.

Logically, the cross-level interactions will be added into the final model since Sommet and Morselli (2017) suggest that a non-significant LR test does not stop one from testing cross-level interactions. In a sense that the combination of environments and target attractiveness along with security measures (e.g. CCTV, burglar alarm) might produce different scenarios of crime prevention effectiveness (Tilley et al., 2015; Welsh & Farrington, 2009), some cross-level interactions between security measures and family income and proportion of poor household per district were tested to better understand the application of hypotheses about lifestyle-routines and SDT. With cross-level interactions included, the possible final model will be like:

$$Y_i = B_{00} + (B_{10} + U_{ij}) \times X_{ij} + B_{01} \times X_j + B_{11} \times X_{ij} \times X_j + U_{0j} \tag{4.4}$$

where B_{11} is the coefficient estimate associated with the cross-level interaction. Six sets of cross-level interactions were tested, including the interactions between (conspicuous) security measures and neighbourhood poverty, (conspicuous) security measures and burglary rates by district and family income and neighbourhood poverty. Table 4.3 displays the model statistics. The statistics show that all those cross-level interactions were not significant, and nor models with cross-level interactions were found significant to improve the models. Therefore, the individual cross-level interactions were not presented in the result section.

Table 4.3 Model statistics for null, single-level and fully specified multilevel logistic regression models and models with cross-level interactions for burglary victimisation in Taiwan, 2015 TAVS

	Null	Single level	Multilevel	Cross-level interactions				
	(Model 1)	(Model 2)	(Model 3)	ConSM x BurgRate	ConSM x NeibPov	SM x BurgRate	SM x NeibPov	FamiIn x NeibPov
Log-lik.	-741.52	-722.93	-674.01	-673.67	-673.68	-673.95	-673.97	-673.11
AIC	1487.04	1469.85	1398.02	1399.34	1399.36	1399.90	1399.94	1398.22
BIC	1500.50	1550.56	1566.16	1574.20	1574.22	1574.76	1574.81	1573.08
LRT (df)		37.19(10)	97.83(13)	0.68(1)	0.66(1)	0.12(1)	0.08(1)	1.80(1)
P-value		*p* < .001	*p* < .001	*p* = .4087	*p* = .4164	*p* = .7253	*p* = .7833	*p* = .1799

Note 1. n = 6,158. Group n = 121. 2. LRT = Likelihood (lik.) ratio test; df = Degree of freedom; ConSM = Conspicuous security measures; BurgRate = Burglary rates by district; NeibPov = proportion of poor households by district; SM = Number of security measures; FamiIn = family income

All regressions were performed in Stata version 15.0, using the “xtmelogit” command for MLM. Multicollinearity was checked using the “collin” package, in which a mean variance inflation factor (VIF) of 1.41 and a maximum of 2.63 (area type urban variable) less than five revealed little concerns of multicollinearity (Akinwande et al., 2015).

4.3.4 Sample size issue in multilevel logistic models

As mentioned, the 2015 TAVS originally recruited 13,016 level-one participants (i.e. households) within 350 level-two clusters (districts). In multilevel models, the number of groups (i.e., higher-level units) is more important than the number of individuals per group (Maas & Hox, 2004; Swaminathan et al., 2011). A small sample size of 50 or less at level two might result in greater biased standard errors than a group size of, say, five. Further, the fixed effect parameters are suggested to have less and negligible biases than the random intercept and random slope (Maas & Hox, 2004; Moineddin et al., 2007). Since the fixed effect parameters (i.e. CIM) rather than the variance components were used in the analysis, ten groups are enough for good estimates (Hox, 2002; Maas & Hox, 2004). Hence, the sample size of 350 at level two in the model is not very susceptible to bias and can give correct estimates of the standard errors according to Maas and Hox (2004)’s rule of thumb.

In addition to Maas & Hox’s (2004) rule of thumb, Moineddin et al. (2007) suggested a minimum of 50 at both group size and group number for a proper multilevel logistic regression model when the prevalent events are low. Low prevalence requires a larger group size. Although the outcome prevalence at the district-level was not very low (227 out of 350 i.e. 64.86%), concerns were raised about the zero-cell problem. Generally speaking, the number of outcomes in each group should be greater than one and the number of individuals per group ideally larger than five (inclusive). A zero-cell problem occurs when violating this principle, resulting in biases and incorrect statistical inferences (Moineddin et al., 2007). Moreover, when this minimum requirement is not met, the random slope and intraclass variation should be avoided to MLM procedures.

To avoid zero-cell concerns, the MLM analyses conducted here deleted districts with no burglary experience and a group size of less than five. That is to say, the presented MLM consisted of merely 6,158 households nested in 121 districts rather than the original 13,016 households in 350 districts. I acknowledge that this is a large loss of data. However, such an approach was judged critical to reduce the risk of biases and incorrect statistical inferences, of which the risk arose particularly in districts that contained merely one participant.

4.4 Results

Table 4.4 displays descriptive statistics for the reduced data sample used in this chapter (individual-level n = 6,158; community-level n = 121). According to Table 4.4, less than three percent of households reported being burgled in the past year[11]. The average district burglary rate was two percent. One thing to note is that public trust in the police appeared to be relatively high. The mean proportion of self-reported trust in police by district was around 84%, for which the standard deviation of 0.05 revealed little differences across districts. Neighbourhood problem solving inclination showed a similar pattern. These figures suggest that informal social control, as measured herein, is relatively strong among Taiwanese society.

The following results are presented by hypothesis. The first three hypotheses are related to household security measures and thus are grouped together. Others are presented separately.

[11] To recap, there were 194 participants reported being burgled (1.49%) out of the original sample of 13,016 participants.

Table 4.4 Descriptive statistics of burglary victimisation variables in Taiwan, 2015 TAVS

Variables		Obs.	%	Mean	SD	Min	Max
Dependent Variable							
Burglary victimisation (1 = yes)		160	2.60				
Household level variables							
Target attractiveness	Family income: household monthly income			4.28	2.28	1.00	11.00
Accessibility	Conspicuous security measures (1= some)	4,738	76.94				
	Awareness of anti-burglary consultancy (1=yes)	1,066	17.31				
	Easy access (1= yes=detached, 2nd floor and below)	1,173	19.05				
Guardianship*	Number of security measures			1.23	1.32	0.00	7.00
	Daytime occupancy (1 = yes)	3,114	50.57				
	Night-time occupancy (1 =yes)	4,626	75.12				
	Lone guardian (1 = yes)	544	8.83				
	Number of male adults			1.71	0.99	0.00	9.00
	Family size			3.68	1.61	1.00	15.00

(continued)

Table 4.4 *(continued)*

Variables		Obs.	%	Mean	SD	Min	Max
Community-level variables							
Guardianship	Population density (person/10,000km^2)			1.00	0.95	0.00	3.98
	Proportion of volunteer patrol team by dist.			0.52	0.16	0.00	1.00
	Proportion of poor households per dist.			0.13	0.10	0.00	1.00
	Mean of years living in the residence by dist.			14.94	1.08	12.78	20.00
	Proportion of neighbourhood problem solving by dist.			0.74	0.06	0.40	1.00
	Proportion of trust in the police by dist.			0.84	0.05	0.60	1.00
	Urban (1=yes)	3,205	52.05				
Proximity to crime	District burglary rates			0.02	0.02	0.00	0.25
	Proportion of neighbourhood disorder by dist.			0.18	0.06	0.00	0.60
	Proportion of young people by dist.			0.32	0.07	0.08	0.68
	Proportion of public security dissatisfaction by dist.			0.10	0.04	0.00	0.29
	Proportion of fear of crime by dist.			0.67	0.06	0.33	0.90
	Proportion of drug exposure by dist.			0.01	0.01	0.00	0.09

Note. 1. Individual-level n = 6,158. Community-level n = 121 (mean = 50.89, SD = 47.50, min = 5, max = 240). 2. Obs. = observed frequency; dist. = district. 3. * Dogs as a guardian was counted as one of the security measures because the analyses were based on different sizes of sample. The descriptive statistics of each security measures can be found in Figure 4.1.

4.4.1 The effectiveness of security measures

H1.a: Households with less security measures are more likely to be burgled.

H1.b: Households without dogs are more likely to be burgled.

H1.c: Households without security bars on windows are more likely to be burgled.

As mentioned previously, unlike many other victimisation surveys carried out in Asia, the design of the TAVS allowed me to distinguish if the security measures were applied before or after a house was burgled. For those households that suffered a burglary, they were asked if specific security measures were installed before and after the incident. This is of benefit to evaluating the effectiveness of security measures and solving the issue in previous Asian research failing to differentiate the timepoints of security installations.

Table 4.5 shows the associations between specific security measures and burglary using Chi-square analyses. The analyses did not exclude households with multiple security measures and thus the results should be taken conservatively. The figures presented in parentheses represent the ratio of observed frequencies divided by the expected frequencies of burglary victimisation. The more the ratio deviates from one, the more the observed frequency differs from the expected frequency. Hence, without controlling for other variables, several security measures were found significantly related to burglary victimisation. Households with dog(s), for example, suffered significantly *more* burglaries than one would expect to observe if they occurred by chance (ratio = 1.26, $p < .05$).

Table 4.5 Association between security and burglary victimisation in Taiwan, 2015 TAVS

Security measures	Burgled (ratio)	χ2	Φ
Dog*	57 (1.26)	3.92	0.02
Light sensor**	13 (0.54)	5.86	-0.02
Door/window burglar alarm**	13 (0.52)	6.67	-0.02
Police connection system**	6 (0.29)	11.72	-0.03
Private security guard**	10 (0.26)	27.22	-0.05
Timer**	2 (0.13)	12.58	-0.03
Iron-barred window	131 (0.93)	2.28	-0.01
Door chain	36 (0.86)	1.14	-0.01
CCTV	53 (0.81)	3.84	-0.02

Note 1. n = 13,016. 2. *significantly higher than the expected, ** significantly lower than the expected, df = 1, $p < .05$. 3. (ratio) = Observed / Expected, the more it deviates from one, the more different. 4. Normally Cramer's V (Φ) wouldn't be negative. The results retrieved via Stata were given as a sign of the direction of the association. 5. Cells in which houses with a timer and being bulged were less than five so a Fisher's exact test was run instead.

Household security measures found to be associated with a reduced risk of burglary in Taiwan were light sensors, burglar alarms, police connection systems, private security guards, and timers. Within these measures, private security guards and timers seemed to function best against burglary victimisation, as shown by the lowest ratios in column two of Table 4.5. That is to say, when considering security measures alone, the likelihood that households with security guards being burgled were much lower than one can expect if burglary occurs by chance alone (ratio = 0.26, $p < .05$). Among those effective anti-burglary measures, timers showed the greatest deviation from one, over 80% lower than the expected (ratio = 0.13, $p < .05$). The effect of security bars on windows, the focus of H1.c, was small and not statistically significant. To this point, without controlling for other factors, security bars on windows seemed to be unrelated to burglary victimisation. This is noteworthy given that iron-barred windows are ubiquitous in Taiwan. To illustrate, see Figure 4.1 which shows the high prevalence (over 70%) of iron-barred windows installed in Taiwanese houses[12], compared to other security measures. Meanwhile, Figure 4.1 also reveals that the aforementioned most effective measure – timers – was the least used.

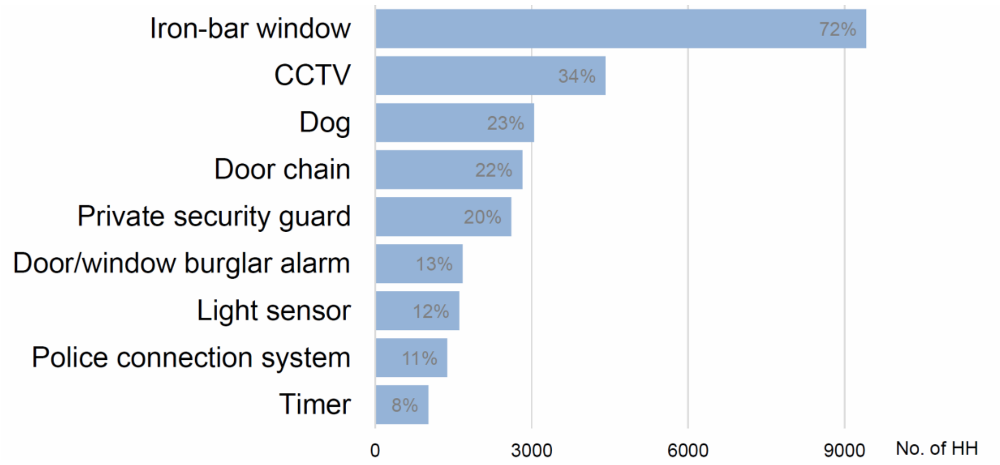


Figure 4.1 Percentage of security measures installed per household in Taiwan, 2015 TAVS. n= 13,016. No. of HH = number of households

The results presented in Table 4.5 are suggestive without being conclusive that security bars on windows had little effect and that security guards worked best against burglary victimisation. However, within-participant effects and collinearity should be taken into consideration. That is, although the survey was neither a repeated measure design nor longitudinal data, a more rigorous approach should be taken, considering that those security measures examined here were not mutually exclusive. A logistic regression would be a better option than the Chi-square analysis as the former allows all security measures to be entered at the same time. However, within-participant effects generate concerns about running a simple logistic regression. That is, as mentioned above, observations are nested in participants as some combination of security measures were more likely to happen and these may due to some specific participants. Thus, participants should be treated as higher-level units.

[12] Here the denominator included both burgled and non-burgled houses. Security measures among burgled households measured security measures installed before a burglary event while those among the non-burgled did not specify such a differential time point.

In doing so, a multilevel logistic regression is better able to disentangle possible within-participant effects from between-participant effects. Moreover, as research suggested, a cluster-mean centring of the level-one predictors was applied to estimate the pooled fixed effects within participants (Enders & Tofighi, 2007). However, after doing so, I found serious collinearity between all security measures existing in the model.

Table 4.6 Individual security measures predicting odds of residential burglary victimisation in Taiwan, 2015 TAVS

Security measures	OR(SE)	95% CI	
Dog	3.07 (1.01) **	1.61	5.86
Light sensor	4.10 (3.14)	0.91	18.41
Police connection system	3.45 (3.63)	0.44	27.18
CCTV	2.22 (1.00)	0.91	5.37
Door/window burglar alarm	1.77 (1.84)	0.23	13.63
Iron-barred window	1.21 (0.33)	0.71	2.07
Door chain	0.99 (1.03)	0.13	7.55
Private security guard	-	-	-
Timer	-	-	-
Intercept	0.02 (0.00) ***	0.01	0.02

Note 1. n = 5,097. 2. LR/Wald Chi2 = 16.42. 3. OR = Odds ratio; CI = Confidence interval, ** *p* < .01, *** *p* < .001. 4. 106 cases of burglary occurred. 5. Private security guard and timer were omitted because of the blank cell problem.

With such a limitation, I used a simple logistic regression as an alternative. To avoid the dependency effects within participants, households with multiple security measures were dropped. This left a sample of 5,097 households relating to 106 burglary events (around 55% of the original 194 events). Table 4.6 shows the effects of individual security measures on residential burglary victimisation. Among households applying a single security measure, no security measures were found to be significant negative predictors. This suggests that a single security measure was not effective against burglary on its own. Among those security measures, it is interesting that the presence of dogs might significantly increase the risk of burglary (OR

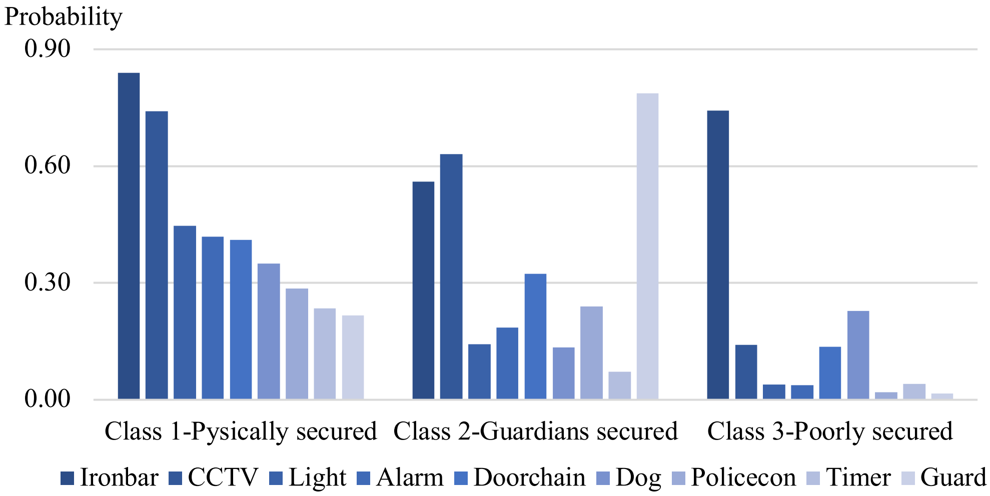
= 3.07, *p* < .01). Households with a dog suffered a higher risk of being burgled – over two times higher than those without a dog, all things being equal. However, the results of model should be interpreted with caution. Two points need to be mentioned. First, private security guards and timers were omitted because of the empty cell problem. Second, a significant postestimation of specification errors was found through the Box-Tidwell test (*p* = .02), implying that further transformation of variables is required.

In response to the aforementioned concerns, a simple solution was to cluster security measures and to examine the clustered effectiveness of security measures on preventing burglary victimisation. Table 4.7 and Figure 4.2 show the classification of household tendency of security measures, using LCA. When house types and family income were controlled, there were 15, 19, and 65 percent of the sampled households being predicted to be in class 1, class 2, and class 3, respectively (see Table 4.7). This suggests that poorly secured households (class 3) were quite common in Taiwan, compared to physically secured and guardians secured households.

Table 4.7 Estimated mean for each security measures in each class controlling house types and income, 2015 TAVS

	Class 1- Physically secured	Class 2- Guardians Secured	Class 3- Poorly secured
Pr (Class)	0.15	0.19	0.65
Probability of			
Iron-barred windows	0.84	0.56	0.74
CCTV	0.74	0.63	0.14
Light sensor	0.45	0.14	0.04
Alarm	0.42	0.18	0.04
Door chain	0.41	0.32	0.14
Dog	0.35	0.13	0.23
Police connection system	0.29	0.24	0.02
Timer	0.24	0.07	0.04
Security guard	0.22	0.79	0.02

Note. 1. n = 13,016. 2. Pr (Class) = Expected proportions of the population in each class. 3. AIC = 76812.076, BIC = 77051.083.



Source: 2015 TAVS

Figure 4.2 Probability for individual security measure by class, 2015 TAVS

Judging by the probabilities of applying certain security measures (see Table 4.7), class 2 showed a great tendency of applying social guardianship-related elements as protection, since the marginal probability of using security guards in the households was relatively high (probability = 0.79). Table 4.7 also shows that respondents in class 2 were less likely to have physical measures like light sensors (probability = 0.14) or alarms (probability = 0.18) in the house. Class 1 in Table 4.7 demonstrates the preference for physical protection such as CCTV (probability = 0.74), iron-barred windows (probability = 0.84), etc. A low probability of having security guards (probability = 0.22) was predicted while that of other physical measures was either high or moderate. Households aligned in Class 3 are shown to be the least secured in terms of the marginal probability of using security measures, except for iron-barred windows (probability = 0.74, also see Figure 4.2).

Table 4.8 reveals the relationship between aligned classification and burglary victimisation. It suggests that poor security was a significant predictor of burglary victimisation. For a poorly secured household the likelihood of being burgled was almost three times that of a socially guarded household. When compared to guardian-secured houses, households with a high probability of physical security measures did not differ significantly in the risk of burglary victimisation. These findings support the hypothesis that houses with less security measures (here referred to as poorly secured households) are more likely to be burgled (H1.a). Moreover, it was found that iron-barred windows alone might not be sufficient to prevent burglary as the poorly secured households were found very likely to have iron-barred windows installed (probability = 0.74), such is their ubiquity in Taiwan (H1.c).

Table 4.8 Security classification predicting burglary victimisation in Taiwan, 2015 TAVS

Predicated class	Odds Ratio	95% CI	
Intercept	0.01(0.00)***	0.00	0.01
Guardians secured (baseline)	-	-	-
Poorly secured	2.52(0.70)***	1.46	4.36
Physically secured	1.15(0.47)	0.52	2.55

Note. 1. n = 13,016. 2. LR/Wald Chi^2 = 19.94. 3. CI = Confidence interval; *** *p* < .001.

Overall, although a Chi-square analysis showed that some security measures might be related to a lower burglary risk (Table 4.5), the results should be taken with caution since this analysis failed to avoid collinearity among security measures, or to control for other individual or community-level factors. The analysis with least collinearity concerns, namely the results found in households with just one security measure in place, suggested that a single security measure was not effective in preventing burglary. Except for the case of dogs (for which a significant and positive relationship was found), the relationship between households with only one security measure and burglary victimisation did not reach significance (see Table 4.6). Additionally, LCA and the following logistic regression analysis found that some level of security measures could prevent burglary victimisation, with poor security shown to be a significant predictor of burglary victimisation. However, the findings also suggest that iron-barred windows alone were found to not be associated with reduced burglary risk, and households with dogs surprisingly suffered a higher risk of burglary than those without. In sum, the current findings partially support H1.a and fail to support H1.b and H1.c. Testing for the effectiveness of multiple security measures requires more complex approaches, which is undertaken in the examination of the remaining hypotheses.

4.4.2 Multilevel logistic regression of burglary victimisation

The analyses above provide basic descriptions of security measures against burglary victimisation. A comprehensive understanding of patterns and predictors of burglary victimisation requires a more sophisticated analysis such as MLM, for the reasons already given. In consideration of the zero-cell problems, a reduced sample was used for the multilevel analysis.

Table 4.9 presents the models in which districts failing to meet the minimum requirement of at least one burglary event, and a group size of five, were dropped (n = 6,158). Although there seemed no differential effects of such revision on variables, I present the revised model to avoid a possible zero-problem concern.

Model 1 included only the outcome variable (i.e. burglary victimisation) while Model 2 included level-one (i.e. individual-level) variables. Based on Model 2, Model 3 also examined community-level variables. Additional models with cross-level interactions were intended to better understand cross-level interactions between some variables such as family income and neighbourhood poverty. However, as given earlier in Table 4.3, none of these interactions improved the specification of models predicting burglary victimisation in Taiwan. Table 4.3 suggests little cross-level interactions between household (conspicuous) security measures, income, and district burglary rates and neighbourhood poverty.

The test of the remaining hypotheses (H2-5) is presented below.

Table 4.9 MLM predicting odds of residential burglary victimisation in Taiwan, 2015 TAVS

Variable	**Model 1**			**Model 2**			**Model 3 (CIM)**		
	α (SE)	**95% CI**		**α (SE)**	**95% CI**		**α (SE)**	**95% CI**	
Intercept	0.03 (0.00)***	0.02	0.03	0.03(0.01)***	0.02	0.05	0.00(0.01)**	0.00	0.23
Household Variables									
Family income ǂ				1.06(0.04)	0.99	1.14	1.07(0.04)	0.99	1.15
Conspicuous security measures (1=yes)				0.68(0.12)*	0.48	0.97	0.77(0.14)	0.53	1.10
Awareness of anti-burglary consultancy (1=yes)				0.95(0.21)	0.62	1.46	1.00(0.22)	0.64	1.54
Easier entry (1=yes=detached, 2nd floor and below)				1.74(0.32)**	1.22	2.48	1.53(0.29)*	1.06	2.21
Number of security measure ǂ				0.77(0.06)***	0.66	0.89	0.74(0.06)***	0.63	0.86
Daytime occupancy (1=yes)				0.66(0.11)*	0.48	0.92	0.60(0.10)**	0.43	0.84
Night-time occupancy (1=yes)				1.14(0.22)	0.78	1.66	1.04(0.20)	0.71	1.53
Lone guardian (1=yes)				1.29(0.38)	0.72	2.29	1.27(0.38)	0.71	2.30
Number of male adults ǂ				0.98(0.11)	0.79	1.22	0.96(0.11)	0.77	1.20
Family size ǂ				1.08(0.07)	0.94	1.23	1.08(0.07)	0.95	1.24

(Continued)

Table 4.9 *(Continued)*

Variable	Model 1			Model 2			Model 3 (CIM)		
	α (SE)	95% CI		α (SE)	95% CI		α (SE)	95% CI	
Community Variables (by district) §									
Population density							0.86(0.15)	0.62	1.20
% Volunteer community patrol team							1.00(0.00)	0.99	1.01
% Poor households							0.95(0.08)	0.80	1.13
Years living in the residence							1.03(0.07)	1.04	0.90
% Neighbourhood problem solving							1.00(0.01)	0.03	0.98
% Trust in the police							1.01(0.02)	0.98	1.04
Urban							0.84(0.25)	0.46	1.51
District burglary rates							1.20(0.03)***	1.14	1.26
% Neighbourhood disorder							1.00(0.01)	0.98	1.03
% Young people							1.00(0.01)	0.98	1.02
% Public security dissatisfaction							1.01(0.02)	0.98	1.05
% Fear of crime							1.00(0.01)	0.98	1.02
% Drug exposure							1.04(0.05)	0.94	1.14
LR/Wald chi2	0.00***			36.42***			147.83***		

Note. 1. Household level n = 6,158; Community level n = 121. 2. α= odds ratio; *p < .05. **p < .01. *** p <.001; CI = Confidence interval. 3. ‡ numerical variables were cluster-mean centred to avoid overdispersion; § proportion was entered as percentages to avoid overdispersion. 4. Housing type alone was significant but became not significant when including the low-floor-dwelling variable in the model (partly because low-floor variable contained too many missing observations). Low-floor variable itself was non-significant. The combined variable as easier entry (i.e. detached or lower floor) was found significant in the models.

H2.a: More attractive households, measured here as household income, are more likely to be burgled.

Target attractiveness is the first variable of target suitability. Although family income was positively related to burglary victimisation, the significance was borderline (OR $_{\text{Model 2}}$ = 1.06, 95% CI [0.99, 1.14]; OR $_{\text{Model 3}}$ = 1.07, 95%CI [0.99, 1.15]. Since very large parts of the 95% confidence interval did not cover the value of 1, family income seemed likely to predict burglary victimisation. I therefore further examined the cross-level interactions of family income and proportion of poor households by district, based on the aforementioned argument that the effect of family income on the probability of burglary victimisation might depend on the wealth of their districts of residence. That is, affluent dwellings located in poorer areas may suffer a higher risk of being burgled than the counterparts (Bowers et al., 2005). However, the cross-level interaction between neighbourhood poverty and household income on burglary victimisation risk was not statistically significant in the Taiwanese context, and a likelihood ratio test showed that including such interaction did not improve the model (see Table 4.3). The result suggests that target attractiveness (i.e. family income) did not reach a statistical significance and such an effect did not interact with the household surroundings (poor vs rich neighbourhood). The analysis therefore did not support H2.a.

H2.b: More accessible households, measured here as the presence of conspicuous security measures, the awareness of police anti-burglary consultancy and easy entry, are more likely to be burgled.

Results of multilevel analysis indicated that conspicuous security measures, including security door chains and iron-barred windows, had a significant influence on preventing burglary (OR $_{\text{Model 2}}$ = 0.68, $p < .05$). This is to say, door chains or iron-barred windows decreased the chances of a household being burgled by over 30 percent, all things being equal. However, this effect was found to mediated by the introduction of neighbourhood effects, in which

Model 3 found conspicuous security measures did not significantly predict an individual household's likelihood of victimisation.

The second measure of accessibility considered here– anti-burglary consultancy – was found to be non-significant in terms of predicting burglary victimisation. This measure was based on the logic that when household members are aware of police service, they are more likely to consult police and are thus more likely to take greater security precautions which might include locking doors and windows. Dwellings with greater security precautions make burglar more difficult to access, and thereby the dwellers are less likely to experience a burglary. A significant and positive relationship (r = 0.04, $p < .05$) found between the awareness and number of security measures supports this logic. However, the relationship was weak. This study acknowledges that anti-burglary consultancy is not a perfect measure of accessibility.

Easier entry to a property was found to be a significant predictor of a residential burglary in both Model 2 and Model 3. Consistent with expectation, households with easier entry, measured herein as detached or lower-floor houses, had a higher risk of victimisation ($\text{OR}_{\text{Model 2}} = 1.74$; $\text{OR}_{\text{Model 3}} = 1.53$, $p < .01$). This suggests that those households exhibited over 50 percent higher chance of being burgled compared to their counterparts, all other things equal.

Overall, tests of H2 found that households which were easier to gain entry to were more likely to be burgled, while measures of target attractiveness (i.e. family income) and other accessibility-related variables (i.e. conspicuous security measures and anti-burglary consultancy) were not found to be statistically significant correlates of burglary in Taiwan. That is to say, the results partially support the hypothesis that more accessible targets (here households) are more likely to suffer burglary (H2.b) but they do not provide sufficient statistical evidence to support the effect of target attractiveness on household burglary risk (H2.a).

H3: Households with fewer guardians present are more likely to be burgled

In addition to the result for H1 presented above, which suggested that single security measures may not be effective against burglary, the MLM found that the likelihood of being burgled decreased as other types of security measures were present in a property (OR $_{\text{Model 2}}$ = 0.77; OR $_{\text{Model 3}}$ = 0.74, $p < .001$). Such a protective effect increased, with the introduction of neighbourhood variables, such as population density, neighbourhood poverty, district burglary rates, neighbourhood disorder, etc. With one unit of security measure increased, a household's chance of being burgled was reduced by over one quarter, all things being equal. This finding provides further support for the previously mentioned H1.a. An important thing to note is that the relationship between the number of security measures and family income was found to be significantly positive (r = 0.14, $p < .001$). This suggests that the number of security measures increased as the income of households increased. This is understandable as, all things being equal, a more affluent household is more likely to be able to afford more (and more secure) household security measures.

Further examination of the relationship between the number of security measures and the proportion of poor households indicates a significantly negative effect (r = -0.07, $p < .001$). This weak but negative relationship suggests that more household security measures were present in more affluent areas. Again, such an interaction between household security measures and neighbourhood poverty was not statistically significant in terms of burglary victimisation (see Table 4.3), suggesting that the effectiveness of security measures did not depend on the area in which households were located (i.e. either poor or rich).

As indicated above, prior research shows that occupancy is an important aspect of guardianship. In this study, daytime occupancy (OR $_{\text{Model 2}}$ = 0.66, p <.05; OR $_{\text{Model 3}}$ = 0.60, $p < .01$) was found to be significantly related to a lowered risk of burglary while night-time occupancy was found to not hold a statistically significant association. Table 4.10 shows the distribution of burglary victimisation by time slots, drawing upon the responses of time when victims believed the burglary took place. It is thus acknowledged that these estimates may not be precise by virtue of the fact that many burglaries occur when no one is at home. The table shows that the self-reported time of victimisation among the Taiwanese sample was roughly evenly distributed across the daytime and night-time. Further, the effect size of daytime occupancy was noticeably large, with a reduction of about one fifth to over 50 percent in burglary risk (95% CI [0.43, 0.84]) when the neighbourhood characteristics were taken into consideration.

Table 4.10 Distribution of burglary victimisation by time slots in Taiwan, 2015 TAVS

Time of burglary	Frequency	Percent	Cum. percent
6-9	4	2.50	2.50
9-12	13	8.13	10.63
12-15	19	11.88	22.51
15-18	21	13.13	35.64
Daytime, not sure	21	13.13	48.77
18-21	13	8.13	56.90
21-24	5	3.13	60.03
0-3	20	12.50	72.53
3-6	13	8.13	80.66
Night-time, not sure	20	12.50	93.16
Not sure	11	6.88	100.00

Note 1. Total n = 160. 2. Freq. = frequency; Cum. percent = cumulative percent.

For other guardianship-related measures – including night-time occupancy, lone guardian of the household, number of male adults and family size, neighbourhood population density and the presence of a volunteer patrol team – were all found to be not significant. The results drawn upon household security measures and day-time occupancy support the hypothesis that households with fewer guardians present are more likely to suffer burglary (H3).

H4: Households with greater exposure and proximity to crime/potential offenders are more likely to be burgled

Proximity to crime, as shown in Table 4.9 presents a somewhat different picture from what was expected on the basis of the research literature. Neighbourhood disorder, the proportion of young people per district, neighbourhood dissatisfaction toward public security, fear of crime, and drug exposure were all found to be not significantly associated with burglary. Only district burglary rates significantly predicted residential burglary ($\text{OR}_{\text{Model 3}}$ = 1.20, $p < .001$). A one percent increase in burglary rates at the district level increased the likelihood of burglary by 20 percent. Given that other variables such as neighbourhood disorder, fear of crime, drug exposure, and so on had little impact on burglary victimisation, the findings presented here provide only partial support for the hypothesis that households with greater exposure and proximity to crime/potential offenders are more likely to suffer burglary (H4).

H5: Households located in 'socially disorganised' neighbourhoods are more likely to be burgled

The findings presented in Table 4.9 provide limited support for this hypothesis. Variables drawn from SDT seemed to have little impact on burglary victimisation in Taiwan, with measures of neighbourhood poverty, residential stability, neighbourhood's ability to solve problems within, public trust in police, and urbanisation all found to be not significant. The analysis therefore did not support H5.

4.5 Discussion

This chapter reported the results of multi-level analyses concerned with the patterns and predictors of residential burglary victimisation in Taiwan, informed by the lifestyle-routine perspective and SDT and using data from the 2015 TAVS. The analyses found that 2.6 % of households (n =160) reported experiencing burglary in the past 12 months, and that greater burglary risk was associated with: (1) dwellings with less security measures (H1.a and H3); (2) households which were easier to gain entry to (H2.b partially supported); (3) the absence of guardians in place (H3 partially supported); and (4) district burglary rates but not with other exposure/proximity-related factors (H4 partially supported). The analyses found limited evidence to support hypotheses regarding the effect of dogs (H1.b), iron-barred windows (H1.c), target attractiveness (H2.a) and SDT on burglary victimisation (H5).

Below I discuss some of the key points arising from this study, and the main limitations.

4.5.1 The application of lifestyle-routine activity approach to burglary victimisation patterns in Taiwan

In this section, I consider the implications of the findings for understanding the role of target suitability, guardianship, and exposure/proximity to crime/potential offenders in helping explain burglary in Taiwan. I then discuss the extent to which the findings reported here do or do not support SDT as an explanation of the role of general environmental factors in terms of burglary victimisation patterns in Taiwan.

4.5.1.1 Target suitability (attractiveness and accessibility)

As mentioned previously, target suitability is a key element of the LRAA. In this study, family income was used as a proxy variable for target (household) attractiveness, as has been done in previous germane research (e.g. Cohen et al., 1981). Results indicated that there was no observable relationship between household income and burglary victimisation risk. Further, given that the cross-level interaction between household income and neighbourhood poverty was not significant, the attractiveness of a dwelling as a burglary target does not seem to depend on the environment in which it is located, at least using the variables considered here. Interestingly, this result does not follow the patterns observed in some Western studies, such as Bowers et al. (2005) who found that the risk of burglary was influenced by where a house was located. Affluent properties located in poorer areas were at especially higher risk of being burgled compared to their counterparts in affluent areas, and poorer houses located in affluent areas. This departure from previous research raises two points. First, the inconsistency might be derived from different measures of affluency/deprivation. Bowers et al.'s (2005) measured affluent properties as detached houses whereas this study used household income given that detached houses may not necessarily imply owners' affluency in Taiwan. Second, no observable relationship was found here between household income and burglary victimisation risk, thereby suggesting that there might be in fact no statistically significant interactions between target attractiveness and neighbourhood economic conditions in Taiwan. Hence, using the variables considered here, the attractiveness of a dwelling as a burglary target does not depend on the neighbourhood in which it is located.

Easy accessibility is another common feature of a suitable burglary target. In this study, houses which were easier to gain entry to were similarly found to have a significantly higher risk of burglary victimisation. Furthermore, dwellings with iron-barred windows and door chains (defined in this thesis as conspicuous security measures) were found to be significantly and negatively related to burglary victimisation at a household level. This was in line with UK findings where window and door locks in combination produced moderate protection against burglary with entry (Tseloni et al., 2017). In Taiwan, the most common entry points for burglary are by doors and windows (Ho, 2013; National Police Agency, 2019b). Hence, dwellings with conspicuous security measures that hinder offenders' access to them were found less likely to be burgled. Interestingly, such a protective function of conspicuous security measures was moderated when community-level variables were considered. While this finding suggests that accessibility was important in predicting burglary victimisation to some extent, it also suggests that conspicuous security measures became less effective in Taiwan when the surroundings of a dwelling were taken into account. Why might this be so? One possible explanation is that the conspicuous security measures are so common in Taiwan that potential burglars may not regard them as a challenge for accessing the dwelling. In fact, it is very common for the burglars to have break-in tools (e.g. hydraulic cutter, steal cutter, or screwdriver, etc.) in hand, allowing them to easily damage door chains or security bars on windows (Ho, 2013)[13]. From an opportunistic perspective, conspicuous security measures would only work if the property is the only one with such obstacles in the neighbourhood. The effect of conspicuous security measures begins to tail off when the neighbourhood within which a house nested are homogenous. The variation in the significance of conspicuous security measures also highlights the necessity to examine burglary victimisation at both individual- and neighbourhood-level, as discussed in Section 4.1.2.

4.5.1.2 Guardianship

Other than easy entry, the most obvious evidence supporting the LRAA is that houses exhibited less risk of burglary when they were occupied or

[13] Damaging door chains (72%) or security bars on windows (66%) was found a common modus operandi for burglary entries in Taiwan. It was very common (more than 50%) for the burglars to have break-in tools (e.g., hydraulic cutter, steal cutter, or screwdriver, etc.) in hand (Ho, 2013).

guarded. The results of MLM indicated that houses with daytime occupancy were less likely to be burgled. Interestingly, night-time occupancy was not significant. There are two possible explanations for this finding. First, this may partly be because a greater portion of burglary victimisation in Taiwan occurred in the daytime. However, concerns are raised as the recalled time of burglary seemed to be distributed evenly in both daytime and night-time (Table 4.10). The other explanation is that the measure of night-time occupancy used did not accurately reflect the true level of household guardianship. This variable was based on participants' responses about their frequency of going out at night in a typical week. Houses were regarded as occupied in the night-time when a participant went out at night less than twice in a typical week. It was more like a lifestyle measure than a measure of the guardianship of a house. Other indirect measures of guardianship like lone guardian, the number of male adults, and family size, were also found to be not significant. While these variables were the most suitable items available in the TAVS to measure the relevant concepts, they are clearly not perfect. These sorts of limitations are common when using secondary data which was not designed to accurately capture theoretical constructs (as mentioned in Section 3.2.3).

The guardianship-related findings also suggest that the more protective measures a house had, either personally or electronically, the lower the burglary risk. Multiple protective measures were shown to significantly prevent burglary in Taiwan. This is seen in the MLM where households with more security measures in place exhibited lower odds of being burgled (see Table 4.9). One issue that requires further attention is the finding that security measures were related to household income and were less prevalent in disadvantaged households/areas. This is understandable as poorer households and communities are less likely to be able to afford security measures. However, their interaction with neighbourhood poverty was not significant (see Table 4.3), suggesting that the effectiveness of security measures did not depend on community deprivation. Multiple security measures seemed to work against burglary victimisation regardless whether the dwelling was in a disadvantaged or an affluent neighbourhood.

The examination of security measures not only supports the hypothesis that guardianship prevents burglary but also indicates that any single security measure might not effectively prevent burglary on its own. Two findings support this argument. First, the negative relationship between burglary victimisation and the number of security measures reveals that multiple security measures had the least victimisation odds. Second, no significant effects could be found in households with single security measures. The LCA results show that the sampled households had three types of security preference. One preference was for physical security measures like CCTV, police connection system, and so on, rather than security guards; the second preference was for private security guards; the third preference was for no security measures with the exception of iron-barred windows. The third type of poorly secured households suffered almost three times of the burglary risk than households with guardianship security (type 2). All these findings imply that security measures, as a guardianship concept in this chapter, are suggested to work better in combination than in a single form. The finding about more security measures being more effective is in line with what has been found in previous research (Thompson et al., 2018; Tseloni et al., 2017).

Furthermore, it is worth highlighting that this study estimated the effect of security measures on burglary victimisation using survey data from 2015, a time when the overall rate of burglary in Taiwan was exceptionally low (see Figure 3.2), owing to the sharp downward trend in burglary in Taiwan starting around 2005. It is therefore possible that the effect of a *single* household security measure might be less in 2015, compared to that at a time when the base burglary rate was much higher. Put differently, the burglars who remain active in 2015 may well be those burglars who are more experienced and successful, and less deterred by security measures than those burglars who were active a decade previously and have since been deterred/abstained. If true, this may explain why the combination of multiple security measures was found more effective in preventing burglary than a single security measure.

This is because remaining (more seasoned) burglars would be less likely to regard a single security measure (say iron-barred windows for example) as an obstacle to breaking into a property. It will be fruitful for future research to explore this issue from the offenders' perspectives, perhaps through semi-structured interviews of those convicted of burglary in Taiwan. In doing so, researchers can not only better understand the potential change in offender population during the Taiwanese crime drop, but also link the observed change with wider research on the international crime drop and particularly the debut crime hypothesis, which suggests that reduced crime opportunities may have reduced the onset and continuance of criminal careers for young people who might otherwise engage in crime (see Farrell et al., 2015).

4.5.1.3 Exposure/proximity to crime/potential offenders

The finding that district burglary rates were a positive predictor of an individual dwelling's burglary risk is as expected and in line with the literature. Extensive research shows that as a result of offenders' routine activities, they are more likely to commit crimes in areas near their central nodes (Rossmo, 1999; Townsley & Sidebottom, 2010) with which they are more familiar (P. L. Brantingham & Brantingham, 1993; Eck, 1993). Dwellings located in neighbourhoods with higher burglary rates would hence experience higher risk of burglary victimisation because those neighbourhoods might be closer to more potential burglars (Mawby, 2001). Further, this linkage may be interpreted as a result of repeat victimisation – particularly near repeat victimisation (see Section 2.3.1), for which a pool of potential burglars forage targets nearby. This possible explanation informs the next Chapter in this thesis which explores (near) repeat burglary victimisation patterns in Taiwan.

Other than burglary rates, exposure/proximity-related variables including neighbourhood disorder, the proportion of young people in districts, security dissatisfaction, fear of crime and drug exposure, all of which were found to be not significant in the MLM. It is noteworthy that the role of proximity to crime/potential offenders in crime is based on the lifestyle perspective and then incorporated into the LRAA. The lifestyle perspective suggests that when sharing a similar lifestyle with potential offenders, victims are more subjected to crime. In the case of burglary victimisation patterns in Taiwan, exposure to potential risk/disorder had no association with whether a house was burgled.

4.5.1.4 Social disorganisation theory

The variables used here which relate to SDT were found to have only a minor impact on burglary victimisation in Taiwan. Measures related to neighbourhood poverty, residential stability, neighbourhood problem-solving, public trust in police, and urbanisation were all found to have no statistically significant association with burglary in Taiwan, based on the MLM. There are two possible explanations. First, this may due to the fact that very few Taiwanese districts fit the profile of being socially disorganised. Additionally, those SDT factors, as being presented in Table 4.4, show little variation across Taiwanese society, and particularly far less variation than the US settings in which SDT was developed and is usually empirically tested. For example, the mean proportion of trust in the police among survey respondents by Taiwanese district was 0.84, with a standard deviation of 0.05. Likewise, the variable of neighbourhood problem-solving had a mean of 0.74 and standard deviation of 0.06. As a result, the first explanation for the identified weak impact of SDT is that high levels of social organisation and small variations within neighbourhoods make SDT-variables unlikely to significantly predict burglary risk in Taiwan.

Second, the weak impact of SDT on burglary victimisation identified in Taiwan might be related to the unit of neighbourhood used by this study. The problem of unit boundaries will be covered later in Section 4.5.2. Briefly, researchers have argued that smaller ecological units of aggregation might be more meaningful than bigger units when seeking to estimate neighbourhood effects on crime (see e.g. E. B. Patterson, 1991). Although the size of community variables used here ranged from 5 to 240 households per district, with an average of around 51 households per district (see Table 4.4), and the aggregation of the district was the smallest unit available in the dataset of use, it might not be small enough to examine the ecological effect of a neighbourhood on burglary victimisation in the context of Taiwan. Overall, the study did not rule out SDT as an explanation to burglary victimisation, but neither did it support it.

4.5.1.5 The overall applicability of lifestyle-routine activity approach to burglary in Taiwan

Based on the findings mentioned above, a few things are clear. First, when a house was occupied in the daytime, it suffered a lower risk of burglary. Second, multiple household security measures were found to function better at reducing burglary than individual security measures. Third, the most prevalent security measure, security bars on windows, was not significantly associated with burglary risk. Put simply, guardianship was an effective preventive factor against burglary in the Taiwanese context yet limited evidence was found to support the role of proximity to risk and social disorganisation in predicting burglary victimisation.

Overall, these findings suggest that the observed burglary patterns in Taiwan partly fit a routine activity perspective. That is, when potential offenders (e.g. in districts with high burglary rates) meet suitable targets (e.g. houses with easy access) in a setting where capable guardians are absent (e.g. houses unoccupied or with less security measures), burglary is more likely to happen. Consequently, this suggests that SCP is effective in tacking burglary in Taiwan, so long as it is tailored to the specific aspects of the burglary problem. As mentioned in Chapter 2 (Section 2.2.3), SCP is concerned with blocking or reducing the opportunities for crime through changing the physical environment in ways which increase offender effort and increase the risks of committing crime (also see Clarke & Eck, 2005). This study supports such an SCP approach, in which for instance multiple security measures were associated with lower levels of burglary in Taiwan. Based on these findings, SCP techniques such as target hardening (e.g. increased security measures), access control (e.g. hindering easy entry), and surveillance (e.g. signs of occupancy/guardianship) are likely to be effective strategies to reduce burglary as shown in the West (again see Section 2.2.3). The application of SCP informed by this study would be discussed in Section 4.5.3.

4.5.2 Limitations

This study has several limitations. I have already acknowledged one limitation regarding the measurement of SDT in the Taiwanese context, and another limitation regarding the generally low incidence of burglary in Taiwan. Put simply, the first limitation about SDT can be discussed in two aspects: (a) the 'boundaries' of neighbourhoods that I used in this study; and (b) the ability to have longitudinal observations of ecological effects within neighbourhoods. The second limitation about the low incidence of burglary matters in the current study for the purposes of examining the effectiveness of security measures in combination.

On the one hand, the measurement of SDT used here relied on the national survey in which the smallest boundary was a 'district'. As indicated above, this may not correspond to the neighbourhood unit of analysis used in the previous Western literature on SDT, such as blocks, census tracts, neighbourhood clusters, police beats, or political constituencies (R. J. Sampson et al., 2002). For instance, in the current study the population of districts at the year of survey was about 2,000 to 556,000 people, with an average of 73,500 people (Department of Household Registration, M.O.I., 2018)

[14]. By contrast, in the US the population of census tracts tends to range from 1,200 people (or 480 housing units) to 8,000 people (3,200 housing

[14] The statistics were based on the sampled area alone, excluding two archipelagos - Matsu County and Kinmen County.

units), with an average of 4,000 people (1,600 housing units) (United States Census Bureau, 2015). The size of these different areal units also differs considerably. District area size in Taiwan, derived from historical boundaries, ranges from 0.88 square kilometres to 1641.86 square kilometres while the spatial size of census tracts in the US depends on the population density of each area.

Given census tracts as subdivisions of a county in the US, districts (subdivisions of cities/counties in Taiwan) might be an equivalent measure of Taiwanese neighbourhood[15]. However, the unit of neighbourhoods might in fact be smaller than districts, considering the differences in the organisational infrastructure of neighbourhoods between Taiwan and Western communities. Several SDT studies in the Chinese context have mentioned the uniqueness of the neighbourhood unit to be used when evaluating ecological effect in Chinese-like contexts (He & Messner, 2019; L. Zhang et al., 2017). Hence, the aggregation of community-level variables to a district level in the current study might not be as appropriate as that in the Western literature. That is, residents' daily interactions (or social ties) may operate at a smaller scale, leaving the aggregation problematic as the interaction is in fact distributed unevenly. The more appropriate unit to examine SDT in Taiwan might be 'village' (*li*) or 'neighbourhood' (*lin*)[16], in accordance with Sampson et al. (2002) defining neighbourhoods as "*ecological units nested within successively larger communities*" (R. J. Sampson et al., 2002, p. 445). A village – a mix of both territorial boundaries and cultural binding – is a subdivision of district and a counterpart unit of streets in the aforementioned Chinese burglary study (L. Zhang et al., 2007), and thus might be more accurate to measure the neighbourhood effects in the context of Taiwan.

On the other hand, the current study is limited in measuring SDT due to the lack of longitudinal observations of ecological effects within

[15] Hierarchically under census tracts are the unit of block groups and then blocks in the US, whereas villages and then neighbourhoods are under the unit of districts in Taiwan.

[16] The units of 'li' and 'lin' derived from the *Baojia* system under Japan-colonial Taiwan (see Read, 2012).

neighbourhoods. As recognised by the Chicago School scholars, the ecological pattern should be observed through *"the history and growth of the city and the local communities which comprise it*" (C. R. Shaw & McKay, 1969, p. 14). The lack of longitudinal observations means it is difficult to draw conclusions about the applicability of SDT to explain observed burglary patterns. Further research is required here.

The second limitation, from an analytical perspective, is the low incidence of burglary (1.49% of the full sample) and 'small' sample (13,016 participants) in the TAVS that makes it challenging to identify the effectiveness of security measures in combination. That is, to examine combinations, two elements need to be considered: 'positive rate' of burglary victimisation and sample size. Using a UK study (Tseloni et al., 2017) as an example, there was an average of 2.66 percent of households with experience of a burglary incident across four sweeps of CSEW (April 2007 to March 2012). The total sample size was not reported; however, an annual number of around 40,000 respondents has been reported since 2001/2002. The UK study was therefore expected to comprise 160,000 respondents. The positive rate and large sample size allowed seven security measures and 128 possible configurations to be examined[17]. The TAVS used in this study contained nine security measures and thus 512 possible configurations would be generated. To reliably explore the effectiveness of these configurations, the samples would need to be increased to a comparable size to that in the UK study[18]. Therefore, this study appeals for an annual crime victim survey available in Taiwan to make longitudinal and comparable data, with the possibility to provide sufficient statistical evidence for the effectiveness of security device configurations.

[17] The final analysis utilised 52 configurations due to a cut-off point of which the configuration should be available in at least 50 households in the sample.

[18] Or even to a larger size given the low prevalence rate of burglary in Taiwan. A simple calculation of sample size is likely to be 285,638 respondents when 52 configurations are to be examined at a prevalence rate of 1.49% in Taiwan, compared to 2.66% (n ≈ 160,000) in the UK.

4.5.3 Prevention implications

The findings reported here have several implications for burglary prevention. Firstly, district burglary rates were the only environmental factor found significantly to predict the risk of burglary victimisation in this study. In the case that other neighbourhood characteristics (e.g. neighbourhood disorder, residential stability, etc.) no statistical evidence was found to indicate which neighbourhood would be more vulnerable than others. It follows that district burglary rates could at least inform the allocation of preventive resources against burglary victimisation. This could be taken together with the allocation of improved and effective security measures within the neighbourhoods with high burglary rates.

The approach mentioned above begs the question: "which security measures are most effective to reduce burglary in Taiwan?" With the effect of neighbourhood heterogeneity controlled, this study sheds light on the changes in the effectiveness of conspicuous security measures against burglary. That is, to secure a dwelling from burglary, house owners should be encouraged to take further precautions other than merely installing conspicuous security measures as their effect may be moderated by neighbourhood homogeneity. The difficulty lies in not only how to identify the most effective combination of household security measures but also how to distribute protection evenly across vulnerable targets (e.g. households within districts with high burglary rates). The former requires a large enough sample to enable analysis of different security configurations, as discussed in the limitations section above. The latter involves an overall strategy of resource distribution. For those who are unable to secure their property with multiple measures, shall the responsibility be transferred to the government?

From the perspective of social justice and considering the great national loss caused by burglaries in Taiwan (an estimated USD$700 million, see S.-Y. Kuo, 2015), it is reasonable to argue that the government plays an important role in protecting properties from burglary. This might be outside the remit of this study. This study however sheds light on what might be effective – the more security measures in place would be better. With finite government budgets, at least the current cheapest solutions (yet less used; see Figure 4.1) – light and timer – are suggested here to be the most effective measures (also see Table 4.5) to be allocated to those premises considered to be most vulnerable.

Crime prevention should never be regarded as the job of the police alone. It is impractical and inappropriate to burden the police with all aspects of crime prevention and neglect the role of other stakeholders. The responsibility of burglary prevention should also shift from police operations alone to house owners, the community, or even construction companies. This echoes the principle embedded in SCP (see Section 2.2.3), for which all stakeholders take responsibility in burglary (and more generally crime prevention). But which approach should stakeholders take? To recap, this study has found easy entry as a type of burglary vulnerability and increased security measures and occupancy as protective factors against burglary. In this sense, it might work to borrow what has been mentioned in Table 2.4 (i.e. examples of SCP techniques against domestic burglary). For example, target hardening (e.g. multiple security measures) and access control techniques (e.g. defensible space) would increase offenders' effort to enter the dwelling and thus prevent burglary. Further, extending guardianship (e.g. leaving signs of occupancy when away from the house), the use of place manager (e.g. apartment complexes with doormen) and strengthening formal surveillance (e.g. burglar alarms or CCTV camera) would increase offenders' risks of entering the dwelling and therefore stop them from doing so.

Nevertheless, security measures are only effective if they are deployed effectively. The effective deployment may be, for example, doors/windows being properly locked and closed, locks and security devices being maintained to a high quality and specification, or timers being effectively scheduled to create the illusion that the property is occupied, and so on. To best ensure the effective deployment of security measures, implemented SCP measures could be supplemented with awareness training toward citizens. Overall, this study informs what might work to prevent burglary and reinforces that burglary prevention would never be the job of a standalone stakeholder. All those involved should take part in burglary prevention.

4.6 Chapter conclusion

The current study aims to find patterns of burglary victimisation in the Taiwan context. Building on the concepts of target suitability (accessibility and attractiveness), guardianship (with some elements drawn upon SDT) and proximity/exposure to potential offenders embedded in the LRAA, this study is the first in the criminological literature to use multilevel modelling to examine whether the LRAA is generalisable to explain burglary victimisation patterns in Taiwan.

The study provides some support for the applicability of the LRAA to burglary victimisation in Taiwan. To be specific, the study found statistically significant relationships between target accessibility, the presence of guardians and burglary victimisation that are in line with the literature. Also, the study reported consistent evidence supporting a stronger effect of multiple security measures than single security measure against burglary victimisation. Yet the study found limited evidence that could support the existence of an interaction between household income and neighbourhood poverty in Taiwan. Furthermore, the findings did not provide strong evidence for the effects of SDT with regard to burglary victimisation.

The study has two limitations: (1) the measurement of SDT should have taken on a smaller neighbourhood unit than districts and on longitudinal observations of ecological patterns in the community; and (2) this study could not examine which combination of security measures worked most effectively in Taiwan due to a small volume of burglary incidents observed in the TAVS.

Overall, this study sheds light on crime prevention and future research in Taiwan. First, SCP techniques such as target hardening, access control and strengthened surveillance are suggested to be working in the Taiwan context.

Second, the relationship between victimisation and neighbourhood burglary rates suggests that there might be some neighbourhoods with a pool of potential offenders nearby. This may lead to neighbourhoods with higher burglary rates experiencing higher levels of burglary risk for dwellings within, on which neighbourhood crime prevention can focus. The study also suggests a possible formation of (near) repeat burglary patterns in Taiwan, which informs the research on repeat burglary victimisation in Chapter 5 to provide further viewpoints of crime prevention against (repeat) burglary victimisation in Taiwan.

Chapter 5 Examining Repeat Burglary Victimisation in Taiwan

Extensive evidence indicates that prior victimisation is a reliable predictor of future victimisation. Repeat victimisation is thus common. Much of the existing research on repeat victimisation has taken place in western industrialised countries; less so in Asian contexts. This chapter aims to answer the research question proposed in Chapter 2: "*Is there evidence of (near) repeat burglary victimisation in Taiwan?*". To answer this research question, two datasets are used: (1) the 2015 TAVS, also used in Chapter 4; and (2) police recorded burglary data from Taoyuan city for the period January 2015 to April 2018. The chapter concludes by comparing the observed findings to those from previous (Western) research and reflecting on the implications of the findings for burglary prevention in Taiwan.

5.1 Background

Repeat victimisation refers to the consistent research finding that crime concentrates on a small minority of targets and places (Bernasco & Steenbeek, 2017; Eck et al., 2007; Weisburd, 2015). The concept was first introduced in the late 1970s, and quickly gathered popularity because of the perceived (and later realised) benefits to crime prevention policy, practice, and resource allocation (Farrell & Pease, 2017; O et al., 2017). Patterns of RV have been identified for a wide range of crime types, from domestic violence and racial attacks to bicycle theft and child abuse (Farrell et al., 1995). Indeed, a recent systematic review of the repeat victimisation literature found a high level of concentration for both personal and property crimes. The synthesised evidence drawing from a large number of studies revealed that the most victimised 20% of properties and persons accounted for 46.7% and 51.5% of victimisations, respectively (O et al., 2017).

Burglary, as one type of property offence, is found to be a classic case for which RV occurs. Indeed, the majority of research into RV has focussed on this offence type. The famous Kirkholt project, for example, investigating burglary levels on a housing estate in Rochdale, England, revealed that the risk of a house being burgled again was four times the risk of a first burglary victimisation (Forrester et al., 1988). Moreover, analysis of the 1998 BCS identified that 19.5% of burglary victims were burgled more than once in the previous twelve months (Mirrlees-Black et al., 1998). The UK is not unique in this regard. The Netherlands, for instance, exhibits a similar pattern of repeat burglary victimisation (Kleemans, 2001; Wittebrood & Nieuwbeerta, 2000). North American research also provides convincing evidence for this kind of concentration pattern (e.g. Polvi et al., 1990; Robinson, 1998). Likewise, analysis of data collected as part of the ICVS concluded that repeat burglary victimisation is a common phenomenon among most industrialised nations, despite some variation across countries. For example, England and Wales was found to have a moderate proportion of repeat burglaries (12%) compared to, say, the US, which experienced a dramatically higher proportion of repeats (33%; see Farrell & Bouloukos, 2001).

There are four recurrent findings in the research literature into RV. First, prior victimisation is shown to be a reliable predictor of future victimisation. Second, a small number of repeat victims typically account for a disproportionately high number of all victimisations. Third, repeats are highly prevalent in high crime areas. Indeed, the repeated victimisation of particular people or places is often found to generate the heat in observed hot spots. Lastly, RV often occurs quickly in the wake of an initial victimisation (Farrell, 1995; Farrell & Pease, 2017).

The last finding on the temporal pattern of risk – the so-called time course of repeat victimisation – extends repeat victimisation research to ‘near’ repeat research. That is, RV, by definition, refers to the repeated victimisation of the *same* target, also sometimes referred to as a ‘direct repeat’. However, an extension of the concept of RV is NRV, which combines elements of spatial and temporal repeat victimisation, and refers to the phenomenon whereby similar crime targets (however defined) that are geographically close to a crime victim are more likely to be victimised themselves in the short term than would be expected on the basis of chance. The term ‘near repeat’ summarises this spatial and temporal tendency of revictimisation risk of nearby comparable targets (Farrell & Pease, 2017).

Like RV, a large body of studies has also identified near repeat patterns. Burglary, for instance, is found to be more likely to occur within 300-400 metres and 1-2 months from the location and time of the initial event in the UK (Johnson & Bowers, 2004a, 2004b). This pattern exists across countries such as Australia (Townsley et al., 2003), the Netherlands, the United States (Johnson et al., 2007), South Africa (Clark, 2018), Brazil (Chainey & da Silva, 2016), and China (P. Chen et al., 2013), and across diverse types of crimes such as gun-shootings (J. Ratcliffe & Rengert, 2008), or sex crimes and threats (Amemiya et al., 2020).

Previous research has identified that the time range and distances of risk clustering varies across countries and types of crime. For example, research in some Chinese cities has found that, in line with near repeat findings more generally, the risk of burglary is highest nearest the sites and time of the initial incidents and decays gradually afterward. The risk was found to be elevated (above chance) for 56 days and one kilometre (Ye et al., 2015), and for three weeks and beyond 100 metres of the initial incident the risk drops dramatically (P. Chen et al., 2013). Research in Houston, Texas, has also found similar patterns of space-time clustering of burglary risk, although the risk lasted for a longer time range (up to 90 days) and distance interval (up to 2.5 kilometres). Meanwhile, a shorter spatial and temporal span has been observed in street robberies (6 days and 400 metres) and aggravated assault (7 days and 1.6 kilometres) (Y. Zhang et al., 2015).

As mentioned in Section 2.3.1, there are two main explanations for (near) repeat victimisation: *event dependence* and *risk heterogeneity* (Johnson & Bowers, 2004b; Lauritsen & Quinet, 1995; Osborn & Tseloni, 1998; Wu et al., 2015), also known as ‘boost’ and ‘flag’ accounts, respectively. The boost account suggests that the initial victimisation boosts the chance of (repeat) victimisation in the future. In the case of burglary, the burglary target becomes more vulnerable or desirable as a result of a successful initial victimisation. That is, burglary success encourages an offender's return visit (Ashton et al., 1998; Martinez et al., 2017). The flag account, on the other hand, refers to a scenario in which there is a stable chance of victimisation independent of victimisation history. Therefore, there is not a correlation between the events that occur in the future and those in the past. The events that will occur against the same target are due to the fact that certain targets are in some way vulnerable and hence attractive to motivated offenders. Prior research identifies several factors that might increase the likelihood of a household being burgled, such as a property being detached and hence easier to access (Osborn & Tseloni, 1998), weak or no security measures in place (Miethe & Meier, 1990), and so on (also see Table 4.1). Indeed, the results presented in the previous chapter indicate why some Taiwanese households experience burglary and others do not. In terms of explaining RV, these specific characteristics are thought of as acting as a 'flag' to prospective offenders that this property is an attractive target to burgle (Pease, 1998).

Beyond the flag and boost accounts, researchers concerned with explaining patterns of NRV also often refer to 'optimal foraging theory' (Bernasco, 2009; Johnson, 2014; Vandeviver et al., 2021). Consistent with the rational choice perspective of offender decision making (Clarke & Cornish, 1985), the optimal foraging theory suggests that offenders seek to be optimal foragers who target multiple suitable properties in a chosen neighbourhood (rather than one single property) in order to try to minimise their effort and maximise their potential rewards (Bowers & Johnson, 2004; Stokes & Clare, 2019). In doing so, offenders are also likely to 'forage' in areas where they have previously been successful (Bernasco et al., 2015) or areas within their 'awareness space' (i.e. familiar locations like home, work, and shopping precincts where offenders spend considerable time) (Townsley & Sidebottom, 2010). In this sense, it is argued that, all things being equal, offenders ought not move on to other locations until the perceived 'rewards' available in the current 'optimal' neighbourhood are gone (Bernasco, 2009; Chainey & da Silva, 2016; Johnson, 2014).

To summarise, then, the risk of (N)RV could be attributed to offenders: (a) foraging in areas where they are familiar; (b) making rational decisions to prey on suitable targets ('*flags*') or targets with prior success of offence ('*boosts*'); and then (c) searching for targets nearby as part of an optimal foraging strategy. In the case of burglary, the *flag* characteristics of a property make it perceived as an easier target and more attractive to a potential offender. Then, the risk of future burglary is *boosted* following an initial successful incident by foraging offenders who tend to revisit the same or nearby locations for a short period to carry out a series of further offences after an initial offence.

Before moving on to the focus of the current study, it is important to report the findings from recent research in England and Wales which suggests that the extent of RV is on the rise (Ignatans & Pease, 2015) albeit against the backdrop of large and consistent reductions in crime overall – the previously mentioned 'international crime drop' (Farrell et al., 2015; Sidebottom, Kuo, et al., 2018). Based on their analyses of the CSEW between 1994 and 2012, Ignatans and Pease (2015) found that although the overall chance of being victimised has fallen, the proportion of total victimisation experienced by the same individual has *increased* from 57% in 1994 to 72% in 2012. This implies that the inequality in victimisation has *increased* against a backdrop of widespread crime reductions. In 1994, for example, the top one percent of victims accounted for 42% of all personal victimisations; in 2012, they accounted for 52%. Similar trends were also found for property crimes (from 22% to 33%) and vehicle related victimisation (16% to 27%) (Ignatans & Pease, 2016a, 2016b). The analysis of data collected as part of the ICVS revealed a similar trend, in which the proportion of total personal victimisation experienced by the top one percent of victims increased by four percent (from 32% in 1992 to 36% in 2000). The greatest growth of 15% was observed in vehicle-related victimisation (from 33% to 48%) (Pease et al., 2018).

The observed inequality in crime experience is but one of ten reasons proposed by Farrell and Pease (2017) for why studying RV is important, displayed in Table 5.1.

Table 5.1 shows the various preventive gains to be had from efforts to reduce RV specifically. Simply put, because crime concentrates on a small number of repeatedly victimised targets (i.e. RV), then gains in prevention can be maximised by targeting (and tailoring) interventions to those targets at greater risk of revictimisation in the short-term. Likewise, if the risk of victimisation spreads to comparable targets in space and time (i.e. NRV), then time-limited predictions can be made about where crime is most likely to occur and preventive resources deployed accordingly. Again, there is strong evidence to support the effectiveness of this approach particularly in reducing residential burglary (Fielding & Jones, 2012; Stokes & Clare, 2019), albeit, as alluded to throughout this thesis, such evidence is not available in the Taiwanese context.

Interestingly, compared to the abundance of research on repeat or near repeat research, an analysis by Pease and colleagues (2018) using Google Scholar suggested that only eight percent of identified studies dealt with both repeat and near repeats in their analysis (Pease et al., 2018). In light of the paucity of information about both kinds of victimisation pattern, especially in an Asian context, this chapter aims to answer the research question stated in Chapter 2, namely "*Is there evidence of (near) repeat burglary victimisation in Taiwan?*". The chapter focusses on burglary victimisation in part because existing research from Western studies provides a comparable reference with which to compare the findings observed here.

Table 5.1 Ten reasons why it is important to study repeat and near repeat victimisation, as proposed by Farrell and Pease (2017)

Summary of reasons	Explanation and potential benefits
1. Limited resources to crime problems	As resources are limited, a focus on repeats would be a cost-effective way of resource allocation to crime problems.
2. Repeat victimisation chronically exploits resources	Repeats are chronic issues so will gradually consume the criminal justice system. A focus of combating repeats will save crime prevention resources.
3. Increased risk per target	Targets have different levels of risk, for which repeated targets indicate an increased risk. Resource allocation should thus depend on individual risk.
4. Short-term repeats	Risk is unevenly distributed across targets. Repeats are so immediate so specific prevention should focus on such high-risk targets.
5. The avoidance of extensive resource allocation	The allocation of crime prevention resources targeted at repeat victims will be more practical than at a generally vague population (e.g. all pupils).
6. Enhanced detection of repeat offenders	A focus of repeat victimisation will make crime detection/prevention start at an early stage
7. Consideration of crime displacement and diffusion of benefits	There are low chances of displacement and high chances of diffusion of benefits, meaning prevention on repeats could maximise the benefits.
8. Enhanced detection of serious and prolific offenders	Stopping volume crime at an early stage.
9. Performance indicators	Repeat victimisation prevention can be developed into an agency and individual performance indicators.
10. Applicability for all crime types	Repeat victimisation is relevant to all crime types, ranging from organised crime to property crimes

Source: Farrell and Pease (2017)

5.2 The current study

As mentioned in Chapter 2, research into repeat and near repeat victimisation is sparse in Asian settings. To recap what was summarised in Chapter 2 about key findings in burglary studies of (N)RV in Asia (see Table 2.2 and Section 2.3.1), there are two general patterns that are noteworthy. First, although repeat burglary patterns have been observed in Asian settings, such studies have shown a large range of concentration – about one tenth of burglaries were found to be RV in Japan (Hino & Amemiya, 2019) whereas about half of burglaries were RV in Taiwan (S.-Y. Kuo, 2015), for example. Second, and in relation to NRV, spatial and temporal clustering of repeat burglaries can also be observed in Asian settings. However, it is difficult to draw firm conclusions about the spatiotemporal range within which the risk significantly communicates.

As indicated above, few studies have investigated the extent and patterns of (near) repeat burglary victimisation in Taiwan, of which most studies tend to provide descriptive rather than inferential statistical information (see Table 2.2). For example, Tseng (2014) reported a spatial range of repeat burglaries of 2.4 kilometres (Tseng, 2014). Two issues arise here, however. First, the conclusion on the radius seemed to be vague as the researcher did not perform any statistical analyses. This hinders the generalisation of findings to a wider context. Second, no information about the decay function was provided in the study so it is difficult to draw practical crime prevention implications.

Based on these research gaps, two hypotheses are tested here:

- H1: There is a significantly higher concentration of repeat burglaries in Taiwan than would be expected on the basis of random victimisation.

If repeat burglary in Taiwan is found to be non-random – provided that the role of event dependence and risk heterogeneity functions similarly in the case of burglary in Taiwan – I would also expect a spatiotemporal near repeat pattern of burglary victimisation to be observed. Hence the second hypothesis:

- H2: Properties located nearby a burglary victim are more likely to be burgled in the short term.

5.3 Data and methods

The following sections describe the two main data sources used in this study, namely the 2015 TAVS and police recorded burglary data from Taoyuan city. I then introduce the analytical strategies to be used in this study, including descriptive analyses, Lorenz curves, the local indicator of spatial autocorrelation (LISA) and the Knox test.

5.3.1 Data

The analysis reported here draws on two datasets. The first dataset is the 2015 TAVS, as was used in the previous chapter. To reiterate, the 2015 TAVS is a large nationally representative survey that used multi-stage stratified sampling and collected data from 13,016 households.

Relevant to this chapter, it is important to note that the 2015 TAVS capped the total number of victimisations that a victim could report – the cap was six victimisations per crime type in the previous year (also see Section 3.2.2.1). Experience of seven or more victimisations over the previous 12-month period was hence coded as simply six and over (n=10). This is common practice in many victimisation surveys and is practiced mainly in an effort to avoid extreme figures prejudicing average crime rates (Budd & Mattinson, 2000). However, such an (arbitrary) counting convention has been shown to misrepresent the true distribution of crime and, in particular, the extent of repeat victimisation: the extent of repeat (chronic) victimisation is undercounted (see Farrell & Pease, 2007a, 2007b). The patterns of repeat victimisation according to the 2015 TAVS should, therefore, be taken with caution and considered to be an underestimation[1].

Further, as the 2015 TAVS contained neither geographic nor temporal information about the victimised households, it is impossible to map the patterns of near repeat burglary using this dataset. Instead, to completement the analysis of the TAVS, this chapter additionally reports analysis of police recorded crime data drawn from a northern metropolitan city in Taiwan - Taoyuan City.

Taoyuan city is the fourth-largest metropolitan area (1,221 square kilometres) and fifth-largest populated city (2,249,037 persons) in Taiwan (Taoyuan City Government, 2020). Its police recorded burglary data is publicly accessible and contains information about the date on which the burglary was believed to have occurred, the location (latitude and longitude coordinates) of the burglary, and the police station and bureau in charge of the reported burglary incident. The police data used in this study covered the period from January 2015 to April 2018 (40 months) and contained 506 recorded burglary incidents. This data source was used to extend the analysis of RV using the TAVS and to also consider patterns of NRV. Note that although the police data is not limited to a cap of six victimisations as in the TAVS, a familiar limitation with the police data is that not all burglaries are reported to and recorded by the police (see Section 3.1.1). However, this data source is expected to supplement the 2015 TAVS and allow me to examine the spatial and temporal patterns of NRV in Taiwan.

5.3.2 Analytical strategy

The analytical strategy used here involved descriptive analyses, Lorenz curves, the LISA test, and lastly the Knox test. The first approach taken for

[1] Note again that the raw dataset retrieved from the 2015 TAVS did not record the exact number of victimisations when a victim reported being victimised of more than six times in the past year. Hence, this thesis could not estimate the extent to which repeat victimisation was undercounted. This issue would be detailed in the limitation section.

testing the first hypothesis is to quantify repeat victimisation. It follows the approach proposed by Tseloni and Pease (2005), in which they presented concentration rates, the percentage of repeat crimes, and the cumulative distribution. The former two elements can be displayed in a table containing the distribution of repeat burglary victimisation based on the 2015 TAVS, while the last measure can best be visualised using a Lorenz curve.

Lorenz curves are a graphical tool to plot the distribution of incidents, commonly used in research into economic inequality (see e.g. Gastwirth, 1972; Jann, 2016; Prendergast & Staudte, 2016). The logic behind Lorenz curves is that by sorting individuals on the basis of some index of interest, for example from the one who has the lowest, say, income, to the one who has the highest income, the cumulative distribution of income is constructed. From an economic perspective, the square box generated is shaped by the X-axis representing the proportion of the population whereas the Y-axis represents the cumulative distribution of total wealth. In a country where income is equally distributed, the curve is expected to be consistent with the main diagonal line of the square box (i.e. from bottom left to right top corner). However, in light of the oft-observed 80-20 rule (the Pareto principle, see e.g. Dunford et al., 2014) assuming the top 20 percent of the population accounts for 80 percent of the national wealth[2], the curve will be pulled towards the low right corner of the box (i.e. with extremely 100% population and 0% income coordinates). The more the curve corresponds to such a shape, the more inequalities are present in the distribution of, in this example, income. Such an approach is also applicable to examine the distribution of crime across victims (see e.g. Bernasco & Steenbeek, 2017; Curiel, 2019; Mohler et al., 2019; Ratcliffe, 2010; Steenbeek & Weisburd, 2016; Tseloni & Pease, 2005).

This study used Lorenz curves to examine the distribution of burglaries in Taiwan. The concept is similar to that used in economics: sorting individuals according to households who experience the lowest number of burglaries, *b*

[2] The bottom 80% population holds 20% of the overall wealth, vice versa.

$_{(1)}$, to those who experience the highest number of burglaries $b_{(N)}$ (over a given time period) so as to build the cumulative distribution of the number of burglaries. The Lorenz curve thus represents the cumulative distribution of the total number of households N and the total number of burglaries B (Curiel, 2019). To the best of my knowledge, this is the first time that crime distribution in Taiwan has been displayed this way.

By analogy with the economic context, in the case where there is no repeat victimisation, the observed Lorenz curve over victims would move towards the equality diagonal of the figure box. In this way, one could expect x% of the victims to experience about x% of the predicted events. If the observed curve is steeper than the equality line (i.e. the 45° line), it reveals that the more heavily victimised suffer disproportionately more crimes (Tseloni & Pease, 2005). Here I need to reiterate the issue of victimisation responses, as measured by the victim survey, being capped at six. Were there to be disproportionality in the experience of burglary, the inequality would be more serious than the data presented as it misses the frequencies over six potentially experienced by some individuals

The Lorenz curves reported here were compared to a simulation of Poisson distributions. The simulation was estimated under the assumption of a factual low crime prevalence and that crime events are randomly distributed over the targeted population (Estévez-Soto et al., 2020). The Gini index is also reported alongside the Lorenz curves as a measure to quantify (burglary) concentration. The index ranges from zero (i.e. no inequality/concentration) to one (i.e. complete inequality/concentration).

A one-sample Kolmogorov Smirnov (KS) test is often used to examine if the distribution of observed incidents statistically differs from a reference distribution (i.e. a randomly generated distribution). If this is the case, then it can be concluded that there is more concentration of burglary incidents than would be expected on the basis of random (repeat) victimisation. Given that the frequency of victimisation is purely discrete and the victimisation population in the 2015 TAVS (n = 194) was greater than a suggested sample size of 30 (see Dimitrova et al., 2017), the KS test is suggested to be performed using an improved R package 'KSgeneral' (Dimitrova et al., 2020).

If there is evidence to support *H1: There is a significantly higher concentration of repeat burglaries in Taiwan than would be expected on the basis of random victimisation*, there might be worth in further examining how the concentration is distributed over targets – say different types of properties and accessibility, for example (Osborn & Tseloni, 1998). Due to the fact that the number of repeatedly burgled households was small (n = 59) in the 2015 TAVS, it is challenging to perform a sophisticated analysis. Therefore, this chapter uses Chi-square analyses to investigate potential differences in (repeat) burglary risk for the various property types (and by extension the ease of accessibility) in Taiwan. The purpose of such analyses is to preliminarily explore the distribution of repeat burglary risk over targets with specific characteristics in Taiwan .

Before statistically testing if properties located nearby a burglary victim are more likely to be burgled in the short term (H2), I perform the LISA to map the police recorded burglaries between 2015 and 2018 as a preliminary analysis. The approach taken here visualises LISA using the local Moran's I statistic and produces maps to illustrate local hotspots of burglary in Taoyuan city. LISA maps are commonly used to examine the degree of spatial randomness and identify crime hotspots – adjacent areas that have similarly high rates of crime (Anselin, 1995; Anselin et al., 2000). As a complement to the Lorenz curves, this could provide both statistical and visualised information about whether there is a significantly higher concentration of burglaries in Taiwan than would be expected on the basis of random victimisation. It is however noted that the unit of LISA analysis to be used differed from that of Lorenz curves. The former LISA analysis would examine police recorded burglaries at an aggregated level of "village' (*li*) nested within districts (see Section 4.5.2 for details) whilst the latter Lorenz curves draw upon individual households in the TAVS as the unit of analysis. The LISA maps might be able to show spatial concentrations of burglaries in Taiwan than would be expected on the basis of random victimisation. Yet, they do not indicate the RV of individual properties. The purpose of presenting LISA maps is to (visually) examine if there is spatial concentration of burglaries in Taiwan, specifically the city of Taoyuan, using police data. If so, it is very likely that there would be some patterns of near repeat burglaries observed in Taiwan. Then, it would make sense to take the following approach to provide further statistical information about NRV.

The analysis of near repeat burglaries reported here utilised Johnson et al.'s (2007) permutation-based test which builds on the Knox test (Knox, 1964). This technique identifies the temporal and spatial distance of paired events and determines whether there are more observed pairs in temporal and spatial proximity than would be expected based on a random distribution. As each event is compared with every other and the spatial and temporal distance between them recorded, ½ n (n-1) pairings will be generated provided n cases, followed by a contingency table containing the number of event pairs that occur within the defined spatial and temporal increments (or bandwidths). This enables comparisons between the observed and expected cell counts under the null hypothesis that the temporal distance and the spatial distance are unrelated. With the existence of near repeats, the observed counts will be significantly higher than the expected ones (Johnson et al., 2007).

There are a few issues with using the Knox test to examine crime repeats. The first issue concerns population bias due to variations in growth rates of populations by geographic subareas (Y. Zhang et al., 2015). As the Knox test does not take population growth into consideration, in a geographic area where there is a rapid expansion (or shrink) in population size within a short period, it would make the Knox test unreliable. However, the population shift bias would not be a critical issue as the population here for burglary is households rather than people, and presumably this doesn’t change much over time, especially for a study period of 40 months in Taiwan.

The second issue with the Knox text is the selection of the bandwidth of the space-time clusters, which heavily relies on prior empirical evidence about the scale at which potential crime clustering may occur. Despite the aforementioned sparsity of research found in Taiwan, thanks to much attention gathered in the west (e.g. Johnson & Bowers, 2004b; Townsley et al., 2003) and some further available in a Chinese context (Wu et al., 2015; Ye et al., 2015), the current study used the bandwidth of 7 days and 100 metres. To generate large enough distortion for different boundary definitions, the choice of cut-off in distance and time is also critical and should be drawn from the literature (Wu et al., 2015). Considering that the risk of burglary victimisation was found to be contagious for 56 days in a Chinese context (Ye et al., 2015) and a longer period of 90 days found in the US (Y. Zhang et al., 2015), the cut-off point in time used here is the conservative figure of 98 days while a spatial cut-off point of at least 3,000 metres was suggested by the literature (Grubesic & Mack, 2008). Further, as researchers have noted that the inclusion of exact repeats would predict better clustering (Y. Zhang et al., 2015), the current near repeat analysis includes pairs of events with 0 distance (practically less than 0.1 metres, see Davies, 2019).

Another issue noted in the literature relating to the measurement of repeat victimisation is the so-called time window effect, which refers to the absence of repeats being observed due to too short an observation period, say one week for example (Farrell et al., 2002). Even though there is a pattern of crime repeat, the shorter the period of data is used, the higher likelihood that the repeat would fall outside the timeframe of measurement. Put differently, an analysis using data containing merely one week would possibly find no repeat victimisation should the incidents happen the week before or after the observed period. There is little chance for those incidents being noted as 'repeats' because their precursors or subsequent offences are not recorded in the dataset being analysed. This results in undercounted RV as well as overcounted single-incident crimes. Briefly, Farrell et al. (2002) have found that data containing a period of one year captures 42% more repeats than that of six months while a three-year one captures 57% more repeats than a one-year counterpart.

RV research often utilises a one-year period although it may contain less than 50% of the actual repeats. This may partly because victim surveys conventionally have a recall period of one year to avoid the memory-decay effect of interviewees. However, the current study uses both data from the victim survey data with a recall period of one year and police records with a period of 40 months would diminish the time-window effect to a great extent.

The near repeat analysis reported in this study used Python with the function defined by Davies (2019) in which function the increment is set to be open to the left by default[3].

5.4 Results

H1: There is a significantly higher concentration of repeat burglaries in Taiwan than would be expected on the basis of random victimisation

Table 5.2 The distribution of burglaries in Taiwan using data from the 2015 TAVS

Burglary Num.	Prevalence	Incidence	% all targets	% victims	% incidence
0	12,822	-	98.51	-	-
1	135	135	1.04	69.59	43.83
2	37	74	0.28	19.07	24.03
3	9	27	0.07	4.64	8.77
4	3	12	0.02	1.55	3.90
5	-	-	-	-	-
≥ 6	10	60	0.08	5.15	19.48
Total	13,016	308	100%	100%	100%

Table 5.2 shows the extent of (repeat) burglary victimisation based on the 2015 TAVS. It shows that burglary in Taiwan is a rare event, at least compared to that of England and Wales. Less than two percent of sampled

[3] In this chapter the temporal and spatial bandwidth were set as 7 days and 100 metres. Hence, the first- and second-time increments would be 0 to 7 days (not inclusive) and 7 (inclusive) to 14 (not inclusive). Equivalently, the spatial bands of distance would be 0.1 to 100 metres (not inclusive), 100 metres (inclusive) to 200 metres (not inclusive), and so on.

households reported being the victim of burglary in 2014 (308 burglaries in total) and 0.5 percent of sampled households experienced two or more burglaries over the one-year study period (173 burglaries in total). Put differently, 56 percent of the total number of reported burglaries took place in these 0.5 percent of sampled households (i.e. the repeatedly victimised households). That is to say, of those households that were burgled over the one-year period, about 70% experienced only one burglary. Around five percent of victimised households experienced six or more burglaries, which accounted for nearly 20 percent of all reported burglaries in the data used here. The observed probability of being burgled one time only is thus 0.01 whereas the probability of repeat victimisation is 0.30, a ratio that is 30 times higher.

Figure 5.1 shows the distribution of burglary over all households and all victims using Lorenz curves. The left panel presents evidence of extreme inequality in terms of burglary victimisation across the sampled population (Gini index = 0.99) since only a very small number of surveyed households in Taiwan were burgled. The inequality is lessened only when those who had been burgled at least once were retained in the analysis (see the right panel, Gini index = 0.30). However, the concentration pattern is still obvious in both panels. In the right panel, the curve becomes steeper from the point of the cumulative 70% of victims on the X-axis. This shows that the top 10% most victimised subjects (n = 194) experienced about 30% of the victimisations (n = 308) while the lower 10% accounted for less than 10% burglaries. Meanwhile, the KS test revealed that the observed distribution of burglaries was significantly different from the null distribution (D = 0.55, $p < .001$). Simply put, the results observed here suggest that there was a significantly higher concentration of repeat burglary than would be expected on the basis of random victimisation. This finding provides support for hypothesis one and conforms with the dominant finding in the research literature, this time in the atypical setting of Taiwan.

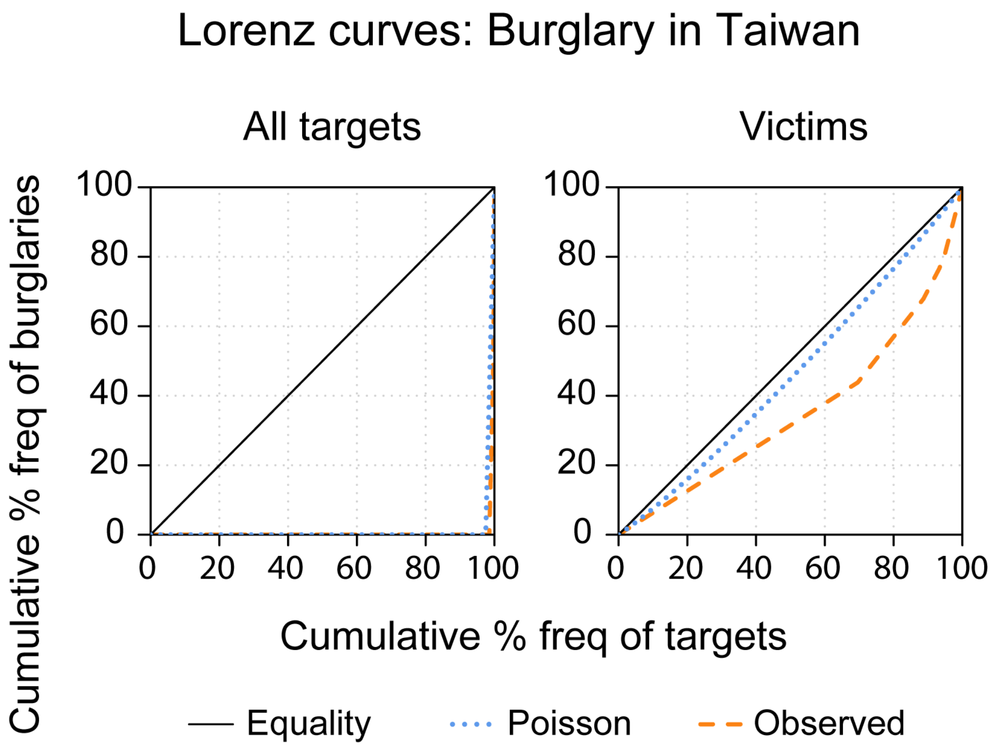


Figure 5.1 Lorenz curves with the observed and expected distributions of burglary victimisation using the 2015 TAVS

Previous research shows that the risk of burglary (re)victimisation is influenced by property type. Taking advantage of the questions asked in the TAVS, Table 5.3 investigates potential differences in (repeat) burglary risk for the various property types (and by extension the ease of accessibility) in Taiwan. It shows that, relative to the prevalence of burglary at each property type, detached houses appeared to be the most likely to be revictimised (40 percent) compared to their counterparts. However, repeats were found not significantly related to property type in general ($\chi^2(4) = 5.08, p = 0.23$), except for semi-detached houses which suffered significantly lower frequencies of repeats than expected (χ^2 (1) = 4.92, p < .05). Houses with easier access (i.e. those detached or located on the second floor[4] or below within an apartment or high-rise building) experienced 1.24 times more revictimisation than

[4] The second floor in Taiwan equals to the first floor in the UK.

expected, all things being equal. However, such a relation was again not statistically significant ($p = 0.10$).

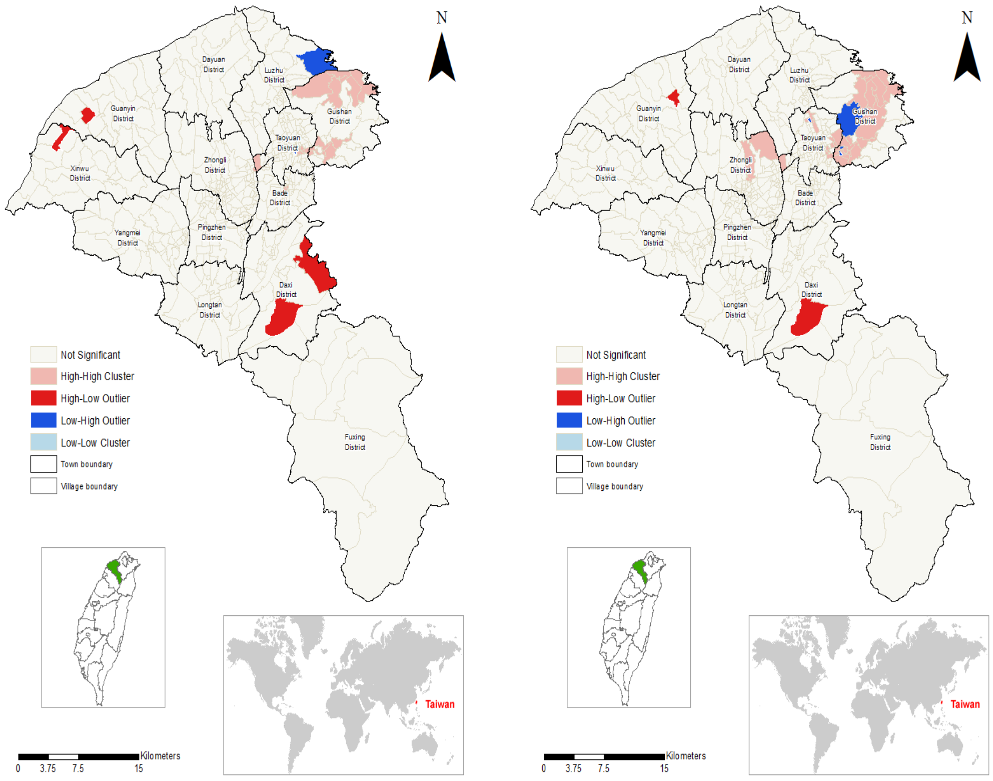
Table 5.3 Risk of revictimisation by different types of property in Taiwan, 2015 TAVS

Property characteristics		Repeats (% by house type)	
		Zero repeats	Revictimised
House type			
Bungalow/detached	Obs.	21(60.00%)	14(40.00%)
	Exp.	24	11
Semi-detached*	Obs.	76(76.77%)	23(23.23%)
	Exp.	69	30
Apartment	Obs.	24(63.16%)	14(36.84%)
	Exp.	26	12
High-rise building	Obs.	10(62.50%)	6(37.50%)
	Exp.	11	5
Other	Obs.	4(66.67%)	2(33.33%)
	Exp.	4	2
Easy access	Obs.	34(61.82%)	21(38.18%)
	Exp.	38	17

Note 1. House type: Pearson $\chi^2(4) = 5.08$, $p = 0.23$. Cramér's V = 0.16. 2. Easy access: Pearson $\chi^2(1) = 2.19$, $p = 0.10$. Cramér's V = 0.11. 3. * indicates cell frequencies that were significantly lower than expected, using a chi-square test with one degree of freedom, $p < .05$. 4. It is difficult to translate the term used in the TAVS as the property type in Taiwan is very different from that in the UK. Briefly, the category of semi-detached may include terraced and town house.

H2: Properties located nearby a burglary victim are more likely to be burgled in the short term.

We now turn our attention to NRV and the analysis of police recorded burglary data. Figure 5.2 shows LISA maps using the local Moran's I statistic to illustrate local hotspots of burglary in Taoyuan between 2015-2018. The left panel (a) shows burglary rates (per 100 households) while the right panel (b) shows burglary counts. Figure 5.2 reveals a cluster of burglaries and hotspots in the study area. For example, Guishan District (see upper-right corner of the study area) represented parts of a cluster with positive spatial autocorrelation, in which the district had the greatest number of areas with a high burglary rate. Three districts were outliers and had a negative spatial autocorrelation, which had villages that had a high burglary rate and were surrounded by areas with low burglary rates. Note that Fuxin district (at the bottom of the study area), by area, is the largest in Taoyuan City; yet it is a mountainous indigenous district. No burglary occurred in this district between 2015-2018. While the aforementioned Lorenz curves provided support for burglary being concentrated over targets, the LISA maps reported here additionally suggest a spatial concentration of burglary in the study area.



a. LISA's burglary by rate

b. LISA's burglary by count

Figure 5.2 LISA maps of burglary hotspots using counts and rates per 100 HHs by villages in Taoyuan, Taiwan, 2015-2018

Table 5.4 shows the results of the (N)RV analysis of burglary risk using police recorded crime data for Taoyuan city (n = 506). The statistics in the table represent the ratios of medians, namely the difference between the observed and the expected counts of data using 999 iterations. The higher the figure the greater the difference between the observed and the expected counts of burglaries. To improve the visualisation of near repeat patterns, the table contains a reduced distance range of 1,000 metres and a time range to less than 42 days. A table showing the spatial and temporal limits of 3,000 metres and 98 days can be found in the Appendix (Table A.1).

Table 5.4 Near-repeat analysis of burglary risk using police recorded burglary data from Taoyuan city, Taiwan, 2015-2018 (n = 506) (999 iterations)

Spatial unit (m)	Temporal unit (day)					
	0 to <7	7 to <14	14 to < 21	21 to < 28	28 to < 35	35 to < 42
Same location	**32.00****	**4.00****	**4.00****	0.00	0.00	0.00
0.1 to <100	2.00	0.00	0.00	0.00	0.00	2.00
100 to <200	**4.00****	**3.00***	2.00	1.00	0.00	1.00
200 to <300	**5.33****	2.00	2.00	1.00	1.00	0.00
300 to <400	**4.00****	1.33	0.67	0.00	2.00	0.67
400 to <500	0.00	**5.33****	0.67	0.00	0.00	0.67
500 to <600	1.20	0.80	1.00	1.00	1.50	0.50
600 to <700	1.67	**3.20****	0.40	0.40	1.60	1.00
700 to <800	0.67	1.60	0.50	0.40	**2.50***	1.00
800 to <900	**2.29****	1.14	0.67	1.33	1.00	**2.00***
900 to <1000	1.25	**2.29****	0.00	1.14	0.67	0.33

Note *Significant at $p < 0.05$. **Significant at $p < 0.01$.

As Table 5.4 shows, the significant values were found mostly on the top left of the table. This suggests that burglary risk in Taiwan was communicable within a range of 3 weeks and 400 metres around a location at which a burglary was previously committed, as would be predicted by the literature. A significant pattern of exact repeat victimisation was found, in which there was evidence of an over-representation of events at the same place up to 21 days after an initial incident. The most significantly over-represented RV range was the spatial zone from 0 to less than 7 days from an initial incident. The chance of another incident was about 32 times greater than if there were no repeat victimisation patterns. In the immediate space-time vicinity to an originator event, the most over-represented space-time range that was statistically significant was the zone from 200 to less than 300 meters and within 7 days from an initial incident. The chance of another incident occurring was over five times greater than if there were no discernible pattern. However, note that within the range of 100 metres, the risk of burglary was found not to be statistically significant. The risk of burglary victimisation seemed to be influenced by its temporal proximity to a victimised target. Yet the spatial pattern of proximity was less evident. H2 is partially supported from the temporal perspective.

Table 5.5 shows the number and proportion of near repeats of all burglary incidents for different spatial and temporal bands. Although the pattern of near repeats observed here was statistically significant for most of the cells that were spatially and temporally closest to originator incidents within 3 weeks and 400 metres, less than 5% of all recorded burglaries were near repeats within 200 metres and 7 days of an originator incident. Meanwhile, around 5% of all recorded burglaries were near repeats within 200 metres and 14 days of an originator incident.

Table 5.5 The proportion of near repeats for different definitions of near in space and time using police recorded burglary data from Taoyuan city, Taiwan, 2015-2018

Near repeat definition	Number of near repeats and % of all burglaries	
	0-7 days	0-14 days
Within 100 m	17(3.36%)	19(3.75%)
Within 200 m	21(4.15%)	26(5.14%)
Within 300 m	29(5.73%)	36(7.11%)

n = 506

5.5 Discussion

This section is formed of two sub-sections: (1) a discussion of the implications of the main findings and (2) a discussion of the limitations in this study.

5.5.1 Implications of findings

This chapter began by setting out that there is a large literature on the patterns of repeat and near-repeat victimisation, particularly burglary victimisation. Presently, however, there is limited knowledge of the extent and patterns of (N)RV in Taiwan. To address this research gap, this chapter reported findings on the extent of repeat and near repeat residential burglary victimisation in Taiwan, using data from both the 2015 TAVS (to explore RV) and police recorded crime statistics from one city in Taiwan (to explore both RV and NRV). The analysis found that the patterns of repeat and near-repeat burglary victimisation observed here were largely in line with that of (the mainly Western) research literature, despite the notable differences in context and crime levels. That is, burglaries were shown to be far more concentrated than would be expected on the basis of chance (H1): 56 percent of self-reported burglaries were repeat victimisation. This figure is far higher than the proportion of repeats found in many western and developed countries, for which a comparative study identified the highest proportion being 33 percent (in the US, see Chainey & da Silva, 2016).

The degree of burglary concentration was similarly higher than what was found in the literature. According to the Lorenz curves reported in Figure 5.1, the top 10% most burgled households in Taiwan accounted for 30% of the burglaries in Taiwan, while the same figure for the UK was 20% (Tseloni & Pease, 2005). The current figure over victims also reveals that RV was more serious over those with high frequencies of burglaries as the line becomes much steeper from the point of the cumulative 70% of frequency of victims. Were the TAVS not capped at six, repeat victimisation would likely be even more concentrated (or more unequally distributed). This informs the necessity of prevention against those super targets (i.e. those with high frequencies of repeat burglaries) given the extreme inequality of repeats identified in Taiwan. Furthermore, future research could usefully focus on the impact of capping in crime surveys in Taiwan. The problem of capping is discussed in the later limitation section.

As mentioned above, given that the risk of RV was not random but heavily concentrated, it is important to identify the household risk factors that give rise to the observed patterns of repeat. However, given there are few revictimised households in the data used here (n = 59), it was not practical to conduct any sophisticated analysis. Instead, a simple Chi-square analysis by house type for (no) repeats revealed that semi-detached houses suffered a significantly lower risk of revictimisation. This is consistent with Bowers et al.’s (2005) finding that semi-detached houses suffered a significantly lower risk of revictimisation than an expected Poisson distribution.

Note that it was challenging to properly translate the property type from a Western context to Taiwan. The category of semi-detached houses may also refer to those terraced and townhouses in Taiwan. In this sense, it would be confusing to apply the aforementioned study to Taiwan as Bowers et al.'s (2005) study also indicated that terraced houses and flats were at significantly higher risk of revictimisation of burglary. I assume that the negative relationship between semi-detached houses and revictimisation risk was partly due to fewer entry points for burglars to break in. This could also explain why the observed counts of revictimisation for detached houses and houses with easy access, although not statistically significant, were higher than expected as those houses potentially contained more easy entries. However, it was not clear why the significant relationship was found only in semi-detached houses. This assumption needs to be tested in further research using data with a larger sample size and more sophisticated analytical strategies. The police data might be a suitable alternative than victim surveys. Unfortunately, the current publicly accessible police data in Taiwan contains only the time and place of burglary occurrence but no information about house types.

With respect to the current police data, the analysis reported above revealed a statistically significant and meaningful pattern of repeat and near repeat victimisation. The risk of burglary victimisation was elevated by spatial and temporal proximity to an initial incident (partially supporting H2). Put differently, the risk decayed by time and space following an initial burglary incident. Interestingly, while the significant pattern was mostly found within the temporal and spatial range of 3 weeks and 400 metres, which was in line with the research literature, the risk within the range of 100 metres was not statistically significant. A possible explanation for this inconsistency concerns residents' precautions and police interventions after the initial burglary. On the one hand, within a radius of 100 metres, residents are very likely to be aware of the initial incident of burglary. As a consequence, they may be more likely to take precautions that reduce their risk of burglary (such as locking their doors, neighbourhood watch, security systems, etc.) or the police were allocated there in the forms of, say, visible foot patrols to deter potential offenders and thereby reduce the risks of near repeat victimisation. On the other hand, the police patrol deployment is common to see in Taiwan once there is an incident occur within a police jurisdiction, though its form may range from vehicle to foot patrols. The aforementioned residents' precautions and police interventions may result in a reduced risk observed in the first spatial band. However, such an explanation needs to be tested empirically, and requires further examinations into both the residents' and police' responses to burglary.

Another thing to note is that, unlike the aforementioned victim data, the police recorded data in Taiwan revealed that the levels of near repeat burglaries were under-represented. The proportion of burglaries that were near repeats was much lower than those found from studies in western countries, or even some Chinese settings. For example, the proportion was 23% within 200 metres and 7 days in Newcastle, UK (Chainey, 2014) and 26% within 120 metres and 14 days in Wuhan city, China (Wu et al., 2015).

Contrarily in Taoyuan, Taiwan where the police data was retrieved, repeat victimisation and near repeat victimisation within 200 metres and 14 days accounted for merely about 5% of all burglaries, which was about one fifth of that in the UK and China. If generalisable, this figure would call into question the cost-effectiveness of any crime prevention programme designed to reduce repeats and near repeats in the short term and over a limited geographic area, as it would only yield an overall burglary reduction by roughly five percent. This finding drawn upon police data is in conflict with the concentration patterns identified by the analysis of TAVS, in which the allocation of crime prevention resources across the 10 percent most heavily victimised households implied a reduction of potentially 30 percent of burglary incidents. Hence, more police datasets across crime types and regions are required to examine if such an underrepresentation is with merely burglary victimisation or a regional issue that merely occurs in Taoyuan city.

Overall, while the concentration of repeat burglary using the victim survey data was found consistent with the literature, the pattern of near repeats generated some inconsistencies with existing studies. The risk of repeats and near repeats tailed off within a temporal range of three weeks. However, within the spatial range of 400 metres, the risk did not decline steadily. Future research should focus more on why the 0.1 to 100-metre interval did not show a constant risk of near repeat victimisation.

5.5.2 Limitations

A few general problems derived from surveys were noted as my Lorenz curve analyses were drawn on victim survey data. These may include common issues such as measurement error, response bias, or telescoping which can be referred to Chapter 3 (see Section 3.1.2). The more serious problem was the effect of capping. The 2015 TAVS allowed for a maximum of six entries being recorded for one type of crime event. As mentioned above, this counting convention is commonly applied in many national victim surveys. The US NCVS, for instance, has allowed their counts of series victimisation capped at ten since data for 2010 (a cap of six before 2010) (Lauritsen et al., 2012) whereas CSEW once capped at five, until a new approach of capping at 98th percentile of victim incident counts for each crime type being introduced in the year ending September 2018 of CSEW (Office for National Statistics, 2019).

Many researchers have found such counting conventions to misrepresent the extent and distribution of crime (Farrell & Pease, 2007a, 2007b). Tseloni and Pease (2005) has also indicated that the entry of actual number rather than a cap of five to BCS would make the property and personal crime incidence increase by about two and 1.5 times respectively. That is to say, provided that this truncation was removed from the 2015 TAVS, crime would be more unevenly distributed as the same number of victims would have the chance to experience more incidents.

Built from this perspective, probing the effect of capping is especially crucial to RV in Taiwan. However, the current data did not allow me to track back the original number of victimisations. Victimisation inequality might be worse than the current analysis found but the extent remained unanswered. The future TAVS should reconsider the application of such counting convention and record the actual entries of victimisation more properly. In this way, the actual crime distribution could be estimated, and criminal justice equality could be improved.

The second limitation concerns the inability to reliably explore the boost account of repeat victimisation. At present, studies on the impact of event dependence and risk heterogeneity on repeat victimisation may require entries of the individual incident as these allow researchers to plot the distribution of time intervals between each event (see e.g. Estévez Soto, 2020). The analysis of the time-course of repeat victimisation was not available given the TAVS of use did not record the individual experience of victimisation other than the time elapsed between the last two incidents.

The third limitation concerns the small volume of local police data used in this study, which contained only 506 burglaries over a 40-month period. The current analysis alternatively utilised police recorded data to examine patterns of repeat and near repeat burglary as it consisted of geographic and temporal information of burglary incidents, in which the current TAVS failed to provide. Let alone that police recorded data is notorious for underreporting practice, the dataset containing merely 506 cases for 40 months was not comparable to the existing literature, especially to other context-alike Chinese studies. For example, there were 1,533 burglaries for merely five months (between 19 May to 31 October 2007) recorded in Beijing (P. Chen et al., 2013), 4,226 burglaries from 1 January to 30 December 2013 for a large city located in south-eastern China (Z. Wang & Liu, 2017), and remarkably 10,548 burglaries for the year of 2013 in Wuhan (Wu et al., 2015), to name some.

Further, the police data lacked information such as house types. It was difficult to analyse the risk factors for burglary victimisation other than near repeat patterns using police data in Taiwan. Hence, I could not tell if the lowered risk of repeat burglary observed in those semi-detached houses was consistent both in victim surveys and police data. The mechanism behind such an argument was not clear, either. I understand that burglary incidents are rare in Taiwan so that the authority may not pay much attention to it. However, it is of great importance to understand why there are some targets at extreme vulnerability and why (and how) patterns of repeat and near repeats in Taiwan is not very in line with the literature. While Taiwan's low burglary incidence might be a deficiency in terms of victimisation research, it is a benefit to understand what makes it less vulnerable. Moreover, were police data and victim surveys being made comprehensive and accessible, the extent and risk factors of crime would be easier to estimate.

The last limitation concerns the lack of longitudinal data in Taiwan to be compared with the growing concentration of RV across countries. Despite Taiwan having witnessed a consistent drop in crime rates with international trends (Sidebottom, Kuo, et al., 2018), the lack of longitudinal data on concentration over victims makes the study unable to examine if the concentration is also in line with some cross-national trends (Pease et al., 2018). If it is the case (i.e. concentration over victims becomes more intensive by time), more resources should then be allocated to those most vulnerable. Put simply, with longitudinal data, future research is applicable and believed to improve crime prevention policies.

5.6 Chapter conclusion

The results reported here indicate a consistent and highly concentrated pattern of repeat and near repeat burglary victimisation in Taiwan, more so than is often found in western settings. In line with previous research, the risk of burglary victimisation in Taiwan was shown to decay across both time and space following an initial burglary incident, covering a period of three weeks and 400 metres. However, the current results also suggest that burglary risk within 100 metres of a prior incident was not elevated to a statistically significant degree. These patterns depart from the consensus in the research literature and may reflect differences in offender targeting strategies and/or the design and layout of properties in Taiwan.

As alluded to above, the findings presented in this chapter may have implications for the effective and efficient distribution of police resources to the most vulnerable burglary targets. While the concentration of burglary across the population is unequal, the prevention against repeats is a viable and cost-effective approach to crime reduction, as has been documented in numerous studies in the UK and US. While the spatial pattern of near repeat burglary victimisation appeared to be less evident in Taiwan, patterns of direct repeats were clearly observed in both the victim survey and the police data analysed here. Taken together, these provide strong evidence that, for the crime of burglary at least, RV is a real phenomenon in Taiwan. It warrants further research to explore the correlates of repeat burglary and the existence of repeat patterns for other crime types.

Chapter 6 Cybercrime victimisation

Using data collected as part of the 2017 Digital Opportunity Survey for Individuals and Households, this chapter deals with two research questions presented in Chapter 2: (1) does the lifestyle-routine activity approach adequately explain patterns of online victimisation in Taiwan? And (2) do victimisation patterns vary across different types of online victimisation experienced in Taiwan? The research presented in this chapter is considered timely: there is an increasing body of literature exploring the applicability of LRAA to cyberspace, but that research is currently largely confined to university students based in Western countries. It is therefore not known if this theoretical framework applies to settings such as Taiwan and to a more representative population of potential victims than university students. To begin to address this research gap, this chapter applies the LRAA to examine four types online victimisation and aims to understand how online environments and individuals' online routine activities are associated with variation in experience of different types of cybercrime.

6.1 Background

This section introduces the reader to the concepts and literature on cybercrime that are relevant to this chapter and which were not fully covered in Chapter 2. It begins by classifying the four types of cybercrime victimisation considered in this study, namely cyber abuse and cyberbullying, cyber fraud, identity theft, and malware and virus attack. I then discuss each crime type from the perspective of the LRAA and how the application of such a framework has implications for the use of SCP in an online context.

6.1.1 Classification of Cybercrime

As the internet enters its fifth decade, it is estimated that over 4.5 billion people, or 58 percent of the world's population, now have access to the internet. North America has the highest internet penetration rate of nearly 95 percent, followed by Europe (87%) and the Middle East (about 70%). Asia is slightly below the world average, with an internet penetration rate of 53 percent (Miniwatts Marketing Group, 2020). Taiwan shows a high internet penetration rate of around 80 percent, comparable with most other industrialised regions (see Section 3.2.2.2).

Environmental criminology maintains that crime follows opportunity, and that these opportunities are often produced by otherwise positive societal developments. The internet is a classic example, as an innovation that brings great and wide-ranging societal benefits but one which also creates opportunities for cyber victimisation. There is now a considerable body of literature on cybercrime, albeit there is no standard definition of what constitutes a cybercrime. The difficulty in defining the term lies in the fact that cybercrime refers not to a single kind of criminal activity but to *"a diverse range of illegal and illicit activities that share in common the unique electronic environment ('cyberspace') in which they take place"* (Yar & Steinmetz, 2019, p. 6).

In light of the challenges of neatly defining cybercrime, scholars have instead chosen to consider cybercrime as 'the computer-mediated activities that are illegal' and further classify it as 'computer-assisted crimes' and 'computer-focused crime' (Yar & Steinmetz, 2019). As indicated in Chapter 2 (Section 2.2.2), the former refers to 'traditional' forms of crime that occurred before the internet but which take a new form when carried out in cyberspace. Examples include certain types of fraud, theft and sexual harassment. The latter category – 'computer-focused crime' – refers to those crimes that were brought about following the advent of the internet and which could not exist if there were no internet. Examples here include hacking and malware attacks. The classification by 'computer-assisted' and 'computer-focused' cybercrime is adopted by organisations such as the UK National Crime Agency.

This terminology, however, has been criticised by researchers for its focus on technology and alleged neglect of the relationships between offenders and targets/victims (Yar & Steinmetz, 2019). An alternative categorisation system using existing legal conceptions has therefore been suggested as: (1) crime against property – including stealing physical or intellectual property (e.g. credit card fraud, piracy) or trespassing on other people's property and/or causing damage (e.g. hacking, viruses); (2) crime against morality – breaching laws on obscenity and decency (e.g. cyber-pornography); (3) crime against the person – doing psychological harm to or encouraging physical harm against other people (e.g. hate speech, stalking, bullying); and (4) crime against the state – activities that endanger the nation or its infrastructure (e.g. terrorism, leakages of official confidential information) (Yar & Steinmetz, 2019). Such a classification system not only links cybercrime more closely to conceptual elements of traditional crimes but paves the way for the application of existing crime science theories to crime patterns in cyberspace. This theme is picked up in the next section.

6.1.2 The application of lifestyle-routine activity approach to cyberspace

As mentioned in Chapter 2, the rational choice perspective is the dominant model for offender decision-making, and is a core plank of EC. It assumes that the decision-making processes of criminals is largely akin to that of non-criminals. Offenders try to gain rewards (broadly defined) from their illicit behaviours in much the same way as non-offenders seek to maximise the benefits of their non-criminal decisions (Cornish & Clarke, 2014). Like their offline counterparts, cybercriminals are also thought to adopt a largely rational decision-making process when making choices about illicit cyber behaviours, weighing up the perceived benefits of their online activities against the expected costs and risks (Bachmann, 2010; Higgins, 2007; Hutchings, 2013; Pittaro, 2007; Rege, 2014).

Based on the assumption that cybercriminals tend to operate in ways which accord with the rational choice perspective, the RAA has thus gradually been used as a framework to examine patterns of cybercrime, where a cybercrime would occur if a motivated offender meets suitable targets in the absence of capable guardians who could otherwise prevent the offence from occurring (e.g. Back, 2016; Barkan, 2006; Jansen & Leukfeldt, 2016; Leukfeldt & Yar, 2016; Rege, 2014; Reyns & Henson, 2016). However, to apply the RAA to the study of cybercrime, researchers have modified the required spatiotemporal convergence of offenders and targets. Simply put, a refined 'cyber lifestyle-routine activities approach' suggests that for a crime to succeed, offenders and targets without capable guardians do not necessarily need to be present in the 'exact' same moment in the same 'physical' location, considering that virtual spaces are fluid and that the presence of online actors is not very predictable. Rather, these three elements are thought to converge in a 'network' and the contact between victims and offenders can be 'delayed' (Reyns, 2017).

To reiterate what was presented in Chapter 2, the LRAA proposes five key factors for explaining victimisation risk: guardianship, exposure to risk, proximity to potential offenders, attractiveness of potential targets, and definitional properties of specific crimes themselves[1] (Cohen et al., 1981). All things being equal, it is held that individuals who are more exposed to risk, are in closer proximity to offenders, are more attractive as targets to offenders, and are not protected by capable guardians, are more likely to be victimised. When applying the LRAA framework to cybercrimes, certain daily activities on the internet are considered "riskier" than others, because they are more likely to expose individuals to motivated offenders in cyberspace, absent the presence of capable and empowered (cyber) guardians. For example, in a study of malware infection among students, faculty, and staff at a US

[1] To recap, Cohen et al. (1981) believe that specific crimes feature specific instrumental actions by potential offenders. For example, offline theft requires less commands of technical knowledge for offenders to commit than do online identity theft. Likewise, burglaries require offenders' more awareness of victims' routine activities (e.g. about if the dwelling is occupied) than general larcenies do.

university, Holt and Bossler (2013) found that legitimate routine computer behaviours (e.g. checking emails, shopping or using instant messaging) did not significantly predict a higher likelihood of malware infection, while involvement in deviant computer use (e.g. viewing online pornography) did.

Hence, research has suggested that different online activities may cause different levels and/or different types of risk and the risk may not depend on the legitimacy of routine computer behaviours (van Wilsem, 2013b). This highlights the necessity of examining risk factors for different types of cyber victimisation. Complementing Chapter 2, the below sections summarise the main findings from the literature on the LRAA as they relate to the four types of cybercrime considered in this study. Then, by reason that the LRAA has implications for preventing crime, the application of SCP drawn upon the LRAA to cyberspace is briefly recapitulated (also see Section 2.2.3.2).

6.1.2.1 Cyber abuse and cyberbullying from lifestyle-routine activity approach

Cyber abuse is a collective term that comprises online abusive interpersonal behaviours including online bullying, stalking, sexual solicitation, and problematic exposure to pornography (Mishna et al., 2011). Despite no consistent definitions of cyber abuse to date, as with cybercrime more generally, most researchers agree that cyber abuse refers to a repetitive and continuous (over time) performance of threatening or annoying behaviour through the use of technology (Brown et al., 2014; Reyns et al., 2011; Vakhitova et al., 2016).

Online bullying, more commonly termed as cyberbullying, is one form of aggression and violence involving electronic technologies. The leading definition has been given by Patchin and Hinduja (2006) as ‘‘*wilful and repeated harm inflicted through the medium of electronic text*” (Patchin & Hinduja, 2006, p. 152). Cyberstalking is then defined as the use of electronic or internet-capable devices to repeatedly pursue an individual, ranging from constant unwanted contact to threats of violence (Mishna et al., 2011; Reyns et al., 2011). A few researchers have categorised cyberstalking and cyber harassment into one narrow concept of cyber abuse, ranging from less severe behaviours such as offensive name-calling and purposeful embarrassment to more severe behaviours including physical threats, sustained harassment, stalking, sexual (or any) harassment (Duggan, 2017; Vakhitova et al., 2016). Sexual solicitation refers to behaviours of requesting that individuals engage in unwanted sexual activities/conversations or to provide personal sexual information while problematic exposure to pornography involves some general pornography-related activities, searching behaviours or commission of criminal offences (for detail see Mishna et al., 2011).

Cyberbullying is arguably the most researched form of cyber abuse. A systematic review has revealed that cyberbullies (i.e. perpetrators) tend to be male, albeit in many cases details of the perpetrators are unknown (Aboujaoude et al., 2015). Research presents a mixed picture in relation to a common victim profile (Slonje et al., 2013; Tokunaga, 2010). Examples can be found of males being more vulnerable than females (Kalia & Aleem, 2017; Salmivalli & Pöyhönen, 2012); few or no significant differences in victimisation by gender (Brown et al., 2014; Hinduja & Patchin, 2008; Q. Li, 2006; Smith et al., 2008); and females being more vulnerable (Aboujaoude et al., 2015; Kowalski & Limber, 2007; J. Wang et al., 2009; Wolke et al., 2017). Similarly, variations have been observed in the relationship between age and cyberbullying victimisation, with some studies finding no association (Brown et al., 2014; Smith et al., 2008; Wolak et al., 2007) and others finding an inverse or curvilinear relationship (Hinduja & Patchin, 2008; Tokunaga, 2010).

Observed inconsistencies in research on cyber bullying may be attributed to a number of factors, including the use of different age groups, countries, and utilising different methodologies (Brown et al., 2014). More importantly, the inconsistencies in victim profiles may also be attributed to the fact that some studies do not account for lifestyle-routine activities as a potential moderator of victimisation risk (e.g. Salmivalli & Pöyhönen, 2012; Wolke et al., 2017). It is because the vulnerability of certain population groups may derive from their online lifestyle-routines rather than demographic factors, given that research suggests a different level of target suitability or exposure to risk such as the use of social media by a number of demographic factors (e.g. gender differences see Hargittai, 2007; Kalia & Aleem, 2017). The neglect of lifestyle-routine factors might therefore contribute to the inconsistent findings of prior research.

First posited by Marcum (2008) and reassessed by Mesch (2009), the RAA and LRAA have been shown to predict cyberbullying and the broader concept of cyber abuse. For example, prior research has found that time spent online communicating with others (e.g. online chatrooms, forums) and sharing personal information (e.g. active social networking, or frequent site profile updating) have a significant positive impact on victimisation risk for online bullying and harassment (Bossler & Holt, 2009; Hinduja & Patchin, 2008; Marcum, 2008; Marcum et al., 2010; Mesch, 2009; Navarro & Jasinski, 2012; Reyns et al., 2011). A more recent study collecting data through an online survey of American adults also provides evidence that greater exposure to risk (measured therein through online involvement such as self-promotion) is a positive predictor of both indirect and direct forms of cyberstalking and cyber harassment (Vakhitova et al., 2019). However, the authors have suggested that when interaction effects are considered within their model, some explanatory effects (e.g. online gaming) are more useful than others.

Notwithstanding that cyberbullying affects different ages, a large body of research using the LRAA has focused on cyberbullying of young people (e.g. Hinduja & Patchin, 2008; Kalia & Aleem, 2017; Marcum, 2008; Mesch, 2009; Navarro & Jasinski, 2012). This may be related to sampling convenience or a belief in a curvilinear relationship between age and victimisation, of which victimisation peaks around middle school age (around 13-15 years) and decreases after older adolescence (Slonje et al., 2013; Tokunaga, 2010). Several scholars have identified the need for more research on cyberbullying among older individuals ((Jenaro et al., 2018; Vakhitova et al., 2016).

6.1.2.2 Cyber Fraud from lifestyle-routine activity approach

Fraud is a form of economic crime involving the *‘‘intentional deception or attempted deception of a victim with the promise of goods, services, or other benefits that are nonexistent, unnecessary, were never intended to be provided, or were grossly misrepresented’’* (Titus, 2001, p. 57). Departing from this definition, an internet (cyber) fraud can be viewed as any type of fraudulent act that involves one or more components of the internet to commit (Koong & Liu, 2006). An example of cyber fraud might be the publication of misleading or deceitful information online (see Smyth & Carleton, 2011); however, the means of deception may utilise any electronic resources, including but not limited to email, chat rooms, message boards or websites (Kunz & Wilson, 2004; Tade & Aliyu, 2011). A typical form of cyber fraud is the Nigerian e-mail fraud, in which individuals receive an e-mail from an alleged heir to millions of dollars that are hidden in accounts all over the world, and that can be released and shared only if the victim agrees to pay, say, several thousand dollars for the lawyer’s fee. The truth is that they never receive the claimed money (Kunz & Wilson, 2004).

Who is most likely to be involved in cyber-fraud? Studies have shown that people with low self-control are more likely to participate in online fraudulent acts (e.g. Holtfreter et al., 2010). Other studies in Nigeria have found that perpetrators of cyber fraud tend to be youths (particularly students) with social media platforms, which are often used as the primary means of locating victims (Ogunleye et al., 2019; Onah & Nche, 2014).

Victim profiles for cyber fraud are mainly limited to demographic characteristics as there are not many studies applying a LRAA framework on cyber fraud in particular. Prior studies have found that, unlike street crime, higher educated people and higher-income households are more vulnerable to fraud victimisation while young people are more often victims, as in the context of street crime (Holtfreter et al., 2006; Titus, 2001). Pratt et al.'s (2010) study, which is one of the few to draw on the LRAA, provided an explanation for variations in vulnerability across sociodemographic populations. The research revealed different lifestyle-routine activity patterns between participants with different sociodemographic characteristics, for which female, older, and African American respondents as well as participants with lower levels of formal education spent significantly less time online compared to their counterparts. Similarly, African American, retired, and less educated participants were less likely to make online purchases. Differences in participants' patterns of online activities might thus affect their experiences of online victimisation as younger and more educated individuals were found significantly more likely to be targets of consumer fraud via the internet. van Wilsem's (2013) study also supported experiences of online fraud victimisation being inversely related to age and positively related to educational level. The author suggested a complementary explanation for such vulnerability – higher educated people might be more skilled in retrieving interesting commercial offers, resulting in a greater probability of falling into the fraudster's trap (van Wilsem, 2013a).

Based on their findings, Pratt et al. (2010) suggested that routine online activity had a greater effect in explaining online fraud victimisation compared to sociodemographic characteristics. Among different routine internet activities, online purchasing, and online forum participation were regarded as key risk enhancing factors in terms of internet fraud victimisation (Pratt et al., 2010; van Wilsem, 2013a).

6.1.2.3 Identity theft from lifestyle-routine activity approach

Identity theft is one form of consumer fraud and is arguably the fast-growing type of fraud around the world (Cavoukian, 2013; Jibril et al., 2020; Kahn & Liñares-Zegarra, 2016; Reyns, 2013; M. L. Williams, 2016). By applying internet tools, malicious actors trap oblivious users into the disclosure of personal identity and financial account credentials. The users are then exploited for illicit purposes such as online payment and banking services (Jibril et al., 2020). 'Phishing' is one common technique employed, by which malicious actors pretend to be a trusted authority using digital means like email. Such spoof emails "*are designed to lead consumers to counterfeit Web sites that trick recipients into divulging financial data such as usernames and passwords*" (Anti-Phishing Working Group, 2020, p. 2).

Given the low levels of apprehension of cybercriminals by law enforcement[2], researchers have little information on the profile of offenders committing online identity fraud (M. L. Williams et al., 2019). Alternatively, several sociodemographic characteristics among victims have been found significantly related to identity theft. These include age, gender, and income; however, the first two characteristics do not show a consistent result across regions. Whilst UK researchers have found that the elderly are at greater risk of identity theft, US studies have found a non-linear correlation given that the risk declines steadily as age increases (beyond 75 and over) and people between the ages of 25 and 54 are believed to be the most vulnerable. Meanwhile, male users appear to be more likely than females to be victims of identity theft in the UK, yet the US shows a more similar pattern between genders (Anderson, 2006; Harrell, 2019; Reyns, 2013).

Perhaps the most profound demographic trait linked to victimisation of identity theft is income; the aforementioned studies have all revealed a significantly positive relationship between the two. Anderson (2006) has attributed possible moderators of identity theft victimisation as variations in the number of accounts, transactions, and credit cards that are held by certain groups. However, associations between victimisation and sociodemographic characteristics are found to be largely moderated by online routine behaviours (Reyns, 2013). This may account for the distinct demographic profiles of victims observed as the users in different regions appear to have different patterns of online activities.

The introduction of online routine behaviours reiterates that participation in certain online activities increases the likelihood of identity theft. Online

[2] A study in the state of Florida, US revealed a clearance rate of four per one hundred in 2002, compared to seven per one hundred for motor vehicle theft and a more significantly distinct rate for robbery (16 per one hundred, $p < .05$) (Allison et al., 2005).

routine activities, including e-banking, shopping, emailing, downloading, and selling on online auction sites have consistently been found to statistically predict domestic online identity theft victimisation in the US, the Netherlands, the UK, and Europe (Pratt et al., 2010; Reyns, 2013; van Wilsem, 2011; M. L. Williams, 2016). Apart from online participation, the location of routine internet access is another important factor to predict identity theft victimisation, for which using computers in public settings (e.g. libraries or universities) is found to be riskier compared to access in the workplace (M. L. Williams, 2016). Suggested reasons might be the fact that computer use in the workplace often involves more rigorous security policies, a higher level of guardianship and single-purpose computers, whereas public computers may have multiple users, use of plug-in devices or more flexible policies of use, leaving the targets to meet potential offenders on networks with low levels of guardianship (Reyns, 2013; M. L. Williams, 2016). This is an interesting finding in the sense that it implicates both online and offline activities in the risk of identity theft victimisation.

Other than participation in certain online activities by individuals, the function of guardianship embedded in the LRAA remains contested in the literature with respect to online identity theft. Leukfeldt (2014) has found that having up-to-date antivirus software as a technically capable guardian has no effect on financial damage caused by phishing attacks. Conversely, Williams's (2016) comparative study between European countries found that the adoption of 'passive' physical guardianship measures (measured therein as using only one computer, email spam filtering, installing antivirus software and secure browsing)[3] is negatively associated with online identity theft victimisation (M. L. Williams, 2016).

[3] The author classified guardianship as: (1) passive physical guardianship (using only one computer, email spam filtering, installing antivirus software and secure browsing); (2) active personal guardianship (changing security settings and passwords); and (3) avoidance personal guardianship (doing less online, such as banking and purchasing goods)

Further, Williams (2016) has suggested a few factors that mediate the association between guardianship and identity theft victimisation across countries: (a) internet penetration rates, and (b) cybersecurity strategy. On the one hand, users residing in countries with lower internet penetration rates (assumed to be a proxy measure for a less-developed internet infrastructure) and adopting passive guardianship as well as ‘avoidance’ guardianship measures (less online activities, e.g. less banking and online purchase), are deemed more likely to experience online identity theft, compared to those adopting these types of guardianship in countries with higher internet penetration (assumed as possibly better-developed infrastructure). Hence, country internet penetration rates have been suggested to be a mediator. On the other hand, the maturity of a cybersecurity strategy has also been shown to moderate the effectiveness of guardianship, in which users with passive guardianship in countries with more mature cybersecurity strategies were found to experience decreased levels of online identity theft. The author has therefore concluded that some sorts of guardianship (e.g. changing security settings and passwords) maintain their level of effectiveness regardless of country-level guardianship (internet penetration and national cybersecurity strategy as the direct measure of country capable guardianship), yet upon which the effectiveness of passive physical guardianship is dependent (M. L. Williams, 2016). This research sheds light on the necessity of examining guardianship from both individual- and environmental/area-level perspectives.

6.1.2.4 Malware and virus from lifestyle-routine activity approach

Malware is a term describing all types of malicious software. Virus is one type of malware despite the fact that these two terms are often used interchangeably. Viruses spread across cyberspace by attaching themselves to files, applications or programmes, and are distributed through infected websites, flash drives, or emails. Once activated by a victimised target, a virus may delete or encrypt files, modify applications, or disfunction systems (McAfee, 2020). Other common types of malwares include worms and spyware. Unlike viruses, the former malware does not need to attach themselves to other programmes and can self-replicate many times, causing immediate harm to devices. The latter virus is a type of software that can steal personal information from users. Once installed onto devices, spyware can use, say, the webcam without the user's knowledge or record everything the user types (i.e. keylogging), enabling keyloggers to steal user's passwords, account numbers, credit card numbers, and other important data (BBC, 2020).

Studies on malware infections have revealed less evidence on victims' sociodemographic profiles. A US study using the 2003 NCVS found that better educated, male, and white people were more likely to be victims of computer viruses (Yucedal, 2010). Some Dutch studies further found that younger populations might suffer a higher risk of digital attacks via email and websites (van Wilsem, 2011); yet targets' value (i.e. financial characteristics) did not play a significant role in predicting malware victimisation. Inversely, individuals with lower incomes were found to be at an increased risk of malware victimisation (Leukfeldt, 2015).

The applicability of LRAA to malware infection is promising as researchers have drawn comparisons between the way malware infects computer systems to how burglars enter a dwelling (Bossler & Holt, 2009). That is, like burglars utilising points of entry and concealing their traits from detection to access a dwelling, malicious software seeks to exploit system weaknesses or vulnerabilities as entry points and avoid (or disable) security measures (e.g. antivirus programmes) to access a device.

Online routine activities, such as proximity to motivated offenders, has been shown to predict malware victimisation as with other forms of cybercrime mentioned above. Yucedal's (2010) study revealed that individuals' participation in leisure online activities such as playing online games, downloading games, programs, and video or music files increased their victimisation risk of spyware in the US. Dutch studies also found that users' online behaviours were a significant predictor of malware victimisation, for which behaviours such as spending more time online, downloading, online gaming, surfing the web (both targeted and untargeted), online purchasing and webcam use enlarged chances of malware victimisation (Leukfeldt, 2015; van Wilsem, 2011). Research using a similar but more recent sample of adults in the Netherlands found similar findings. Further, contrary to Leukfeldt's (2015) prior argument that "*Internet users who visit all kinds of (legitimate) sites are at greater risk*" (Leukfeldt, 2015, p. 29), the research suggested that legitimate uses of internet like searching for information online and reading social media messages were not strongly associated with greater risks of malware victimisation (Holt et al., 2020).

These correlations might be explained as a result of proximity to motivated offenders. However, it is noticeable that some researchers have explicitly suggested that, unlike other types of online victimisation, malware victimisation depends on proximity to *malware* rather than to offenders (Bossler & Holt, 2009; Holt & Bossler, 2013). In this sense, cyber deviance such as pirating media or viewing pornography can increase an individual's proximity to malware due to their frequent behaviours of downloading and opening suspect files (Bossler & Holt, 2009; Choi, 2008). This argument implies that the deviance itself may not directly increase the risk of victimisation, yet the behaviour of downloading and opening suspect files does. Vulnerability thus depends more on proximity to malware than to proximity to motivated offenders, causing downloading files (either via email or websites) to be constantly more risky than passive web surfing. This complies with Holt et al.'s (2020) findings.

Surprisingly, evidence on the effectiveness of physical guardianship (e.g. virus-scanner) against malware infection is mixed. Choi's (2008) study using a sample of students from a university in Pennsylvania, suggested that computer security software (i.e. antivirus software, firewall, and antispyware software) functioned as capable guardians in the digital world whereas other more recent studies have found no statistically significant effect of such software on levels of victimisation (Bossler & Holt, 2009; Leukfeldt, 2015;

Ngo & Paternoster, 2011). The latter researchers have pointed out a common problem with many such security measures as they are merely able to detect known variants but not new variants (most common by means of files). They cannot prevent cybercriminals from exploiting an unknown flaw in the software. However, one thing to note is that those studies have not included the installation time of security software as a reference. As I have mentioned in Chapter 4 (Section 4.1.2), failure to identify the installation time of security devices may give rise to a false positive relationship between victimisation and the presence of security measures due to the reactive protective measures taken by the victims following their victimisation. The mixed effectiveness of security measures against malware infection might thus be moderated by issues of time ordering, yet this argument remains debatable given the limited evidence.

6.1.2.5 Situational crime approach to cyberspace

As described in Chapter 2, the LRAA has implications for preventing crime. If crime occurs when key elements converge, preventing that convergence will lead to crime reductions. To this end, cybercrime researchers informed by the LRAA have suggested that there is great utility in devising situational strategies (i.e. increasing the effort, increasing the risks, reducing rewards, reducing provocations and removing excuses) in cyberspace (e.g. Hinduja & Kooi, 2013; Reyns, 2010; Stockman, 2014). Examples of increasing the effort may include the use of target hardening techniques such as enhanced and up-to-date computer security (Choi, 2008) and improving access control via frequent password changes and multifactor authentication to access devices (Anandarajan & Malik, 2018), thereby making it more difficult for online offenders to access potential victims. Similarly, reducing provocations (e.g. reducing peer pressure and imitation) might be used to make the recruitment of money mules more difficult, given that evidence reveals that social ties and peer pressure are important factors (Leukfeldt & Kleemans, 2020). More examples of how SCP techniques apply to cybercrime prevention can be found in Section 2.2.3.2.

6.2 The current study

It is encouraging that in recent years there has been an increasing number of studies investigating online victimisation patterns in non-western contexts, including India, Turkey, Singapore, Japan, and South Korea (Ang & Goh, 2010; Aoyama et al., 2012; Aricak et al., 2008; Kalia & Aleem, 2017; Tippett & Kwak, 2012; Topçu et al., 2008). However, research on cybercrime victimisation is disproportionately centred on cyber abuse, or more specifically on ‘cyberbullying’, with an attendant focus on the experiences of young people, which may not be representative of the population of internet users more generally (Marcum et al., 2010; Yar & Steinmetz, 2019). As Ngo and Paternoster (2011) have suggested, simply being online may not be inherently risky; the risk depends on what someone is doing when online. Activities that involve active interaction with others (e.g. participation in online forums) might lead to a higher level of risk in terms of cyber abuse, in comparison with some passive activities that typically do not involve interaction with others (e.g. watching YouTube videos or downloading files), whereas downloading might cause other risks such as malware infection. In sum, there is a scarcity of research which considers the relationship between different online activities and different types of cybercrime.

The purpose of this study is to examine whether the LRAA can help understand online victimisation in Taiwan. This study is important for several reasons. First, to my knowledge, this is the first attempt to examine general cyber victimisation patterns in Taiwan. Second, there is a gap in the literature that attempts to explain patterns of online victimisation in an Asian context, especially utilising a theoretical basis. Third, there is presently an imbalance in the cybercrime literature, which is heavily oriented towards studies focussing on cyberbullying (or cyber abuse) and less so other types of online victimisation. Fourth, the representative dataset used here overcomes the concerns about some previous studies that makes use of data collected from convenience samples, mainly university students. The data analysed here is derived from a large and nationally representative sample. Lastly, by gaining an improved and theoretically-informed understanding of the patterns of different types of cybercrime victimisation, policymakers, and practitioners can better develop strategies to address specific types of cybercrime.

Two research questions are considered here: (1) does the LRAA adequately explain patterns of online victimisation in Taiwan? And (2) do victimisation patterns vary across different types of online victimisation in Taiwan?

Derived from these two research questions are five specific hypotheses which are tested in this study:

- H1.a.: Individuals who are more exposed to risk, are more attractive as targets to offenders and are not protected by capable guardians are more likely to be victims of online verbal abuse
- H1.b: Individuals who are more exposed to risk, are more attractive as targets to offenders and are not protected by capable guardians are more likely to be victims of data breach/identity theft
- H1.c: Individuals who are more exposed to risk, are more attractive as targets to offenders and are not protected by capable guardians are more likely to be victims of fraud
- H1.d: Individuals who are more exposed to risk, are more attractive as targets to offenders and are not protected by capable guardians are more likely to be victims of virus infection
- H2: The predictor variables that explain the risk of victimisation are different for types of cybercrime – verbal abuse, virus infection, identity theft, and fraud.

6.3 Data and measures

The following sections describe the data – the DOSIH – and variables to be used in this study.

6.3.1 Data

The data used in this chapter come from the DOSIH conducted in 2017. Briefly, the DOSIH used a stratified random sampling method to collect data from a representative sample of 9,337 citizens aged 12 years old and above in Taiwan, with the utilisation of CATI. The surveys were primarily designed to understand generational and regional inequalities in accessing the internet and computer devices rather than cybercrime victimisation. To my knowledge, no research has been done on cybercrime victimisation using these data at the time of writing. Full details of the data used here were given in Chapter 3 (Section 3.2.2.2).

Researchers have mentioned that without the internet, cybercrime could and would not exist (Yar & Steinmetz, 2019). Therefore, it makes sense that only those with internet access should be recruited as research targets in terms of cybercrime. After eliminating those survey respondents without internet access, the sample used in this study dropped moderately by over a quarter to 6,806 participants.

6.3.2 Measures

The dependent variables here include four types of self-reported cybercrime victimisation. The independent variables draw on the key theoretical concepts associated with the LRAA as they relate to the online environment. Below are descriptions of those variables.

6.3.2.1 Dependent variables

There were four dependent variables used in this study, with each representing a specific type of online victimisation: verbal abuse, identity theft (and/or data breach), fraud, and virus infection.

The first item used to capture respondents' experience of verbal abuse was "*During the past year, have you suffered any online verbal attack?*" Verbal attack ("*yanlun gongji*") in the context of the survey, was close to the concept of online bullying described above albeit not limited to repeated harm. Regardless of whether the attack came from one or multiple perpetrators, repetition of the attack is required in both online and offline definitions of bullying (Brown et al., 2014; Reyns et al., 2011; Vakhitova et al., 2016). Due to the lack of mentioning repetition in the question, it was not appropriate to use the term online bullying in this study. With respect to the wording of the question and ambiguity in cyber abuse mentioned above, the first type of cybercrime victimisation used in this study was hence described as 'verbal abuse'.

The second survey item was "*During the past year, have you suffered personal information leakage (e.g. credit card/phone number) or account theft because of internet use?*", which referred to the concept of a data breach and identity theft. The third item measured online fraud, in which the question "*During the past year, have you suffered fraud because of internet use?"* was used. The last type of victimisation was virus infection, measured by the item: *"During the past year, have your PC or phone contaminated with a virus because of internet use?"* All the dependent variables used in this study were dichotomously coded as 1 representing experience of a certain type of online victimisation over the past year and 0 for no experience. It is noted that, unlike the TAVS data analysed in the previous two chapters, the total number of victimisations experienced by survey respondents in the past year was not measured in the DOSIH. I will cover this issue in the limitations section further on.

6.3.2.2 Demographic controls

Based on research that suggested participation in online routine activities is a function of age and gender (Pratt et al., 2010), several individual characteristics items extracted from the DOSIH were entered as covariates in the analysis presented here. These included gender, age, education, and employment[4]. Firstly, I expected gender as an intermediate risk factor to alter participants' online lifestyle- routines to cybercrime victimisation, for which males might be more prone to engage in verbal abuse and risky online activities than females (Kalia & Aleem, 2017). For other demographic control variables: age was extracted from the item measuring participants' age, ordinally with "1" representing people aged 12 to 14 years old, "2" for people aged 15 to 19 years old, "3" for 20 to 29 years old, correspondingly to "6" for 50 to 59 years old, "7" for 60 and 64 years old, and "8" to people aged 65 years old and older. The other item asking participants' year of birth was not used due to a huge portion of missing responses (near 20 percent). The classification of age was not ordinally optimal; yet it was the most applicable item that could be used in this study. The assumed direction for age was that young people might be more likely to suffer verbal abuse whilst the direction remained open to other types of victimisations, reflecting the dominant findings in the research literature (Duggan, 2017; Holt et al., 2020; Reyns, 2013; van Wilsem, 2013a).

The third demographic variable – university – referred to people with a higher education degree (say university or postgraduate degrees), for which it was hypothesised here that a higher likelihood of victimisation (particularly with regard to cybercrime against property) would be observed in better-educated groups. This was based on the assumption that they might be more likely to spend more time online and more likely involved in retrieving interesting commercial offers, as has been proposed in prior studies (van Wilsem, 2013a). The last demographic variable was employment, which referred to participants' employment status. Those unemployed was used here as the baseline for those who were students and employed. Students were believed to be more likely to suffer fraud and identity theft as it was hypothesised that they are more likely to share (more) personal information on social networking sites (Leukfeldt, 2014; van Wilsem, 2013a).

[4] Income was dropped from the models. The reason was detailed in 6.4. Analytical approach - Logistic regression

6.3.2.3 Exposure/proximity to risk independent variables

Exposure to risk and proximity to cyber offenders might overlap and not be completely separate (Vakhitova et al., 2019). The main difference may lie in the domain to which a user enters. In the case of cyberbullying, for example, users performing online activities in their own domain (e.g. posting on the personal Facebook page) have exposure to cyber risk whereas entering someone else's domain (e.g. other's Facebook pages) may lead to greater proximity to potential cyber offenders. Yet the boundary of the domain is not always clear and may not make sense for other types of online victimisation. Hence, this study did not distinguish between the online activities associated with proximity or exposure to potential offenders but categorised them into exposure/proximity to risk.

The measure of exposure and proximity to risk was operationalised by two sets of items: general internet use and types of online activities.

General internet use

Given that the survey did not contain the exact time that participants spent on the internet, general internet use was operationalised here via the number of activities that one reported having participated in online. The ordinal number of activities was treated as a measure of participants' diversity in online routine activities, for which higher scores indicated more general internet and thus were hypothesised to be associated with greater exposure to risk/motivated offenders, as has been suggested by previous research (Hinduja & Patchin, 2008; Marcum et al., 2010).

Types of online activities

The second operationalisation of exposure and proximity to risk contained six types of online activities: (1) searching information (Info search); (2) instant messaging (MG via social media); (3) watching online videos; (4) gaming; (5) posting on Facebook; and (6) online purchasing. The questions were:

(1) *"During the past year, have you searched new information needed on the internet (all kinds of information are included)? How about the frequency?"*

(2) *"During the past year, have you used any instant messaging applications or social media, say Line, Facebook for instance? How about the frequency?"*

(3) *"During the past year, have you used the internet to participate in activities related to music and video such as watching a video or listening to music? How about the frequency?"*

(4) *"During the past year, have you played online games or mobile games? How about the frequency?"*

(5) *"During the past year, have you posted articles, photos or videos on Facebook or blog? How about the frequency?"*

(6) *"During the past year, have you made any online purchase, either on your own or group buying? How about the frequency?"*

The responses to these questions were recoded inversely to the original dataset, with "0" referring to "no use", "1" as "less than once a month", "2" as "at least once a month", "3" as "at least once a week", "4" as "once a day", and "5" as "several times a day". As proposed by the LRAA, increased participation in certain online activities is expected to be associated with greater opportunities for potential targets to meet potential offenders on the virtual network (Bossler & Holt, 2009; Marcum et al., 2010); and therefore, I assumed positive relationships between frequencies of online activities and a higher risk of online victimisation. However, it was argued that the activities that predict risk might differ for different types of online victimisation, as found in the literature mentioned above.

Online activities as exposure/proximity or target suitability

Notably, some researchers have operationalised online routine activities as target visibility under the RAA framework, dividing the online activities into low-level visibility (e.g. e-mail, targeted browsing and online messaging) or high-level visibility (e.g. untargeted browsing, online chat rooms, and online gaming) (e.g. Leukfeldt, 2015). Although some conceptions were transportable to the LRAA, the current study suggests a clarification between target suitability and exposure/proximity to risk. Exposure/proximity would refer to lifestyle-routines (i.e. active participation in online behaviours) that introduced the opportunity for the convergence of offenders and targets whereas target suitability is more like some 'passive' characteristics of the users (or habits of internet use) that make them valuable, visible, or accessible to the offenders (i.e. acronym of VIVA as detailed in later sections). There is no right and wrong here as this terminology might derive from the application of RAA or LRAA.

6.3.2.4 Target attractiveness/vulnerability independent variables

According to Cohen and Felson (1979), target suitability is subject to an individual's availability as a victim, as well as his or her attractiveness to the offender. Researchers have suggested four elements that determine the extent to which a victim is attractive to a motivated offender: value, inertia, visibility, and accessibility (VIVA) (Felson & Clarke, 1998). In terrestrial research, target attractiveness has been operationalised by material desirability such as family income, social class, or ownership of expensive and portable goods. Nevertheless, considering the specifics of the online context and the way in which offenders meet victims as distinguished from the offline world, translating this concept to the new environment of cyberspace might be a challenge. For example, inertia may refer to the size of digital files; however, it is difficult to be transported to the virtual environment (Leukfeldt & Yar, 2016; Yar, 2005). Further, given that the aforementioned traditional variables of material desirability were found to have no consistent associations with the risk of cyber victimisation across the literature (Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011), the operationalisation of target attractiveness requires refinement and modification with more focus on a redefined target value, visibility, and accessibility.

The variables under the concept of target attractiveness/vulnerability (or say suitability) in this study included aggressive posting, disability, Wi-Fi use, and the mobility of internet access. As cybercrime can be categorised into two aspects – 'crime against property' and 'crime against the person', most of the variables used here would have two different implications in terms of target attractiveness, which would be given as below.

Aggressive posting

Aggressive posting to capture target suitability (i.e. activities that make the student more attractive to motivated offenders) can be viewed as a target value to potential verbal abusers as they would be more likely to respond to the aggressive posting whereas, for other types of crime against property, it is more like increased target visibility. The item used was *"Compared to yourself in the real world, how do you perceive yourself when posting online?"* People who perceived themselves as "more aggressive" were coded as "1", here denoting aggressive posting.

Disability

Research has found individuals with either physical or mental disabilities, suffer a higher risk of online victimisation[5] (Rose et al., 2015; Sourander et

[5] Otherwise in the offline context, research has also suggested an increased risk of both personal and property victimisation among people with a physical disability (Mueller-Johnson et al., 2014) and mental or intellectual disability (Fogden et al., 2016; Hughes et al., 2012; Nixon et al., 2017; Silver et al., 2005; Tsigebrhan et al., 2014; Wilson et al., 1996; Wilson & Brewer, 1992). An additional example could be found in the fact that people with intellectual disabilities are commonly abused by their carers (Petersilia, 2001). Such an opportunity complies with the LRAA, which suggests target accessibility/availability in the

al., 2010). Wilson et al. (1996) have suggested that the higher risk might be due to the nature of their disability, meaning that an impaired person would probably be less adaptable to everyday circumstances or potential offenders might see more (and easier) opportunities to take advantage and exploit that person. A systematic review including ten primary studies on the correlation between cyber victimisation and people living with chronic conditions or disabilities found a consistently higher risk of victimisation among the population with chronic conditions and disabilities (Alhaboby et al., 2019). The relationship is more profound especially in terms of bullying, in which studies have suggested a higher risk of offline and online bullying victimisation among people with disabilities (Beckman et al., 2020; Didden et al., 2009; Kowalski et al., 2016; Rose et al., 2011; Schroeder et al., 2014; Sourander et al., 2010).

A disability may have two different aspects in terms of target attractiveness for cyber victimisation. For verbal abusers, people with disabilities might be a target with value whereas, in other forms of crime against property (i.e. fraud, identity theft, and virus), disability might mean greater accessibility to potential offenders. Disability was measured in the survey data by respondents' self-reported disability – *"Do you or your family have a disability identification?"*. Note that this item included both physical and mental disability. Respondents who were disabled or both respondents and their family members who were disabled were coded as "1". Respondents who were not disabled or those who were not disabled yet had a family member with disability were coded as "0" as family impairment did not exactly reflect targets' appeals to offenders.

victims' living environment, absence of a capable guardian (less protection if the guardians are perpetrators themselves), exposure to risk and proximity to potential offenders (conflicts due to carer stress or provocative incidents) (Fogden et al., 2016).

Wi-Fi use

The third variable of target attractiveness is Wi-Fi use. The security vulnerability arises when connecting to a poorly secured Wi-Fi network. Users fall prey to cybercriminals who can illegally gain access to their personal information and devices. One may argue that Wi-Fi use also relates to the exposure concept as potential offenders may be more likely to prey on targets using public (less secure) Wi-Fi connections. The reason that this chapter constructs Wi-Fi use under the concept of target attractiveness/vulnerability rather than exposure is because target attractiveness/vulnerability refers to how visible a target is online whereas the exposure concept is about what a target does online (Näsi et al., 2021).

With respect to its nature, Wi-Fi use might increase a targets' visibility or accessibility in terms of crime against property (e.g. identity theft and virus infection) whereas the impact of using Wi-Fi might be less obvious in terms of online bullying. Whilst several antivirus companies, including Norton and Kaspersky, having warned about the risk of using public Wi-Fi (AO Kaspersky Lab, 2020; NortonLifeLock Inc., 2020), one thing to note is that the item *"Have you used wireless internet connection?"* used in this analysis did not specify if the connection was a public or home Wi-Fi. However, this was the most appropriate item that could be used as a measure of targets' attractiveness. In line with Holt et al.'s (2020) finding that a secured wireless connection decreased the risk of malware victimisation, the risk of Wi-Fi use was expected to be a positive predictor of cybercrime against property yet its influence on verbal abuse to be open.

Mobility of internet access

Lastly, the mobility of internet access used in this study is referred to as participants' most frequent use of certain devices that have an unrestricted connection to the internet beyond a fixed place (e.g. laptops, tablets, and smartphones)[6]. Such mobility of internet access was expected to increase users' visibility and accessibility to potential offenders as they could access the internet anytime and anywhere. This variable might blur its boundary with guardianship in the context of cyber abuse as internet use outside their main residence may imply a lack of capable guardians (e.g. parents) present (Marcum et al., 2010). Again, the classification between target, guardianship, exposure and proximity embedded in LRAA is not clear cut. There are some overlaps between these elements so that there is no right and wrong way to classify a risk factor under an element. Overall, this study assumed a higher risk of online victimisation observed among people who access the internet more often and in more locations using multiple devices.

6.3.2.5 Guardianship independent variables

Reynald et al. (2018) have argued that there are differences in the conception of guardianship in the RAA and the LRAA, in which the former is explicitly limited to 'persons' who can provide supervision, and therefore target-hardening objects and informal social control are excluded. The latter holds a more relaxed perspective toward guardianship as any person and/or object that may function in ways that make crime less likely. In this vein, according to the LRAA, guardianship in cyberspace might refer to both persons (e.g. law enforcement officers, parents, or family members) or objects (e.g. antivirus software, firewall software, family safety tool services, and apps) that make cybercrime less likely. The form of guardianship may vary according to different types of cybercrime. For example, guardianship against virus infection might be the installation of antivirus software or firewalls while parental supervision might act as a form of guardianship against cyber abuse.

[6] In terms of time use, which device below is used most to access the internet? (1) desktop (2) laptop (3)tablet (4)smartphone (5)TV (6) wearable devices (e.g. watch, hear rate monitor, smart glasses, virtual reality devices) (7)smart home appliance (Chromecast, google home, amazon echo) (96)other______(specify) (97)none of these (98) refuse to answer

Like their offline study counterparts, previous studies have used multiple items to measure online guardianship. These include persons (e.g. supervision, restriction, or monitoring from parents, family, or teachers) and forms of software (blocking or filtering software, antivirus software) (e.g. Marcum et al., 2010). This study adopted a classification summarised by Vakhitova et al. (2016), by which physical guardianship denoted protective computer software against computer criminals (e.g., antivirus, anti-spyware, firewall programs, system updates), personal guardianship denoted respondents' skill levels with computers and technology (Ngo & Paternoster, 2011), and additionally, social guardianship denoted capable supervision from others such as peer deviance assessment (as negative proxy see Bossler & Holt, 2009; Reyns et al., 2011), presence of others while using a computer, and parent/guardian monitoring the use of their child's computer (Marcum et al., 2010).

There were not many items available in the DOSIH to be utilised as measures of guardianship. The variables included are live-in family and programming ability.

Live-in family

The most relevant individual-level variable to be used in this study is the number of family living in the same residence, with the logic being that more live-in family members, all things equal, might provide a higher level of supervision on participants' online activities. This logic is in line with Marcum et al. (2010), who found that a 'parent/guardian monitoring the use of a computer' was negatively related to the risk of adolescent victimisation. Noticeably, more recent research suggested that 'live-in guardians' might not discourage students' cyber-harassment victimisation in real-time as internet use is often solitary and a measure of the live-in family members cannot therefore accurately reflect if internet/computer users and their guardians stay in the same room (Reyns et al., 2016).

Programming ability

The second measure of guardianship used here relates to participants' programming ability measured by the question *"Have you learned programming or can you command any programming language?"* As mentioned, researchers have regarded computer knowledge and skills as a form of personal guardianship, or specifically a protective factor against target accessibility and by extension victimisation (Leukfeldt, 2014; Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011; Vakhitova et al., 2016). It is assumed that a higher level of computer literacy represents a higher level of security and risk awareness online. In line with this rationale, studies have found that victims' risk awareness positively predicts actual risk assessment and therefore is negatively linked to online victimisation (Choi, 2008; Marcum, 2008). This study thus would expect participants' programming ability to be a form of guardianship, thereby showing a negative relationship with cybercrime victimisation.

6.3.2.6 Environmental independent variables

Environmental variables included here are measures of urbanisation, internet penetration, and the role of the government as a 'super controller'. These variables were regarded as proxies of guardianship and examined at two community levels – the district-level and city-level.

Urbanisation and internet penetration

High internet penetration may act as a proxy for more secure infrastructure and hence was used here as an indirect measure of district/city-level guardianship. This was supported by a comparative study that found a significantly negative association between levels of country internet penetration and identity theft victimisation (M. L. Williams, 2016). Urbanisation and internet penetration were thus entered into the statistical models developed here as environmental factors associated with cyber victimisation. I used respondents' household locations for measuring urbanisation by district level, using the same process as that described in Chapter 4 (Section 4.3.2). Yet, with regard to urbanisation by city-level, I alternatively classified it as those located in the six municipals in Taiwan. Internet penetration was retrieved by the number of people with access to the internet by district/city from the original sample of 9,337 respondents. Despite the fact that a higher penetration rate may also increase the pool of potential victims on the network, based on the literature I assumed that urbanisation and higher levels of district/city internet penetration would reduce the risk of online victimisation.

The role of the government as a 'super controller'

Lastly, the role of government as a super controller was inspired by the arguments about governments' supervision over media and internet-based service providers to combat internet crime (R. Sampson et al., 2010; Vakhitova et al., 2016). This was measured through the question *"During the past year, have you received any information actively provided by the government, e.g. disaster alert or electronic newspaper? How about the frequency?"* The frequencies were retrieved from the original sample of 9,337 respondents and aggregated by district and city level, respectively. The role of government as a super controller (variable named as government notification coverage) was an exploratory variable. Despite the fact that the above survey question was not limited to public alerts of cybersecurity, I assumed that a higher level of coverage and governmental supervision would be associated with a lower level of online victimisation.

6.4 Analytical approach – Logistic regression

The reason for using (multilevel) logistic regression was covered in Chapter 4 (i.e. burglary chapter). The same rationale applies in this chapter. The dependent variables used herein included four types of cybercrime victimisation – verbal abuse (bullying), virus, fraud, and identity theft. All were coded as binary variables. Embedded in the opportunity framework, the independent variables consisted of (a) demographic variables; (b) variables related to all online activities that could be constructed as proximity to potential offenders/exposure to risk; (c) target attractiveness/vulnerability; (d) guardianship; and further (e) environmental factors. Table 6.1 presents the variable framework and descriptive statistics (I will return to this table later in the results section).

In multivariate analysis, a suppressor effect refers to the fact that the significance of some variables depends on the fact that another variable is controlled (Agresti & Finlay, 1997). To deal with such a suppressor effect, backward elimination is often used as the method of stepwise regression, whereby all possible variables are initially contained in the model. This approach reduces the risk of ruling out variables involved in suppressor effects (Menard, 2002). In line with backward elimination, sets of logistic regression analyses including all related variables (25) were conducted in the very beginning of the analyses reported here. Yet unlike my models for burglary victimisation, the postestimation (Box-Tidwell) showed that models for online victimisation might be over-parametrised. To reduce the risk of over-fitting and hence lack of precision, I followed the suggested stepwise modelling strategy (see Molitor et al., 2010; Peng & So, 2002), utilising p-values as the criterion for the variable selection process.

Nevertheless, the models were refitted by only keeping covariates with $p < .05$ for at least one type of victimisation in the earlier analyses, with a focus on the comparisons between types of victimisations and an additional concern that some variable might have influential power only if others were kept in the models. Moreover, as researchers have mentioned that the $p < .05$ criterion for retention of variables in the models might be too strict (Bendel & Afifi, 1977), I relaxed the $p < .05$ criterion to better reveal any possible statistically significant relationships. 'Searching information' and 'Gaming' were

Table 6.1 Concept framework and descriptive statistics drawn from the 2017 DOSIH, Taiwan

Variables	Obs.	%	Mean	SD	Min	Max
Dependent Variables						
Verbal abuse (1=yes)	218	3.20				
Info leak/ ID theft (1=yes)	715	10.51				
Online fraud (1=yes)	309	4.54				
Virus infection (1=yes)	946	13.90				
Demographic controls						
Age†			4.69	1.79	1.00	8.00
Male (1=yes)	3,282	48.22				
Uni (1=yes)	2,618	38.47				
Employment						
Unemployed(baseline)	1,757	25.82				
Employed	4,027	59.17				
Student	1,022	15.02				
Individual-level IV						
Exposure to risk/ Proximity to offenders						
Num. of online activity			7.16	2.98	0.00	14.00
Info search			2.75	1.71	0.00	5.00
MG via social media			4.52	1.13	0.00	5.00
Video watching			3.11	1.76	0.00	5.00
Gaming			1.76	2.08	0.00	5.00
Facebook posting			1.13	1.39	0.00	5.00
Purchasing			1.01	1.09	0.00	5.00
Target attractiveness/ vulnerability						
Aggressive posting	156	2.29				
Disability	175	2.57				
Wi-Fi use	5,863	86.14				
Mobile net access	5,623	82.62				
Guardianship						
Num. of live-in family			3.79	1.84	1.00	27.00
Programming ability (1=yes)	1,465	21.53				
District-level IV						
Urban (1=yes)	984	14.46				
Percentage of internet penetration			0.76	0.13	0.09	1.00
Gov. notification coverage			0.53	0.20	0.00	3.00
City-level IV						
Urban (1=yes)	1,934	28.42				
Percentage of internet penetration			0.74	0.08	0.58	0.87
Gov. notification coverage			0.51	0.08	0.36	0.71

Note 1. N = 6,806; District groups = 356; city groups = 22. 2. Obs. = observed frequency; Info search = searching information; MG = messaging; Gov. = government. 3. †Age is an ordinal variable coded participants' ages as 1 = 12-14 yrs., 2 = 15-19 yrs., 3 = 20-29 yrs., 4= 30-39 yrs., 5 = 40-49 yrs., 6 = 50-59 yrs., 7 = 60-64 yrs., 8 = 65 yrs. and over.

retained in the models concerning their effect sizes and the relaxed *p* criterion set at .10. The refined models consisted of 18 variables. The seven variables dropped from the model were income, online course, internet calling, search product review, e-banking, e-hospital appointment, the weighted factor of government website access.

Table 6.2 presents null, single-level and multilevel versions of estimated logistic regression models for the four types of cyber victimisation (a to d), in which goodness of fit would be detailed later in the findings section (6.5.1). Briefly, the likelihood ratio tests (LRT) for the models with all variables did not show any significant improvement from those with refined variables. Further, AIC and BIC values across all four types of cybercrime for the latter models were smaller than those for the former models (e.g. verbal abuse, $AIC_{Refined}$ - $AIC_{All\ var}$ = 1801.59 - 1809.60 = -8.01; $BIC_{Refined}$ - $BIC_{All\ var}$ = 1931.28 – 1987.06 = -55.78), suggesting that the refined single-level models were more appropriate for estimating cybercrime victimisation compared to models with all variables included (Akaike, 1974; Raftery, 1995).

Further, multicollinearity in single-level refined models was not significant, as VIFs were very small, with the largest being 3.23 and an average of 1.58 – lower than a value of ten which is generally regarded by researchers as signs of problematic multicollinearity (Wooldridge, 2012). An examination of outliers and influential cases using scatter plots of standardized residuals and Cook’s distance values did not indicate any outlier or influential cases. The analysis was run in Stata 15.

Table 6.2 Model statistics for null, single-level, and multilevel logistic models of cybercrime, 2017 DOSIH

a. Verbal abuse

	Single level				Multilevel			
	Null	Demo	Refined	All var	Refined	District	Refined	City
Log-lik.	-964.62	-949.74	-881.80	-878.80	-881.80	-880.34	-881.80	-880.75
AIC	1931.25	1911.48	1801.59	1809.60	1803.59	1806.69	1803.59	1807.50
BIC	1938.07	1952.43	1931.28	1987.06	1940.10	1963.68	1940.10	1964.49
LRT	-	29.77***	165.65***	6.00	-	2.90	-	2.09
n	6806	6806	6806	6806	6806	6806	6806	6806
Groups	-	-	-	-	356	356	22	22

b. Identity theft

	Single-level				Multilevel			
	Null	Demo	Refined	All var	Refined	District	Refined	City
Log-lik.	-2287.15	-2223.056	-2152.06	-2149.63	-2152.06	-2151.62	-2152.00	-2148.68
AIC	4576.30	4458.11	4342.12	4351.26	4344.12	4349.23	4344.00	4343.36
BIC	4583.12	4499.07	4471.81	4528.72	4480.63	4506.22	4480.51	4500.35
LRT	-	128.18***	270.17***	4.86	-	0.88	-	6.65
n	6806	6806	6806	6806	6806	6806	6806	6806
Groups	-	-	-	-	356	356	22	22

(continued)

Table 6.2 *(continued)*

c. Fraud

	Single-level				Multilevel			
	Null	Demo	Refined	All var	Refined	District	Refined	City
Log-lik.	-1257.37	-1225.732	-1192.55	-1189.09	-1192.55	-1191.34	-1192.55	-1190.27
AIC	2516.75	2463.46	2423.09	2430.19	2425.09	2428.68	2425.09	2426.54
BIC	2523.57	2504.42	2552.78	2607.65	2561.60	2585.66	2561.60	2583.53
LRT	-	63.28***	129.65***	6.90	-	2.43	-	4.55
n	6806	6806	6806	6806	6806	6806	6806	6806
Groups	-	-	-	-	356	356	22	22

d. Virus

	Single-level				Multilevel			
	Null	Demo	Refined	All var	Refined	District	Refined	City
Log-lik.	-2743.74	-2709.331	-2622.93	-2619.97	-2622.93	-2620.30	-2622.93	-2621.58
AIC	5489.47	5430.66	5283.85	5291.97	5285.85	5286.60	5285.85	5289.17
BIC	5496.30	5471.62	5413.54	5469.44	5422.36	5443.59	5422.36	5446.16
LRT	-	68.81***	241.62***	5.88	-	5.25	-	2.68
n	6806	6806	6806	6806	6806	6806	6806	6806
Groups	-	-	-	-	356	356	22	22

Note 1. ****p* < .001. 2. Log-lik.: Log-likelihood; LRT: likelihood ratio tests. 3. Degree of freedom for LRT: single-level models with only demographic variables (Demo) vs null: df = 5; single-level models with refined variables (Refined) vs null: df = 18; Refined vs single-level models with all variables (All var): df = 7; multilevel models with district/city level variables (District/City) vs Refined: df = 3. 4. The seven variables dropped from the model were income, online course, internet calling, search product review, e-banking, e-hospital appointment, the weighted factor of government website access. The three variables added to multilevel models are (1) urban; (2) government notification coverage by district and city; and (3) the percentage of internet penetration by district and city.

6.5 Results

Using data from the 2017 DOSIH, Table 6.1 shows that virus infection (about 14%) was the most common type of cybercrime experienced by respondents in the past year, followed by identity theft (about 11%), fraud (about 5%) and finally verbal abuse (about 3%). The table further suggests that internet users tended to be more involved in instant messaging via social media and video watching than other online activities. Meanwhile, Wi-Fi use and mobile internet access were highly prevalent among the DOSIH participants (both over 80%). Otherwise, environmental variables such as internet penetration and government notification were found to show little variation at either the district or city level.

Below I present findings by first comparing the results of statistical modelling, and then model interpretations by demographic controls and the LRAA for the four types of cyber victimisation.

6.5.1 Comparing statistical modelling results

Table 6.2 shows model statistics for the null, single level with demographic, refined and all variables, and multilevel versions of estimated logistic models. Multilevel models were random intercept models including fixed effects of individual-level and district/city-level. To make an equivalent number of groups comparable between models with refined and environmental variables, the multilevel refined models included only individual-level variables but allowed a fixed district/city level effect varying within groups. Hence, the Log-likelihood, AIC, and BIC values differed between the multilevel refined models and the single-level refined models that had no environmental effects. The goodness of fit was assessed using LRT. AIC and BIC values were given as a supplement, for which smaller numbers indicate better goodness of fit.

The LRT of single level models with all variables versus null models are not presented in Table 6.2. Yet, they were all statistically significant (*p*

< .001). The value for verbal abuse was 171.65, identity theft 275.04, fraud 136.56, and virus infection was 247.50. Single-level models across all four types of cybercrime were found to be significantly different than null models in terms of LRT, suggesting the appropriateness of using logistic regressions. Comparing the models, AIC and BIC values of single-level refined models were all smaller than their counterpart models of demographic controls and all original variables. Table 6.2. d. reveals the refined models in virus infection smaller values of AIC and BIC ($AIC_{Refined} – AIC_{Demo}$ = 5283.85 - 5430.66 = -146.81; $BIC_{Refined} – BIC_{Demo}$ = 5413.54 - 5471.62 = -58.08). It is a bit tricky to explain the goodness of fit for fraud (Table 6.2.c) as AIC and BIC represent different results ($AIC_{Refined} – AIC_{Demo}$ = 2423.09 - 2463.46 = -40.37; $BIC_{Refined}$ - BIC_{Demo} = 2552.78 – 2504.42 = 48.36). There have been arguments about which has been favoured in model fitting (see Dziak et al., 2012); however, the LRT presented in Table 6.2.c shows significant improvement with the LRAA variables included in the model (LRT = 66.37, *p* <.001). Hence, the results presented here indicate the single-level refined models fitting and better in predicting overall four types of cyber victimisation, compared to models with all variables or only demographic controls.

Conversely, all LRT statistics presented in the multilevel models show that multilevel models did not significantly improve fit when compared to single-level refined models. Further, AIC and BIC values for the single level refined models were found to be smaller than those in the multilevel models (either district or city) across all four types of cybercrime, suggesting that the single-level refined models were more appropriate for estimating cybercrime victimisation (Akaike, 1974; Raftery, 1995). The goodness of fit assessment presented here suggests the extent to which unobserved district/city characteristics (i.e. urbanisation, government notification coverage, and percentage of internet penetration) contributed to variations in online victimisation was not statistically influential.

6.5.2 Findings by demographic controls

Table 6.3 shows the extent to which demographic controls predict online victimisation. Several demographic controls were found to be statistically significant factors, with odds ratio (OR) greater than 1 revealing a greater risk of victimisation, and vice versa. Younger respondents were more likely to suffer verbal abuse and identity theft incidents, with one unit decrease in the age category leading to 16 percent (OR = 0.84, $p < .01$) and 18 percent (OR = 0.82, $p <.001$) increase in the likelihood of victimisation respectively, provided all other conditions being equal. Conversely, those targeted for virus infection tended to be older, with one unit increase in the age category leading to a 10 percent increase in the odds of virus infection victimisation (OR = 1.10, $p <.001$), holding other variables equal. Age did not provide statistically significant evidence for online fraud victimisation.

Gender was found to hold a statistically significant association for individual online victimisation yet the role differed across types of cybercrime. Male respondents were found to be at higher risk of verbal abuse (OR = 1.35, $p < .05$) and virus infection (OR = 1.41, $p < .001$) whilst females were found to be at higher risk of identity theft (OR = 0.81, $p < .05$) and online fraud (OR = 0.66, $p < .001$). The greatest risk deviation was amongst virus infection, in which males exhibited over 40 percent higher risk than their female counterparts, holding other conditions equal.

Those targeted for online victimisation tended to be better educated, except for verbal abuse where no statistically significant variation was observed. Those with a university or above degrees suffered an increased 68 percent (OR = 1.68, $p < .001$), 57 percent (OR = 1.57, $p < .001$) and five percent (OR = 1.05, $p < .01$) risk of identity theft, fraud and virus infection than those without a higher education degree, holding everything else equal.

Table 6.3 Demographic cyber victimisation using data drawn on the 2017 DOSIH, Taiwan

Variables	Verbal abuse			Identity theft			Online fraud			Virus infection		
	OR(S.E.)	95% C.I.		OR(S.E.)	95% C.I.		OR(S.E.)	95% C.I.		OR(S.E.)	95% C.I.	
Intercept	0.06(0.02)***	0.03	0.13	0.23(0.05)***	0.16	0.38	0.07(0.02)***	0.04	0.12	0.09(0.02)***	0.06	0.13
Age	0.84(0.05)**	0.75	0.94	0.82(0.03)***	0.77	0.87	0.92(0.04)	0.84	1.01	1.10(0.03)***	1.04	1.16
Male	1.35(0.19)*	1.03	1.78	0.81(0.07)*	0.69	0.96	0.66(0.08)***	0.52	0.83	1.41(0.10)***	1.22	1.62
Education-Uni	1.14(0.17)	0.86	1.52	1.68(0.14)***	1.42	1.98	1.57(0.19)***	1.23	1.99	1.05(0.08)**	0.91	1.22
Employment												
Unemployed(baseline)												
Employed	0.96(0.19)	0.65	1.41	1.18(0.13)	0.95	1.46	1.27(0.20)	0.94	1.72	0.98(0.09)	0.82	1.17
Student	1.03(0.32)	0.56	1.88	0.57(0.11)**	0.40	0.83	0.38(0.12)**	0.21	0.71	0.72(0.13)	0.51	1.03
LR/Wald chi2	135.88***			141.99***			66.37***			172.81***		

Note 1. n = 6,806. 2. * *p* < .05; ** *p* < .01; *** *p* < .001.

Table 6.4 Predictors of cyber victimisation using data drawn on the 2017 DOSIH, Taiwan

Variables	Verbal abuse			Identity theft			Online fraud			Virus infection		
	OR(S.E.)	95% C.I.		OR(S.E.)	95% C.I.		OR(S.E.)	95% C.I.		OR(S.E.)	95% C.I.	
Intercept	0.00(0.00)***	0.00	0.01	0.03(0.01)***	0.01	0.06	0.01(0.00)***	0.00	0.02	0.02(0.01)***	0.01	0.04
Age	1.02(0.07)	0.89	1.16	0.91(0.04)*	0.85	0.98	1.02(0.06)	0.91	1.13	1.22(0.04)***	1.14	1.30
Male	1.26(0.19)	0.94	1.70	0.90(0.08)	0.76	1.07	0.76(0.10)*	0.59	0.98	1.42(0.11)***	1.22	1.65
Education-Uni	0.75(0.12)	0.55	1.03	1.16(0.11)	0.97	1.39	1.13(0.15)	0.87	1.47	0.77(0.06)**	0.66	0.91
Employment												
Unemployed(baseline)												
Employed	0.86(0.17)	0.58	1.28	1.00(0.11)	0.80	1.24	1.11(0.18)	0.82	1.51	0.86(0.08)	0.72	1.04
Student	1.32(0.41)	0.72	2.44	0.68(0.13)*	0.47	1.00	0.51(0.16)*	0.28	0.96	0.78(0.14)	0.54	1.12
Individual-level variables												
Exposure to risk/ proximity to offenders												
Num. of online act.	1.08(0.04)*	1.00	1.18	1.15(0.03)***	1.10	1.20	1.14(0.04)***	1.07	1.22	1.12(0.02)***	1.08	1.17
Info search	1.04(0.06)	0.93	1.16	1.02(0.03)	0.96	1.09	0.95(0.04)	0.86	1.04	1.05(0.03)	1.00	1.11
MG via social media	1.09(0.11)	0.89	1.34	1.04(0.06)	0.94	1.16	1.14(0.10)	0.96	1.36	0.90(0.03)**	0.84	0.96
Video watching	1.11(0.06)	0.99	1.24	1.07(0.03)*	1.00	1.14	1.00(0.04)	0.92	1.09	1.08(0.03)**	1.03	1.14
Gaming	1.07(0.04)	0.99	1.15	0.98(0.02)	0.94	1.02	0.96(0.03)	0.91	1.02	0.98(0.02)	0.94	1.02
Facebook posting	1.29(0.07)***	1.17	1.43	1.05(0.03)	0.99	1.12	1.04(0.05)	0.94	1.13	0.97(0.03)	0.91	1.02
Purchasing	0.99(0.08)	0.85	1.15	1.05(0.05)	0.96	1.15	1.19(0.08)**	1.05	1.35	1.01(0.04)	0.93	1.10
Target attractiveness/ vulnerability												
Aggressive posting	3.83(0.97)***	2.34	6.29	1.19(0.28)	0.74	1.90	1.40(0.48)	0.72	2.73	2.37(0.44)***	1.65	3.42
Disability	2.39(0.84)*	1.20	4.75	1.21(0.33)	0.71	2.07	1.13(0.45)	0.52	2.46	1.49(0.30)*	1.00	2.20
Wi-Fi use	1.33(0.39)	0.75	2.35	1.08(0.16)	0.80	1.45	0.94(0.20)	0.62	1.41	1.39(0.17)**	1.09	1.77
Mobile net access	0.80(0.14)	0.56	1.14	1.01(0.11)	0.81	1.25	1.36(0.24)	0.96	1.91	0.80(0.07)*	0.67	0.95
Guardianship												
Live in family	1.04(0.04)	0.97	1.12	1.01(0.02)	0.97	1.06	0.98(0.03)	0.92	1.05	1.05(0.02)**	1.01	1.09
Programming ability	1.57(0.25)**	1.15	2.13	1.12(0.11)	0.92	1.35	1.14(0.16)	0.86	1.51	1.11(0.10)	0.93	1.33
LR/Wald chi2	165.65***			270.17***			129.65***			241.62***		

Note 1. n = 6,806. 2. * *p* < .05; ** *p* < .01; *** *p* < .001. 3. Num. of online act. = number of online activities; Info search = searching information online; MG = instant messaging

Employment did not show strong correlations with online victimisation. Compared to those respondents who were unemployed, respondents with employment did not suffer a statistically higher risk of online victimisation. Students experienced a reduced likelihood of victimisation for identity theft (OR = 0.57, $p < .01$) and online fraud (OR = 0.38, $p < .01$), compared to those who are unemployed.

6.5.3 Findings by lifestyle-routine activity approach

The final models predicting online victimisation are presented in Table 6.4. The effects of demographic characteristics on cyber victimisation changed when the LRAA concepts were introduced. Younger people still suffered a higher risk of identity theft yet no statistically significant variations were observed in relation to verbal abuse victimisation. For one unit decrease in the age category, the odds of identity theft victimisation increased by nine percent (OR = 0.91, $p < .05$), if every other element was equal. Those targeted for virus infection still tended to be older, yet with one unit increase in the age category leading to a 22 percent increase in the odds of virus infection victimisation (OR = 1.22, $p <.001$), holding other variables equal.

Gender did not provide statistical support for predicting verbal abuse and identity theft anymore. The predictions for the other two types of victimisations remained in a similar direction as without the LRAA variables. Females suffered an increase of 24 percent odds of fraud victimisation (OR = 0.76, $p < .05$) compared to their male counterparts, holding other elements equal. Conversely, males suffered an increased 42 percent likelihood of virus infection (OR = 1.42, $p < .001$) than their female counterparts, holding other elements equal.

Education showed the greatest change after LRAA variables were introduced into the models. It was now found to only significantly predict virus infection victimisation but not others. That is, when holding all other elements including LRAA concepts equal, those with higher education degrees contrarily suffered a reduced likelihood of virus infection (OR = 0.77,

$p < .01$). Figure 6.1 reveals the different tendency of using instant messaging by education, in which those with higher education degrees showed a higher level of participation. The link between this tendency and the reverse influence of education on virus infection is picked up in the discussion section.

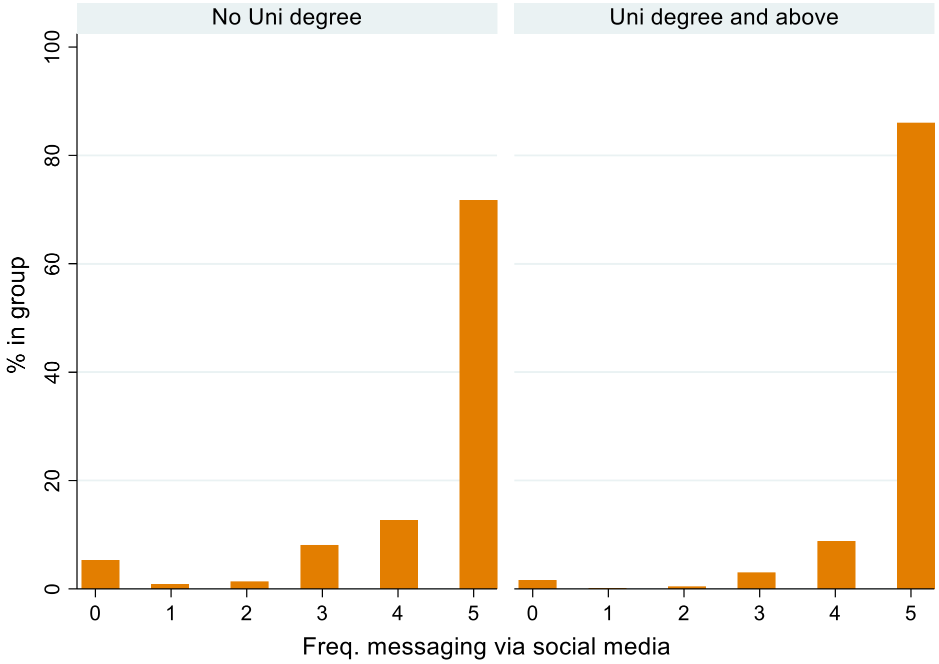


Figure 6.1 Percent of instant messaging tendency by participants' education

The impact of employment on online victimisation remained similar. Holding all other variables equal, respondents with employment did not suffer a statistically higher risk of online victimisation than their unemployed counterparts. Students still experienced a reduced likelihood of victimisation in identity theft (OR = 0.68, $p < .05$) and online fraud (OR = 0.51, $p < .05$), compared to those unemployed provided that everything else was equal.

The below sections presented the results by key concepts of the LRAA.

6.5.3.1 Proximity/ exposure to risk for cybercrime victimisation

The number of activities that a respondent participated in online remained a significant predictor of online victimisation. With one unit increase in online participation, the likelihood of victimisation increased by eight percent for verbal abuse (OR = 1.08, $p < .05$), 15 percent for identity theft (OR = 1.15, $p < .001$), 14 percent for fraud (OR = 1.14, $p < .001$), and 12 percent for virus infection (OR = 1.12, $p < .001$), provided everything else equal.

Respondents who watched online videos more frequently showed an increased risk of identity theft (OR = 1.07, $p < .05$) and virus infection (OR = 1.08, $p < .01$). With one unit increase in this activity, the odds of victimisation increased by seven and eight percent, respectively. Watching videos online did not statistically predict victimisation of verbal abuse or online fraud. The more frequently respondents posted articles, photos, or videos on Facebook or blogs, the higher their risk of verbal abuse (OR = 1.29, $p < .001$); yet no significant correlations were observed for other types of cyber victimisation. That is, one unit increase in the activity on Facebook or blog posting resulted in 29 percent increased odds of verbal abuse victimisation but for no other types of victimisations. Purchasing had a similarly unique effect on fraud victimisation alone. For those who participated in online purchasing more frequently, an increase of one unit increased the risk of fraud victimisation by 19 percent (OR = 1.19, $p < .01$) .

Noticeably, unlike activities presented above that showed a significant and positive relationship with certain types of victimisations, the more frequently respondents used instant messaging via social media, the less likely they would fall prey to virus infection (OR = 0.90, $p < .01$). Searching for information and gaming did not statistically predict online victimisation.

6.5.3.2 Target attractiveness/vulnerability for cybercrime victimisation

Self-reported tendency of aggressive posting was found to be a significant predictor of verbal abuse (OR = 3.83, *p* < .001) and virus infection (OR = 2.37, *p* < .001). Respondents with aggressive posting behaviours suffered an increased risk of victimisation by 280 percent and 130 percent, respectively, in verbal abuse and virus infection, compared to those without such behaviours when all other elements were held equal. Aggressive posting behaviours were not associated with identity theft and fraud.

Respondents with disabilities showed similar patterns of online victimisation. Those with self-reported disabilities experienced an increased risk of victimisation by about 140 percent and 50 percent respectively in verbal abuse (OR = 2.39, *p* < .05) and virus infection (OR = 1.49, *p* < .05), compared to those without such disabilities when all other elements were held equal. Disabilities were not a significant predictor of identity theft and fraud.

The use of Wi-Fi and mobility of internet access were found only significant in predicting virus infection, yet in the opposite direction. Although a positive predictor across all types of victimisations, respondents were only found to experience a statistically significant increase in virus infection by about 40 percent (OR = 1.39, *p* <.01) with the use of Wi-Fi connection. The mobility of internet access revealed a different picture. Users with devices that allowed them to access the internet everywhere were found less likely to suffer an incident of virus infection, for which a decreased likelihood of victimisation by 20 percent was observed in those with mobility of internet access (OR = 0.80, *p* <.05) compared to those without such mobility, holding everything equal. Likewise, the directions were consistent but not significant for the other three types of online victimisation.

6.5.3.3 Guardianship for cybercrime victimisation

The number of family members living in the same household as the respondents were found positively related to cyber victimisation; however, it was only statistically significant in virus infection. With a one-person increase in the households, the respondent's odds of receiving virus infection were increased by five percent (OR = 1.05, *p* <.01).

Respondents with programming skills were found positively related to cyber victimisation. Nevertheless, like the number of live-in families, it was only statistically significant in one type of victimisation – verbal abuse. Those with such computer skills experienced an increased risk of being verbally abused by over 50 percent compared to those without such skills (OR = 1.57, *p* <.01), provided everything equal.

6.5.4 Findings summarised by types of crime

Younger and male respondents suffered a higher risk of verbal abuse. However, after introducing LRAA variables, demographic characteristics were no longer significantly related to verbal abuse victimisation. The level of online participation and posting behaviours (say exposure to risk) and aggressive posting and disability (say target attractiveness), were found positively linked to verbal abuse victimisation. The impact of guardianship was not obvious in terms of preventing victimisation of verbal abuse. These findings partially supported the hypothesis "*H1.a.: Individuals who are more exposed to risk, are more attractive as targets to offenders and are not protected by capable guardians are more likely to be victims of online verbal abuse*"; however, evidence of guardianship remained weak with respect to verbal abuse.

In terms of identity theft, female and better-educated participants suffered a higher risk of victimisation, yet the impact was moderated when LRAA-variables were introduced. After LRAA-variables were taken into consideration, elderly and student respondents were less likely to suffer victimisation than their counterparts. The level of online participation and watching videos online, as exposure to risk, were found positively linked to identity theft victimisation. The effect of target attractiveness and guardianship was not found statistically significant. These findings partially supported the hypothesis "*H1.b: Individuals who are more exposed to risk, are more attractive as targets to offenders and are not protected by capable guardians are more likely to be victims of data breach/identity theft*", where online activities provided supportive evidence as risk factors yet target attractiveness and guardianship might lack sufficient support in the case of identity theft.

With respect to fraud, better-educated participants suffered a higher risk of fraud yet again the effect was found to be moderated by the LRAA variables. After such variables were introduced, male and student respondents remained less likely to experience online fraud. Similar to identity theft, only two risk exposure factors (i.e. the number of online activity and purchasing) were found positively linked to fraud victimisation. Likewise, the effect of target attractiveness and guardianship was not found to be statistically significant. These findings also provided partial support for the hypothesis "*H1.c: Individuals who are more exposed to risk, are more attractive as targets to offenders and are not protected by capable guardians are more likely to be victims of fraud*", where certain online activities could provide supportive evidence as risk factors, but the influence of target attractiveness and guardianship remained limited in explaining the victimisation pattern of online fraud.

Lastly, many predictors were found to be significant for virus infection, compared to other types of online victimisation. Better educated individuals suffered a higher risk of virus infection but became less vulnerable when LRAA variables were introduced, while elderly and male respondents remained more vulnerable than their counterparts. Briefly, those with higher education degrees, more frequent use of instant messaging, and having more internet access were found less likely to suffer virus infections. Conversely, respondents who were male, elderly, had more diversity in their online activity and frequent involvement in watching online videos (i.e. exposure to risk), had disabilities, self-reported aggressive posting tendency and use of Wi-Fi (i.e. target attractiveness) were more vulnerable to virus infection. The victimisation of virus infection seemed to provide more statistical evidence supporting the hypothesis "*H1.d: Individuals who are more exposed to risk, are more attractive as targets to offenders and are not protected by capable guardians are more likely to be victims of virus infection*". However, the concept of guardianship seemed to be contradictory in supporting H1.d, where a larger number of live-in family members was found significantly related to the risk of virus infection.

Notably, the aforementioned results further suggested that the predictor variables that explain the risk of victimisation seemed to be different for different types of cybercrime. However, as some types of victimisations shared the same risk factors, the evidence supporting *"H2: The predictor variables that explain the risk of victimisation are different from types of cybercrime – verbal abuse, virus infection, identity theft, and fraud."* remains debatable.

6.6 Discussion

This chapter sets out to examine systematically patterns of cybercrime victimisation in Taiwan, drawing on the LRAA to understand how online routine activities and the online environment itself provide opportunities for different types of crime to occur.

Using data from the 2017 DOSIH, cybercrime victimisation was found to be related to participants' demographic characteristics. Yet as the literature suggested, most of those effects were found to be moderated by online routine activities and lifestyles. For example, younger and male respondents were initially found more likely to be involved in verbal abuse incidents, yet such correlations became less obvious when taking into account their online routine behaviours. With regard to the impact of online routines on verbal abuse victimisation, the final analytical models produced here (see Table 6.4) reveals that a higher frequency of posting information on Facebook or blogs resulted in participants' higher risk of verbal abuse. This is because the posting behaviour might involve communicating with people online and sharing personal information which increased the likelihood of online victimisation. This finding is consistent with the literature, of which it is suggested that the intensity of social media use and online self-disclosures positively relate to individuals' cybercrime victimisation (Bossler & Holt, 2009; Hinduja & Patchin, 2008; Marcum, 2008; Marcum et al., 2010; Marttila et al., 2021; Mesch, 2009; Mitchell et al., 2007; Navarro & Jasinski, 2012; Reyns et al., 2011).

Below I discuss how the LRAA can be used to explain online victimisation in Taiwan.

6.6.1 Lifestyle-routine activity approach on explaining online victimisation

The finding of the aforementioned moderating effect was further in line with previous studies suggesting that users' demographic characteristics might not be the most important predictors in cyber victimisation compared to users' online routine activities (e.g. Kalia & Aleem, 2017). This provides support for the applicability of LRAA to an online context as individuals' online routine activities and lifestyle moderated and accounted for the risk of cyber victimisation (H1).

Further, in compliance with previous research (Holt et al., 2020), the aforementioned risk of verbal abuse derived from posting in social media did not raise the risk of other types of online victimisation. Likewise, online purchasing was significantly related to cyber fraud but no other types of victimisations. These 'risky' routine activities might increase participants' chances to meet specific and motivated offenders online (in the absence of capable guardians) and thus increase participants' risk of victimisation. This additionally supported the notion that specific crimes occur due to specific opportunity structures, as is a core plank of EC. The predictor variables that explain the risk of victimisation seemed to be different for different types of cybercrime (H2).

However, as some types of victimisations shared the same risk factors, the evidence supporting H2 remains debatable. For example, the diversity of online participation was a consistent risk factor for all four types of cybercrime. This was in line with previous findings, as the diversity could be regarded as a proxy of time that one spent online. It was predicted that the more diverse one's online activities, the greater his or her exposure/proximity to risk or potential offenders. Watching videos online was found to increase the likelihood of identity theft and virus infection. There might be a few reasons behind this. Firstly, watching online content might involve downloading software, plug-in applications or the video itself, for which the behaviour of downloading was found to be a risk factor for malware infection and identity theft (Holt et al., 2020; Holt & Bossler, 2013; Reyns, 2013; Yucedal, 2010). Further, although the survey did not ask by which means did the respondents watch a video, there might be some chance that some illicit avenues or pirate websites were involved, thereby increasing respondents' exposure to malicious software or say, potential offenders.

Additionally, a few types of cybercrime also shared target attractiveness/vulnerability in common. For example, aggressive posting tendency and disability, in line with theoretical assumptions, were found to be significant predictors of victimisation of verbal abuse and virus infection. The explanation might be different depending on the traits of crimes against person (here as verbal abuse) and property (virus infection). As mentioned above, aggressive posting might be regarded as a proxy for target value to verbal abusers whereas aggressive posting might denote increased visibility to virus attackers. Likewise, people with disabilities might be a target with value to verbal abusers whereas disability might make such individuals more accessible and thus vulnerable to potential offenders committing virus attacks.

Although some predictors were found in common across types of online victimisation, they did not follow a uniform pattern of online routine activity.

For example, the activity that caused the risk of verbal abuse (e.g. posting on Facebook) was way different from others. Similarly, the activity that caused the risk of fraud (e.g. purchasing) did not lead to the risk of other types of victimisations. Although some victimisation shared a few risk factors in common, it was too arbitrary to apply a specifically single form of online activity to explain the patterns and mechanisms of all kinds of online victimisation. Hence, the current findings do provide some evidence for H2 and suggest supports for RQ2 *"Do victimisation patterns vary across types of online victimisation?"*, meaning that there were still variations in different types of online victimisation based on the observed results.

Probably the most serious issue with the analyses reported here concerns the evidence relating to H1, which attempted to answer my research question of "*Does the LRAA apply to online victimisation in Taiwan?*" As mentioned above, the current evidence partially supports the notion that online routine activities play an important role in predicting individuals' online victimisation. However, the transposability of all of LRAA's concepts to the virtual context remains uncertain based on the current study. Limited evidence was found that target attractiveness was influential for identity theft and online fraud. Moreover, little evidence was found to support the function of guardianship in cyberspace. In fact, the directions of guardianship-related elements (i.e. number of live-in family and programming ability) were all positively related to online victimisation, in which the number of the live-in family was statistically significant to virus infection while programming ability to verbal abuse.

The explanation for the positive relationship between the number of live-in family members and virus infection might be the fact that more family members living in the same residence would lead to multiple uses of the same device as well as the same internet protocol address (i.e. IP), increasing the exposure to risk and thus the likelihood of virus infection. This explanation was in line with the direction of the mobility of internet access, which was also in the opposite direction as expected. Such a negative direction with virus infection implied that the mobility beyond residence might restrict the device to a single user which was a proxy against virus infection rather than target visibility/accessibility to potential offenders.

Such arguments reiterate questions about the transportability of guardianship to the online context, an issue mentioned in previous studies reviewed earlier. The research suggested that due to the private nature of computer use, the function of "live-in guardians" might not work in the immediate online environment and such a measure was unable to reflect if users stayed in the same room with their capable guardians (Reyns & Henson, 2016). In line with such an explanation, it was not surprising to find that the live-in family might not function well against all types of online victimisation.

In addition, programming ability, contrary to literature that suggested it was an aspect of guardianship (Leukfeldt & Yar, 2016) or a protective factor against target accessibility (Leukfeldt, 2014), was found to be a positive predictor of verbal abuse (or to other types of victimisations yet not statistically significant). This study argued that computer ability was more like an indirect proxy of exposure to risk given that this characteristic might leave targets sharing a similar lifestyle with the potential offenders (especially the crime against property which often requires advanced computer skills).

Given that the current and previous findings on online guardianship did not provide strong empirical support that it protects against online victimisation (Bossler et al., 2012; Holt & Bossler, 2008; Marcum et al., 2010; Ngo & Paternoster, 2011; Reyns et al., 2011), the current study questions the validity of using live-in family and computer ability as measures of online guardianship. Perhaps a more appropriate way to operationalise guardianship might be to use individuals' intensity of social networking (see Vakhitova et al., 2019). The suggested operationalisation is in line with the finding that the use of instant messaging via social media was a negative predictor of virus infection. The more intense the respondents used instant messaging, the less likely they would fall prey to virus infection. Likewise, better-educated respondents used to be vulnerable to virus infection but the likelihood of victimisation was moderated or even reversed when the frequency of instant messaging was taken into consideration as they appeared to be more involved in such means of social networking.

The use of social networking as a measure of social guardianship would have another benefit as parental supervision was found less effective due to their lack of knowledge of social networking sites and their children's online engagement. Several researchers have argued that parental guardianship had little effect in reducing cyber victimisation as originally suggested by the LRAA (Kalia & Aleem, 2017). Hence, until we can find better measures of online guardianship (e.g. respondents' social networking) on the evidence to date we must conclude that the LRAA does not provide a satisfactory explanation of cyber victimisation; the little evidence to date implies that guardianship functions differently online and offline.

Based on the current finding it appears that both the research questions can be only partially answered. On the one hand, the LRAA might apply to online victimisation in Taiwan, especially in terms of one's lifestyle-routine activities which played a more and consistent role in predicting certain types of cyber victimisation. Yet the concept of guardianship warrants more appropriate measures and some alternation distinct from traditional offline crime. On the other hand, victimisation patterns and mechanisms were found to vary across types of online victimisation, though some characteristics and routine activities (e.g. online participation, aggressive posting, or disability) led to a shared risk.

6.6.2 Practical insights drawn on findings

Practically speaking, findings about the effect of lifestyle-routine activities on cybercrime victimisation could inform crime prevention. For example, watching videos was found to be a positive risk factor for individuals' experience of identity theft and virus infection, thereby the responsibility of video website owners becomes critical. The owners' effort on providing a secure online environment may thus protect their users from these types of online victimisation. Further implications would have something to do with the behaviour of aggressive posting. Compared to other online activities/behaviours, self-reported tendency of aggressive posting was especially a highly risky behaviour given its effect size. As mentioned, respondents with aggressive posting behaviours suffered an increased risk of victimisation by over 280 percent and 130 percent respectively for verbal abuse and virus infection, compared to those without such behaviours when all other elements were held equal. This implies that prevention strategies like awareness campaigns aiming at reducing ones' aggressive posting behaviours might work against verbal abuse and virus infection at a strong level.

Similarly considering the effect size, the vulnerability of disabled internet users requires attention as those disabled experienced an increased risk of victimisation by about 140 percent in verbal abuse, compared to those without such disabilities when all other elements were held equal. To my best knowledge, there is no empirical evidence on what works to keep disabled people safe online. However, one may consider the application of SCP in the cyberspace (see Section 2.2.3.2 or Table 2.5), with a focus on the population with disabilities. For example, increasing the effort (target hardening e.g. awareness campaign, education, etc), increasing the risks (e.g. real-name registration system for online bullying prevention), reducing the rewards (e.g. shielding offensive posts), reducing provocations (e.g. shielding posts containing aggressive contents) and removing excuses (e.g. warning banners on website, warning violators, suspension or restricted access to network) might help in protecting those vulnerable from falling prey to verbal abuse.

Last but not least, the results also suggest that the main body of research participants in prior studies – young people or students – might have limitations as these participants might not be vulnerable to certain types of cybercrime. In fact, students were found significantly less likely to become victims of identity theft and cyber fraud, and no statistically significant association was found between age and cyber abuse and virus infection. The recruitment of students as research targets might therefore introduce bias, especially when previous studies have centred on cyberbullying among students and young people. The current study, using a more representative sample, is therefore expected to inform cybercrime prevention among wider populations (say like adults).

6.6.3 Unexplained environmental effects

The comparisons between single-level and multilevel models presented above revealed that the function of environmental factors in cyberspace might be different from what was found in an offline context (say, for burglary). No evidence in this study was found to support the impact of environmental factors on cybercrime victimisation in Taiwan. That is, government notification coverage might not significantly function as a super controller, and urbanisation and district/city internet penetration might not be a proxy of infrastructure to significantly indicate regional guardianship, either.

The interpretations might be the fact that the units used to measure environmental factor was not appropriate (too huge or too tiny). On the one hand, the immediate environment in terms of verbal abuse might be school, peer, or workplace, on which victimisation the district/city-level factors were far remotely to have an impact. On the other hand, for other types of cybercrime against property, the unit of district/city-level was too tiny to observe enough variations between groups. Research that found internet penetration as a proxy of higher-level guardianship was based on a country-level comparison (M. L. Williams, 2016), where the variations may vary significantly between countries. Given Taiwan is a small island, the level of urbanisation, infrastructure, or cybersecurity strategy would not vary as greatly as those between countries and therefore such environmental factors as regional level guardianships were not obvious in terms of online victimisation.

6.6.4 Limitations

The study shares the strengths and the limitations of most secondary data studies, as stated in Chapter 3 (3.2.3). The strengths are that the sample size and representativeness of the survey data are much greater than could have been achieved as a PhD student. Nevertheless, the limitation is that I had no say over the questions.

There were a few limitations in this study. The first relates to the measures of online victimisation, which used four single-items asking victims if they had any experience of verbal abuse or virus infection, etc. The responses were potentially biased (e.g. social desirability bias, recall problems, etc.) or might require a different level of awareness (e.g. most virus could conceal itself). Additionally, the wording about victimisation of identity theft introduced confounds, combining two concepts in one question. That is, there were actually two types of victimisations placed within the question "*During the past year, have you suffered personal information leakage (e.g. credit card/phone number) or account theft because of internet use?*". This made the examination of victimisation patterns more difficult as a specific crime might have a specific pattern and mechanism.

The second limitation concerns many basic yet important concepts missing in the DOSIH. First, there was no exact (or even approximate) time that one spent online, leading to the difficulty to examine the time-adjusted risk of online participation. Second, there was no information about users' participation in legitimate or deviant online behaviours. For example, watching video online did not specify if the users are accessing legal or pirate websites. The classification of the legitimacy of online activities might strengthen if there was any difference in exposure/proximity to the risk and potential offenders.

The third limitation relates to missed concepts in the DOSIH in that there were few items available to measure, say, guardianship. As mentioned above, the number of live-in family members did not fully reflect the level of guardianship. An additional question like if the respondents received supervision/monitoring when using the computer would help in better understanding guardians' real effect on online victimisation risk. Further, there were no items that could be operationalised as physical guardianship (e.g. firewalls, antivirus software), which led to the application of LRAA to cybercrime less comprehensive in the context of Taiwan. Most of the research to date has found that physical guardianship has no effect (see Holt et al., 2020); yet the effect of guardianship might be mediated by participants' reaction to online victimisation as earlier burglary research failed to identify if the timing of security measure installation (before or after burglary). Unfortunately, the DOSIH did not allow me to examine if physical guardianship influenced online victimisation, let alone the operationalisation as what I did in Chapter 4 – the timing of security in place. Social guardianship was also limited in this study as the DOSIH merely allowed the operationalisation of internet penetration and government notification (yet not limited to cybersecurity). The results suggest that such operations did not provide sufficient evidence to the LRAA and the role of government as a super controller (i.e. social guardianship from the government) required further precise measures.

Last but not least, missed concepts in the DOSIH are the lack of information about respondents' offline lifestyle routines. Previous research suggests that offline context might affect online victimisation as they might share similar characteristics (Bossler & Holt, 2009; van Wilsem, 2011). Further offline information might include environmental factors, such as perceptions of community climate and perceptions of safety, employment setting (workplace stressors), and community setting (culture diversity, etc.). The lack of such information made the link between online and offline victimisation unclear. More importantly, this led to the scarcity in guardianship measure (e.g. deviant peer as social guardianship) and environmental factors as mentioned above. Overall, the lack of proper measures of online victimisation, time of internet use, guardianship and offline lifestyle-routines in the DOSIH limited the examination of LRAA to some extent.

The last limitation is not about the DOSIH itself but the issue with model comparisons. Poor goodness of fit scores with multilevel models limited the examination of cross-level interactions as I did in Chapter 4. While comparative studies have observed a higher risk of online victimisation among the richer countries, they have also revealed a significant cross-level interaction between individual wealth and victimisation that moderates the regional effects. That is, respondents with low status yet living in richer countries were found to suffer a significantly higher risk of victimisation, compared to their equivalent living in poorer countries (M. L. Williams, 2016). Their findings shed light on whom to protect via examining users' offline and online characteristics. However, the poor fit of multilevel models made the identification of the most vulnerable population more challenging.

6.7 Chapter conclusion

In conclusion, this chapter has applied multiple logistic regressions to identity whether the LRAA is transportable to online victimisation in Taiwan and whether victimisation patterns vary across types of online victimisation. The findings supported the notion that different types of victimisations might have different patterns and different underlying causal mechanisms. Certain activities and user characteristics might require additional caution as they raise a shared risk of victimisation while some activities remain a specific risk factor to a specific crime. Online routine activities also moderate the impact of demographic differences in online victimisation in Taiwan and therefore the focus of crime prevention should shift to routine activities rather than certain demographic groups.

Overall, the findings provide partial support for the application of LRAA to cyberspace in Taiwan. However, the effect of guardianship was found to be limited. The application of SCP to online victimisation may thus need some reconsideration as there was little evidence for the effectiveness of personal and social guardianship as currently operationalised. Note that this study should not be taken as invalidating the role of guardianship in protecting against online victimisation in Taiwan. The effectiveness of physical guardianship is unclear due to the lack of operationalisation. The study therefore highlights that it is necessary to include physical guardianship, along with the timing of installation/update of such protective measures necessary to the future surveys. Furthermore, it is also vital to include items related to social guardianship and offline information. The operationalisation of social guardianship (e.g. immediate supervision, social networking) and the offline environment is critical to better understand the transportability of LRAA from an offline to an online context. In this way, more practical prevention strategies can be informed.

Chapter 7 Cybercrime Poly-victimisation

The previous chapter explored the differences between victims and non-victims of cybercrime in Taiwan. This chapter examines if there are any differences in those individuals who experienced a single form of cybercrime versus those who experienced multiple different kinds of cybercrime, defined here as poly-victimisation. Based on the findings reported in previous chapters that applied the lifestyle-routine activity approach to cybercrime, two additional research questions are to be answered in this chapter: (1) is there evidence of online poly-victimisation in Taiwan? and (2) do victimisation patterns vary between single and poly-victims? To answer these questions, this chapter makes use of Bayesian Profile Regression models, a hitherto underutilised statistical technique in crime research. To my awareness, this is the first study to examine the profiles of poly-victims in the context of cybercrime.

7.1 Background

As indicated previously in this thesis, it is well-established that criminal victimisation is not randomly distributed among a population. Evidence consistently shows that some individuals experience victimisation more often than others, a phenomenon referred to as ‘repeat victimisation’. Chapter 5 demonstrated that repeat victimisation, at least with respect to burglary, is prominent in Taiwan as it is elsewhere. Repeat victimisation refers to the repeated experience of a single form of crime. Some individuals experience multiple crime types in a given time period. To distinguish this phenomenon from repeated victimisation for a single crime type, the term poly-victimisation is used to describe cases where individuals experience one or more incidents of *different* crime types during a given period of time (a calendar year for instance) (Tanksley et al., 2020). An example of poly-victimisation is when an individual suffers a bike theft, receives a fraudulent call that incurs a financial loss, and has his/her laptop hacked, all within a one-year period. The diversity in crime types experienced by this individual makes poly-victimisation distinct from repeat victimisation, which was the focus of Chapter 5.

Note that the term 'multiple victimisation' is sometimes used instead of poly-victimisation (e.g. Tseloni & Pease, 2005). However, other studies have used 'multiple victimisation' to describe incidents in which multiple offenders commit a crime or in which more than one victim is affected in a single incident (e.g. Sparks, 1981). To avoid confusion, the term 'poly-victimisation' is now generally preferred by researchers to describe victimisations experienced by an individual, involving multiple different forms of crime over a given time period (e.g. Finkelhor et al., 2009; Le et al., 2016; Turner et al., 2017).

Poly-victimisation can be further distinguished from the notion of 'crime multipliers', a concept introduced by Felson (2010). Whist both poly-victimisation and crime multipliers involve multiple different forms of crime, the main difference between these two concepts is that poly-victimisation does not imply causality between crime events. By contrast, the term crime multiplier describes a sequence of related crime incidents, in which the completion of one crime increases the likelihood that another crime will occur. To illustrate, imagine if the individual's multiple victimisations are a sequence of crime events. A possible scenario would be: a thief steals a phone; they illegally sell it to someone who knows it is a stolen phone; the buyer illegally accesses personal information stored in the stolen phone; they then make purchases with that information online. This sequence involves four illegal acts – theft of phone, illegal purchase of a stolen item, unauthorised access of credentials, and unauthorised payment, for which the probability of each subsequent crime occurring is 'multiplied' following the initial theft (see Felson, 2010). However, for poly-victimisation, multiple different crimes need not be causally related. The example of poly-victimisation mentioned in the paragraph above – bike theft, receiving a fraudulent call, and hacking –

might comprise independent and unrelated events involving different offenders. Therefore, the use of poly-victimisation in this thesis does not imply any causal links between crime events, other than say the victim's behaviour and/or attributes may make him or her vulnerable to multiple different online victimisations.

The existence of poly-victimisation among some high-risk individuals is not a new finding and research identifying it can be dated back to at least the 1980s. For example, based on the 1972-1975 US National Crime Survey, Reiss (1980) presented a 'crime-switch matrix' to cross-tabulate poly-victimisation experienced by the same individuals, including rape, assault, robbery, larceny and burglary, concluding that personal larceny and attempted assault was the most frequent combination of poly-victimisation observed in the data. Reiss further identified that the recurrence of crimes against the same targets (either households or house members) was more frequent than would be expected on the basis of chance alone (Reiss, 1980). Similar clustering is also observed in violence. For example, research suggests that a child who has been physically assaulted is more likely to also experience sexual assault either during a survey period (Finkelhor, Turner, et al., 2011) or in his or her lifetime (Finkelhor et al., 2009).

Poly-victimisation experiences are often accompanied by serious consequences, such as mental health issues (Álvarez-Lister et al., 2017; Schaefer et al., 2018), self-harm (Baldwin et al., 2019) or suicidal thoughts/plans (Le et al., 2016), and distress symptoms (Finkelhor, Shattuck, et al., 2011). Studies have shown that poly-victimisation is related to a greater number of mental health problems than single criminal victimisation (Hamby et al., 2018) or than the repeated experience of the same form of victimisation (Turner et al., 2017). Noticeably, compared to research on repeat victimisation, poly-victimisation remains a less researched field. As mentioned in Chapter 2 (Section 2.3.2), results returned from searches on

Google scholar between 2016 and 2020[1] for "poly AND victim" is around one fourth of that found for searches of "repeat AND victim".

To recap briefly what has been covered in Section 2.3.2, to date the majority of studies on poly-victimisation have focussed on children and adolescents as victims of violence (Almeida et al., 2020; Kretschmar et al., 2017; Leoschut & Kafaar, 2017) and their relationship with mental health (Álvarez-Lister et al., 2017; Haahr-Pedersen et al., 2020; Lätsch et al., 2017). This line of research has subsequently identified a series of risk factors associated with an increased likelihood of experiencing multiple forms of violence. Among the few studies applying an ecological approach to explore poly-victimisation, a study using a Finnish sample has identified robust correlates between poly-victimisation and personal/family backgrounds among pupils aged 12-13 (sixth graders) and 15-16 (ninth graders) years. It suggests that a LRAA may help explain poly-victimisation (Ellonen & Salmi, 2011). That is, their study suggested that poly-victims tend to spend most of their free time alone and spend a lot of time in public spaces, while those who spend most of their free time with their family appear to report relatively low levels of poly-victimisation. Moreover, alcohol consumption, drug use, smoking, and delinquency are found to be associated with the self-reported experience of poly-victimisation. Other identified risk factors include personal vulnerability such as a chronic disease and disability (Le et al., 2016)[2].

[1] I used "poly AND victim" as a keyword to search on Google scholar and it returned 9,430 results, compared to 35,300 results for "repeat AND victim" since 2016. The search was conducted on 16th August 2020.

[2] In relation to family/environmental factors, Ellonen & Salmi's (2011) research has also suggested correlations between poly-victimisation and family structure as well as other kinds of living situations. For example, compared to those children who live in a nuclear family or a stepfamily with a biological father and stepmother, those who live with a single-parent father or with a mother and a stepfather report more poly-victimisation. Other living situations related to poly-victimisation include a poor family financial situation, frequent parental fighting, seeing parents intoxicated, and poor family communication (e.g. not having dinner together, or parents not knowing with whom their children spent free time) (Ellonen & Salmi, 2011).

In recent years, academic attention has increasingly been paid to the subject of cyber poly-victimisation as the internet is expanding. Noticeably most of the studies on cyber poly-victimisation focus on separate, fairly narrow categories of online victimisation experiences, such as cyberbullying and harassment (e.g. Cénat et al., 2019; Q. Chen et al., 2018; Mitchell et al., 2018). Such a focus of cyber poly-victimisation implies two points. First, research on online poly-victimisation has exhibited a similar focus on youth poly-victims to that in an offline context. Second, little research on cyber poly-victimisation has been centred on other types of online poly-victimisation, such as malware or unauthorised access to devices.

The narrow focus of research on online (poly)victimisation makes it unclear if the LRAA applies to online poly-victimisation beyond cyberbullying/harassment. However, at least certain victim characteristics have been suggested by research in the context of poly-victimisation. In Mitchell's et al. (2018) study on harassment involving technology use (i.e., internet and cell phone) across the US, poly victims tended to be older youths (aged 16-20 years than 10-15 years), living in single-parent homes, of Hispanic ethnicity, with delinquency, drinking alcohol experience, trauma symptomatology, and getting lower grades in school[3]. An overlap between both a victim and a perpetrator was also observed among poly victims. Mitchell et al.'s (2018) study further found poly-victims interacted with peers in more intense and risky ways with respect to technology use. For example, they tended to have much larger online social networks, a higher level of text message communications, use the internet more intensely (more than five hours per day), and were found more likely to exchange digital photos. These findings suggested that online behaviours may contribute to cyber poly-victimisation. However, it is noted that this finding on the positive relationship between involvement in social networking and cyber poly-victimisation indicated a contradictory notion to previous offline research, which suggested a negative direction – poly victims were often alienated or

[3] Note that gender was found no statistical implications for cyber poly victims in this study.

isolated from peer social networks (Finkelhor et al., 2007b; Lätsch et al., 2017). The role of social networking might therefore be different for online and offline poly-victimisation, and/or vary by different types of cybercrime. This uncertainty suggests that more research is warranted.

To summarise then. First, presently research on poly-victimisation is adolescent-limited; it has overwhelmingly focussed on youth issues either in an offline or online context; thus, less is known about the extent, nature and patterns of poly-victimisation among other population groups. Second, research on cyber poly-victimisation is centred mostly on cyberbullying. Knowledge about the extent and patterns of other types of cyber poly-victimisations, such as malware or unauthorised access to device, is limited. Third, little research has systematically applied a LRAA to explore patterns of cyber poly-victimisation and in particular the profile of poly cyber victims, other than cyber bullied/harassed victims. Finally, as with criminological research more generally, there is presently little research on cybercrime in Taiwan. This final empirical chapter in this thesis seeks to address these research gaps.

7.2 The current study

As mentioned in Chapter 6 and above, many existing cyber-related studies share a common weakness: by focusing on one single form of cyber victimisation (especially cyberbullying), they fail to shed light on the extent and patterns of poly-victimisation. The primary focus on one form of cyber victimisation alone creates a variety of problems. First, it underestimates the burden of victimisation that an individual has experienced. For example, those who have their electronic device attacked by viruses may also suffer identity theft. There might be some link between these two types of cybercrime; however, it is often the case that cybercrime research treats forms of cyber victimisation in isolation, excluding other forms in a single model. Second, existing research largely fails to show the interrelationships among different forms of online victimisation. Victimisations may cluster due to high-risk environments. In the case where only one form of online victimisation is assessed, the interconnections (or shared risk factors) are very likely to be overlooked. Hence, researchers should aim to examine the intersection of multiple victimisations, also known as poly-victimisation.

The previous chapter aimed to distinguish non-victims from victims in the context of cybercrime in Taiwan. This chapter, as a complement to Chapter 6, aims to understand the differences in victims of a single form of cybercrime from those who experience multiple forms of cybercrime over the study period (i.e. poly-victims). Consequently, the purposes of this study are to (a) explore the prevalence of poly victimisation among the Taiwanese population and (b) examine the differences between single victimisation and poly-victimisation. Two research questions are considered here: (1) is there evidence of online poly-victimisation in Taiwan? and (2) do victimisation patterns vary between single and poly-victimisation online? The following hypotheses are proposed:

- H1: There is significantly higher concentration of poly-victimisation than would be expected on the basis of random victimisation.

If poly-victimisation is found to be non-random, and given that Chapter 6 found that different types of victimisations exhibited different patterns, it is expected that there should be some patterns of poly-victimisation to be observed. Based on prior findings that some online activities act as specific risk factors for specific crimes, and that poly-victimisation is more complex than one single form of victimisation, the second hypothesis is:

- H2: Poly-victims participate in more online activities than single victims (defined here as victims with one victimisation).

By saying more involved online, it means that it is hypothesised that poly-victims would demonstrate various and a higher level of participation in sorts of online activities.

7.3 Data and measures

This section describes the data used for analyses. Briefly, the dataset is the same as that used in Chapter 6 – the DOSIH. Dependent variables are individuals' experience of (poly)victimisation while independent variables were designed to capture aspects of the LRAA. Most of the variables used in the current study were also covered in Chapter 6. The reader should refer to the previous chapter for more detailed descriptions of these variables (Section 6.3.2), with the following section focussing only on those variables that did not feature in the previous chapter and are specific to the current analysis.

7.3.1 Data

The data used in this chapter were taken from the DOSIH conducted in 2017. Details on the nature, strengths, and limitations of these data were provided in Chapter 3 (Section 3.2.2.2) and Chapter 6 (Section 6.3.1). Briefly, the DOSIH used a stratified random sampling method to collect data from a representative sample of 9,337 citizens aged 12 years and above residing in Taiwan. The DOSIH utilised computer-assisted telephone interviewing (CATI) to collect the data. The surveys were primarily designed to understand generational and regional differences in access to and experience of the internet and computer devices. Cybercrime victimisation was not the primary focus of the survey. However, questions were asked about respondents' experiences of cybercrime that closely resemble items commonly used in victimisation surveys. To my knowledge, no research has examined cybercrime victimisation, let alone cyber poly-victimisation, using the DOSIH datasets.

Two sub-samples of data are used here. The first analysis uses data relating to all survey respondents who reported having access to/experience of the internet. This is because, as mentioned in Chapter 6 and elsewhere (Yar & Steinmetz, 2019), the recruitment of data from samples without internet access could produce inaccurate and misleading results on the extent of cybercrime – someone who doesn’t go online cannot be the victim of a cybercrime. Therefore, the first subset of data used in this study included 6,806 participants (who reported using the internet) out of the original 9,337 survey respondents. Next, in order to investigate the differences between single victims and poly-victims, the second part of analysis reported in this chapter uses data relating on to those survey respondents who reported being the victim of cybercrime (n = 1,715). Survey respondents who did not experience any cybercrimes over the survey period were hence excluded from this part of the analyses.

7.3.2 Dependent variables for cyber poly-victimisation

The dependent variables (DVs) used here drew on respondents’ self-reported experience of cybercrime victimisation as measured in the DOSIH. In the DOSIH, a binary response of victimisation for each type of cybercrime was recorded. As the purpose of this chapter is to distinguish single victims from poly-victims, DVs were recoded into four categories: (1) verbally abused victims; (2) victims who experienced one property-related cybercrime; (3) victims who experienced multiple property-related cybercrimes; and (4) mixed poly-victims. The first two categories refer to single victimisation; the first category contains victims suffering verbal abuse alone, while the second contains those who experienced only one type of property-related cyber victimisation – either identity theft, fraud, or virus infection. The last two categories refer to poly-victimisation; the third refers to poly-victims who suffered different forms of property-related cybercrime, while the last category refers to poly-victims who experienced a mix of both verbal abuse and property-related cybercrimes. Note that the 2017 DOSIH only measured participants’ experiences of cybercrime victimisation as a binary response (yes or no), without entries on the exact times of victimisation. Hence, the DVs used in this chapter did not contain a category of multiple verbally abused victims due to the lack of information about multiple experiences of such an offence. Instead, poly-victims were categorised by property-related poly-victims and mixed poly-victims.

Table 7.1 shows the categories used to describe respondents' experiences of cyber (poly-)victimisation. Four codes represent different types of cyber victimisation, with "0" denoting verbally abused victims and "3" denoting mixed type of poly-victimisation.

Table 7.1 Description of cyber (poly)victimisation, DOSIH 2017, Taiwan

Risk code	Category	Number of victimisations	Description
0	Verbally abused victims	1	One experience of verbal abuse
1	One property-related victim	1	One experience of identity theft, fraud, or virus
2	Property-related poly-victim	≥ 2	Only experience of multiple (or say poly) property-related cybercrime
3	Mixed poly-victim	≥ 2	Mixed experience of verbal abuse and property crime

n = 1,715

7.3.3 Independent variables for cyber poly-victimisation

The independent variables (IVs) used here were those used in the previous chapter (see Section 6.3.2), namely variables relating to exposure/proximity to risk online, target attractiveness/vulnerability online and online guardianship.

7.3.3.1 Demographic controls for cyber poly-victimisation

Based on the literature and the findings reported in Chapter 6, demographic variables, judged to have a mediating effect on individuals' lifestyles, were also included in the analysis to examine if there is any significant difference in victims' profiles between single and multiple forms of cybercrime victimisation. The demographic controls were age, income, employment, university degree holder, and gender.

To recap, age was recorded as ordinal responses (1 to 8)[4] rather than a continuous variable. A preliminary analysis of clustering of users' ages found three clusters. Hence, the variable of age was categorised into three groups, in which 0 represents those who are aged 12 to 19 years old, 1 for adulthood between 20 and 49 years old, and 2 for those aged 50 years or older.

Income was dichotomised on the basis of median monthly income – NT$30,000 to less than NT$40,000 (about GBP£785 ~ GBP£1,045)[5], with "0" standing for earning less than or equal to the average and "1" for earning more than the average monthly income. The remaining three variables were also binary, with "0" referring to those who were female, unemployed, and without a university degree, and "1" referring to those who were male, employed, and held a university degree.

Again, this study included demographic variables as a control of mediating effect on person's routine-lifestyles. Hence, a conservative expectation of their relationship with cybercrime (poly)victimisation was held.

Further, extensive evidence shows that an individual's routines and lifestyle choices play a significant role in the probability of being victimised (Cohen & Felson, 1979; Jensen & Brownfield, 1986). The analysis thus included lifestyle-routine IVs – personal online activities, vulnerability and guardianship. Below I discuss them in turn.

[4] "1" representing people aged 12 to 14 years old, "2" for people aged 15 to 19 years old, "3" for 20 to 29 years old, correspondingly to "6" for 50 to 59 years old, "7" for 60 and 64 years old, and "8" to people aged 65 years old and older.

[5] Taiwan's median regular earning was about NT$39,000 (approx. £1,000) per month in 2017. Data was released on 24 December 2018 by the National Statistics, R.O.C. (Taiwan) at https://www.stat.gov.tw/ct.asp?xItem=43645&ctNode=6357&mp=4

7.3.3.2 Exposure/proximity to risk independent variables for cyber poly-victimisation

There were 13 types of online activities considered: (1) taking online courses (Course); (2) searching for information online (InfoSearch); (3) instant texting message (Message); (4) watching videos online (Video); (5) playing online games (Gaming); (6) free internet calling (Call); (7) Facebook posting (FBpost); (8) searching for product review (ReviewSH); (9) online purchasing (Purchase); (10) online banking(Banking); (11) retrieving information on government websites (GovInfo); (12) making payment on government websites (GovPay); and (13) downloading data from government websites (GovDL). To simplify the visualisation of clustering, online activities with their scale of participation were recoded into three levels – 0 as less frequent ("no use" and "less than once a month"), 1 as moderately frequent ("at least once a month" and" at least once a week"), and 2 as very frequent ("once a day" and "several times a day"). This three-level scale applied to all variables of online activities involved in this study. It was expected that poly-victims, if distinct from single victims, would demonstrate more various and a higher level of exposure to online activities (H2).

7.3.3.3 Target attractiveness/vulnerability independent variables for cyber poly-victimisation

Vulnerability, as conceptualised in this study, comprised four variables – aggressive posting, disability, Wi-Fi use, and hospital e-booking (also known as hospital e-Service). The former three variables were binary, with "0" standing for participants without aggressive posting, disability and Wi-Fi use, respectively, and "1" denoting aggressive posting, presence of a self-reported disability and Wi-Fi use. The last variable, hospital e-booking, was measured in three-levels – "0" as less frequent ("no use" and "less than once a month"), "1" as moderately frequent ("at least once a month" and" at least once a week"), and "2" as very frequent ("once a day" and "several times a day"), in line with other variables of online activity mentioned above. This variable is a measure of vulnerability, in a sense that the more frequent an individual uses hospital e-booking, the more likely that they have health problems (e.g. chronic diseases). All things being equal, this may make them more vulnerable to cybercrime (Le et al., 2016).

Drawing on the findings of the previous chapter, it was predicted that aggressive posting would be more likely to relate to verbal abuse victimisation. However, given that it was also found in the previous chapter that the effect of aggressive posting was less consistent across property-related victimisation, no prediction about its link to poly-victims is made in the current study. Otherwise, poly-victims were expected to demonstrate a higher level of vulnerability – disability, Wi-Fi use, and hospital e-booking than were victims of single cyber victimisation.

7.3.3.4 Guardianship independent variables for cyber poly-victimisation

Three variables were used here as proxies for online guardianship – living with someone, mobile internet access, and government notification. The variable "living with someone" was recorded in a binary fashion, with "0" representing the respondents living alone and "1" representing living with someone else. Living with others is regarded a concept of guardianship in an offline context; yet considering the solitary aspect of the internet use, I held an open attitude toward the guardianship of live-in family in an online context.

Mobile net access was measured by respondents' access to the internet via portable devices such as smartphones or laptops, with "0" denoting no possession of such a device. It was assumed that access to portable devices was linked to increased exposure to the internet without others' supervision (guardianship). As above, the expectation was that poly-victims would demonstrate a higher level of mobile net access than did victims of single victimisation.

Government notification variable indicates the frequency that respondents received warning from the government about the disaster (e.g., tsunami, earthquake) alerts. It was recoded into a three-level response, with "0" as less frequent ("no use" and "less than once a month"), "1" as moderately frequent ("at least once a month" and" at least once a week"), and "2" as very frequent ("once a day" and "several times a day"). It was assumed that government notification would be linked to infrastructure construction. A higher level of government notification might indicate a higher level of infrastructure, so a higher level of government supervision of internet security, and so a lower chance of cyber victimisation. Provided that patterns of single cybervictimisation are distinct from poly-victimisation, it was expected to demonstrate a different yet lower level of government notification among poly-victims as they may receive less supervision of internet security from the authority.

Table 7.2 shows the descriptive statistics of the variables used to model (poly)victimisations (n = 1,715) in this chapter[6]. It shows that single property-related cybercrime victims constituted nearly 70 percent of cybercrime victims in the 2017 DOSIH, followed by property-related poly-victims (17.96%), one-time verbally abused victims (7.46 %) and mixed type poly-victims (5.25%). The majority of respondents tend to be adults (58.78%), those earning less than the average (68.05%), employed (75.98%), those without a university degree (55.92%), and males (50.38%).

Table 7.2 further indicates some notable patterns of online behaviours among DOSIH respondents, of which respondents were less involved in government websites related activities. Conversely, respondents were more involved in activities such as instant text messaging, watching videos, or making free internet calls. With regard to target attractiveness/vulnerability,

[6] The descriptive statistics of variables drawn upon a greater sample including both cyber-victims and non-victims (n = 6,806) can be referred to Chapter 6 (Table 6.1).

Table 7.2 Descriptive statistics of variables, 2017 DOSIH, Taiwan

Variables	Frequency	%
Victimisation		
One Verbal abuse victim (0)	128	7.46%
One property-related victim (1)	1,189	69.33%
Property-related poly-victim (2)	308	17.96%
Mixed poly-victim (3)	90	5.25%
Age		
Young people (12-19 yrs.) (0)	155	9.04%
Adulthood (20-49 yrs.) (1)	1,008	58.78%
Older people (>=50 yrs.) (2)	552	32.19%
Income (GdIncome)		
Earn less than the avg. (0)	1,167	68.05%
Earn more than the avg. (1)	548	31.95%
Employment		
Unemployed (0)	412	24.02%
Employed (1)	1,303	75.98%
Education (Uni)		
Without Uni degree (0)	959	55.92%
With Uni degree (1)	756	44.08%
Gender		
Female (0)	851	49.62%
Male (1)	864	50.38%
Online course (Course)		
Little usage (0)	1,420	82.80%
Moderate usage (1)	248	14.46%
Frequent usage (2)	47	2.74%
Information searching (InfoSH)		
Little usage (0)	294	17.14%
Moderate usage (1)	737	42.97%
Frequent usage (2)	684	39.88%
Instant messaging (Instant message/MSG)		
Little usage (0)	50	2.92%
Moderate usage (1)	109	6.36%
Frequent usage (2)	1,556	90.73%
Watching video online (Video)		
Little usage (0)	249	14.52%
Moderate usage (1)	536	31.25%
Frequent usage (2)	930	54.23%

(continued)

Table 7.2 *(continued)*

Variables	Frequency	%
Online gaming		
Little usage (0)	941	54.87%
Moderate usage (1)	218	12.71%
Frequent usage (2)	556	32.42%
Free internet calling (call)		
Little usage (0)	283	16.50%
Moderate usage (1)	701	40.87%
Frequent usage (2)	731	42.62%
Facebook posting (FBpost)		
Little usage (0)	944	55.04%
Moderate usage (1)	651	37.96%
Frequent usage (2)	120	7.00%
Product review search (ReviewSH)		
Little usage (0)	733	42.74%
Moderate usage (1)	783	45.66%
Frequent usage (2)	199	11.60%
Online purchase (Purchase)		
Little usage (0)	992	57.84%
Moderate usage (1)	694	40.47%
Frequent usage (2)	29	1.69%
Online banking (Banking)		
Little usage (0)	1,193	69.56%
Moderate usage (1)	439	25.60%
Frequent usage (2)	83	4.84%
Retrieving information on government websites (GovInfo)		
Little usage (0)	1,289	75.16%
Moderate usage (1)	393	22.92%
Frequent usage (2)	33	1.92%
Payment on government websites (GovPay)		
Little usage (0)	1,670	97.38%
Moderate usage (1)	42	2.45%
Frequent usage (2)	3	0.17%
Downloading data from government websites (GovDL)		
Little usage (0)	1,610	93.88%
Moderate usage (1)	95	5.54%
Frequent usage (2)	10	0.58%

(continued)

Table 7.2 *(continued)*

Variables	Frequency	%
Online posting tendency		
Non-aggressive posting (0)	1,642	95.74%
Aggressive posting (1)	73	4.26%
Disability		
No disability (0)	1,439	83.91%
Has disability (1)	276	16.09%
Wi-Fi access (Wi-Fi)		
No Wi-Fi access (0)	168	9.80%
Had Wi-Fi access (1)	1,547	90.20%
Hospital e-booking service (HPbook)		
Little usage (0)	1,452	84.66%
Moderate usage (1)	262	15.28%
Frequent usage (2)	1	0.06%
Live-in family		
Live alone (0)	91	5.31%
Live with someone else (1)	1,624	94.69%
Internet mobility		
Fixed-spot internet access (0)	330	19.24%
Flexible internet access (1)	1,385	80.76%
Government notification		
Little usage (0)	1,432	83.50%
Moderate usage (1)	247	14.40%
Frequent usage (2)	36	2.10%

n = 1,715

nearly five percent of respondents reported having an aggressive posing tendency, about 16% reported themselves with a disability, over 90% had Wi-Fi access, and about 15% moderately used hospital e-Service. For guardianship-related variables, about 95% of respondents reported living with others, around one fifth had no mobility of the internet access, and 15% received government notification on a moderate frequency.

All the independent variables were first entered into the model of analysis, and a variable selection procedure was then conducted. The analysis of the use and procedure of variable selection is detailed in the section below on analytical strategy.

7.4 Analytical strategy

Following the strategy employed in Chapter 5, this study uses descriptive statistics and Lorenz curves to explore if there is a pattern of poly-victimisation for cybercrime in Taiwan to test the hypothesis "*There is a significantly higher concentration of poly-victimisation than would be expected on the basis of random victimisation*" (H1).

The descriptive statistics and Lorenz curves to be used in this study would demonstrate how cybercrime victimisation concentrates across targets (n = 6,806). These approaches are similar to the analyses presented in Chapter 5, in which the distribution of repeat victimisation was displayed. However, it is noted that the concentrations to be displayed in the current study refer to the distribution of poly-victimisation and not instances of repeat victimisation as presented in Chapter 5.

This means, in this study, the distribution of victimisations would accumulate when a respondent experienced multiple types of cybercrime, but the extent and concentration of poly-victimisation should not be understood as repeat victimisation of a same type of crime. Simply put, the illustration of relevant figures could be taken similarly to repeat victimisation analyses in

Chapter 5 yet not identically. Following these measures, a more advanced analytical strategy – Bayesian profile regression – is used to examine if victimisation patterns and mechanisms vary between single and poly-victimisation in an online context (H2).

7.4.1 Bayesian profile regression

The logistic regression is the conventional statistical technique to deal with data with a binary outcome. However, in the current study it would be desirable to include all four types of cybercrime victimisation and poly-victimisation in one model, suggesting the use of generalised linear regression. However, the use of generalised linear regression would need to be taken with caution when the model consists of highly inter-related independent variables (Molitor et al., 2010; B. H. Patterson et al., 2002). Where highly-correlated independent variables are introduced into analyses, the association between the outcome and one independent variable could reach a high level of statistical significance by that specific variable alone but not in the presence of many other correlated variables. This is because that specific variable may account for most of the multivariate significance while the other variables make little contribution. It is thus challenging to tell if the high level of significance is being achieved by one independent variable or the introduction of other independent variables. Where this is the case, an innovative way to address these problems has recently been developed in health and medical research (El-Saifi et al., 2019; Hastie et al., 2013; Mattei et al., 2016) and will be used here –BPR.

Figure 7.1 is a correlation matrix for the 14 ordered online activities (i.e. 13 exposure IVs and one vulnerability IV) asked about in the DOSIH survey. The principal diagonal displays the distribution chart for each variable. The cells below the principal diagonal display the scatterplots represented by the intersection of the row and column variables. The cells above the principal diagonal display the Spearman's rank correlation coefficients between

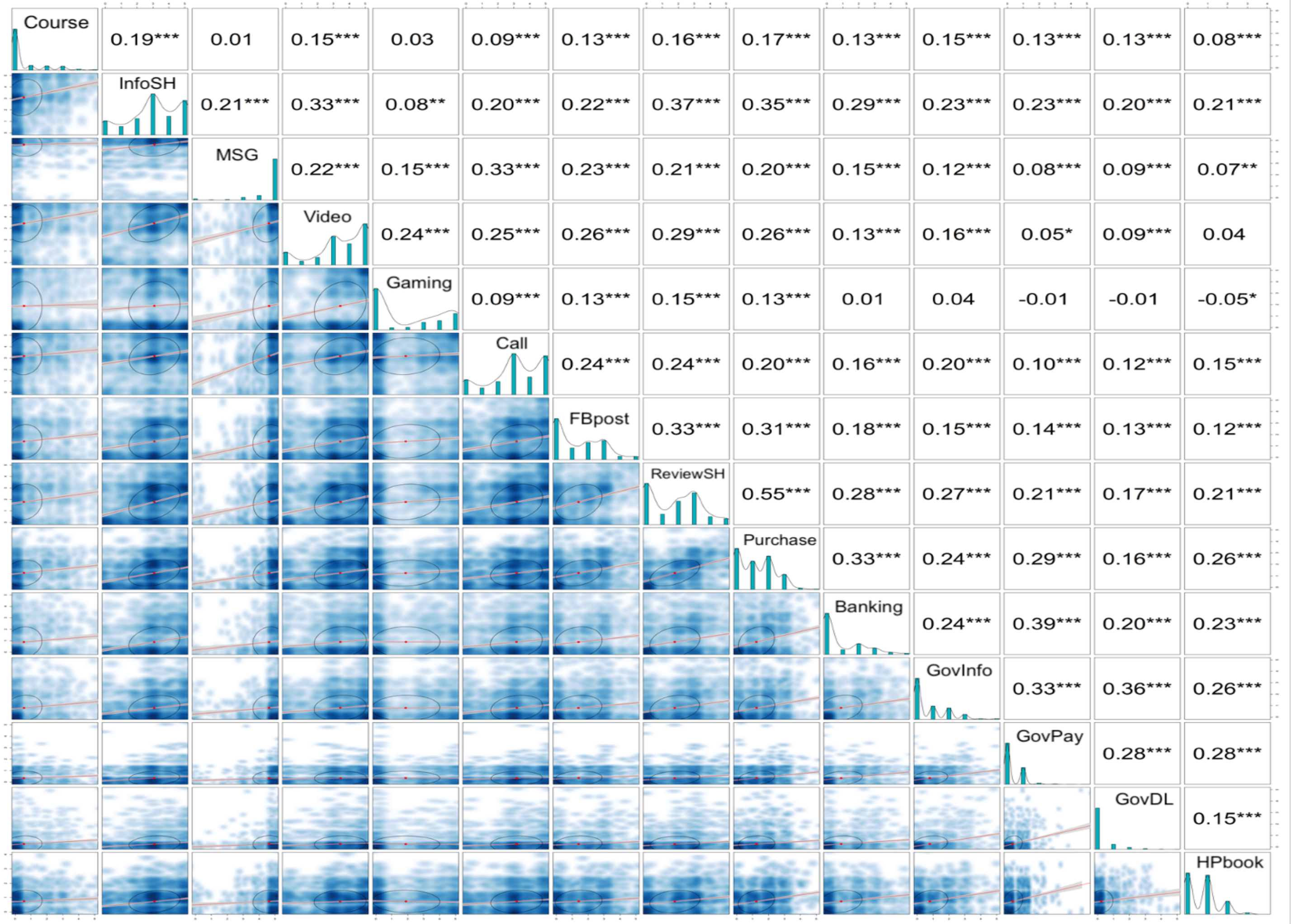
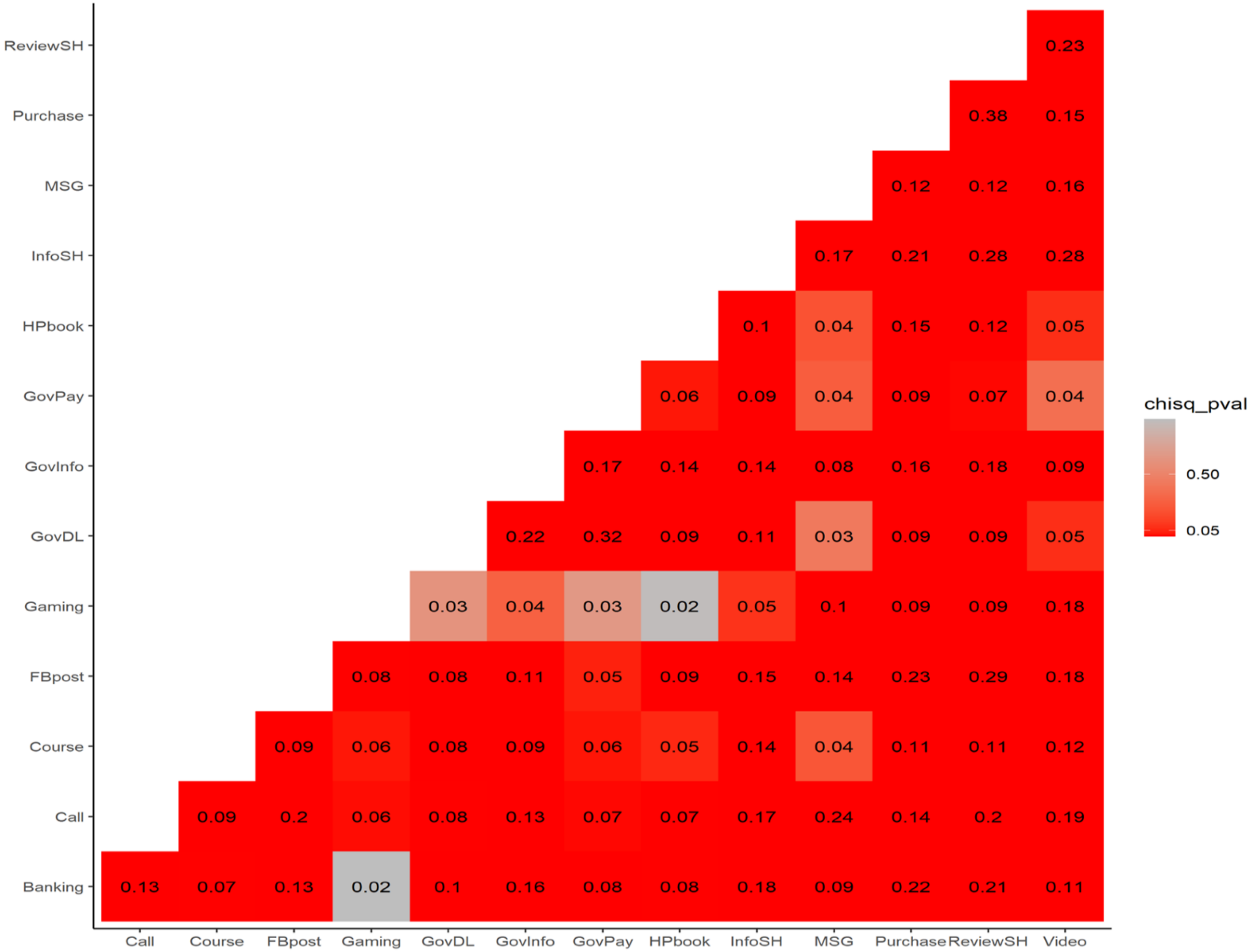


Figure 7.1 Correlation matrix for ordered variables of online activities from 2017 DOSIH, Taiwan. * p < .05; **p<.01; ***p< .001

variables. For example, taking online courses and searching for information online were significantly and positively related (rho = 0.19, $p < .001$). Taken together, Figure 7.1 suggests that many of these variables are highly correlated. The most highly correlated variables were online purchasing and searching product reviews online (rho = 0.55, $p < .001$). The highly intercorrelated nature of these variables suggests that using a standard regression model might be problematic. Although the posterior collinearity check of the logistic regression in Chapter 6 did not reach a worrying level (VIF = 1.63, less than 3), it is still worth considering if there is an alternative analytical strategy to complementarily examine patterns and predictors of cybercrime (poly)victimisation in one model.

My first approach to deal with intercorrelation concerns was to simplify the levels of online activities from six to three. However, variables of online activities with three levels had a similar intercorrelation issue. Figure 7.2 is a replication of Figure 7.1, except that Pearson Chi-square analyses were performed instead of Spearman's correlation and statistics of Cramer's V were provided in cells below the main diagonal. Most of the cells were shown in red as significantly correlated ($p < .001$) with each other, suggesting intercorrelation issues that were similar to Spearman's correlation matrix.

A profile analysis was then considered, as it enabled me to classify research targets from a heterogeneous population into smaller, more homogenous subgroups based on their values. For profile analysis, variables are not limited to continuous variables but can be combinations of continuous, count, and/or categorical variables as indicators of latent class. Compared to the classical analysis of logistic regression demonstrating the importance of individual predictors, profile analysis offers additional insights into what dimensions of exposure are linked to the outcome risk (Hastie et al., 2013).



	Call	Course	FBpost	Gaming	GovDL	GovInfo	GovPay	HPbook	InfoSH	MSG	Purchase	ReviewSH	Video
ReviewSH													0.23
Purchase												0.38	0.15
MSG											0.12	0.12	0.16
InfoSH										0.17	0.21	0.28	0.28
HPbook									0.1	0.04	0.15	0.12	0.05
GovPay								0.06	0.09	0.04	0.09	0.07	0.04
GovInfo							0.17	0.14	0.14	0.08	0.16	0.18	0.09
GovDL						0.22	0.32	0.09	0.11	0.03	0.09	0.09	0.05
Gaming					0.03	0.04	0.03	0.02	0.05	0.1	0.09	0.09	0.18
FBpost				0.08	0.08	0.11	0.05	0.09	0.15	0.14	0.23	0.29	0.18
Course			0.09	0.06	0.08	0.09	0.06	0.05	0.14	0.04	0.11	0.11	0.12
Call		0.09	0.2	0.06	0.08	0.13	0.07	0.07	0.17	0.24	0.14	0.2	0.19
Banking	0.13	0.07	0.13	0.02	0.1	0.16	0.08	0.08	0.18	0.09	0.22	0.21	0.11

Figure 7.2 Correlation matrix with Cramer’s V for variables of online activities

Superior to traditional clustering methods such as latent class and profile analysis, BPR allows the number of groups to vary within subgroups and an outcome variable of interest to be entered into the model, considering the influence of outcome variable on cluster membership. This is because BPR takes a Dirichlet process to cluster respondents with similar independent variable profiles and associates them with outcomes via a regression model (Molitor et al., 2010). That is to say, BPR can model the risk of groups of participants rather than the risk of individual participants taken from conventional regression methods.

A simple example of how the model could be used to explore associations between a categorical outcome and an independent variable is the associations between skin cancers (outcome) and sun exposure (independent variables). The outcome may contain no or some type of skin cancer while the independent variables contain sun exposure characteristics – for example, intensity, duration, and the use of sunscreen – that are categorised into three discrete and ordinal levels as appropriate. Assume subjects of study are split into three clusters based on the analysis of cancer risk: cluster 1 containing subjects at high risk for skin cancer, cluster 2 containing subjects at average risk, and cluster 3 containing subjects at low risk. By looking at the average profile (i.e. probabilities of independent variable values) in the high-risk cluster 1, one might find, for example, a higher-than-average probability of being in the highest intensity category, the longest duration category, and a reduced probability of applying sunscreen. However, in practice, there might be more than three clusters, which provide a more subtle interpretation of associations between risk and independent variable combinations.

Suppose the cancer study above recruits N subjects and has J independent variables of interest, where i denotes an individual subject, and j denotes an independent variable. For each subject, y_i represents an observed outcome (of skin cancer) and $x_i = (x_{i,1},\ldots,x_{i,J})$ represents an independent variable profile (of sun exposure). Taking formulation from Hastie et al.'s (2013) study, for each subject of individual that is independent of every other, the joint probability model for the outcome y_i and profile X_i can be specified algebraically as[7]:

$$p\{Y_i, X_i \vert\, \theta = (\theta_{0,} \psi_1, \theta_{1,} \psi_2, \theta_{2,} \dots)\} = \sum_{c=1}^{\infty} \Psi_c p\{Y_i \vert \theta_c, \theta_0\} p\{X_i \vert \theta_c, \theta_0\}$$

(7.1)

where ψ_c denotes the weight of the c^{th} cluster, Θ_c the cluster-specific parameter, and Θ_0 some global parameters. The outcome y_i and profile X_i are conditional on Θ_c and Θ_0. To make inference, let Z_i be the additional allocation parameter and $Z_i = c$ denotes that individual i is assigned to the c^{th} cluster. Should prior allocation probabilities be given as $p\ (Z_i = c) = \psi_c$, then one can make posterior inference on the groupings of the individual based on $Z = (Z_1, Z_2, \dots, Z_N)$.

In the case where outcome and independent variables are nominal like the cancer study example:

$$X_{i,j} \vert\, Z_i = c \sim Multinomial\big(1, \phi_{Z_{i},j}\big).$$

(7.2)

where $\boldsymbol{\phi}_{c,\ j} = (\phi_{c,j,1}, \phi_{c,j,2}, \dots, \phi_{c,j,Lj})$ represents the vector of probabilities associated with cluster c for each of the possible levels L_j that could be observed for independent variable j (Hastie et al., 2013).

Given that Stata merely allows traditional profile clustering analysis but not BPR, I used the R (3.6.0 version) package ‘PReMiuM’ to perform the BPR analysis.

7.4.2 Examining clustering output

To specify the model and estimate how many clusters would be investigated, an exploratory approach is usually taken. The exploratory approach should depend on theory and previous research. This approach involves estimating one more group than is expected and it is suggested that additional clustering is estimated until a statistically proper and/or practical solution is no longer

[7] Vakhitova et al.’s (2019) study was the first attempt to apply BPR to crime research and a simplified yet clear description of BPR could be found in their Appendices.

obtained (Berlin et al., 2014). An effective way to identify the optimal clustering is to use the posterior output as suggested by Molitor et al. (2010). The PReMiuM package enables R users to manipulate models in which the number of groups can be changed from iteration to iteration of the sampler. The optimal clustering was identified by Silhouette width statistics, which could be found in Table 7.3. The figures suggest that the optimal number of groups would be four, with each cluster size as 608, 278, 362, 467, respectively.

Table 7.3 Support for different numbers of clusters

Number of clusters	3	4	5	6	7	8	9	10	11	12
Mean of support	0.57	0.63	0.56	0.60	0.54	0.53	0.55	0.56	0.58	0.57

n = 1,715.

7.4.3 Variable selection

In the case that the proposed model of profiles is constructed by a great number of independent variables, it is common to see a considerable number of independent variables that do not contribute to the clustering. A variable selection procedure is thus often required to avoid the risk of over-fitting the model. As suggested by the relevant literature (Burnham & Anderson, 2002; Papathomas et al., 2012; Vakhitova et al., 2019), I conducted some statistical procedures of variable selection in the PReMiuM package. The rationale behind this was to identify the variables that were most influential in the formation of clusters, which was determined by figures of posterior inclusion probability distributions (in R as rho statistics). Table 7.4 provides these rho statistics across variables.

Table 7.4 Posterior median inclusion probability of variables

Variables	Rho median	Kept in the refined model
Demographic controls		
Age	1.00	V
Income	0.93	V
Employment	0.78	V
Education	0.77	V
Male	0.56	
Exposure to risk/ Proximity to offenders		
Watching video online	0.95	V
Online gaming	0.91	V
Online purchasing	0.84	V
Information search	0.82	V
Product review search	0.82	V
Facebook posting	0.77	V
Online banking	0.70	V
Retrieving information on government websites	0.68	
Free internet calling	0.62	
Instant message	0.52	
Online course	0.49	
Downloading data from government websites	0.46	
Payment on government websites	0.31	
Target attractiveness/ vulnerability		
Wi-Fi use	0.87	V
Hospital e-booking service	0.72	V
Aggressive posting	0.00	
Disability	0.00	
Guardianship		
Government notification	0.08	
Live-in family	0.00	
Mobile net access	0.00	

n = 1,715

Figure 7.3 and Figure 7.4 demonstrate posterior inclusion probability distributions for subjects' vulnerability and guardianship variables. The figures indicate that, for example, "Wi-Fi use" contributed to the explanatory model with the median inclusion probability being greater than 80 percent, while aggressive posting tendency did not, with the median inclusion probability being nearly zero. Hospital e-booking service and disability had a similar interpretation. In line with Chapter 6 that suggested little effect of the traditional concept of guardianship on cybercrime victimisation, all three variables of guardianship were found to make little contribution to the model exploring patterns of single victims and poly-victims. Therefore, variables related to guardianship were excluded in the current BPR model.

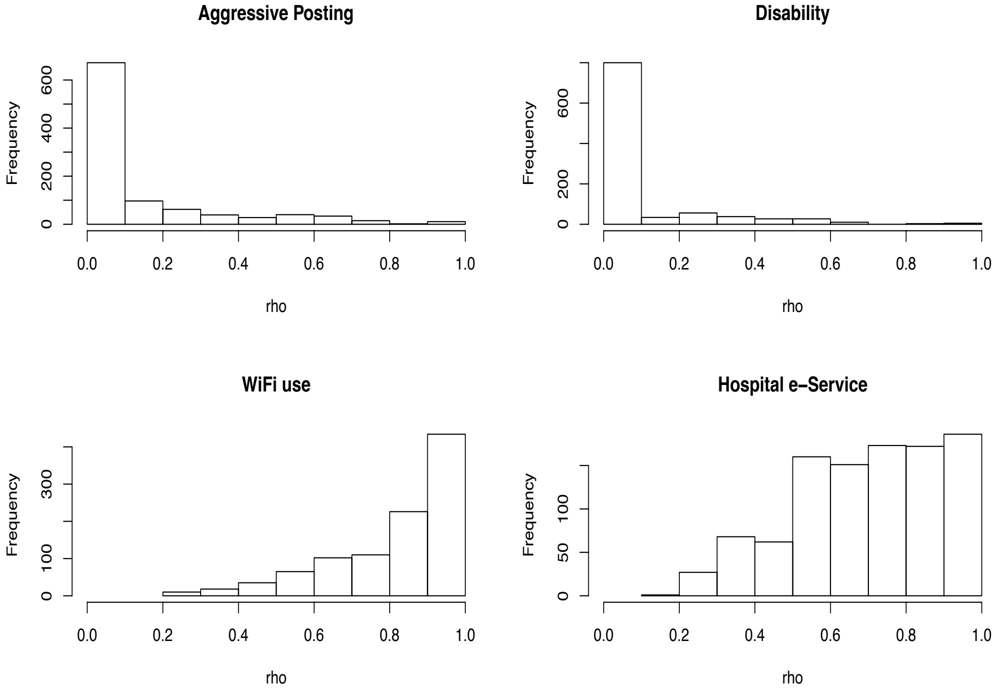


Figure 7.3 Posterior probability distributions of vulnerability variables based on 10,000 iterations of the BPR algorithm

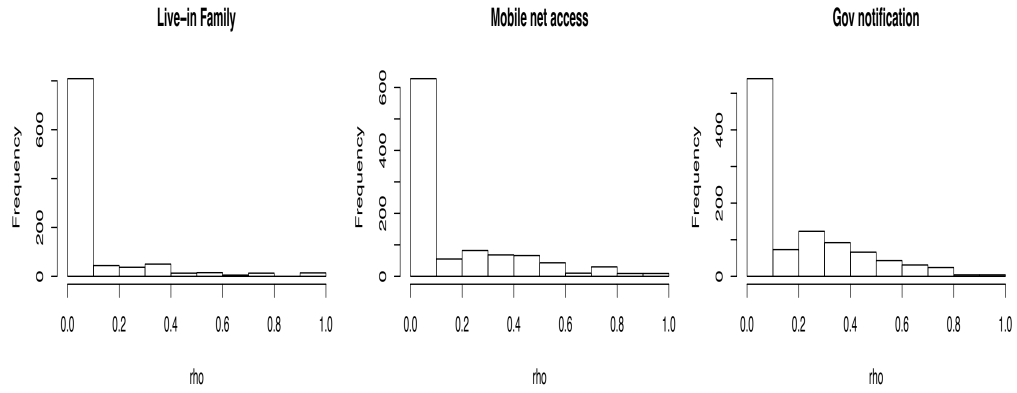


Figure 7.4 Posterior probability distributions of guardianship variables based on 10,000 iterations of the BPR algorithm

Figure 7.5 shows posterior inclusion probability distributions for four variables of online activities – online banking, gaming, watching the video, and instant message. Noticeably, the histogram of instant message does not have clear cuts, in which the inclusion probabilities are uniformly distributed (see the bottom right panel of Figure 7.5). This variable is shown to be less informative than others with high median inclusion probabilities of over 90 percent (say, online gaming or watching video online). This figure does not imply that the effect of instant message should be ignored but more information will be required beyond this dataset.

Based on the current dataset and previous research, it was reasonable to select independent variables with a cut point of 70 percent in terms of posterior median inclusion probabilities. The number of variables was reduced from 25 to 13 (see Table 7.4).

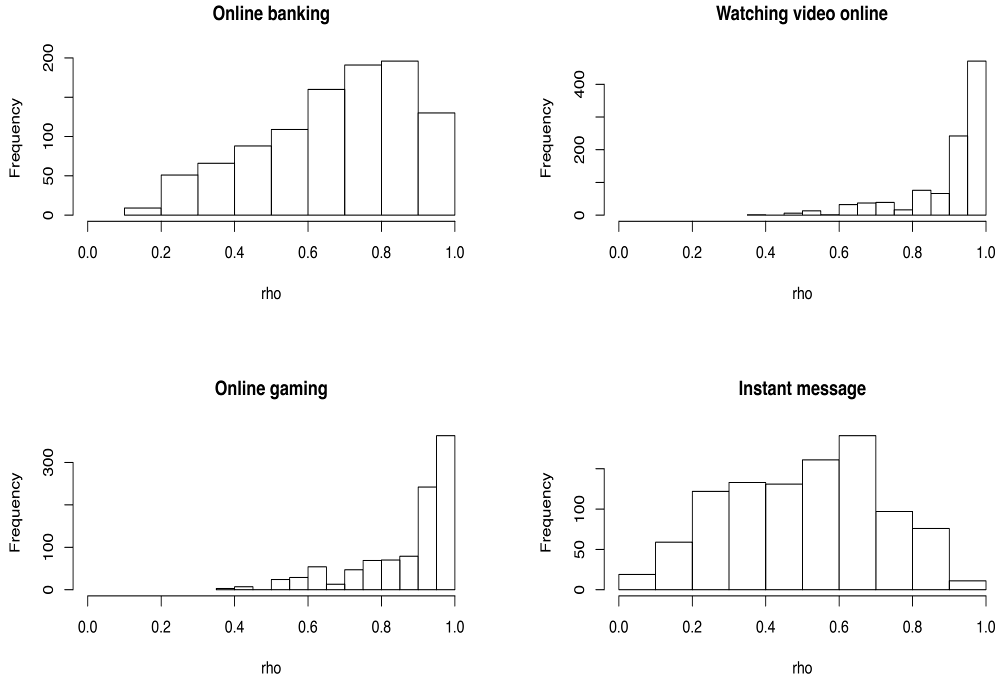


Figure 7.5 Posterior probability distributions of online activity variables based on 10,000 iterations of the BPR algorithm

7.5 Results

As indicated above, three sets of results are reported here, namely the descriptive statistics, the Lorenz curves and the BPR. The descriptive statistics are given first to show the extent of poly-victimisation in Taiwan, a phenomenon that hitherto has not been systematically analysed in Taiwan. Then, I present the results using Lorenz curves to test H1: "*There is significantly higher concentration of poly-victimisation than would be expected on the basis of random victimisation*". The final set of results are those generated by BPR and relate to H2: *"Poly-victims participate in more online activities than single victims."*

7.5.1 Descriptive statistics of poly-victimisation

Table 7.5 illustrates the prevalence and concentration of online victimisation in Taiwan using data from the 2017 DOSIH. The table shows that nearly six percent of individuals reported experiencing two or more forms of online victimisation in the past year (871 incidents in total, i.e., nearly 40 percent of the 2,188 reported cases of cybercrime). Such poly victims (n = 398) also constituted more than one fifth of the general victim population (n = 1,715) and their incidents made up around 40 percent of all reported cybercrime incidents among the survey sample.

Table 7.5 The distribution of online (poly)victimisation in Taiwan using data from the 2017 DOSIH

Number of victimisations	Prevalence	Incidence	% All targets	% Victims	% Incidence
0	5,091	-	74.80	-	-
1	1,317	1,317	19.35	76.79	60.19
2	329	658	4.83	19.18	30.07
3	63	189	0.93	3.67	8.64
4	6	24	0.09	0.35	1.10
Total	6,806	2,188	100	100	100

Figure 7.6 presents the distribution of cyber poly-victimisation by cybercrime type. There were 11 types of poly-victimisations according to the current data. Types of online victimisation were abbreviated as B (verbal abuse), I (identity theft), F (fraud), and V (virus). The most common type of poly-victimisation in the data analysed here was the combination of identity theft and virus victimisation (IV, 39.20%) whilst the least common was that of verbal abuse, fraud, and virus (BFV, 0.75%). Victims were less likely to experience verbal abuse with other types of cybercrime. Visually, there were two general patterns of poly-victimisation observed in the data analysed here

– crimes against the person (verbal abuse) and crimes against property (identity theft, fraud, and virus).

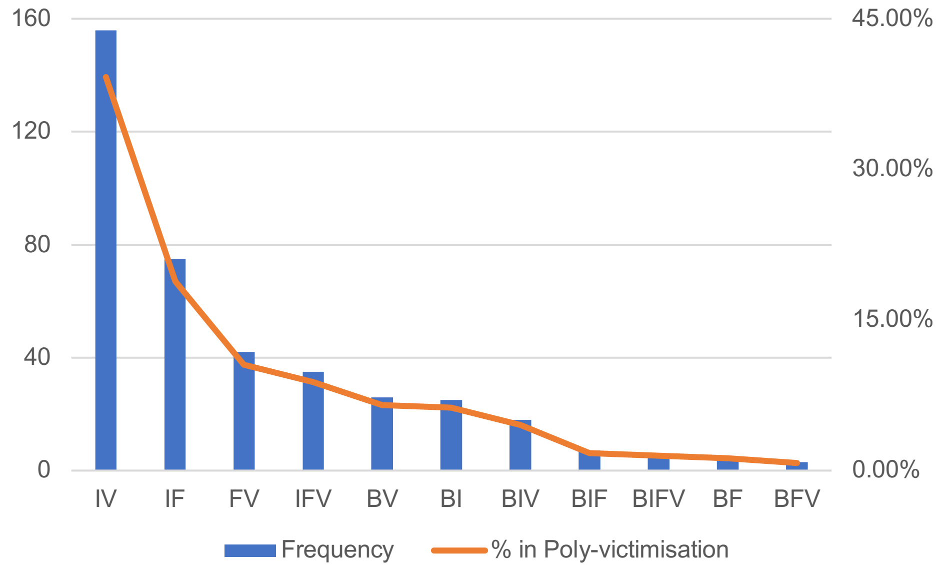


Figure 7.6 Distribution of cyber poly-victimisation by types in Taiwan using data from the 2017 DOSIH (n = 1,715). Types of victimisations are abbreviated as B (verbal abuse), I (identity theft), F (fraud), and V (virus).

7.5.2 Concentration of poly-victimisation

Figure 7.7 comprises Lorenz curves showing the observed and expected distributions of cybercrime victimisation in Taiwan. The left panel presents an inequality in cyber victimisation across the population (Gini index = 0.79) whilst the inequality of online victimisation risk was lessened over victims (see the right panel, Gini index = 0.17). Concentration patterns are clearly discernible. The top 10% most victimised respondents (n= 1,715) accounted for about 20% of all victimisations (n = 2,188) while the lower 10% accounted for less than 10% of incidents. Additionally, there was a significantly higher concentration of multiple forms of online victimisation over victims than would be expected on the basis of random victimisation (The KS test: D =

0.52, $p < .001$). There is therefore statistical evidence to support H1: *There is significantly a higher concentration of poly-victimisation than would be expected on the basis of random victimisation*.

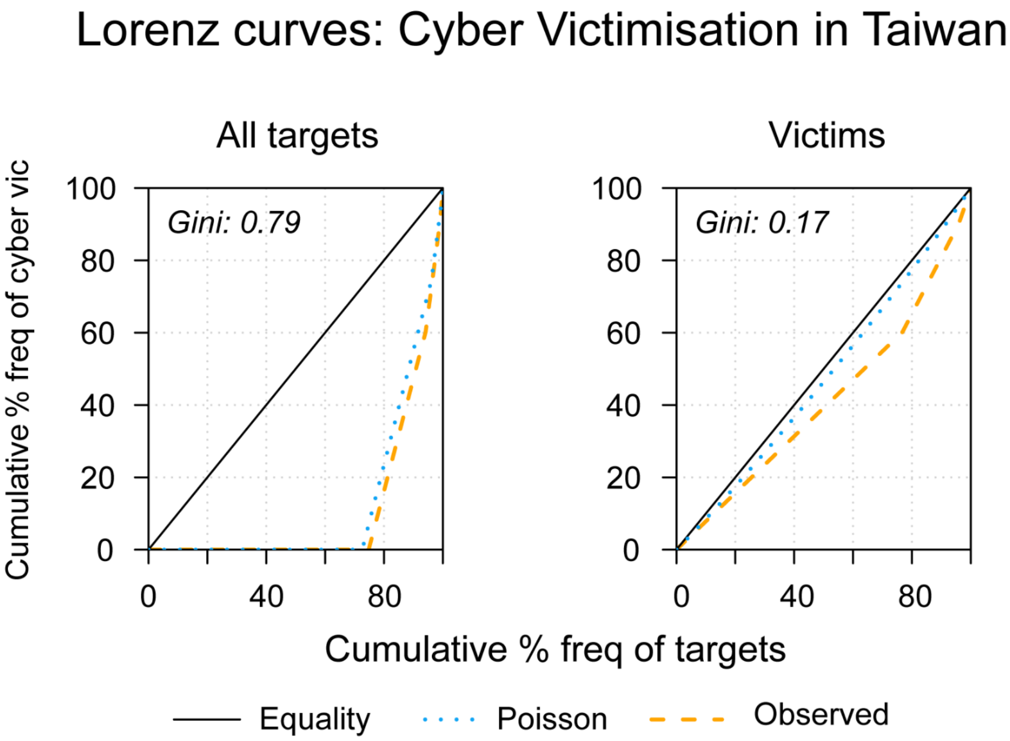


Figure 7.7 Lorenz curves with the observed and expected distributions of cybercrime victimisation in Taiwan using data from the 2017 DOSIH

7.5.3 Patterns of single victimisation vs. poly-victimisation

Figure7.8-7.10 show the effect of demographic characteristics, vulnerability and online activities, along with risk profiles identified by BPR, respectively. These analyses reveal four profiles for the four categories of cyber victim – "0" for verbal abuse, "1" for one property-related victimisation, "2" for property-related poly-victimisation, and "3" for mixed poly-victimisations.

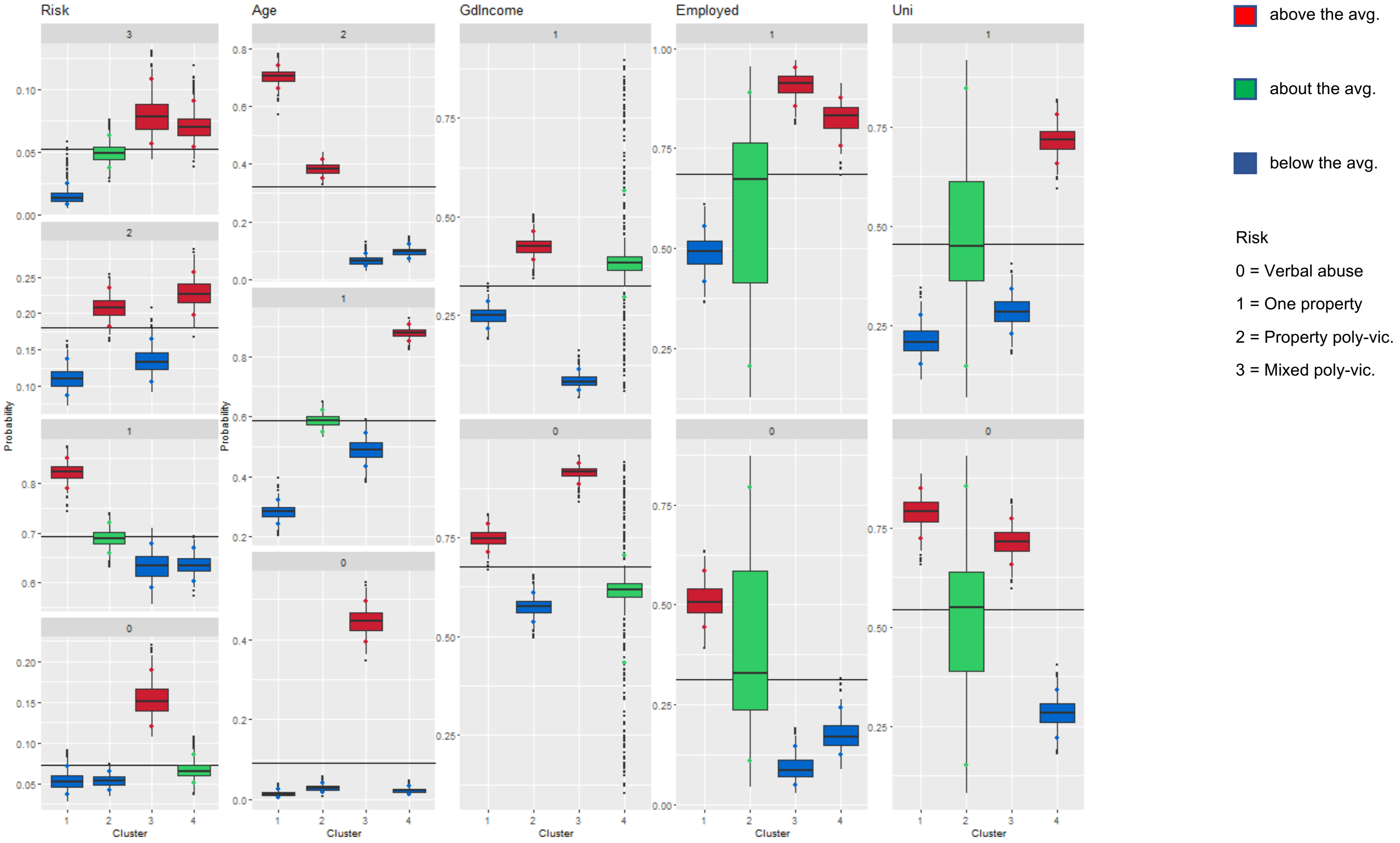


Figure7.8. Demographic controls and risk of profiles identified by BPR. The red-coloured boxes indicate that the 90% credible intervals for the cluster-specific profile parameter are above the average over clusters, the green-coloured boxes indicate that the intervals are about the average, and the blue-coloured boxes indicate that the intervals are below the average.

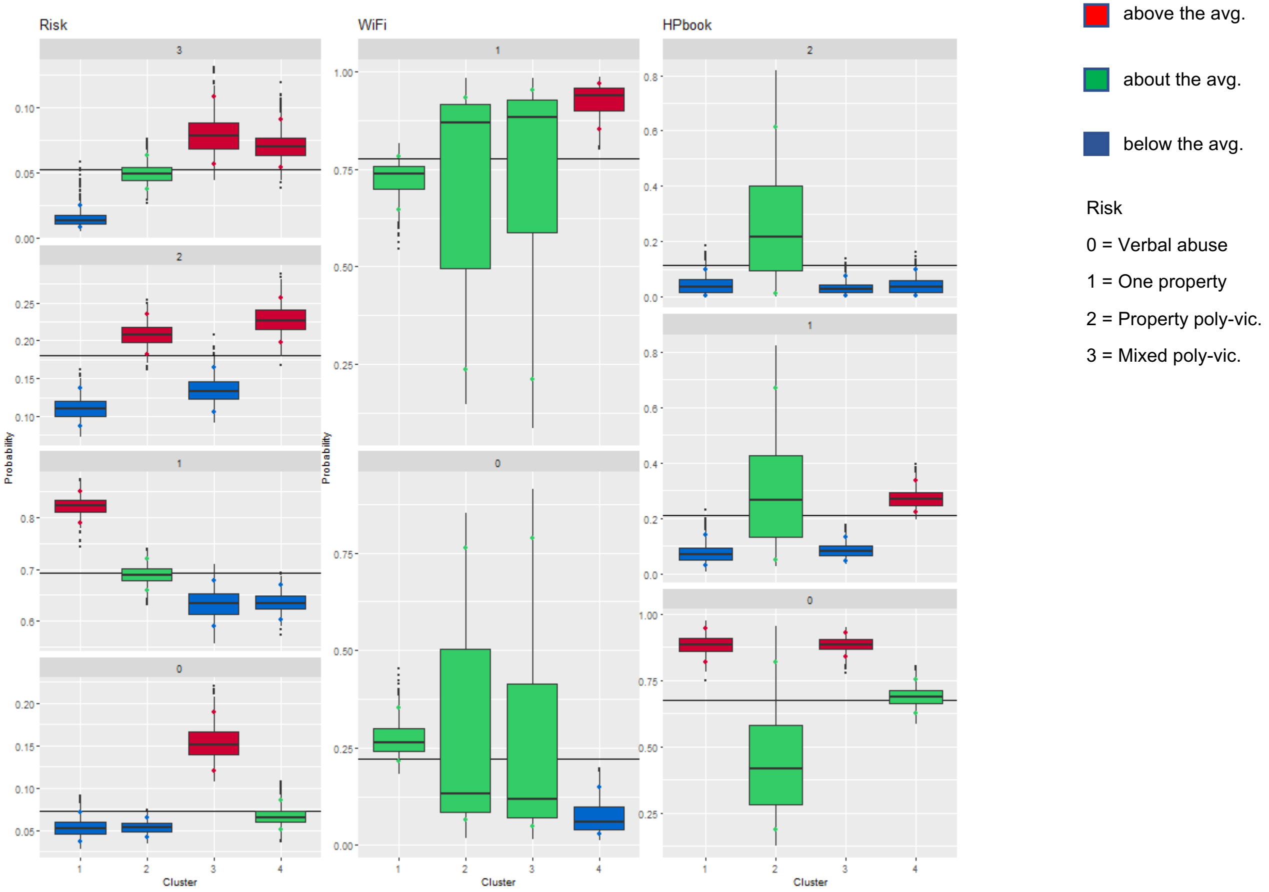


Figure 7.9 Vulnerability and risk of profile identified by BPR. The red-coloured boxes indicate that the 90% credible intervals for the cluster-specific profile parameter are above the average over clusters, the green-coloured boxes indicate that the intervals are about the average, and the blue-coloured boxes indicate that the intervals are below the average.

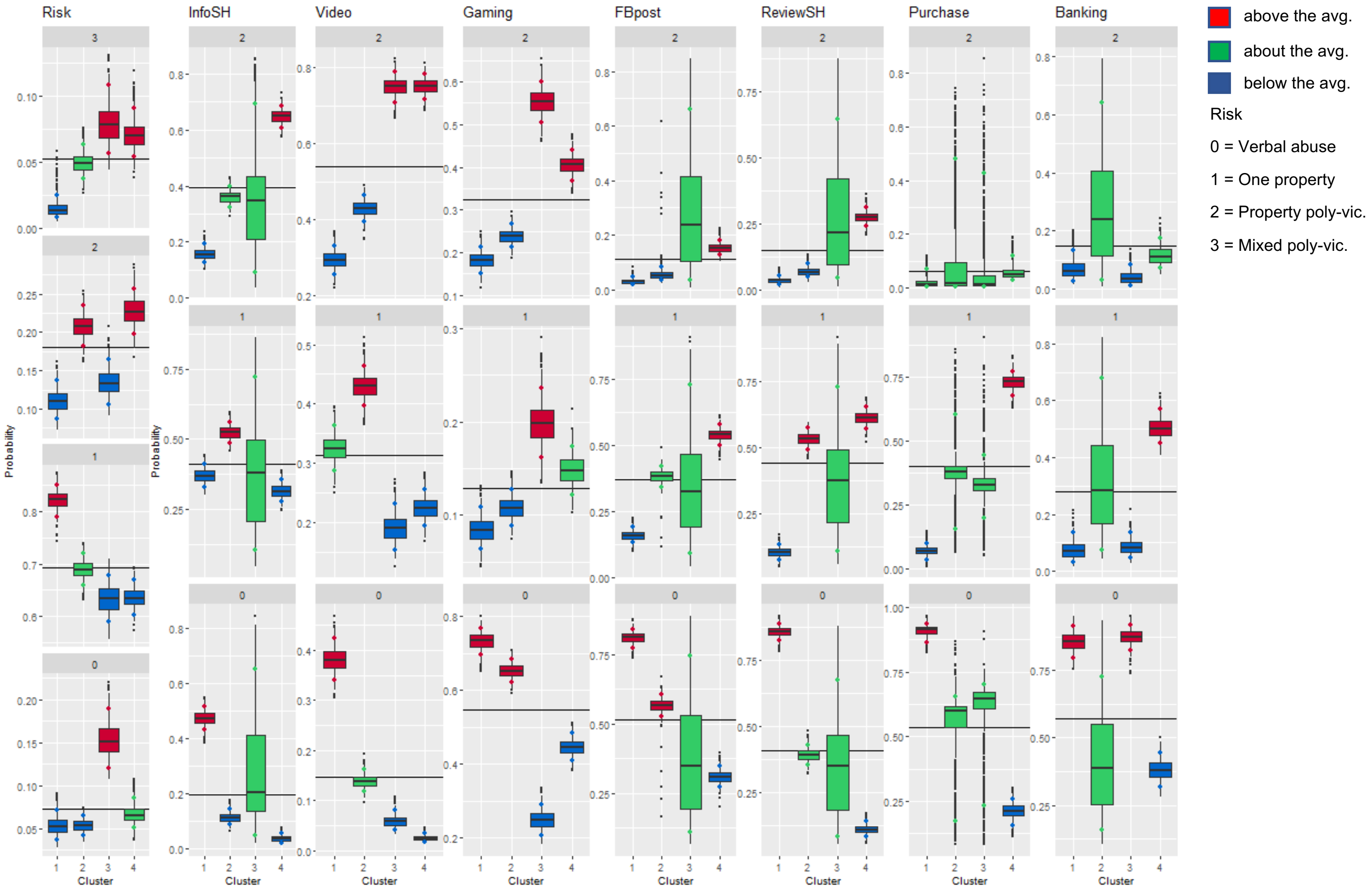


Figure 7.10 Online activities and risk of profile identified by BPR. The red-coloured boxes indicate that the 90% credible intervals for the cluster-specific profile parameter are above the average over clusters, the green-coloured boxes indicate that the intervals are about the average, and the blue-coloured boxes indicate that the intervals are below the average.

Columns correspond to the risk of (poly)victimisation and independent variables, with the posterior distribution of the probability of each category displayed and cluster labels specified on the horizontal axis. The coloured points on the boxplots highlight the 5% and 95% quantiles, therefore representing the 90% credible intervals. The red-coloured boxes further indicate that the 90% credible intervals for the cluster-specific profile parameter are above the average over clusters. The green-coloured boxes indicate that the intervals are about the average, whilst the blue-coloured boxes indicate that the intervals were below the average.

Table 7.6 summarises four profiles of cyber (poly)victimisation and the characteristics of group members. The results revealed that there were four clusters of victims in the Taiwan sample (n = 1,715). Cluster 1 contained single property-related victims that were above the average over the cluster, meaning that this group consisted mostly of victims with one victimisation of either fraud, identity theft, and virus attack. The cluster also contained those who were elderly, financially inferior, unemployed and those who did not hold a university degree. With all the seven activities marked as little use, the cluster members were suggested to be not very active online. Likewise, they also made little use of hospital e-booking services (a measure of individual's vulnerability), suggesting that the cluster members might be less likely to have health problems.

Cluster 2 contained property-related poly-victims who were above the average over the cluster, meaning that group members were statistically and significantly more likely to experience multiple types of property-related cybercrime – a group of poly-victims but experiencing only property-related crimes (not online crimes against the person). Demographic characteristics in Table 7.6 show that those victims were elderly yet earning more than the monthly median wage. Compared to Cluster 1, Cluster 2 members were more active online – moderately involved in searching information, watching videos, and searching product reviews. Yet they seldom posted things on

Facebook or played online games. No vulnerability related variables were found to be statistically meaningful.

Table 7.6 Summary of cybercrime victimisation profiles identified by BPR

Profile	1: One property-related victims	2: Property-related poly-victims	3: Verbal abused victims and mixed poly-victims	4: Property poly-victims and mixed poly-victims
Demographic	Older people, earning less than the average, unemployed, no university degree	Older people, earning more than the average	Young people, earning less than the average, employed, no university degree	Adults, employed, university degree
Vulnerability	Little use of hospital e-service	-	Little use of hospital e-service	Wi-Fi access, moderate use of hospital e-service
Online behaviours	A lower level of online participation	Moderately searching information online, moderately watching video online, moderately searching product reviews; seldom posting things on Facebook, seldom playing online games	Frequently watching video online, frequently playing online games, seldom doing online banking	Very active online

n = 1,715

Cluster 3 contained both verbally abused victims and mixed poly-victims. The cluster members were found to be young people, earning less than the average, employed, without a university degree. Compared to Clusters 1 and 2, these cluster members were more active online. They were found frequently participating in watching online videos and playing online games. Yet they made little use of online banking and hospital e-booking services. One thing to note is that verbally abused victims seemed not to be distinguished from other types of poly-victims, as those who experienced one victimisation of verbal abuse were grouped with mixed poly-victims in this cluster. This means that those who suffered verbal abuse online were very likely to share similar characteristics with mixed poly-victims.

Cluster 4 consisted of property-related poly-victims and mixed poly-victims. These cluster members were found statistically more likely to be employed, at adulthood, and with a university degree. Among all clusters, Cluster 4 contained group members who were the most active online. They were frequently involved in searching information, watching online videos, online gaming, posting things on Facebook, searching product reviews, and moderately doing online purchases and banking. Cluster 4 was the only group that contained members having statistically higher than the mean value of Wi-Fi usage, suggesting Wi-Fi use was a shared factor between people experiencing property-related poly-victimisation and mixed poly-victimisation.

Overall, three out of the four profiles contained poly-victims, with only one group – Cluster 1– relating to victims with one property-related victimisation. These profiles may contain victims with different demographic characteristics. Yet, more importantly, a significantly different pattern is observed in participants' levels of online participation between poly-victims and victims with one property-related victimisation. Victims experiencing only one victimisation were the group that reported being the least active online whilst victims experiencing multiple victimisations of property-related and mixed types of cybercrime were the most active. That is to say, online routine activities appeared to be significantly correlated with online risk among survey respondents, and the more one was involved online the more diverse risks he or she might suffer. This argument is particularly evident in terms of property-related cybercrimes. These findings provide evidence that supports H2: *Poly-victims participate in more online activities than single victims.*

7.6 Discussion

Chapter 6 looked at online victimisation across four types of cybercrime. It therefore distinguished victims from non-victims on the basis of their online lifestyle-routines. Building on the analyses and informed by the LRAA, this chapter examined the differences between victims who experienced one cybercrime victimisation and those who experienced multiple types of victimisations, referred herein as poly-victimisation. To this aim, the study used a subset of the 2017 DOSIH dataset comprising 1,715 individuals who reported experiencing at least one type of cybercrime victimisation in the past year.

Below I discuss the two hypotheses tested in this study and a further three key points to emerge from the analyses reported here. Then, prevention implications of the results and limitations are presented.

7.6.1 Factors associated with cyber poly-victimisation

The prevalence rate of cyber poly-victimisation based on the 2017 DOSIH in Taiwan was around five percent. The most common type of poly-victimisation was identified as identity theft and virus victimisation whilst the least common type was individuals experiencing verbal abuse, fraud, and virus. Victims were less likely to experience verbal abuse alongside other types of cybercrime. Using the Lorenz curves to examine the concentration of poly-victimisation, the results presented above have provided statistical support for H1: *There is significantly a higher concentration of poly-victimisation than would be expected on the basis of random victimisation*.

Based on the patterns of poly-victimisation observed in the descriptive analysis, there were four categories of victimisation defined in Chapter 7: verbal abuse, one property-related victimisation (either fraud, identity theft, or virus infection), property-related poly-victimisation (two or more victimisations of fraud, identity theft, or virus infection), and mixed poly-victimisation of verbal abuse and property-related cybercrime. Using the BPR, it is noted that verbally abused victims did not demonstrate a distinctive profile from other types of victims. It was very likely that those being verbally abused and those with experiences of mixed victimisation shared some common characteristics. It was those who were young, earning less than the average, employed, holding no university degree, frequently watching videos online, frequently playing online games, yet seldom doing online banking that would be likely to experience one-time verbal abuse or mixed poly-victimisation. Other than the unclear profiling between verbally abused victims and other types of victims, the current BPR analysis has identified that poly-victimisation does exist in Taiwan online context.

Additionally, to reaffirm what is stated in Chapter 6, online activities were found to play a major role in the risk of cybercrime victimisation while there was little evidence of a role for guardianship and victim vulnerability. There are three points that could be drawn on the BPR – comparing single victimisation from poly-victimisation. The first point concerns implications taken from comparisons between clusters; the second concerns the application of LRAA in explaining an individual's risk of poly-victimisation; and the last discusses the inconsistency between literature and findings in this study that could inform future research.

First, the comparison between Cluster 1 and Cluster 2 delivers messages about the differences between single victimisation and poly-victimisation. The two clusters demonstrate different online behaviours, alongside slightly different demographic profiles. These two profiles both represent older people but differ with regard to earning and online lifestyle variables such as searching information, watching video, and searching product reviews online. This suggests that older people from a prosperous background showed a moderate tendency of searching information online as well as watching video online and searching product review, and they were also more likely to experience property-related poly-victimisation.

Furthermore, it is clear that exposure to risk/proximity to offenders, measured in this study as participation in online activities, is significantly related to one's risk of poly-victimisation. The more active an individual participates online, the higher (or say more different) risk of online victimisation that one would experience, especially in terms of property-related victimisation. This finding supports H2: *Poly-victims participate in more online activities than single victims,* particularly with regard to property-related cybercrime. Moreover, correlations between poly-victimisation and the diversity and intensity of internet use partly support the finding that poly-victims of cyber harassment tend to use the internet more intensely (Mitchell et al., 2018). This implies that the current study extends the correlations between poly-victimisation and the diversity/intensity of internet use to a wider scope of property-related poly-victimisation beyond cyber bullying/harassment.

Additionally, drawing on the comparison between Cluster 2 (i.e. property poly-victims) and Cluster 4 (i.e. property poly-victims and mixed poly-victims), it is suggested that victims who were most active online – being highly involved in a diversity of online activities – were those who were most prone to the mixed type of poly-victimisation. This does not only suggest devoted online participation as an increased risk of poly-victimisation but also reaffirm that poly-victimisation is activity-specific. That is to say, a moderate user of the internet, who seldom posts things on Facebook and seldom plays online games, might be likely to experience property-related poly-victimisation but is less subject to mixed poly-victimisations. Echoing the findings in Chapter 6, this supports the applicability of the lifestyle approach to an online context, with regard to both single victimisation and poly-victimisation.

Combined with what is mentioned above, the second point that can be taken from this study is the application of LRAA to cyber poly-victimisation. Whilst online lifestyle was correlated with an individual's risk of poly-victimisation, other concepts of target attractiveness and guardianship were not found to play a significant role. This echoes the findings on lifestyle-routine approaches in Chapter 6, where online lifestyle was found more influential than guardianship and target attractiveness on cyber victimisation. Two implications can be drawn. First, online lifestyle, target attractiveness and guardianship may have a different explanatory power in explaining online (poly)victimisations. The varying degree of explanatory power is due to the chosen proxies. Research has questioned the measure of target attractiveness and guardianship in an online context (Vakhitova et al., 2019). For example, the choice of government notification as guardianship in the analysis was guided by the concept that the government may act as a super controller combating internet crime (R. Sampson et al., 2010; Vakhitova et al., 2016). Further, respondents' high frequencies of receiving government notification may indicate a better-developed infrastructure. All these factors are expected to lead to a higher level of government supervision as well as a more secure infrastructure against cybercrime victimisation. However, this measure might not accurately reflect the authorities' actual function as a super controller in preventing cyber (poly)victimisation and therefore the study found the frequency of government notification a limited contribution to profiling poly-victimisation. All these arguments suggest that the measures of target attractiveness and guardianship in an online context be re-examined and improved.

The second implication that guardianship did not play a significant role in online poly-victimisation is that guardianship may act very differently from offline to online contexts. This argument can be supported by the study suggesting that offline guardianship does not act as a protective factor against individuals' victimisation of cyberstalking (Reyns et al., 2016). This is because offline guardians cannot supervise, monitor, or protect potential victims from being victimised online, due to the fluidity of the internet and privacy of computer use. Hence, a live-in family does not protect individuals from either single victimisation or poly-victimisation online as it does in traditional crime, say burglary (see Chapter 4). Briefly, the examination into the application of LRAA to cyber poly-victimisation found that individuals' online lifestyles were related to their risk of poly-victimisation. Further, this study suggests improvements to be made with measures of target attractiveness and guardianship in an online context.

Last but not least, the current study suggests a limited effect of social networking on poly-victimisation, given that the BPR found that instant messaging (say as a measure of the intensity of social networking) had little contribution to distinguishing single victimisation from poly-victimisation. This finding is not in line with research stating that poly-victims are often alienated or isolated from peer social networks (Finkelhor et al., 2007b; Lätsch et al., 2017). Two possible explanations are proposed for the limited effect of social networking on poly-victimisation found in the current study. First, the current study examines poly-victimisations covering both crime against person (verbal abuse) and crime against property (identity theft, fraud, and virus) while the aforementioned research (Finkelhor et al., 2007b; Lätsch et al., 2017) applied a smaller scope of cyberbullying/harassment to probe into poly-victimisations. Put simply, social networking might exert a significant effect against certain types of poly-victimisations (e.g. cyberbullying and harassment) but its effect becomes less obvious when one examines poly-victimisation with a wide range of cybercrime. The second explanation is that instant messaging might be both a measure of social networking and a proxy for one's proximity to potential offenders. As one uses instant messaging, he or she does not only network with others but also exposes him/herself to potential offenders and risk of cyber-attack, either against property or person. This does not mean that social networking is not an important factor against cybercrime, but it does not necessarily help us distinguish victims with one victimisation from those with poly-victimisation. Untangling the effect of social networking on cyber (poly)victimisation would be a fruitful topic for future research.

7.6.2 Prevention implications

The results presented in the current study show that some personal characteristics and online behaviours were significantly related to an increased risk of poly-victimisation. It follows that addressing these factors could inform online crime prevention strategies.

The first implication concerns the vulnerability of users and, in particular, those who use Wi-Fi and hospital e-booking services. The use of Wi-Fi as a correlated risk factor for the mixed type of poly-victimisation informs a need for a more secure Wi-Fi connection system being provided by the system operators. Additionally, users should also be aware that they need to turn to the more secure alternatives of 4G/5G connections when dealing with their personal information, e-banking, and so forth. Another vulnerability variable, measured in this study as respondents' frequency of using hospital e-booking services, can inform prevention strategies as well. Briefly, the study found a relationship between mixed type poly victims and their moderate level of hospital e-booking service. How this finding can inform prevention can be discussed in two aspects: (a) the booking system itself was a risk factor and (b) the booking system was a risk indicator of a person's vulnerability. On the one hand, the hospital booking system itself might be a risk factor (e.g. insecure system) that puts users at greater risk of cyber threats. If this is the case, the hospital e-booking service should be developed to a more secure system, with its vulnerabilities identified and addressed. The website owner – hospital authority – should take responsibility for system security. This argument calls for regular security reviews conducted by hospital (or further official) authority, yet information about hospital cybersecurity reviews is not available in Taiwan at this moment.

On the other hand, this study also considers respondents' use of hospital e-booking as a measure of their vulnerability. This means that a person who uses booking services more frequently is considered more likely to have health problems (e.g. chronic diseases) that, all things being equal, may make them more vulnerable to cybercrime (Le et al., 2016). If so, prevention efforts could also be tailored to these vulnerabilities, for example, through the running of specific public service awareness campaign targeted at at-risk population groups. Based on the BPR results, the aforementioned awareness campaign is suggested to be demographic-specific. That is, considering Wi-

Fi use and hospital e-booking service are related exclusively to victims at adulthood, being employed, and with a university degree, possible awareness campaigns targeting at Wi-Fi users and hospital e-booking users (or say those with health problems) may therefore be more demographic-specific.

The second prevention implication concerns individuals' specific online activities identified as risk factors for the mixed type of poly-victimisation. These activities were Facebook posting and online video gaming in particular. Although crime prevention tends to be more effective when crime-specific, prevention strategies targeted at victims with a high risk of mixed forms of cybercrime victimisation may have cross-crime benefits and thus may be more cost-effective. Prevention efforts targeting behaviours rather than demographic characteristics may also avoid any (ethical) concerns about the identification and targeting of select population groups. In the current case, prevention schemes targeting posting behaviours on social media may have a diffusion of benefits for verbal abuse and poly-victimisation more generally. The responsibility to implement preventative strategies in this area clearly falls outside the remit of the police, and in particular falls on Facebook and other social media companies. There has been a thread of written work highlighting the responsibility of Facebook and other social media companies to institute prevention strategies against cybercrime (Paquet-Clouston et al., 2018; Sallavaci, 2018; M. L. Williams & Burnap, 2016; M. L. Williams & Pearson, 2016). In addition to reinforcing the critical role of social media companies in cybercrime prevention, this study suggests feasible prevention strategies (albeit ascertaining their empirical effect goes beyond this study). Strategies might include e-safety awareness campaigns, real-name registration systems, blinding critical personal information, or automated fraud detection, protecting internet users from experiencing multiple forms of cybercrime. Those strategies would not only deal with a single form but multiple forms of cybercrime at the same time. Again, to what extent do those strategies work against (poly) cybercrime warrants future evidence.

Overall, prevention implications should be differentiated by demographic populations, along with individuals' online activities and behaviours. The current study has identified clear clusters of cyber (poly)victimisation and thus highlights the importance of tailored prevention schemes based on demographic populations. For example, those who are elderly, earning more than the average yet seldom involved in Facebook and online gaming are potential targets of property-related poly-victimisation. Poly-victimisation prevention needs to take these characteristics into consideration. That is to say, awareness campaigns against property-related poly-victimisation might be least likely to utilise social media as the targeted audience do not frequently access those venues. However, as they do moderately search information and product reviews online, awareness campaigns via the utilisation of searching engines might be a strength. Another group of populations that could be provided with specific prevention is those who are young, earning less than the average, employed, and hold no university degree. As they frequently watch video online, frequently play online games, seldom do online banking, yet possibly experience the mixed type of poly-victimisation, the authority could consider forums of online video and games as venues for prevention schemes.

It is noteworthy that the aforementioned prevention implications are drawn from victims' perspectives. Future research might additionally utilise interviews with offenders, as their perspectives might shed further light on many of the findings reported here. Specifically, offender interviews can help better understand how cybercriminals go about selecting targets and what online behaviours – the use of Wi-Fi, hospital e-booking services, or other internet-related behaviours – increase (or decrease) victimisation risk. With a better understanding of cyber offender modus operandi, relevant stakeholders might better identify flaws in the system, reduce crime opportunities and tailor cybercrime prevention strategies accordingly.

7.6.3 Limitations

As the current study uses the same dataset – the DOSIH – as used in Chapter 6, a few limitations can be briefly restated: (a) the potential for bias (e.g. social desirability bias, recall problems, etc.) resulting from single-item measures of cybercrime victimisation; (b) wording of victimisation containing two concepts in one question (i.e. personal information leakage and account theft); (c) no exact measures on time that one spent online; (d) no information about users' legitimacy of online activities (e.g. accessing legal or pirate websites when watching video online); (e) few items available to measure the concept of guardianship, especially physical guardianship (e.g. firewalls, antivirus software); (f) lack of environmental factors such as perceptions of community climate and perceptions of safety, employment setting (workplace stressors) and community setting (culture diversity, etc.) to understand the environmental effect on cybercrime victimisation.

Three additional limitations are raised in the current study. First, there is no information by which to understand respondents' offline victimisation(s). As some recent cyber studies have suggested a connection between offline and online abuse – one form of poly-victimisation (Cénat et al., 2019; Q. Chen et al., 2018), the current dataset falls short of providing information about offline victimisation. Put differently, those who experience verbal abuse online may also be verbally abused offline. The lack of such offline information restrains the current study from exploring if lifestyle or poly-victimisation of group members vary offline within a cluster. The lack of such offline information may derive from the purpose of the DOSIH survey itself, which was to understand regional inequality in internet access rather than levels of cyber victimisation. However, future integration of the TAVS and the DOSIH would help overcome current knowledge gaps regarding this online-offline connection.

Second, survey responses do not contain information on repeat victimisation. Whilst poly-victimisation is an important but less explored field, the research reported here would have been enriched if data were available on the extent of repeat cybercrime victimisation. This is of great importance with comparative studies between contexts, either for cultural differences or online/offline comparison. Furthermore, the data could have been better if respondents' reporting victimisation to the police was recorded.

Research on reporting practices may shed light on repeat victimisation or differences in reporting determinants between types of online (or offline) victimisation (e.g. van de Weijer et al., 2019)[8].

Last but not least, the current DOSIH does not record sequences of victimisation, or the time of each reported victimisation. Little information could be drawn to examine if cybercrime incidents are sequential, for which one crime generates the opportunity for other crimes to occur. That is, for example, an identity theft (or information leakage) may generate another online fraud. Likewise, a virus attack may result in victimisation of identity theft, and further lead to another incident of fraud. Whilst the study suggests distinctive profiles of online activities between single victims and poly-victims for property-related crime, it is not clear whether the poly-victimisation is a mechanism of the 'crime multiplier' effect (Felson, 2010). The inclusion of victimisations in sequence to the DOSIH would enable researchers to explore such a mechanism and further to make meaningful implications for crime prevention.

7.7 Chapter conclusion

This chapter used the Lorenz curve to identify that poly-victimisation was not randomly distributed over victims and was more concentrated than on a random basis. This study further applied the BPR to classify (poly)victims of cybercrime. The current findings suggest that victims with one victimisation demonstrated different characteristics from poly-victims and users' online lifestyle were related to their risk of being poly-victimised. Those who were highly involved in diverse online activities were more likely to suffer mixed types of cybercrime victimisation, compared to their counterparts living without frequent internet use.

[8] The study uses data drawn from four waves of Dutch cross-sectional population surveys (N=97,186 victims) and finds that: 1) cybercrimes are among the least reported types of crime; 2) the determinants of crime reporting are different between traditional crimes and cybercrimes, between different types of cybercrime (i.e. identity theft, consumer fraud, and hacking)

From a practical prevention perspective, it is also worthwhile to consider a specific group of populations alongside their online tendency. For example, awareness campaigns against Wi-Fi security might target potential victims in adulthood, being employed, and with a university degree. Additionally, the prevention strategy against property-related cybercrime could be elderly-focus and cooperating more with the searching engine than social media platforms. It is because the vulnerable population of concerns for property-related poly-victimisation is very likely to be those who are elderly, from a prosperous background, without frequent use of social media (say Facebook in this study) yet having a moderate tendency of watching video and searching information or product review online. Likewise, prevention schemes via venues of forums of online video and games could consider the characteristics of the population – people who are young, earning less than the average, employed, and without university degree. While the prevention might be beneficial from demographic-specific perspectives, this chapter also sheds light on cross-crime benefits even when prevention is focused on a single crime type. That is to say, because poly-victims seem to share some characteristics in common, prevention against property-related crime may have a diffusional effect on poly-victimisation.

Finally, the current study calls for the improvement of datasets – say the DOSIH or TAVS. The inclusion of respondents' victimisations in sequence, experiences of repeat cybercrime victimisation, crime reporting behaviours to the police, and a combination of online/offline lifestyles might bring some important perspectives to crime research and the practice of cybercrime prevention.

Chapter 8 Discussion

This final chapter provides an overview of the main theoretical and applied implications of the research presented here. It also discusses key limitations and suggests directions for future research. The chapter begins by reminding the reader of the main aims of and motivation for this thesis. This is followed by short summaries of the key findings as they relate to the thesis research questions. Then, I compare the findings of this research with those of past studies and discuss their theoretical and practical implications. Lastly, this chapter discusses the strengths and limitations of my study and suggests directions for future research.

8.1 Overview of study aims and motivation

As indicated at the outset of this thesis, EC marks a shift in the orientation of criminological research. It casts opportunity as a causal factor in crime and pays greater attention to the causal role played by factors (both people and objects) existing in the immediate environment in which crime takes place. The routine activity approach (RRA) forms one of three theoretical perspectives that underpin EC, the other two pillars being crime pattern theory and the rational choice perspective (Wortley & Townsley, 2016).

Drawing on the RAA and individuals' lifestyle as risk factors for criminal victimisation, the LRAA sets out an opportunity framework for how environmental factors provide opportunities for crime to occur. To recap, the LRAA suggests five elements – attractiveness of potential targets, lack of guardianship, exposure, proximity to potential offenders and definitional properties featured by specific crime (or understood as crime-specific knowledge or instrumental actions by potential offender) – as risk factors that influence opportunities for crime to occur (Cohen et al., 1981). Numerous studies have applied the LRAA to examine patterns of crime in the Western context, with regards to both traditional crime (e.g. Bowers et al., 2005; Cohen et al., 1981) and more recently cybercrime (e.g. Vakhitova et al., 2016).

This thesis was primarily focused on understanding the patterns of crime victimisation in Taiwan, a non-Western context where the LRAA has been less researched. Two broad types of crime were considered, including both offline and online victimisation. Four research objectives were investigated: (1) victimisation of burglary; (2) repeat and near repeat victimisation of burglary; (3) victimisation of cybercrime; and (4) poly-victimisation of cybercrime. Using data drawn from the TAVS, the DOSIH, and police datasets, this thesis aimed to identify both the risk factors for and mechanisms that might explain different types of victimisations in the Taiwanese context, informed by EC in general and the LRAA in particular.

My interest in researching criminal victimisation patterns in Taiwan from an opportunity perspective was driven, in part, by identified gaps in the literature. Taiwan's lack of research-informed crime prevention and policing, recognised through my previous police work, strengthened this research interest. My interest was to examine if crime patterns found in Western contexts are also observed in the non-Western society of Taiwan, where crime rates are comparatively low (albeit have still fallen dramatically in recent decades), and by extension whether the popular LRAA is generalisable to the Taiwanese context, both for traditional crimes (such as burglary) and cybercrimes. In pursuing this interest, this thesis makes two broad contributions to the research literature. First, it contributes evidence on the applicability (or not) of the LRAA to a non-western context with low crime rates. Second, it helps identify risk factors and enrich knowledge for crime prevention purposes in Taiwan in both the online and offline context.

Six research questions were thus proposed in this thesis:

Question 1: Does a LRAA adequately explain burglary victimisation patterns in Taiwan?

Question 2: Is there evidence of (near) repeat burglary victimisation in Taiwan?

Question 3-a:	Does the LRAA adequately explain patterns of online victimisation in Taiwan?
Question 3-b:	Do victimisation patterns vary across different types of online victimisation in Taiwan?
Question 4-a:	Is there evidence of online poly-victimisation in Taiwan?
Question 4-b:	Do victimisation patterns vary between single and poly-victimisation online?

8.2 Overview of main findings

The studies presented in this thesis are centred on two main types of crime victimisation – burglary and cybercrime. There are four empirical chapters, of which the first two centre on burglary and the rest on cybercrime. Chapter 4 and Chapter 6 deals with the prevalence of certain types of crime whilst Chapter 5 and Chapter 7 deal with matters of crime concentration, either repeat victimisation or poly-victimisation. The goal was to tell the story of (repeat) victimisation in offline (burglary) and online (cybercrime) context in Taiwan, informed by the LRAA framework.

Below I summarise the main findings from this thesis as they relate to the above six research questions.

RQ 1. Does a LRAA adequately explain burglary victimisation patterns in Taiwan?

Building on the concepts of target suitability (accessibility and attractiveness), guardianship and proximity/exposure to potential offenders, Chapter 4 investigated patterns of burglary victimisation in Taiwan, using data collected as part of a nationally representative victimisation survey.

The study provided partial support for the applicability of LRAA to burglary victimisation in Taiwan. To be specific, the study found statistically significant relationships between measures of target accessibility, guardianship and burglary victimisation – particularly at the individual household level – that are in line with the (mainly western) research literature. Also, the study provided evidence supporting the hypothesis that multiple household security measures provide greater protection against burglary victimisation than single security measures, as has been found in burglary research conducted elsewhere (Tseloni et al., 2017; van Dijk, 2008).

However, the findings reported here did not provide evidence for a relationship between exposure and proximity to crime/potential offenders and SDT and burglary. Furthermore, unlike the dominant finding in the literature suggesting that risk of burglary depends on the interaction between target attractiveness and the environment (Bowers et al., 2005), this study found limited evidence that could support the existence of such an interaction (between household income and neighbourhood poverty) in Taiwan.

RQ2. Is there evidence of (near) repeat burglary victimisation in Taiwan?

Whilst repeat burglary victimisation is common in many western industrialised countries, the prevalence and patterns of repeat residential burglary in Taiwan remains less clear. Drawing on victim survey data and local police crime statistics, the study reported in Chapter 5 explored if there are patterns of repeat and near repeat burglary victimisation in Taiwan.

The findings indicated a consistent and highly concentrated pattern of repeat burglary victimisation in Taiwan, more so than is often found in western settings. To be specific, repeat burglary patterns were found, in line with the literature, and at a level that is greater than would be expected on the basis of chance. Digging deeper into these patterns of repeats, it was also found that semi-detached houses in Taiwan suffered a significantly lower risk of burglary revictimisation than would be expected according to a Poisson distribution, consistent with Bowers et al.'s (2005) study from the UK. Also in line with previous research, the risk of burglary victimisation in Taiwan was found to decay across both time and space following an initial burglary incident, covering a period of around three weeks and 400 metres. However, the findings also suggested that burglary risk within 100 metres of a prior incident was not elevated to statistically significant degree, differing to the common finding in prior western studies.

It is noted that the concentration of repeat victimisation was found to be far higher in Taiwan than in their western counterparts. In this study, 56 percent of burglaries were repeats, whereas the highest counterpart documented in the literature that I am aware of is 33 percent reported in a US study (Farrell & Bouloukos, 2001). Likewise, the concentration of repeat burglaries was found to be comparatively high in Taiwan, with the top 10% most burgled households accounting for about 30% of all burglaries among the sampled households. The equivalent statistic in the UK is less than 20% of all burglaries (Tseloni & Pease, 2005). Moreover, considering the capping convention of six victimisations in the TAVS (also see Section 5.5.2), the true concentration of repeats is likely to be even higher in Taiwan than the current study suggests.

The levels of near repeat burglary victimisation found when analysing local police recorded crime data were noticeably lower than those found in western countries, or even in some Chinese settings. For example, this thesis found that burglaries within 200 metres and 14 days (or seven days) accounted for just five percent of all burglaries, whereas the same statistic is around 23% within 200 metres and seven days in the UK (Chainey, 2014) and 26% within 120 metres and 14 days in Wuhan city, China (Wu et al., 2015). Drawing on both the TAVS and police data, it seems that burglaries in Taiwan were found to be more concentrated on the same targets but less on those targets nearby.

RQ3-a. Does the LRAA adequately explain patterns of online victimisation in Taiwan?

The study in Chapter 6 examined whether the LRAA applied to a wide range of cybercrime victimisation – verbal abuse, identity theft, fraud and virus infection. The aim was to understand, using a nationally representative and hitherto underutilised dataset, how different online environments and behaviours made individuals more or less likely to experience different forms of cybercrime in Taiwan.

The study found evidence to partially support the argument that the LRAA could be applied to explain online victimisation patterns in Taiwan, particularly with regard to individuals' routine activities and lifestyles. Two findings were noteworthy. First, the effect of participants' demographic characteristics on online victimisation were moderated by their online lifestyle-routines, as the emerging cybercrime literature suggests (Kalia & Aleem, 2017; Reyns et al., 2011). For example, younger and male respondents were initially found more likely to be involved in verbal abuse incidents, yet such correlations became less obvious when taking into account their online routine behaviours. Second, the more diverse an individual's online activities were, the greater the level of exposure/proximity to potential offenders and, by extension, the greater the risk of victimisation. This is again in line with both the cybercrime literature in particular (Bossler & Holt, 2009; Reyns et al., 2011) and crime opportunity theories more generally.

Although the moderated risk of cybercrime victimisation by individuals' online routine activities and lifestyle implied that online behaviours played an important role in online victimisation, the concepts of target attractiveness and guardianship were challenged in the Taiwanese context, at least as these concepts were measured herein. The study therefore echoed the argument that due to the generally private nature of computer use, the function of "live-in guardians" might not work in the immediate online environment (Reyns & Henson, 2016).

RQ3-b. Do victimisation patterns vary across different types of online victimisation in Taiwan?

The answer to this question depends on how we explain patterns and mechanism. Generally speaking, the patterns and mechanism may be explained by individual's online lifestyle-routines. Yet risk factors were found to vary across types of victimisations as some activities seemed to be 'risky' for one specific type of cybercrime alone, as would be predicted by the LRAA. For example, posting on social media was found to be related to an increased risk of being verbally abused online but unrelated to other types of cybercrime. This finding reinforces a central pillar of EC: that different crimes are brought about by different opportunity structures and therefore it is important, from both a theoretical and prevention perspective, to be crime-specific. Whilst generally discussed in the context of traditional (offline) crimes, this study suggests that the same is also true for online crimes in the atypical setting of Taiwan. Lumping all cybercrimes together may miss important patterns and important opportunities for intervention.

However, some risk factors, such as the tendency to post aggressive messages, having a disability or watching videos online were found consistently related to at least two types of cybercrime victimisation. The most consistent risk factor across all types of cybercrime considered here was an individual's diversity of online participation, measured here as an individual's involvement in different kinds of online behaviours. Again, all these findings suggest that although the general pattern and mechanism of online victimisation were found to be related to users' lifestyle-routines, risk factors may depend on specific types of victimisations.

RQ4-a Is there evidence of online poly-victimisation in Taiwan?

Chapter 7 examined if there is a pattern of online poly-victimisation in Taiwan. Based on patterns of poly-victimisation observed in the descriptive analysis, there were four categories of victimisation defined in Chapter 7: verbal abuse, one property-related victimisation (either fraud, identity theft, or virus infection), property-related poly-victimisation (two or more victimisations of fraud, identity theft, or virus infection), and mixed poly-victimisation of verbal abuse and property-related crime. The last two categories, both referred as poly-victimisation, represent an individual's experience of two different crime types over the study period.

Using these four categories, the main findings of Chapter 7 were that poly-victimisation did exist in the Taiwan online context. Online activities played an expected role in terms of risk of cybercrime victimisation, though guardianship and vulnerability also remained less evident as a victimisation predictor, as was the case in Chapter 6. The study further suggested that there is a pattern of poly-victimisation in Taiwan. That is, victims who were very active online – or say highly involved in a diversity of online activities – were found to be at the highest risk of suffering poly-victimisation. Contrarily, a moderate internet user who seldom posted things on Facebook and seldom played online games might be more likely to experience property-related poly-victimisation but less likely to experience mixed poly-victimisation. Hence, yes, the findings reported here indicate that there is a pattern of online poly-victimisation in Taiwan and the pattern is suggested to be related primarily to users' online lifestyle-routines.

RQ4-b. Do victimisation patterns vary between single and poly-victimisation online?

The study further probed into the differences between victims who experienced one cybercrime victimisation and those who experienced multiple types of victimisations, referred herein as poly-victimisation. The study suggested that some forms of single cybercrime victimisation differed from poly-victimisation but some forms did not. On the one hand, the differences in victims' characteristics between single victimisation and poly-victimisation of property-related cybercrime were suggested to be their earning and levels of involvement in online activities. Older people earning more than the average tended to show a moderate tendency of searching information online as well as watching videos online and searching product reviews, and they were also more likely to experience property-related poly-victimisation. On the other hand, older people from a disadvantaged background (earning less than the average, unemployed and without a university degree) and who were less active online were found likely to experience single victimisation of property-related cybercrime but not poly-victimisation.

Overall, the study did not find meaningful differences between those who experienced single victimisation of verbal abuse compared to those who suffered poly-victimisation. However, the study did find differences between those who experienced single victimisation of property-related cybercrime to those who experienced property-related poly-victimisation. In other words, victimisation patterns were found to vary between single and poly-victimisation of property-related cybercrime and those variations can be explained by individuals' online lifestyle-routines.

8.3 Theoretical implications

The thesis found both consistent and inconsistent evidence with past research. They have theoretical implications in three main aspects: the generalisability of the LRAA, theoretical implications for repeat victimisation and poly-victimisation and implications for crime research.

8.3.1 Generalisability of lifestyle-routine activity approach

EC, and the LRAA in particular, has long been applied to explain patterns of criminal victimisation in the West. Yet an opportunity framework (i.e. LRAA) has been less common in research in non-Western settings. Although most of the industrialised Asian countries experience less crime compared with Western countries (del Frate & Mugellini, 2012; Sidebottom, Kuo, et al., 2018), empirical research on crime victimisation from the perspective of the LRAA could still help researchers better understand crime patterns and their underlying causal mechanisms, and generate knowledges for practical crime prevention efforts.

Exploring the generalisability of the LRAA to Taiwan is centred on two aspects in this thesis: traditional offline victimisation of burglary and online victimisation. To conclude beforehand, this thesis suggests that the LRAA can explain patterns of victimisation in Taiwan, to some extent. Yet, the extent to which it applies may vary for offline and online crimes.

8.3.1.1 Lifestyle-routine activity approach to burglary victimisation in Taiwan

Based on the examination of the LRAA into burglary victimisation in Taiwan, this thesis suggests that the LRAA is applicable in explaining patterns of burglary victimisation in Taiwan, to some extent. To be specific, two main points were found consistent with the literature: target attractiveness and guardianship at an individual household level. First, the thesis found a households' level of target attractiveness positively related to risk of burglary victimisation (Miethe & McDowall, 1993; Miethe & Meier, 1990). Second, guardianship at an individual level works to explain burglary victimisation. On the one hand, occupancy was found to be significantly negatively correlated to victimisation (Maguire et al., 2010). On the other hand, security measures were found to be effective protection against burglary victimisation, and combinations thereof found to be especially effective (Tseloni et al., 2017).

However, in line with the aforementioned Asian studies (Roh et al., 2010; L. Zhang et al., 2007), proximity/exposure factors and guardianship drawn on the SDT at the neighbourhood level were found less evident in explain burglary victimisation in Taiwan. These findings concern the generalisability of LRAA (and SDT) to burglary victimisation in Taiwan, of which individual-level factors were more evident than were neighbourhood-level ones.

8.3.1.2 Lifestyle-routine activity approach to cybercrime victimisation in Taiwan

To my knowledge, limited research has examined a comprehensive range of cybercrimes from the perspective of the LRAA. A great body of research has had an exclusive focus on cyberbullying in particular. Moreover, no prior research in Taiwan had paid any attention to cybercrime victimisation from an EC perspective. This thesis therefore added to this under researched area.

Firstly, in line with the literature, this study found that individuals' online lifestyle played a consistent role in predicting their risk of victimisation for all forms of cybercrime (Vakhitova et al., 2016). Generally speaking, the more an individual went online[1], the higher their risk of cybercrime victimisation. Also, individuals' routine activities and lifestyles were found related to their victimisation in an online context, of which risk arose by certain lifestyle-routines (e.g. verbal abuse by Facebook and aggressive posting, virus infection by watching videos, or fraud by online purchases).

However, this research found limited evidence on the effectiveness of guardianship and the role of target attractiveness in online victimisation in the Taiwanese context, possibly because the measures of guardianship used here were a departure from those used in previous research. Overall then, the evidence presented here suggests that the LRAA might be generalisable to Taiwan, yet modification of how the concept of guardianship is measured may be needed.

8.3.2 Repeat victimisation vs poly-victimisation

To recap, there are several recurrent findings about RV and its underlying mechanisms: (1) repeats are highly prevalent in high crime areas; (2) a small

[1] Note in this thesis, general internet use was operationalised via the number of activities that one reported having participated in online, rather than the exact time that they spent online (see Section 6.3.2).

number of repeat victims typically account for a disproportionately high number of all victimisations; (3) prior victimisation is a reliable predictor of future victimisation (involving the 'flag' and 'boost' mechanism); and (4) RV tends to occur quickly in the wake of an initial victimisation and the risk depends on the temporal and spatial proximity to the initial crime target (see Chainey & da Silva, 2016; Farrell, 1995; Farrell & Pease, 2017).

In relation to the findings from this thesis, firstly, repeats were found also to be prevalent in low crime areas like Taiwan. Further based on this finding, the second implication is that Taiwan experienced a consistent yet far higher concentration of victimisations across a small number of repeat burglary victims. Third, the generally consistent patterns of RV identified in Taiwan have suggested that the 'flag' mechanism is relevant to Taiwan, whereas the boost mechanism was not examined in this thesis due to lack of data (see Section 5.5.2 for detail). Fourth, the findings on the decaying risk of victimisation by time from the initial burglary event also partially support the last recurrent finding concerning the time course of RV.

However, the inconsistency found in the spatial proximity to the initial event (particularly within 100 metres of a prior incident) suggests atypical patterns of near repeat burglary in Taiwan. The decay function might be influenced by unknown factors, such as crime prevention efforts which serve to reduce the risk of near repeats. More empirical studies are needed to better understand whether the findings related to NRV found here are representative of Taiwan and, if so, why they might depart from what is typically found in comparable studies conducted elsewhere.

Furthermore, with respect to the lesser explored area of poly-victimisation, several noteworthy findings emanated from this thesis. The findings suggested a population inequality of cybercrime victimisation in an online context as was observed in the offline context (Tseloni & Pease, 2005). That is to say, a small number of victims in Taiwan accounted for a disproportionately high number of all online victimisations. This finding expands on the previous result about the concentration of crime by the same form over the same targets, to that of multiple forms of victimisation experienced by the same targets, and further to an online population. This also implies a possibility to apply the existing theories about RV to poly-victimisation. For example, the identified vulnerabilities exhibited by individuals' online lifestyle-routines could act as a 'flag' mechanism in explaining poly-victimisation beyond the widely researched RV.

8.3.3 Implications for future research

This thesis has implications for future research in two main areas: (1) the use of BPR in the study of poly-victimisation and (2) research on crime patterns in Taiwan.

8.3.3.1 Statistical approach of Bayesian profile regression to crime research

Beyond the contributions discussed above, the thesis also contributes to the field of quantitative criminology by applying Bayesian regressions to model crime victimisation. Two specific contributions are made here. First, the thesis provides an alternative approach to modelling data containing highly inter-related variables, for which the conventional way of using a generalised linear regression to model categorical outcome variables is criticised for generating potentially biased inferences (Molitor et al., 2010; B. H. Patterson et al., 2002). The BPR, by modelling the risk of groups of participants rather than the risk of individual participants taken from conventional regression methods, would avoid making such potential biased inferences (Molitor et al., 2010).

The second contribution to quantitative criminology relates to an innovative approach to model crime victimisation in general, and poly-victimisation in particular. Although the BPR has recently been applied in health and medical research (e.g. El-Saifi et al., 2019; Hastie et al., 2013; Mattei et al., 2016), it has received little attention in crime research. As far as

I am aware, Vakhitova et al.'s (2019) study was the first to apply the BPR to crime data. However, that study dealt with cyber abuse (defined by them as receiving abusive messages or comments online) alone and did not consider other types of cybercrime. This thesis provides additional support to the applicability of BPR to criminology by modelling a wider range of cybercrimes and by exploring poly-victimisation. It is argued that this statistical technique has much wider applications for quantitative criminology.

8.3.3.2 Crime research in Taiwan

The thesis contributes to crime research in Taiwan in two main ways. First, it is noteworthy that crime research in Taiwan tends to focus on criminality (or the distant causes of crime) rather than the immediate environment that provides opportunities for crime to occur. The thesis took a different perspective, focussing on patterns of victimisation through the lens of EC, in particular the LRAA. When introducing the (multilevel) opportunity framework to explore the conventional crime of burglary and emerging forms of cybercrime (e.g. verbal abuse, identity theft, fraud and virus), the thesis demonstrates the utility of crime opportunity theories in the Taiwan context. It also suggests that use of crime opportunity theories to examine other forms of crime pattern in Taiwan might be fruitful. Second, presently research on cybercrime in Taiwan has mainly sought to provide an overview of the problem (e.g. L. S. F. Lin & Nomikos, 2018; Lu et al., 2006); less attention has been paid to investigating the patterns and predictors of online victimisation. In drawing on the LRAA, this thesis provides statistical evidence to model the patterns and correlates of a range of cybercrimes in Taiwan, using nationally-representative data.

The importance of this thesis lies in not only developing a new focus of crime research in Taiwan that bridges the gap between the Western literature, but in stressing the possibility that by altering the immediate environment rather than dispositional characteristics of offenders, single victimisation, RV and poly-victimisation in Taiwan can be prevented. How crime prevention can be informed by this thesis will be discussed in the next section.

8.4 Implications for practice

This thesis has implications for practice in three main areas: burglary prevention, cybercrime prevention, and improvement for crime victim survey designs in Taiwan. The last one might not be intuitively related to practical crime prevention but is of great importance in order to broaden the knowledge base about crime patterns in Taiwan which in turn can inform and sharpen crime prevention efforts in Taiwan.

8.4.1 Prevention implications for burglary

The thesis informs burglary prevention in two areas: resource allocation and possible prevention approaches. First, this thesis highlights an uneven distribution (particularly temporally) of burglary across the population in Taiwan. Put simply, the identified temporal regularity (within 21 days following the initial incident) could usefully inform the allocation of preventive resources to those recently burgled properties. Moreover, the extreme vulnerability observed in direct repeats over spatially near repeats would help deploy police resources to particularly troublesome targets. Allocating preventive resources to past victims quickly should reduce repeats thereby reducing a chunk of crime overall, as has been demonstrated through various studies in the UK (for summarised key findings see Laycock, 2001). The thesis thus has an important implication for prioritising police work especially in terms of proactive policing. Put differently, given that the police task often involves deployment to deal with calls for services (reactive policing), the inequality of vulnerability over the population observed in this thesis can guide proactive policing and distributive justice in policing.

Crime prevention is not just the responsibility of the police alone. The identification of the most vulnerable targets should not only inform proactive policing but also resource mobilisation by relevant stakeholders. House owners, construction companies, community or even the social welfare system are all regarded as relevant stakeholders, and, as discussed below, can play a role in burglary prevention in Taiwan, based on the findings reported here.

Although the thesis did not examine SCP specifically, prevention against burglary in Taiwan could draw on the key concepts of *"increase the effort", "increase the risks", "reduce the rewards", "reduce provocations" and "remove excuses"* underpinning SCP (Clarke, 2016) (also see Section 2.2.3). Specifically taking the findings of this thesis with the effect of neighbourhood heterogeneity controlled, the studies presented in Chapter 4 suggested the effectiveness of multiple security measures against burglary, rather than that of conspicuous security measures (defined in the study as security bars on windows and door chains). The presence of multiple security measures likely increases offenders' efforts to break into the property, increase their risks of being identified or arrested, and thus prevent a burglary from being completed, as seen in studies elsewhere (Thompson et al., 2018; Tseloni et al., 2017). Therefore, to secure a dwelling from being burgled, house owners must be encouraged to take further precautions other than merely installing the prevalent security bars on windows as a protection. At least at this stage, the timer is suggested as an add-on security measure in terms of burglary prevention.

Another risk factor that may inform SCP would be easy access of a dwelling. The easier a dwelling is accessed by potential offenders, the higher the risk of burglary. This suggests better access control may lead to burglary reductions. Security measures such as door chains or security bars on windows (or say conspicuous security measures) that block offenders' access to the dwellings might be a choice. Nevertheless, a previous Taiwanese study reported damaging door chains and security bars on windows as a common modus operandi for burglary entries in Taiwan (Ho, 2013). The current study has further found that the conspicuous security measures do not work properly when neighbourhood effects are taken into account. The thesis thus calls for further analyses of free text police data or interviews with burglars to better understand burglars' entries and the plausibility of access control against burglary victimisation in Taiwan. In this way, the stakeholders can be informed by improvements in house designing to control potential offenders' access to potential crime targets (i.e. increasing the effort). Construction companies, the community, and even the local department involving urban and rural development affairs (or some referred as agents of urban planning) are all involved as stakeholders.

Otherwise, we may look the finding about easy access as a risk factor from a different angle of crime prevention. Until the aforementioned examination into burglars' entries and the plausibility of access control taking place, households with easy access should adopt extra security than conspicuous security measures. This is because those dwellings are the 'hot' target for burglary, as presented in this thesis. Simply put, while SCP informs how we can systematically prevent burglary in Taiwan, the thesis strengthens its own importance in identifying the most vulnerable households. In this vein, the house owners, community, construction companies, and the (local) authority can work together in burglary prevention, targeting dwellings with easy access in particular.

Overall, the suggested preventive approaches may require further research to explore which combination of security measures outperform others and by which means do offenders gain access to houses. Policies should also draw on evaluating the cost and effect size derived from the specific prevention measures put in place, or, say if the effect size outweighs the cost of the combined security measures of interest. If it is not the case, cheaper but somehow effective combinations would be taken as an alternative. With future analyses into cost-effectiveness of prevention approaches, the thesis can inform prevention against repeats and further application of SCP to burglary prevention in Taiwan more fruitfully.

8.4.2 Prevention implication for cybercrime

Results from the thesis suggested that online behaviours have an important impact on the risk of cybercrime victimisation and cybercrime poly-victimisation. Table 8.1 summarises the observed relationships between online (poly)victimisation and the individual risk factors identified in Chapters 6 and 7. The table is presented here because it sheds light on possible cybercrime prevention strategies designed to counter or mediate the identified risk factors. For example, strategies targeted at aggressive posting behaviours would be expected to mediate an individual's risk of verbal abuse, virus infection and further to mixed type poly-victimisation. The table also suggests profiles of poly-victims as presented in Chapter 7, which may inform prevention efforts, particularly in relation to the demographic characteristics of victims. Take property-related poly-victimisation, for example, the findings presented here show that elderly individuals earning above average exhibit higher risks victimisation. Equipped with this knowledge, prevention efforts might therefore focus on this at-risk group as a priority.

Following on from Table 8.1, Table 8.2 suggests plausible prevention strategies for online (poly)victimisation based on the findings presented here and drawing on Clarke's (2016) 25 SCP techniques. It is noted again that although it is argued by Clarke that SCP needs to be crime-specific, prevention strategies targeted at victims with higher risks of poly-victimisation may have cross-crime benefits and thus may be cost-effective. For example, prevention efforts targeted at risky online behaviours such as posting on Facebook might lead to reductions in verbal abuse as well as poly-victimisation. Similarly, prevention efforts targeted at the riskier use of Wi-Fi connections might prevent both viruses and the mixed type of poly-victimisation. With the attempt to increase the offenders' effort to carry out virus attacks or other forms of cybercrime, it is suggested that stakeholders should provide a secure Wi-Fi connection system and that individuals turn to

Table 8.1 Summary of risk factors for cybercrime victimisation using data from 2017 DOSIH, Taiwan

Variables / Type of victim	**Verbal abuse**	**Identity theft**	**Fraud**	**Virus**	**Property-related poly-victim**	**Mixed type poly-victim**
Socio-demographics						
Age		-		+	Elderly	Adulthood
Gender			Female	Male		
Good income					+	
University degree				-		+
Employed (vs unemployed)						+
Student (vs unemployed)		-	-			
Disability	+			+		
Online behaviours						
Number of online activities	+	+	+	+	+	+
Instant messaging				-		
Searching Info online					+	+
Searching product review					+	+
Video watching		+		+	+	+
Gaming					-	+
Facebook posting	+				-	+
Purchasing			+			
Aggressive posting	+			+		+
Online banking						+
Wi-Fi use				+		+

Note: '- ' negatively related to victimisation; '+' positively related to victimisation; a cell left blank means no statistically significant effect could be drawn on.

Table 8.2 Prevention of online (poly)victimisation drawn on SCP based on findings of cybercrime victimisation in Taiwan, 2017 DOSIH

SCP	Targeted behaviours	Suggested prevention	Techniques/modified situation	Stakeholders	Possible benefits of diffusion
Increasing the effort	Posting on Facebook	• e-safety awareness campaigns	Targets' awareness of verbal abuse/poly-victimisation are hardened and offenders need more effort to commit crime	Social media companies & authority	Verbal abuse & mixed poly-victimisation
	• Wi-Fi use • Online banking	• secure Wi-Fi connection systems • using 4G/5G connections when dealing with credential information	Access to credential information is controlled and offenders need more effort to commit crime	Service providers & internet users	Virus & mixed poly-victimisation
Increasing the risks	Posting on Facebook	• real-name registration systems	Reduced anonymity makes offenders more likely to be exposed	Social media companies & authority	Verbal abuse & poly-victimisation
	Searching behaviours for either information or product review	• automated fraudulent websites detection	Strengthened surveillance makes offenders more likely to be exposed	Searching engine companies	Property-related & mixed poly-victimisation
	Video watching	• crackdown on illicit/pirated websites	Using place managers to monitor the online environment and increase offenders' risk of exposure	Law enforcement authority & users	Identity theft, virus, property-related & mixed poly-victimisation
Reducing the rewards	Posting on Facebook	• blinding critical personal information	Concealed targets reduce offenders' expected rewards or benefits	Social media companies	Verbal abuse & poly-victimisation
	Video watching	• reasonable price for streaming service	Users turn to legal service, illicit markets are disrupted, and offenders are less privileged in the domain	Streaming service providers & users	Identity theft, virus, property-related & mixed poly-victimisation
Reducing provocations	Aggressive posting	• blocking offensive or aggressive posts	Disputes and possible emotional arousal that provoke the crime are reduced	Social media companies & forum managers	Verbal abuse, virus & mixed poly-victimisation

the alternatives of 4G/5G connections when dealing with their credential information or online banking. Those strategies would not only deal with single form of cybercrime but have a potential diffusion to other forms of victimisation or poly-victimisation (see Table 8.2).

Yet in the current case, such a diffusion of benefits might be more evident for property-related poly-victimisation. This particularly applies when strong evidence has supported video-watching behaviour as a very 'risky' factor to forms of single cybercrime (identity theft and virus infection) and poly-victimisation (property-related and mixed poly-victimisation). It would thus be targeted as a typical example to maximise cost-effectiveness of crime prevention (see Table 8.2). The responsibility of such cost-effective crime prevention might involve three stakeholders – law enforcement, streaming service providers and last but not least, the service users.

With regard to law enforcement, the authority's responsibility to crackdown on illicit/pirated websites becomes critical so that offenders are less likely to perpetrate in such domains (*increasing the risks*). This is particularly important given the increase in pirate streaming services due to the lockdown measures associated with the Covid-19 pandemic. Many nations have witnessed such a rise, including the UK where visits to piracy websites increased by 57 percent in one month between February and March 2020 (Sweney, 2020). It is thus noted that law enforcement would not and should not withdraw from SCP against cybercrime.

Furthermore, the battle against online pirates is not merely the responsibility of law enforcement (e.g., Europol) but also rests with website owners. Hence, those owners are the second stakeholder to be considered. They are not only expected to protect users' legal access but also to combat the illicit access to contents. Netflix, for example as a giant streaming service provider, has launched a designated team battling against online pirates since 2017 (Dassanayake, 2018). More providers such as Amazon Prime, Apple TV+, Disney+, etc. are expected to take part in the battle. By virtue of watching video online identified as a very 'risky' factor for (poly)victimisation in findings drawn upon this thesis, website owners (or say streaming service providers in particular) should take their responsibility in cybercrime prevention, of which possible prevention strategy can be referred in Table 8.2.

Last but not least, internet users are one of the stakeholders who should avoid the illicit avenues of online video. This does not place enormous burden to victims and should not be taken as a victim blaming for those who experience cybercrime. It is to inform internet users about the potential risks of watching videos online that might incur and their responsibility to limit their access to illicit contents. When there are less consumers going to the illicit market, there would be less providers, thereby less risky places for the potential targets and perpetrators to meet virtually (see Table 8.2).

Overall, results from the thesis highlight that individuals' online lifestyle-routines have an important impact on the risk of cybercrime (poly)victimisation. Prevention against cybercrime is thus likely to work by targeting certain online behaviours with the application of SCP (see Table 8.2), though the actual effect of individual strategy may warrant future evidence.

8.4.3 Implications for data improvements

In conducting this thesis, several weaknesses in the analysed datasets were acknowledged. This section sets out some of the ways in which these datasets might be improved in an effort to improve the quality of (crime) research using those data. The suggested improvements relate to the TAVS, Taiwanese police recorded crime data and the DOSIH.

- There are four suggested improvements for the TAVS:
  1. Use of a smaller unit to measure neighbourhood characteristics: the unit used in the current TAVS might be too broad to evaluate in a fine-grained way the effects of, say, social disorganisation and the immediate environment on crime. Put differently, residents'

daily interaction (or social ties) in *"ecological units nested within successively larger communities"* (R. J. Sampson et al., 2002, p. 445) may operate at a smaller scale (say like 'villages' or 'neighbourhoods') in Taiwan. The current aggregation of districts as measures of neighbourhood effects might therefore be too crude and hence problematic as it does not adequately account for variations within districts. Therefore, the smallest unit of community included in the TAVS is suggested to be villages or neighbourhoods so that neighbourhood characteristics related to social guardianship (amongst other things) in Taiwan can be better measured.

2. Increasing the frequency of crime victim surveys (say like annually) and collecting longitudinal data: the current TAVS lacks longitudinal data, which limits the breadth and depth of research in two important ways. First, as recognized by Chicago School scholars, ecological patterns need to be observed through the history and growth of local communities/neighbourhoods (C. R. Shaw & McKay, 1969). The lack of longitudinal data thus makes it difficult to understand the full ecological patterns (e.g. neighbourhood deterioration, changes in residential mobility, etc.) in operation in Taiwanese communities, thereby making it difficult to explore the link between variations in socio-ecological patterns and crime over time (R. J. Sampson, 2002; R. J. Sampson et al., 2002), particularly in a context where signals of social organisation are thought to be high (see Section 4.5.1.4). Second, as international trends suggest a growing concentration of crime over victims by time (Pease et al., 2018), the future TAVS is suggested to increase longitudinal data allowing researchers to examine if Taiwan similarly follows such a trend of concentration. A supply of longitudinal data with the TAVS would aid Taiwan in identifying the most vulnerable victims and the allocation of crime prevention resources by time.

3. Improving the practice of capping at six victimisations: the current TAVS only allows survey respondents to report a maximum of six victimisations per crime type over the one-year survey period. Such a practice, referred to as the capping convention, has drawn criticism for underestimating the extent and concentration of crime (Farrell & Pease, 2007a; J. Williams, 2016). It is likely that the capping conventions of the TAVS has resulted in a similar underestimation of RV in this thesis. Hence, it might help better estimate the true extent of RV in Taiwan should the TAVS re-examine and improve its capping convention, probably referred to the innovative approach of the 98th percentile of victim incident counts in the Crime Survey for England and Wales (also see Section 3.2.2.1).
4. Increase the information collected on RV: the current TAVS does not record information on each victimisation but merely the time interval between the two most recent cases reported by the victims. Thus, I was unable to plot the distribution of time intervals between each event and analyse the time-course of RV from the perspective of victims. This meant that I was also unable to explore state dependence ('boost' mechanism) as a causal explanation for RV in Taiwan, using a 'hurdle' approach to model time intervals between crimes against the same target (Estévez Soto, 2020). The suggested improvement in records of each victimisation would thus help provide a better theoretical examination of RV in Taiwan.

- There are two suggested improvements for Taiwanese police recorded crime data:
  1. Adding house characteristics of the burgled dwellings to police data: the current police data does not record information such as house layouts, or ways of burglar entry. This makes it difficult to compare if the risk factors are consistent with the TAVS. For example, it is not clear if the lowered risk of RV for semi-detached

houses observed in the TAVS complies with that in police data. Should more details within police recorded data be available, it would be possible to explore why there are some targets at extreme vulnerability and why (and how) patterns of (N)RV in Taiwan do or do not differ from the literature. Both have theoretical and practical implications. Put differently, enriched police datasets in Taiwan could bridge the gap in comparative studies between western and non-western contexts and between Taiwanese victim surveys and police data.

2. More local police data being released to the public or researchers: the publicly available burglary data containing geographic information occurs in Taoyuan city alone. The reason for the sparsity in data is complex. Simply put, the authorities hold a conservative attitude toward publishing geographic burglary data because they are concerned about accountability and the impact on house pricing nearby burglary hot spots. Whist there was an underrepresentation issue of repeat burglaries identified in the thesis, it is not clear if such an underrepresentation is a nationwide issue. Should more localised police data be released, future research could assess the generalisability of the findings reported here.

- Four improvements are suggested to the DOSIH:
  1. Appropriate wording and measures of cybercrime victimisation, including RV: using single items to ask participants' experiences of cybercrime victimisation is potentially at a risk of biased measurement derived from social desirability bias, recall problems, awareness of victimisation, concealment of crime itself, and so on. Not to mention that the item measuring identity theft is actually a double-barrelled question containing both victimisation of personal information leakage and account theft. This might generate misleading responses. Furthermore, the current DOSIH does not record RV or the sequence of cybercrime victimisation,

making it impossible to estimate the concentration of cybercrime victimisation in Taiwan. Improved survey wording and measures of cybercrime victimisation, e.g. sequences of events by type and if the events are repeats, would make future results more reliable and comprehensive, informing practical prevention strategies.

2. An improved measures of users' online behaviours: future surveys are suggested to include items such as individual time spent online and the legitimacy of online activities (e.g. accessing legal or pirate websites when watching video online). The modification also concerns posting behaviour on Facebook. As more social media platforms gain popularity, the DOSIH would need to extend the question set beyond Facebook alone. Also, given that posting behaviour in fact covers a wide range of related behaviours (e.g. whether SNS profile is public or private, with photo showing face or not, with geographic information revealed or not), the future DOSIH should consider follow-up questions to get a better sense of the specific online behaviours which are taking place. In this way, future research that utilises the DOSIH could identify patterns of cybercrime victimisation from a more comprehensive perspective.
3. An improved measure of guardianship: the DOSIH is suggested to include both physical (e.g. firewalls or antivirus) and social guardianship (e.g. the networking or deviant peers) that are absent in the current survey. This is of particular importance for crime prevention in the future.
4. Inclusion of individuals' offline lifestyle-routines: the current DOSIH does not contain information about an individual's offline lifestyle-routine activities and environmental factors such as perceptions of community climate and perceptions of safety, employment setting (workplace stressors) and community setting (culture diversity, etc.) that are important to explore the environmental effect on cybercrime victimisation. The suggested

improvement would thus help us understand the link between online and offline victimisation, potentially informing better crime prevention strategies.

Overall, it is also suggested that the future TAVS should recruit cybercrime victimisation in the survey or alternatively the DOSIH should borrow knowledges of measures on victimisation from the TAVS. Future integration of the TAVS and the DOSIH would help overcome current knowledge gaps regarding the online-offline connection.

8.5 Strengths, limitations and future research

A strength of this thesis is its use of large and hitherto underutilised nationally representative datasets. The thesis is also noted for drawing evidence from multiple data sources – police recorded crime data, crime victim surveys, and surveys that were not initially designed for research into cybercrime victimisation. Further, this thesis covers both online and offline victimisation, RV and a less discussed field of poly-victimisation, expanding the scope of crime research to a wide range.

Nevertheless, the thesis has identified three limitations in general. Avenues for future research informed by these limitations are discussed simultaneously.

The first limitation derives from the use of secondary data. The thesis sought to examine patterns and mechanisms of crime victimisation with the application of the opportunity framework in a non-western context. Multiple representative and national surveys were thus accessed and used to examine victimisation comprehensively for burglary and cybercrime. Yet while this thesis attempts to cover a wide range of topics regarding victimisation in Taiwan, it is also noted that the datasets used here have aforementioned limitations that can be summarised as: (1) a possible underestimation of crime (either burglary or cybercrime) in Taiwan; (2) limited ability to explore the temporal patterns of victimisation from the victim’s perspective; (3) limited ability to examine if there are interrelations between online and offline context; (4) limited ability to generalise the findings to a longitudinal patterns of victimisations. All these limitations can be dealt by the suggested improvement in datasets mentioned above (see Section 8.4.3).

Future research should, thus, with the aforementioned improvement of data being put into practice, estimate the extent of undercounting of criminal victimisation in Taiwan, say for example through comparing police recorded crime and survey data for crimes types which are well recorded (Farrell & Pease, 2007a; Lauritsen et al., 2012). Additionally, should entries of time sequence for each victimisation be available in either the TAVS or the DOSIH, it is suggested that future research reviews the 'boost' mechanism in Taiwan, both in offline and online settings. Researchers are also suggested to further examine the effect of crime multipliers on online poly-victimisation, in particular, after the sequences of such victimisation are included in future surveys. Furthermore, I suggest future research bridge the gap between online and offline contexts – say for example examining if there is an overlap between online and offline victimisation, a link between online victimisation and offline lifestyle-routine activities, or the other way round (i.e. if online lifestyle-routines are related to offline victimisation[2]). Last but not least, future research should also examine trends of crime (concentration) and capture long-term social disorganisation and chronical environment issues in Taiwan, with the use of more sweeps of survey to the analysis if applicable.

The second limitation derives from the inherently low-crime setting as Taiwan, featuring a small sample of victims to be analysed. Research on crime in such a setting can be a double-edged sword. The strength is that the identification of the differences in mechanisms and patterns of victimisation across contexts can inform us what makes individuals less vulnerable to other counterparts in the world, and further inform what can be done with crime prevention from practical and comparative perspectives. Yet a small sample

[2] Examples: (1) individuals' exposure of personal information online (e.g. locations of the house, vacation plans or flaunting money) might attract potential burglars to their vacant property or attract extortion; (2) individuals' aggressive posting on social media might attract online vigilantes to dox and result in offline victimisation such as bullying, abuse, force of threats, etc.

of victims is also a limitation. It is challenging to perform advanced analyses that require a greater sample size because numbers of (repeat) incidents, say burglary for instance, are not comparable to those in the literature.

I suggest that future research on RV should draw on police data at a larger scale. An increased sample size has three implications. First, it could enable a better comparison with relevant studies in Taiwan and elsewhere – say greater China and western counterparts. Second, drawing on Taiwanese police data at a larger scale could allow for the assessment of whether the observed (under)representation of NRV found in the thesis is generalisable. Third, it could help explore the applicability of research on the effective combination of security measures beyond the current victim survey, generating knowledge for crime prevention.

With respect to deciding what security measures to implement, an important consideration is the cost-effectiveness of crime prevention strategies. However, prior research suggests that evidence on the cost-effectiveness of prevention measures is sorely lacking in the crime prevention literature, and that this needs to change if we want to improve and develop crime prevention and policing (Tompson et al., 2021). Likewise, there is a similar lack of cost-benefit analysis with respect to crime prevention in Taiwan. Information on the costs associated with implementing and maintaining different prevention measures is limited. Hence, reliable cost-benefit analysis cannot be undertaken with the data used here, either. Cost-benefit evaluation is thus suggested as a direction for future research, further informing crime prevention and policing.

The third limitation is about generalising the findings to other contexts. Despite that some of the patterns identified herein are in line with those observed in the literature, two concerns would be noted: (1) online versus offline contexts and (2) victims' versus offenders' perspectives. First, the identified inconsistencies may reflect the unique and complex nature of online and offline crime in Taiwan and the generalisation would thus be taken very cautiously in countries where crime or culture is fundamentally different. To be specific, the thesis merely provided statistical supports for the effect of target attractiveness and guardianship on burglary victimisation at the individual level whilst exposure/proximity at the neighbourhood level remained less statistically obvious. Conversely in an online context, the findings presented herein suggest individuals' online lifestyle-routines to be important risk factors for cybercrime victimisation whist guardianship at either individual or environmental levels were found less evident. Hence, the generalisation of findings across online-offline and to other contexts beyond Taiwan warrants cautions. Second, the thesis draws patterns of crime mainly from victim surveys and police data, with a limited scope of offenders. Caution should be exercised when generalising the findings to the applicability of LRAA from an offender's perspective.

As mentioned in both Section 4.5 and Section 7.6.2, future research might interview offenders, as their perspective might shed further light on many of the findings reported in this thesis. This line of research can be both in relation to burglary (say, the effect of security measures) and cybercrime (say, offender targeting strategies). The collection of data may thus include anonymous online surveys for cybercriminals or interviews with convicted burglars.

Overall, directions of future research may include the exploration of links between online-offline victimisation and the cost-benefit analysis, in a way to inform crime prevention strategies. Future research in Taiwan should also consider incorporating other avenues like offender interviews to construct a more comprehensive picture of LRAA in Taiwan, and further expand scopes to the other two pillars underpinning the EC – the rational choice perspective and crime pattern theory – in the Taiwan context.

8.6 Conclusion

This thesis aimed to understand the patterns of crime victimisation in Taiwan, a non-Western context where the utility of the LRAA and crime opportunity theories has been little discussed. Two types of crime were considered – burglary and cybercrime, covering both offline and online contexts of Taiwan.

In regard to theoretical implications, the thesis suggests that the generalisability of LRAA to Taiwan should be taken with caution. This is because the thesis found limited evidence to support the role of exposure/proximity and social disorganisation on burglary victimisation and that of guardianship on online victimisation. Additionally, two important departures from the literature in regard to RV in Taiwan were observed. First, the extent of RV was found to be higher in Taiwan than that is found in the western literature. Second, NRV research in Taiwan found a consistent regularity in time but irregularity in space compared with what the literature suggests.

Given the applied nature of the LRAA and EC in general, the findings reported in this thesis have implications for practical crime prevention in Taiwan. Based on the two noted patterns of RV in Taiwan mentioned above, crime prevention against repeats can be tailored and targeted. That is, prevention may focus more on direct repeats than spatial near-targets, until further research can determine if and explain why where is a spatial irregularity within the 100-metre range following the initial target. Otherwise, SCP seems to be an applicable strategy in Taiwan. Based on the risk factors identified in the thesis, it is plausible that SCP efforts aimed at addressing these risk factors could reduce opportunities for both offline (burglary in particular) and online offences (verbal abuse, identity theft, fraud, virus, and poly-victimisation). The current thesis does not statistically examine the effectiveness of SCP in Taiwan, so that one may argue if the thesis contributes empirically to the field of crime prevention. However, as mentioned early in Section 1.2.2, Taiwan has neither established evidence-based policing movements nor traditions of researchers working closely with practitioners. Mindful of these barriers, this thesis informs what can be done in Taiwanese crime prevention based on identified risk factors. Hence, it is however still the case that the findings presented in the thesis bear relevance to crime prevention in Taiwan.

Overall, the thesis looks forward to seeing data improvement as suggested above so that future crime research in Taiwan can bridge the identified gaps in the literature.

References

Aarts, E., Verhage, M., Veenvliet, J. V., Dolan, C. V., & van der Sluis, S. (2014). A Solution to Dependency: Using Multilevel Analysis to Accommodate Nested Data. *Nature Neuroscience*, *17*(4), 491–496. https://doi.org/ 10.1038/nn.3648

Aboujaoude, E., Savage, M. W., Starcevic, V., & Salame, W. O. (2015). Cyberbullying: Review of an Old Problem Gone Viral. *Journal of Adolescent Health*, *57*(1), 10–18. https://doi.org/10.1016/ j.jadohealth.2015.04.011

Agresti, A., & Finlay, B. (1997). *Statistical Methods for the Social Sciences* (3rd Edition). Prentice Hall.

Akaike, H. (1974). A New Look at the Statistical Model Identification. *IEEE Transactions on Automatic Control*, *19*(6), 716–723. https://doi.org/ 10.1109/TAC.1974.1100705

Akinwande, M. O., Dikko, H. G., & Samson, A. (2015). Variance Inflation Factor: As a Condition for the Inclusion of Suppressor Variable(s) in Regression Analysis. *Open Journal of Statistics*, *05*(07), 754–767. https://doi.org/10.4236/ojs.2015.57075

Alhaboby, Z. A., Barnes, J., Evans, H., & Short, E. (2019). Cyber-Victimization of People With Chronic Conditions and Disabilities: A Systematic Review of Scope and Impact. *Trauma, Violence, & Abuse*, *20*(3), 398–415. https://doi.org/10.1177/1524838017717743

Allen, J., & Felson, M. (2012). *Routine Activities and Crime, Night and Day*. 21st Environmental Criminology and Crime Analysis Conference, Stavern, Norway.

Allison, S. F. H., Schuck, A., & Lersch, K. (2005). Exploring the Crime of Identity Theft: Prevalence, Clearance Rates, and Victim/Offender Characteristics. *Journal of Criminal Justice*, *33*(1), 19–29. https://doi.org/10.1016/j.jcrimjus.2004.10.007

Almeida, T. C., Ramos, C., Brito, J., & Cardoso, J. (2020). The Juvenile Victimization Questionnaire: Psychometric Properties and Poly-Victimization Among Portuguese Youth. *Children and Youth Services Review*, *113*, 105001. https://doi.org/10.1016/j.childyouth.2020.105001

Althubaiti, A. (2016). Information Bias in Health Research: Definition, Pitfalls, and Adjustment Methods. *Journal of Multidisciplinary Healthcare*, *9*, 211–217. https://doi.org/10.2147/JMDH.S104807

Álvarez-Lister, M. S., Pereda, N., Guilera, G., Abad, J., & Segura, A. (2017). Victimization and Poly-Victimization in Adolescent Outpatients from Mental Health Centers: A Case-Control Study. *Journal of Family Violence*, *32*(2), 197–205. https://doi.org/10.1007/s10896-016-9831-1

Amemiya, M., Nakaya, T., & Shimada, T. (2020). Near-Repeat Victimization of Sex Crimes and Threat Incidents Against Women and Girls in Tokyo, Japan. *Crime Science*, *9*(1), 5. https://doi.org/10.1186/s40163-

020-00114-9

Anandarajan, M., & Malik, S. (2018). Protecting the Internet of Medical Things: A Situational Crime-Prevention Approach. *Cogent Medicine*, *5*(1), 1513349. https://doi.org/10.1080/2331205X.2018.1513349

Andersen, L. H., Anker, A. S. T., & Andersen, S. H. (2016). A Formal Decomposition of Declining Youth Crime in Denmark. *Demographic Research*, *35*(44), 1303–1316. https://doi.org/10.4054/DemRes.2016.35.44

Anderson, K. B. (2006). Who are the Victims of Identity Theft? The Effect of Demographics. *Journal of Public Policy & Marketing*, *25*(2), 160–171. https://doi.org/10.1509/jppm.25.2.160

Ang, R. P., & Goh, D. H. (2010). Cyberbullying Among Adolescents: The Role of Affective and Cognitive Empathy, and Gender. *Child Psychiatry & Human Development*, *41*(4), 387–397. https://doi.org/10.1007/s10578-010-0176-3

Anselin, L. (1995). Local Indicators of Spatial Association—LISA. *Geographical Analysis*, *27*(2), 93–115. https://doi.org/10.1111/j.1538-4632.1995.tb00338.x

Anselin, L., Cohen, J., Cook, D., Gorr, W., & Tita, G. (2000). Spatial Analyses of Crime. *Criminal Justice*, *4*, 213–262.

Anti-Phishing Working Group. (2020). *Phishing Activity Trends Report 4th Quarter 2019*. APWG. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

AO Kaspersky Lab. (2020). *How to Avoid Public WiFi Security Risks*. https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Aoyama, I., Utsumi, S., & Hasegawa, M. (2012). Cyberbullying in Japan: Cases, Government Reports, Adolescent Relational Aggression, and Parental Monitoring Roles. In Q. Li, D. Cross, & P. K. Smith (Eds.), *Cyberbullying in the Global Playground: Research from International Perspectives* (1st ed.). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119954484

Aricak, T., Siyahhan, S., Uzunhasanoglu, A., Saribeyoglu, S., Ciplak, S., Yilmaz, N., & Memmedov, C. (2008). Cyberbullying Among Turkish Adolescents. *CyberPsychology & Behavior*, *11*(3), 253–261. https://doi.org/10.1089/cpb.2007.0016

Aromaa, K., & Heiskanen, M. (Eds.). (2008). *Victimisation Surveys in Comparative Perspectives: Papers from the Stockholm Criminology Symposium 2007*. European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI).

Ashton, J., Brown, I., Senior, B., & Pease, K. (1998). Repeat Victimisation: Offenders Accounts. *International Journal of Risk, Security and Crime Prevention*, *3*(4), 269–279.

Averdijk, M., & Elffers, H. (2012). The Discrepancy Between Survey-Based Victim Accounts and Police Reports Revisited. *International Review of Victimology*, *18*(2), 91–107. https://doi.org/10.1177/0269758011432955

Bachmann, M. (2010). *The Risk Propensity and Rationality of Computer*

Hackers. https://www.semanticscholar.org/paper/The-Risk-Propensity-and-Rationality-of-Computer-Bachmann/bf093c90e7cba8c50b1244db02902973f3f5d896

Back, S. (2016). *Empirical Assessment of Cyber Harassment Victimization via Cyber-Routine Activities Theory* [Master's Theses and Projects, Bridgewater State University]. https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1029&context=theses

Back, S., & LaPrade, J. (2020). Cyber-Situational Crime Prevention and the Breadth of Cybercrimes among Higher Education Institutions. *International Journal of Cybersecurity Intelligence and Cybercrime*, *3*(2), 25–47. https://doi.org/10.52306/03020320RGWS2555

Baldwin, J. R., Arseneault, L., Caspi, A., Moffitt, T. E., Fisher, H. L., Odgers, C. L., Ambler, A., Houts, R. M., Matthews, T., Ougrin, D., Richmond-Rakerd, L. S., Takizawa, R., & Danese, A. (2019). Adolescent Victimization and Self-Injurious Thoughts and Behaviors: A Genetically Sensitive Cohort Study. *Journal of the American Academy of Child & Adolescent Psychiatry*, *58*(5), 506–513. https://doi.org/10.1016/j.jaac.2018.07.903

Bandura, A. (1976). Social Learning Analysis of Aggression. In E. Ribes-Inesta & A. Bandura (Eds.), *Analysis of Delinquency and Aggression* (p. 273). Lawrence Erlbaum Associates.

Barkan, S. E. (2006). *Criminology: A Sociological Understanding* (3rd ed.). Prentice-Hall. https://digitalcommons.library.umaine.edu/fac_monographs/157

Barrera, D. J. (2018). The Role of "Problematic" and "Improved" Indicators of Risky Lifestyles in the Self-Control/Lifestyle Framework of Victimization Among Filipino Adolescents. *Asian Journal of Criminology*, *13*(3), 175–191. https://doi.org/10.1007/s11417-018-9265-1

Barringer-Brown, C. (2015). Cyber bullying among Students with Serious Emotional and Specific Learning Disabilities. *Journal of Education and Human Development*, *4*(2(1)). https://doi.org/10.15640/jehd.v4n2_1a4

Battin, J. R., & Crowl, J. N. (2017). Urban Sprawl, Population Density, and Crime: An Examination of Contemporary Migration Trends and Crime in Suburban and Rural Neighborhoods. *Crime Prevention and Community Safety*, *19*(2), 136–150. https://doi.org/10.1057/s41300-017-0020-9

BBC. (2020). *What Are Viruses and Malware?* Bitesize. https://www.bbc.co.uk/bitesize/topics/zd92fg8/articles/zcmbgk7

Beauregard, E., & Martineau, M. (2015). An Application of CRAVED to the Choice of Victim in Sexual Homicide: A Routine Activity Approach. *Crime Science*, *4*(1), 24. https://doi.org/10.1186/s40163-015-0036-3

Beckman, L., Hellström, L., & Kobyletzki, L. von. (2020). Cyber Bullying Among Children with Neurodevelopmental Disorders: A Systematic Review. *Scandinavian Journal of Psychology*, *61*(1), 54–67. https://doi.org/10.1111/sjop.12525

Beebe, N. L., & Rao, V. S. (2005, December). Using Situational Crime

Prevention Theory to Explain the Effectiveness of Information Systems Security. *Proceedings of the 2005 SoftWars Conference*. the 2005 SoftWars Conference, Las Vegas, NV.

Beebe, N. L., & Rao, V. S. (2010). Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process. *Communications of the Association for Information Systems*, *26*(17), 329–358. https://doi.org/10.17705/1CAIS.02617

Bendel, R. B., & Afifi, A. A. (1977). Comparison of Stopping Rules in Forward "Stepwise" Regression. *Journal of the American Statistical Association*, *72*(357), 46–53. https://doi.org/10.1080/01621459.1977.10479905

Bennett, T., Holloway, K., & Farrington, D. P. (2007). Does Neighborhood Watch Reduce Crime? A Systematic Review and Meta-Analysis. *Journal of Experimental Criminology*, *2*(4), 437–458. https://doi.org/10.1007/s11292-006-9018-5

Berlin, K. S., Williams, N. A., & Parra, G. R. (2014). An Introduction to Latent Variable Mixture Modeling (Part 1): Overview and Cross-Sectional Latent Class and Latent Profile Analyses. *Journal of Pediatric Psychology*, *39*(2), 174–187. https://doi.org/10.1093/jpepsy/jst084

Bernasco, W. (2008). Them Again?: Same-Offender Involvement in Repeat and Near Repeat Burglaries. *European Journal of Criminology*, *5*(4), 411–431. https://doi.org/10.1177/1477370808095124

Bernasco, W. (2009). Foraging Strategies of Homo Criminalis: Lessons from Behavioral Ecology. *Crime Patterns and Analysis*, *2*(1), 5–16.

Bernasco, W., Johnson, S. D., & Ruiter, S. (2015). Learning Where to Offend: Effects of Past on Future Burglary Locations. *Applied Geography*, *60*, 120–129. https://doi.org/10.1016/j.apgeog.2015.03.014

Bernasco, W., & Steenbeek, W. (2017). More Places than Crimes: Implications for Evaluating the Law of Crime Concentration at Place. *Journal of Quantitative Criminology*, *33*(3), 451–467. https://doi.org/10.1007/s10940-016-9324-7

Block, C. R., & Block, R. L. (1984). Crime Definition, Crime Measurement, and Victim Surveys. *Journal of Social Issues*, *40*(1), 137–159. https://doi.org/10.1111/j.1540-4560.1984.tb01086.x

Blumstein, A., Rivara, F. P., & Rosenfeld, R. (2000). The Rise and Decline of Homicide—And Why. *Annual Review of Public Health*, *21*(1), 505–541. https://doi.org/10.1146/annurev.publhealth.21.1.505

Boslaugh, S. (2015). Using Secondary Data. In G. Guest & E. E. Namey (Eds.), *Public Health Research Methods* (pp. 253–277). SAGE Publications.

Bossler, A. M., & Holt, T. J. (2009). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, *3*(1), 400–420.

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting Online Harassment Victimization Among a Juvenile Population. *Youth & Society*, *44*(4), 500–523. https://doi.org/10.1177/0044118X11407525

Bottoms, A., & Costello, A. (2010). Understanding Repeat Victimization: A Longitudinal Study. In S. G. Shoham, P. Knepper, & M. Kett (Eds.), *International Handbook of Criminology* (1st ed., pp. 675–706). Routledge.

Bowers, K. J., & Johnson, S. D. (2003). *The Role of Publicity in Crime Prevention: Findings from the Reducing Burglary Initiative* (Research Study 272). Home Office. https://www.researchgate.net/profile/Shane-Johnson-7/publication/32884810_The_Role_of_Publicity_in_Crime_Prevention_Findings_from_the_Reducing_Burglary_Initiative/links/0deec5298ca2e36924000000/The-Role-of-Publicity-in-Crime-Prevention-Findings-from-the-Reducing-Burglary-Initiative.pdf

Bowers, K. J., & Johnson, S. D. (2004). Who Commits Near Repeats? A Test of the Boost Explanation. *Western Criminology Review*, *5*(3), 12–24.

Bowers, K. J., Johnson, S. D., & Pease, K. (2005). Victimisation and Re-victimisation Risk, Housing Type and Area: A Study of Interactions. *Crime Prevention and Community Safety*, *7*(1), 7–17. https://doi.org/10.1057/palgrave.cpcs.8140205

Bradford, B., & Jackson, J. (2010, November 17). *Cooperating with the Police: Social Control and the Reproduction of Police Legitimacy*. ASC Annual Meeting, San Francisco Marriott, San Francisco, California. https://www.researchgate.net/publication/228223955_Cooperating_with_the_Police_Social_Control_and_the_Reproduction_of_Police_Legitimacy

Bradford, B., & Jackson, J. (2016). Cooperating with the Police as an Act of Social Control—Trust and Neighbourhood Concerns as Predictors of Public Assistance. *Nordisk Politiforskning (Nordic Journal of Studies in Policing)*, *3*(2), 111–131. https://doi.org/10.18261/issn.1894-8693-2016-02-04

Brantingham, P. J., & Brantingham, P. L. (1981). Notes on the Geometry of Crime. In P. J. Brantingham & P. L. Brantingham (Eds.), *Environmental Criminology* (pp. 27–54). Sage Publications. https://www.ojp.gov/ncjrs/virtual-library/abstracts/notes-geometry-crime-environmental-criminology-p-27-54-1981-paul-j

Brantingham, P. J., Brantingham, P. L., & Anderson, M. A. (2016). The Geometry of Crime and Crime Pattern Theory. In R. Wortley & M. Townsley (Eds.), *Environmental Criminology and Crime Analysis* (2nd ed., pp. 98–115). Routledge.

Brantingham, P. L., & Brantingham, P. J. (1993). Nodes, Paths and Edges: Considerations on the Complexity of Crime and the Physical Environment. *Journal of Environmental Psychology*, *13*, 3–28.

Brown, C. F., Demaray, M. K., & Secord, S. M. (2014). Cyber Victimization in Middle School and Relations to Social Emotional Outcomes. *Computers in Human Behavior*, *35*, 12–21. https://doi.org/10.1016/j.chb.2014.02.014

Budd, T. (2001). *Burglary: Practice Messages from the British Crime Survey* (Briefing Note 5/01). Home Office.

Budd, T., & Mattinson, J. (2000). *British Crime Survey Training Notes*

(Crime Surveys Section, Crime and Criminal Justice Unit, Research and Development Statistics Directorate). Home Office.

Bullock, K., Clarke, R. V., & Tilley, N. (2010). *Situational Prevention of Organised Crimes* (1st ed.). William Publishing. https://www.routledge.com/Situational-Prevention-of-Organised-Crimes/Clarke-Bullock-Tilley/p/book/9780415628037

Burnham, K. P., & Anderson, D. R. (2002). *Model Selection and Multimodel Inference: A Practical Information-Theoretic Approach* (2nd ed.). Springer-Verlag. https://doi.org/10.1007/b97636

Bursik, R. (1988). Social Disorganization and Theories of Crime and Delinquency: Problems and Prospects. *Criminology*, *26*(4), 519–552.

Bursik, R. J. (2000). The Systemic Theory of Neighborhood Crime Rates. In *Of Crime & Criminality: The Use of Theory in Everyday Life* (pp. 87–104). SAGE Publications, Inc. https://doi.org/10.4135/9781452232232.n5

Cantillon, D., Davidson, W. S., & Schweitzer, J. H. (2003). Measuring Community Social Organization: Sense of Community as a Mediator in Social Disorganization Theory. *Journal of Criminal Justice*, *31*(4), 321–339. https://doi.org/10.1016/S0047-2352(03)00026-6

Cavoukian, A. (2013). Privacy by Design and the Promise of SmartData. In I. Harvey, A. Cavoukian, G. Tomko, D. Borrett, H. Kwan, & D. Hatzinakos (Eds.), *SmartData*. Springer. https://doi.org/10.1007/978-1-4614-6409-9_1

Cénat, J. M., Smith, K., Hébert, M., & Derivois, D. (2019). Polyvictimization and Cybervictimization Among College Students From France: The Mediation Role of Psychological Distress and Resilience. *Journal of Interpersonal Violence*, 0886260519854554. https://doi.org/10.1177/0886260519854554

Census and Statistics Department, Hong Kong Special Administrative Region. (2020). *Thematic Household Survey: Personal Computer and Internet Penetration* (No. 69; p. 77). Census and Statistics Department, Hong Kong Special Administrative Region. https://www.censtatd.gov.hk/en/data/stat_report/product/C0000052/att/B11302692020XXXXB0100.pdf

Central Police University. (2015). *2015 Taiwan Area Victimisation Survey: Telephone Interview Report*. National Police Agency, Ministry of the Interior.

Chainey, S. P. (2014). *Examining the Extent to Which Hotspot Analysis Can Support Spatial Predictions of Crime* [Doctoral Dissertation, University College London]. https://discovery.ucl.ac.uk/id/eprint/1458643/1/SChainey%20PhD%20Final%20Version.pdf

Chainey, S. P., & da Silva, B. F. A. (2016). Examining the Extent of Repeat and Near Repeat Victimisation of Domestic Burglaries in Belo Horizonte, Brazil. *Crime Science*, *5*(1), 1. https://doi.org/10.1186/s40163-016-0049-6

Chen, P., Yuan, H., & Li, D. (2013). Space-Time Analysis of Burglary in Beijing. *Security Journal*, *26*(1), 1–15. https://doi.org/10.1057/sj.2011.4

Chen, Q., Lo, C. K. M., Zhu, Y., Cheung, A., Chan, K. L., & Ip, P. (2018). Family Poly-Victimization and Cyberbullying Among Adolescents in a Chinese School Sample. *Child Abuse & Neglect*, *77*, 180–187. https://doi.org/10.1016/j.chiabu.2018.01.015

Chiew, L. S., Amerudin, S., & Yusof, Z. M. (2020). A Spatial Analysis of the Relationship Between Socio-Demographic Characteristics with Burglar Behaviours on Burglary Crime. *IOP Conference Series: Earth and Environmental Science*, *540*, 1–11. https://doi.org/10.1088/1755-1315/540/1/012050

Choi, K.-S. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, *2*(1), 308–333.

Clark, J. A. G. R. (2018). *The Near Repeat Risk Calculation of Residential Burglaries in Hillcrest, Kwazulu-Natal, South Africa: A Criminological Analysis* [Master's thesis, University of South Africa]. https://www.researchgate.net/publication/335220280_THE_NEAR_REPEAT_RISK_CALCULATION_OF_RESIDENTIAL_BURGLARIES_IN_HILLCREST_KWAZULU-NATAL_SOUTH_AFRICA_A_CRIMINOLOGICAL_ANALYSIS

Clarke, R. V. (1995). Situational Crime Prevention. *Crime and Justice*, *19*, 91–150.

Clarke, R. V. (Ed.). (1997). *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Criminal Justice Press.

Clarke, R. V. (2016). Situational Crime Prevention. In R. Wortley & M. Townsley (Eds.), *Environmental Criminology and Crime Analysis* (2nd Edition, pp. 286–303). Routledge.

Clarke, R. V., & Cornish, D. B. (1983). Editorial Introduction. In R. V. Clarke & D. B. Cornish (Eds.), *Crime Control in Britain* (pp. 3–54). State University of New York Press.

Clarke, R. V., & Cornish, D. B. (1985). Modeling Offenders' Decisions: A Framework for Research and Policy. *Crime and Justice*, *6*, 147–185.

Clarke, R. V., & Eck, J. E. (2005). *Crime Analysis for Problem Solvers In 60 Small Steps*. Center for Problem-Oriented Policing. https://cops.usdoj.gov/pdf/crimeanalysis60steps.pdf

Clarke, R. V., Perkins, E., & Smith, Jr., D. J. (2001). Explaining Repeat Residential Burglaries: An Analysis of Property Stolen. In G. Farrell & K. Pease (Eds.), *Repeat Victimization* (pp. 119–132). Criminal Justice Press.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory. *American Sociological Review*, *46*(5), 505–524. https://doi.org/10.2307/2094935

Coleman, C., & Moynihan, J. (1996). *Understanding Crime Data: Haunted by the Dark Figure*. Open University Press. https://catalyst.library.jhu.edu/catalog/bib_1835820

Copes, H. (1999). Routine Activities and Motor Vehicle Theft: A Crime Specific Approach. *Journal of Crime and Justice*, *22*(2), 125–146. https://doi.org/10.1080/0735648X.1999.9721097

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention. *Crime Prevention Studies*, *16*, 41–96.

Cornish, D. B., & Clarke, R. V. (Eds.). (2014). *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Transaction Publishers.

Cornish, D. B., & Clarke, R. V. (2016). The Rational Choice Perspective. In R. Wortley & M. Townsley (Eds.), *Environmental Criminology and Crime Analysis* (2nd ed., pp. 29–61). Routledge. http://ebookcentral.proquest.com/lib/ucl/detail.action?docID=4717777

Coupe, T., & Blake, L. (2006). Daylight and Darkness Targeting Strategies and the Risks of Being Seen at Residential Burglaries*. *Criminology*, *44*(2), 431–464. https://doi.org/10.1111/j.1745-9125.2006.00054.x

Criminal Investigation Bureau. (2020). *Crime Statistics–2019*. Criminal Investigation Bureau, National Police Agency, Ministry of the Interior, Republic of China. https://cib.npa.gov.tw/ch/app/data/doc?module=wg136&detailNo=793294146201743360&type=s

Curiel, R. P. (2019). Is Crime Concentrated or Are We Simply Using the Wrong Metrics? *ArXiv: Physics and Society*. http://arxiv.org/abs/1902.03105

Dassanayake, D. (2018, June 25). *Netflix Piracy Crackdown: Online Giant Steps up Clamp down on Illegal Streaming*. Express.Co.Uk. https://www.express.co.uk/life-style/science-technology/979412/Netflix-online-piracy-movies-TV-shows-illegal-streams

Davies, T. (2019). *Near Repeat*. GitHub Repository. https://github.com/tobydavies/NearRepeat

del Frate, A. A., & Mugellini, G. (2012). The Crime Drop in 'Non-Western'countries: A Review of Homicide Data. In J. van Dijk, A. Tseloni, & G. Farrell (Eds.), *The International Crime Drop: New Directions in Research* (pp. 134–155). Palgrave Macmillan.

Denson, N., & Ing, M. (2014). Latent Class Analysis in Higher Education: An Illustrative Example of Pluralistic Orientation. *Research in Higher Education*, *55*(5), 508–526. https://doi.org/10.1007/s11162-013-9324-5

Department of Household Registration, M.O.I. (2018). *Household Statistics (renkou tongji ziliao)* [Text/html]. Department of Household Registration, Ministry of the Interior. Republic of China(Taiwan). https://www.ris.gov.tw/app/portal/346

Department of Household Registration, M.O.I. (2020). *Statistics: Table 6. Population Density and Total Area for Counties and Cities* [Text/html]. Department of Household Registration, Ministry of the Interior. Republic of China(Taiwan). https://www.ris.gov.tw/app/en/3910

Department of Statistics. (2017, June 13). *2014 Health and Welfare Indicators* [Html]. Ministry of Health and Welfare; Ministry of Health and Welfare. https://www.mohw.gov.tw/cp-134-30212-2.html

Di Gennaro, G., & La Spina, A. (2016). The Costs of Illegality: A Research Programme. *Global Crime*, *17*(1), 1–20. https://doi.org/10.1080/17440572.2015.1128621

Didden, R., Scholte, R. H. J., Korzilius, H., Moor, J. M. H. de, Vermeulen, A., O'Reilly, M., Lang, R., & Lancioni, G. E. (2009). Cyberbullying Among Students with Intellectual and Developmental Disability in Special Education Settings. *Developmental Neurorehabilitation*, *12*(3), 146–151. https://doi.org/10.1080/17518420902971356

Dimitrova, D. S., Kaishev, V. K., & Tan, S. (2017). Computing the Kolmogorov-Smirnov Distribution when the Underlying cdf is Purely Discrete, Mixed or Continuous. *City Research Online*. https://openaccess.city.ac.uk/id/eprint/18541

Dimitrova, D. S., Kaishev, V. K., & Tan, S. (2020). *KSgeneral: Computing P-Values of the K-S Test for (Dis)Continuous Null Distribution* (0.1.2) [Computer software]. https://github.com/raymondtsr/KSgeneral

Directorate-General of Budget, Accounting and Statistics, Executive Yuan, R.O.C (Taiwan). (2020). *Statistical Yearbook of the Republic of China 2019*. https://eng.stat.gov.tw/public/data/dgbas03/bs2/yearbook_eng/Yearbook2019.pdf

Duggan, M. (2017). *Online Harassment 2017*. Pew Research Center. https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

Dunford, R., Su, Q., & Tamang, E. (2014). The Pareto Principle. *The Plymouth Student Scientist*, *7*(1), 140–148.

Dziak, J. J., Coffman, D. L., Lanza, S. T., & Li, R. (2012). *Sensitivity and Specificity of Information Criteria* (No. 12–119; Technical Report Series). The Methodology Center, The Pennsylvania State University. https://www.methodology.psu.edu/files/2019/03/12-119-2e90hc6.pdf

Eck, J. E. (1993). The Threat of Crime Displacement. *Problem Solving Quarterly*, *6*(3), 1–7.

Eck, J. E. (2003). Police Problems: The Complexity of Problem Theory, Research and Evaluation. In J. Knutsson (Ed.), *Problem-Oriented Policing: From Innovation to Mainstream* (pp. 79–113). Criminal Justice Press.

Eck, J. E., Clarke, R. V., & Guerette, R. T. (2007). Risky Facilities: Crime Concentration in Homogeneous Sets of Establishments and Facilities. *Crime Prevention Studies*, *21*(225–264), 40.

Ellingworth, D., Farrell, G., & Pease, K. (1995). A Victim Is a Victim Is a Victim - Chronic Victimization in Four Sweeps of the British Crime Survey Symposium: Repeat Victimization. *British Journal of Criminology*, *35*, 360–365.

Ellonen, N., & Pösö, T. (2011). Violence Experiences in Care: Some Methodological Remarks based on the Finnish Child Victim Survey. *Child Abuse Review*, *20*(3), 197–212. https://doi.org/10.1002/car.1181

Ellonen, N., & Salmi, V. (2011). Poly-Victimization as a Life Condition: Correlates of Poly-Victimization among Finnish Children. *Journal of*

Scandinavian Studies in Criminology and Crime Prevention, *12*(1), 20–44. https://doi.org/10.1080/14043858.2011.561621

El-Saifi, N., Moyle, W., Jones, C., & Alston-Knox, C. (2019). Determinants of Medication Adherence in Older People with Dementia from the Caregivers' Perspective. *International Psychogeriatrics*, *31*(3), 331–339. https://doi.org/10.1017/S1041610218000583

Enders, C. K., & Tofighi, D. (2007). Centering Predictor Variables in Cross-Sectional Multilevel Models: A New Look at an Old Issue. *Psychological Methods*, *12*(2), 121–138. https://doi.org/10.1037/1082-989X.12.2.121

Engström, A. (2020). Conceptualizing Lifestyle and Routine Activities in the Early 21st Century: A Systematic Review of Self-Report Measures in Studies on Direct-Contact Offenses in Young Populations. *Crime & Delinquency*, 0011128720937640. https://doi.org/10.1177/0011128720937640

Estévez Soto, P. R. (2020). *Organised Crime and Repeat Victimisation: Modelling Victimisation Patterns Against Mexican Businesses* [Doctoral dissertation, University College London]. https://discovery.ucl.ac.uk/id/eprint/10090180/

Estévez-Soto, P. R., Johnson, S. D., & Tilley, N. (2020). Are Repeatedly Extorted Businesses Different? A Multilevel Hurdle Model of Extortion Victimization. *Journal of Quantitative Criminology*. https://doi.org/10.1007/s10940-020-09480-8

Farrell, G. (1995). Preventing Repeat Victimization. *Crime and Justice*, *19*, 469–534. https://doi.org/10.1086/449236

Farrell, G. (2013). Five Tests for a Theory of the Crime Drop. *Crime Science*, *2*(1), 5. https://doi.org/10.1186/2193-7680-2-5

Farrell, G., & Bouloukos, A. C. (2001). International Overview: A Cross-National Comparison of Rates of Repeat Victimization. In G. Farrell & K. Pease (Eds.), *Repeat Victimization* (pp. 5–25). Criminal Justice Press.

Farrell, G., Laycock, G., & Tilley, N. (2015). Debuts and Legacies: The Crime Drop and the Role of Adolescence-Limited and Persistent Offending. *Crime Science*, *4*, 16. https://doi.org/10.1186/s40163-015-0028-3

Farrell, G., & Pease, K. (2007a). The Sting in the Tail of the British Crime Survey: Multiple Victimisations. In M. Hough & M. Maxfield (Eds.), *Surveying Crime in the 21st Century* (pp. 33–54). Criminal Justice Press. https://www.researchgate.net/publication/331385294_The_sting_in_the_tail_of_the_British_Crime_Survey_Multiple_victimisations

Farrell, G., & Pease, K. (2007b). Crime in England and Wales: More Violence and More Chronic Victims. *Civitas Review*, *4*(2), 1–8.

Farrell, G., & Pease, K. (2014). Repeat Victimization. In G. Bruinsma & D. Weisburd (Eds.), *Enclopedia of Criminology and Criminal Justice* (1st ed., pp. 4371–4381). Springer. https://doi.org/10.1007/978-1-4614-5690-2

Farrell, G., & Pease, K. (2017). Preventing Repeat and Near Repeat Crime

Concentrations. In N. Tilley & A. Sidebottom (Eds.), *Handbook of Crime Prevention and Community Safety* (2nd ed.). Routledge. https://www.researchgate.net/publication/312939118_Preventing_repeat_and_near_repeat_crime_concentrations

Farrell, G., Phillips, C., & Pease, K. (1995). Like Taking Candy: Why Does Repeat Victimization Occur? *The British Journal of Criminology*, *35*(3), 384–399.

Farrell, G., Sousa, W. H., & Weisel, D. L. (2002). The Time-Window Effect in the Measurement of Repeat Victimization: A Methodology for Its Examination, and an Empirical Study. *Crime Prevention Studies*, *13*, 15–27.

Farrell, G., Tseloni, A., & Tilley, N. (2014). Why the Crime Drop? In M. Tonry (Ed.), *Crime and Justice* (Vol. 43, pp. 421–490). University of Chicago Press. https://www.researchgate.net/publication/273692757_'Why_the_Crime_Drop'_in_M_Tonry_Ed_Crime_and_Justice_vol_43_pp421-490_Chicago_University_of_Chicago_Press

Farrington, D. P. (1986). Age and Crime. *Crime and Justice*, *7*, 189–250.

Favarin, S. (2018). This Must Be the Place (to Commit a Crime). Testing the Law of Crime Concentration in Milan, Italy. *European Journal of Criminology*, *15*(6), 702–729. https://doi.org/10.1177/1477370818757700

Felson, M. (2010). What Every Mathematician Should Know About Modelling Crime. *European Journal of Applied Mathematics*, *21*(4–5), 275–281. http://dx.doi.org/10.1017/S0956792510000070

Felson, M. (2016). The Routine Activity Approach. In R. Wortley & M. Townsley (Eds.), *Environmental Criminology and Crime Analysis* (2nd ed., pp. 87–97). Routledge.

Felson, M., & Boba, R. L. (2010). *Crime and Everyday Life* (4th ed.). SAGE Publications.

Felson, M., & Clarke, R. V. (1998). Opportunity Makes the Thief: Practical Theory for Crime Prevention. In Barry Webb (Ed.), *Police Research series, Paper 98*. Home Office.

Felson, M., & Cohen, L. E. (2011). Human Ecology and Crime: A Routine Activity Approach. In *Crime Opportunity Theories: Routine Activity, Rational Choice and their Variants*. Routledge. https://doi.org/10.4324/9781315095301-4

Field, A. (2009). *Discovering Statistics Using SPSS* (3rd edition). SAGE Publications.

Fielding, M., & Jones, V. (2012). 'Disrupting the Optimal Forager': Predictive Risk Mapping and Domestic Burglary Reduction in Trafford, Greater Manchester. *International Journal of Police Science & Management*, *14*(1), 30–41. https://doi.org/10.1350/ijps.2012.14.1.260

Finkelhor, D., Ormrod, R. K., & Turner, H. A. (2007a). Poly-Victimization: A Neglected Component in Child Victimization. *Child Abuse & Neglect*, *31*(1), 7–26. https://doi.org/10.1016/j.chiabu.2006.06.008

Finkelhor, D., Ormrod, R. K., & Turner, H. A. (2007b). Re-Victimization Patterns in a National Longitudinal Sample of Children and Youth.

Child Abuse & Neglect, *31*(5), 479–502. https://doi.org/10.1016/j.chiabu.2006.03.012

Finkelhor, D., Ormrod, R., Turner, H., & Holt, M. (2009). Pathways to Poly-Victimization. *Child Maltreatment*, *14*(4), 316–329. https://doi.org/10.1177/1077559509347012

Finkelhor, D., Shattuck, A., Turner, H. A., Ormrod, R., & Hamby, S. L. (2011). Polyvictimization in Developmental Context. *Journal of Child & Adolescent Trauma*, *4*(4), 291–300. https://doi.org/10.1080/19361521.2011.610432

Finkelhor, D., Turner, H., Hamby, S., & Ormrod, R. (2011). *Polyvictimization: Children's Exposure to Multiple Types of Violence, Crime, and Abuse.* (NCJ235504 (pgs. 1-12); OJJDP Juvenile Justice Bulletin). US Government Printing Office. https://scholars.unh.edu/ccrc/25

Fogden, B. C., Thomas, S. D. M., Daffern, M., & Ogloff, J. R. P. (2016). Crime and Victimisation in People with Intellectual Disability: A Case Linkage Study. *BMC Psychiatry*, *16*(1), 170. https://doi.org/10.1186/s12888-016-0869-7

Forrester, D., Chatterton, M., & Pease, K. (1988). *The Kirkholt Burglary Prevention Project, Rochdale*. Home Office.

Frith, M. J., Johnson, S. D., & Fry, H. M. (2017). Role of the Street Network in Burglars' Spatial Decision-Making*. *Criminology*, *55*(2), 344–376. https://doi.org/10.1111/1745-9125.12133

Fu, Y. C. (2015). *2014 Taiwan Social Change Survey (Round 6, Year 5): Religion (C00310_2)* (NSC 102-2420-H-001-007-SS2). Survey Research Data Archive, Academia Sinica; doi:10.6141/TW-SRDA-C00310_2-1.

Gastwirth, J. L. (1972). The Estimation of the Lorenz Curve and Gini Index. *The Review of Economics and Statistics*, *54*(3), 306–316. JSTOR. https://doi.org/10.2307/1937992

Gottfredson, M. R., & Hindelang, M. J. (1977). A Consideration of Telescoping and Memory Decay Biases in Victimization Surveys. *Journal of Criminal Justice*, *5*(3), 205–216. https://doi.org/10.1016/0047-2352(77)90039-3

Government Equalities Office. (2013). *Disability: Equality Act 2010—Guidance on Matters to Be Taken into Account in Determining Questions Relating to the Definition of Disability*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/570382/Equality_Act_2010-disability_definition.pdf

Grove, L. E., & Farrell, G. (2012). Once Bitten, Twice Shy: Repeat Victimization and its Prevention. In B. C. Welsh & D. P. Farrington (Eds.), *The Oxford Handbook of Crime Prevention* (pp. 404–419). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780195398823.013.0020

Grove, L. E., Farrell, G., Farrington, D. P., & Johnson, S. D. (2012). *Preventing Repeat Victimization: A Systematic Review*. Swedish National Council for Crime Prevention.

Grubesic, T. H., & Mack, E. A. (2008). Spatio-Temporal Interaction of Urban Crime. *Journal of Quantitative Criminology*, *24*(3), 285–306.

https://doi.org/10.1007/s10940-008-9047-5

Haahr-Pedersen, I., Ershadi, A., Hyland, P., Hansen, M., Perera, C., Sheaf, G., Bramsen, R. H., Spitz, P., & Vallières, F. (2020). Polyvictimization and Psychopathology Among Children and Adolescents: A Systematic Review of Studies Using the Juvenile Victimization Questionnaire. *Child Abuse & Neglect*, *107*, 104589. https://doi.org/10.1016/j.chiabu.2020.104589

Hamby, S., Taylor, E., Jones, L., Mitchell, K. J., Turner, H. A., & Newlin, C. (2018). From Poly-Victimization to Poly-Strengths: Understanding the Web of Violence Can Transform Research on Youth Violence and Illuminate the Path to Prevention and Resilience. *Journal of Interpersonal Violence*, *33*(5), 719–739. https://doi.org/10.1177/0886260517744847

Hammond, L., & Youngs, D. (2011). Decay Functions and Criminal Spatial Processes: Geographical Offender Profiling of Volume Crime. *Journal of Investigative Psychology and Offender Profiling*, *8*(1), 90–102. https://doi.org/10.1002/jip.132

Hargittai, E. (2007). Whose Space? Differences Among Users and Non-Users of Social Network Sites. *Journal of Computer-Mediated Communication*, *13*(1), 276–297. https://doi.org/10.1111/j.1083-6101.2007.00396.x

Harrell, E. (2019). *Victims of Identity Theft, 2016* (NCJ 251147; p. 29). The Bureau of Justice Statistics of the U.S. Department of Justice. https://www.bjs.gov/content/pub/pdf/vit16.pdf

Harrison, L., & Hughes, A. (Eds.). (1997). *The Validity of Self-reported Drug Use: Improving the Accuracy of Survey Estimates*. U.S. Department of Health and Human Services, National Institutes of Health, National Institute on Drug Abuse, Division of Epidemiology and Prevention Research.

Hastie, D. I., Liverani, S., Azizi, L., Richardson, S., & Stücker, I. (2013). A Semi-Parametric Approach to Estimate Risk Functions Associated with Multi-Dimensional Exposure Profiles: Application to Smoking and Lung Cancer. *BMC Medical Research Methodology*, *13*(1), 129. https://doi.org/10.1186/1471-2288-13-129

He, D., & Messner, S. F. (2019). Social Disorganization Theory in Contemporary China: A Review of the Evidence and Directions for Future Research. *Asian Journal of Criminology*. https://doi.org/10.1007/s11417-019-09291-2

Hearnden, I., & Magill, C. (2004). *Decision-Making by House Burglars: Offenders' Perspectives* (Findings 249). Home Office. https://doi.org/10.1037/e463472008-001

Hebenton, B., & Jou, S. (2005). In Search of Criminological Tradition: The Development of Criminology in Taiwan. *Crime, Law and Social Change*, *44*(3), 215–250. https://doi.org/10.1007/s10611-005-9002-4

Heiskanen, M., & Laaksonen, S. (2021). Victim Surveys. In J. C. Barnes & D. R. Forde (Eds.), *The Encyclopedia of Research Methods in Criminology and Criminal Justice* (pp. 153–157). John Wiley & Sons, Inc. https://doi.org/10.1002/9781119111931.ch28

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Does Gender Matter in the Virtual World? Examining the Effect of Gender on the Link Between Online Social Network Activity, Security and Interpersonal Victimization. *Security Journal*, *26*(4), 315–330.

Higgins, G. E. (2007). Digital Piracy, Self-Control Theory, and Rational Choice: An Examination of the Role of Value. *International Journal of Cyber Criminology*, *1*(1), 33–55.

Hillier, B. (2004). Can Streets Be Made Safe? *URBAN DESIGN International*, *9*(1), 31–45. https://doi.org/10.1057/palgrave.udi.9000079

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Ballinger.

Hinduja, S., & Kooi, B. (2013). Curtailing Cyber and Information Security Vulnerabilities Through Situational Crime Prevention. *Security Journal*, *26*(4), 383–402. https://doi.org/10.1057/sj.2013.25

Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. *Deviant Behavior*, *29*, 129–156. https://doi.org/10.1080/01639620701457816

Hino, K., & Amemiya, M. (2019). Spatiotemporal Analysis of Burglary in Multifamily Housing in Fukuoka City, Japan. *Cities*, *90*, 15–23. https://doi.org/10.1016/j.cities.2019.01.030

Hipp, J. R., & Roussell, A. (2013). Micro- and Macro-Environment Population and the Consequences for Crime Rates. *Social Forces*, *92*(2), 563–595.

Hirschi, T., & Gottfredson, M. (1983). Age and the Explanation of Crime. *American Journal of Sociology*, *89*(3), 552–584.

HMIC. (2014). *Crime-Recording: Making the Victim Count*. HMIC. https://www.justiceinspectorates.gov.uk/hmicfrs/publications/crime-recording-making-the-victim-count/

Ho, M.-C. (2013). *Research on the Analysis of Modus Operandi and Prevention of Residential Burglary* (No. 102301010000C0006). Ministry of the Interior. https://www.moi.gov.tw/files/site_node_file/8037/%E3%80%90%E8%AD%A6%E6%94%BF%E7%BD%B2%E3%80%91%E4%BD%8F%E5%AE%85%E7%AB%8A%E7%9B%9C%E7%8A%AF%E7%BD%AA%E6%89%8B%E6%B3%95%E5%88%86%E6%9E%90%E8%88%87%E9%98%B2%E5%88%B6%E4%B9%8B%E7%A0%94%E7%A9%B6.pdf

Hohl, K., & Stanko, E. A. (2015). Complaints of Rape and the Criminal Justice System: Fresh Evidence on the Attrition Problem in England and Wales. *European Journal of Criminology*, *12*(3), 324–341. https://doi.org/10.1177/1477370815571949

Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The Capable Guardian in Routine Activities Theory: A Theoretical and Conceptual Reappraisal. *Crime Prevention and Community Safety; London*, *15*(1), 65–79. http://dx.doi.org.libproxy.ucl.ac.uk/10.1057/cpcs.2012.14

Hollis-Peel, M. E., Reynald, D. M., van Bavel, M., Elffers, H., & Welsh, B. C. (2011). Guardianship for Crime Prevention: A Critical Review of the Literature. *Crime, Law and Social Change*, *56*(1), 53–70.

https://doi.org/10.1007/s10611-011-9309-2

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1–25. https://doi.org/10.1080/01639620701876577

Holt, T. J., & Bossler, A. M. (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420–436. https://doi.org/10.1177/1043986213507401

Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, E. R. (2020). Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization. *Social Science Computer Review*, *38*(2), 187–206. https://doi.org/10.1177/0894439318805067

Holtfreter, K., Reisig, M. D., & Blomberg, T. G. (2006). Consumer Fraud Victimization in Florida: An Empirical Study General Issue. *St. Thomas Law Review*, *18*(3), 761–790.

Holtfreter, K., Reisig, M. D., Leeper Piquero, N., & Piquero, A. R. (2010). Low Self-Control and Fraud: Offending, Victimization, and Their Overlap. *Criminal Justice and Behavior*, *37*(2), 188–203. https://doi.org/10.1177/0093854809354977

Homel, R., & Clarke, R. V. (1997). A Revised Classification of Situational Crime Prevention Techniques. In S. P. Lab (Ed.), *Crime Prevention At a Crossroads*. Anderson. https://www.semanticscholar.org/paper/A-Revised-Classification-of-Situational-Crime-Homel-Clarke/1bd6a24bf745f3d9b50feaa63fdead7829db13f9

Hope, T. (1984). Building Design and Burglary. In R. V. Clarke & T. Hope (Eds.), *Coping with Burglary: Research Perspectives on Policy* (pp. 45–59). Springer Netherlands. https://doi.org/10.1007/978-94-009-5652-0_4

Hopper, N. A. (2015). *Exploring the Impact of Non-Response in the Crime Survey for England and Wales* (No. 73; Survey Methodology Bulletin, pp. 60–76). Office for National Statistics. http://webarchive.nationalarchives.gov.uk/20160105160709/http:/www.ons.gov.uk/ons/guide-method/method-quality/survey-methodology-bulletin/smb-73/survey-methodology-bulletin-73---spring-2015.pdf

Hox, J. (2002). *Multilevel Analysis Techniques and Applications*. Lawrence Erlbaum Associates Publishers.

Huang, T.-S. (2011). The Research of Crime Prevention in Residential Burglary for Home Safety. *Police Science Quarterly*, *41*(5), 163–191.

Hughes, K., Bellis, M. A., Jones, L., Wood, S., Bates, G., Eckley, L., McCoy, E., Mikton, C., Shakespeare, T., & Officer, A. (2012). Prevalence and Risk of Violence Against Adults with Disabilities: A Systematic Review and Meta-Analysis of Observational Studies. *The Lancet*, *379*(9826), 1621–1629. https://doi.org/10.1016/S0140-6736(11)61851-5

Hunter, J., & Tseloni, A. (2016). Equity, Justice and the Crime Drop: The Case of Burglary in England and Wales. *Crime Science*, *5*(1), 3. https://doi.org/10.1186/s40163-016-0051-z

Hutchings, A. (2013). Hacking and Fraud: Qualitative Analysis of Online Offending and Victimization. In K. Jaishankar & N. Ronel (Eds.), *Global Criminology: Crime and Victimization in the Globalized Era* (pp. 93–114). CRC Press.

Ignatans, D., & Pease, K. (2015). Distributive Justice and the Crime Drop. In *The Criminal Act: The Role and Influence of Routine Activity Theory* (pp. 77–87). Palgrave Macmillan. http://eprints.hud.ac.uk/id/eprint/26078/

Ignatans, D., & Pease, K. (2016a). On Whom Does the Burden of Crime Fall Now? Changes Over Time in Counts and Concentration. *International Review of Victimology*, *22*(1), 55–63. https://doi.org/10.1177/0269758015610854

Ignatans, D., & Pease, K. (2016b). Taking Crime Seriously: Playing the Weighting Game. *Policing: A Journal of Policy and Practice*, *10*(3), 184–193. https://doi.org/10.1093/police/pav029

International Crime Victims Survey (ICVS). (2021). *Sources for the ICVS*. https://wp.unil.ch/icvs/sources-for-the-icvs/

Jackson, J., & Bradford, B. (2010). What is Trust and Confidence in the Police? *Policing: A Journal of Policy and Practice*, *4*(3), 241–248. https://doi.org/10.1093/police/paq020

Jann, B. (2016). Estimating Lorenz and Concentration Curves. *The Stata Journal*, *16*(4), 837–866. https://doi.org/10.1177/1536867X1601600403

Jansen, J., & Leukfeldt, E. R. (2016). Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology*, *10*(1), 79–91. http://dx.doi.org.libproxy.ucl.ac.uk/10.5281/zenodo.58523

Jeffery, C. R. (1971). Crime Prevention Through Environmental Design. *American Behavioral Scientist*, *14*(4), 598–598. https://doi.org/10.1177/
000276427101400409

Jenaro, C., Flores, N., & Frías, C. P. (2018). Systematic Review of Empirical Studies on Cyberbullying in Adults: What We Know and What We Should Investigate. *Aggression and Violent Behavior*, *38*, 113–122. https://doi.org/10.1016/j.avb.2017.12.003

Jensen, G. F., & Brownfield, D. (1986). Gender, Lifestyles, and Victimization: Beyond Routine Activity. *Violence and Victims; New York*, *1*(2), 85–99.

Jibril, A. B., Kwarteng, M. A., Nwaiwu, F., Appiah-Nimo, C., Pilik, M., & Chovancova, M. (2020). Online Identity Theft on Consumer Purchase Intention: A Mediating Role of Online Security and Privacy Concern. In M. Hattingh, M. Matthee, H. Smuts, I. Pappas, Y. K. Dwivedi, & M. Mäntymäki (Eds.), *Responsible Design, Implementation and Use of Information and Communication Technology* (pp. 147–158). Springer International Publishing. https://doi.org/10.1007/978-3-030-45002-1_13

Jobes, P. C., Barclay, E., Weinand, H., & Donnermeyer, J. F. (2004). A

Structural Analysis of Social Disorganiztion and Crime. *The Australian and New Zealand Journal of Criminology*, *37*(1), 114–140.

Johnson, S. D. (2008). Repeat Burglary Victimisation: A Tale of Two Theories. *Journal of Experimental Criminology*, *4*(3), 215–240. https://doi.org/10.1007/s11292-008-9055-3

Johnson, S. D. (2014). How Do Offenders Choose Where to Offend? Perspectives from Animal Foraging. *Legal and Criminological Psychology*, *19*(2), 193–210. https://doi.org/10.1111/lcrp.12061

Johnson, S. D., Bernasco, W., Bowers, K. J., Elffers, H., Ratcliffe, J., Rengert, G., & Townsley, M. (2007). Space–Time Patterns of Risk: A Cross National Assessment of Residential Burglary Victimization. *Journal of Quantitative Criminology*, *23*(3), 201–219. https://doi.org/10.1007/s10940-007-9025-3

Johnson, S. D., & Bowers, K. J. (2004a). The Stability of Space-Time Clusters of Burglary. *British Journal of Criminology*, *44*(1), 55–65. https://doi.org/10.1093/bjc/44.1.55

Johnson, S. D., & Bowers, K. J. (2004b). The Burglary as Clue to the Future: The Beginnings of Prospective Hot-Spotting. *European Journal of Criminology*, *1*(2), 237–255. https://doi.org/10.1177/1477370804041252

Johnson, S. D., & Bowers, K. J. (2010). Permeability and Burglary Risk: Are Cul-de-Sacs Safer? *Journal of Quantitative Criminology*, *26*(1), 89–111. https://doi.org/10.1007/s10940-009-9084-8

Johnson, S. D., & Loxley, C. (2001). *Installing Alley-Gates: Practical Lessons from Burglary Prevention Projects*. Policing and Reducing Crime Unit, Home Office Research, Development and Statistics Directorate. https://popcenter.asu.edu/sites/default/files/tools/implementing_responses/PDFs/Johnson.pdf

Johnson, S. D., Summers, L., & Pease, K. (2009). Offender as Forager? A Direct Test of the Boost Account of Victimization. *Journal of Quantitative Criminology*, *25*(2), 181–200. https://doi.org/10.1007/s10940-008-9060-8

Jones, C. (2010). Archival Data: Advantages and Disadvantages for Research in Psychology. *Social and Personality Psychology Compass*, *4*(11), 1008–1017. https://doi.org/10.1111/j.1751-9004.2010.00317.x

Junger-Tas, J., & Marshall, I. H. (1999). The Self-Report Methodology in Crime Research. *Crime and Justice: A Review of Research*, *25*, 291–368.

Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young Adults. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 129–137. https://doi.org/10.1089/cyber.2016.0728

Kahn, C. M., & Liñares-Zegarra, J. M. (2016). Identity Theft and Consumer Payment Choice: Does Security Really Matter? *Journal of Financial Services Research*, *50*(1), 121–159. https://doi.org/10.1007/s10693-015-0218-x

Kalia, D., & Aleem, S. (2017). Role of Routine Activity Theory in Cyber

Victimization among Adolescents: A Gendered Perspective. *Phonix - International Journal for Psychology and Social Sciences*, *1*(3), 1–121.

Kelling, G. L. (1997). Crime Control, the Police, and Culture Wars: Broken Windows and Cultural Pluralism Lecture 1. *Perspectives on Crime and Justice: Lecture Series*, *2*, 1–28.

Kelling, G. L., & Coles, C. M. (1997). *Fixing Broken Windows: Restoring Order And Reducing Crime In Our Communities*. Simon and Schuster.

Kelly, L., & Karsna, K. (2018). *Measuring the Scale and Changing Nature of Child Sexual Abuse and Child Sexual Exploitation: Scoping Report*. Centre of Expertise on Child Sexual Abuse. https://www.csacentre.org.uk/documents/scale-and-nature-scoping-report-2018/

Kennedy, L., & Forde, D. (1990). Risky Lifestyles and Dangerous Results: Routine Activities and Exposure to Crime. *Sociology and Social Research: An International Journal*, *74*(4), 208–211.

Khade, N. B., Wang, X., & Decker, S. H. (2018). Examining the Link Between Childhood Physical Abuse and Risk for Violent Victimization in Youth and Young Adulthood in China. *Journal of Interpersonal Violence*, *36*(9–10), 1–28. https://doi.org/10.1177/0886260518794002

Kim, J., Bushway, S., & Tsao, H.-S. (2016). Identifying Classes of Explanations for Crime Drop: Period and Cohort Effects for New York State. *Journal of Quantitative Criminology*, *32*(3), 357–375. https://doi.org/10.1007/s10940-015-9274-5

Kleemans, E. R. (2001). Repeat Burglary Victimisation: Results of Empirical Research in the Netherlands. In G. Farrell & K. Pease (Eds.), *Repeat Victimization* (pp. 53–68). Criminal Justice Press.

Kleemans, E. R., & Van de Bunt, H. G. (2008). Organised Crime, Occupations and Opportunity. *Global Crime*, *9*(3), 185–197. https://doi.org/10.1080/17440570802254254

Knox, G. (1964). Epidemiology of Childhood Leukaemia in Northumberland and Durham. *Journal of Epidemiology & Community Health*, *18*(1), 17–24. https://doi.org/10.1136/jech.18.1.17

Koong, K. S., & Liu, L. C. (2006). An Examination of Internet Fraud Occurrences. *International Journal of Cyber Criminology*, *5*(2), 441–449.

Kowalski, R. M., & Limber, S. P. (2007). Electronic Bullying Among Middle School Students. *Journal of Adolescent Health*, *41*(6, Supplement), S22–S30. https://doi.org/10.1016/j.jadohealth.2007.08.017

Kowalski, R. M., Morgan, C. A., Drake-Lavelle, K., & Allison, B. (2016). Cyberbullying Among College Students with Disabilities. *Computers in Human Behavior*, *57*, 416–427. https://doi.org/10.1016/j.chb.2015.12.044

Kretschmar, J. M., Tossone, K., Butcher, F., & Flannery, D. J. (2017). Patterns of Poly-Victimization in a Sample of At-Risk Youth. *Journal of Child & Adolescent Trauma*, *10*(4), 363–375. https://doi.org/10.1007/s40653-016-0109-9

Kubrin, C. E., & Wo, J. C. (2016). Social Disorganization Theory's Greatest

Challenge: Linking Structural Characteristics to Crime in Socially Disorganized Communities. In A. R. Piquero (Ed.), *The Handbook of Criminological Theory* (pp. 121–136). John Wiley & Sons, Inc. https://doi.org/10.1002/9781118512449.ch7

Kunz, M., & Wilson, P. (2004). *Computer Crime and Computer Fraud*. University of Maryland: Department of Criminology and Criminal Justice. https://www.montgomerycountymd.gov/cjcc/resources/files/computer_crime_study.pdf

Kuo, S.-Y. (2015). Opportunity, Choice, and Burglary Victimization in Taiwan. *International Journal of Offender Therapy and Comparative Criminology*, *59*(8), 873–891. https://doi.org/10.1177/0306624X13520439

Kuo, T.-L. (2017). *Under-Recording Practices and the Determinants: From the Perspective of Police in Taiwan* [Master's thesis]. University College London.

Langton, L., Berzofsky, M., Krebs, C., & Smiley-McDonald, H. (2012). *Victimizations Not Reported to the Police, 2006-2010* (NCJ 238536). US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://www.dgfpi.de/tl_files/pdf/medien/2012-08-20_NCVS_USA_Victimizations-not-reported-dot-Police_2006-2010.pdf

Lantz, B., & Ruback, R. (2017). A Networked Boost: Burglary Co-Offending and Repeat Victimization Using a Network Approach. *Crime & Delinquency*, *63*(9), 1066–1090. https://doi.org/10.1177/0011128715597695

Lätsch, D. C., Nett, J. C., & Hümbelin, O. A. (2017). Poly-Victimization and Its Relationship With Emotional and Social Adjustment in Adolescence: Evidence From a National Survey in Switzerland. *Psychology of Violence*, *7*(1), 1–11. https://doi.org/10.1037/a0039993

Lauritsen, J. L., Owens, J. G., Planty, M. G., Rand, M. R., & Truman, J. L. (2012). *Methods for Counting High-Frequency Repeat Victimizations in the National Crime Victimization Survey* (NCJ 237308; p. 33). Bureau of Justice Statistics.

Lauritsen, J. L., & Quinet, K. F. D. (1995). Repeat Victimization Among Adolescents and Young Adults. *Journal of Quantitative Criminology*, *11*(2), 143–166. https://doi.org/10.1007/BF02221121

Lauritsen, J. L., Rezey, M. L., & Heimer, K. (2016). When Choice of Data Matters: Analyses of U.S. Crime Trends, 1973–2012. *Journal of Quantitative Criminology*, *32*(3), 335–355. https://doi.org/10.1007/s10940-015-9277-2

Laycock, G. (2001). Hypothesis-Based Research: The Repeat Victimization Story. *Criminal Justice*, *1*(1), 59–82. https://doi.org/10.1177/1466802501001001004

Le, M. T. H., Holton, S., Nguyen, H. T., Wolfe, R., & Fisher, J. (2016). Victimisation, Poly-Victimisation and Health-Related Quality of Life Among High School Students in Vietnam: A Cross-Sectional Survey. *Health and Quality of Life Outcomes*, *14*(1), 155. https://doi.org/10.1186/s12955-016-0558-8

Le, M. T. H., Holton, S., Romero, L., & Fisher, J. (2018). Polyvictimization Among Children and Adolescents in Low- and Lower-Middle-Income Countries: A Systematic Review and Meta-Analysis. *Trauma, Violence, & Abuse*, *19*(3), 323–342. https://doi.org/10.1177/1524838016659489

Lee, Y., Eck, J. E., O, S., & Martinez, N. N. (2017). How Concentrated Is Crime at Places? A Systematic Review from 1970 to 2015. *Crime Science*, *6*(1), 6. https://doi.org/10.1186/s40163-017-0069-x

Lemieux, A. M., & Felson, M. (2012). *Risk of Violent Crime Victimization During Major Daily Activities*. https://search-proquest-com.libproxy.ucl.ac.uk/docview/1081338409/abstract/A8D60D32A46C4ACAPQ/1

Leoschut, L., & Kafaar, Z. (2017). The Frequency and Predictors of Poly-Victimisation of South African Children and the Role of Schools in Its Prevention. *Psychology, Health & Medicine*, *22*(sup1), 81–93. https://doi.org/10.1080/13548506.2016.1273533

Leukfeldt, E. R. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E. R. (2015). Comparing Victims of Phishing and Malware Attacks: Unraveling Risk Factors and Possibilities for Situational Crime Prevention. *International Journal of Advanced Studies in Computer Science and Engineering*, *4*(5), 26–32.

Leukfeldt, E. R., & Kleemans, E. R. (2020). Cybercrime, Money Mules and Situational Crime Prevention. In S. Hufnagel & A. Moiseienko (Eds.), *Criminal Networks and Law Enforcement: Global Perspectives On Illegal Enterprise*. Routledge. https://www.researchgate.net/publication/334090389_Cybercrime_money_mules_and_situational_crime_prevention

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Li, Q. (2006). Cyberbullying in Schools: A Research of Gender Differences. *School Psychology International*, *27*(2), 157–170. https://doi.org/10.1177/0143034306064547

Li, X., Stanton, B., Fang, X., & Lin, D. (2006). Social Stigma and Mental Health among Rural-to-Urban Migrants in China: A Conceptual Framework and Future Research Needs. *World Health & Population*, *8*(3), 14–31. https://doi.org/10.12927/whp.2006.18282

Lin, K.-L., & Shen, S.-A. (2016). The Impact of Parental Dysfunction to Juvenile Conduct Problem and Sexual Offending behavior. *Journal of Research in Delinquency and Prevention*, *8*(1), 191–238.

Lin, L. S. F., & Nomikos, J. (2018). Cybercrime in East and Southeast Asia: The Case of Taiwan. In A. J. Masys & L. S. F. Lin (Eds.), *Asia-Pacific Security Challenges: Managing Black Swans and Persistent Threats* (pp. 65–84). Springer International Publishing. https://doi.org/10.1007/978-3-319-61729-9_4

Lin, W.-H., & Mieczkowski, T. (2011). Subjective Strains, Conditioning Factors, and Juvenile Delinquency: General Strain Theory in Taiwan. *Asian Journal of Criminology*, *6*(1), 69–87. https://doi.org/10.1007/s11417-009-9082-7

Liu, Z., Zhang, Y., Tian, L., Sun, B., Chang, Q., & Zhao, Y. (2017). Application of Latent Class Analysis in Assessing the Competency of Physicians in China. *BMC Medical Education*, *17*. https://doi.org/10.1186/s12909-017-1039-4

Lo, W. Y. W. (2016). The Concept of Greater China in Higher Education: Adoptions, Dynamics and Implications. *Comparative Education*, *52*(1), 26–43. https://doi.org/10.1080/03050068.2015.1125613

Loftin, C., & McDowall, D. (2010). The Use of Official Records to Measure Crime and Delinquency. *Journal of Quantitative Criminology*, *26*(4), 527–532. https://doi.org/10.1007/s10940-010-9120-8

Lu, C., Jen, W., Chang, W., & Chou, S. (2006). Cybercrime & Cybercriminals: An Overview of the Taiwan Experience. *Joutnals of Computers*, *1*(6), 11–18.

Lwin, M. O., Li, B., & Ang, R. P. (2012). Stop Bugging Me: An Examination of Adolescents' Protection Behavior Against Online Harassment. *Journal of Adolescence*, *35*(1), 31–41. https://doi.org/10.1016/j.adolescence.2011.06.007

Maas, C. J. M., & Hox, J. J. (2004). Robustness Issues in Multilevel Regression Analysis. *Statistica Neerlandica*, *58*(2), 127–137. https://doi.org/10.1046/j.0039-0402.2003.00252.x

Maguire, M., & McVie, S. (2017). Crime Data and Criminal Statistics: A Critical Reflection. In A. Liebling, S. Maruna, & L. McAra (Eds.), *The Oxford Handbook of Criminology* (6th ed., pp. 163–189). Oxford University Press. https://doi.org/10.1093/he/9780198719441.003.0008

Maguire, M., Wright, R., & Bennett, T. (2010). Domestic burglary. *The Handbook of Crime. Uffculme, Devon: Willan*.

Magura, S., & Kang, S.-Y. (1996). Validity of Self-Reported Drug Use in High Risk Populations: A Meta-Analytical Review. *Substance Use & Misuse*, *31*(9), 1131–1153. https://doi.org/10.3109/10826089609063969

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily Trends and Origin of Computer-Focused Crimes Against a Large University Computer Network: An Application of the Routine-Activities and Lifestyle Perspective. *British Journal of Criminology*, *53*(2), 319–343. https://doi.org/10.1093/bjc/azs067

Marcum, C. D. (2008). Identifying Potential Factors of Adolescent Online Victimization for High School Seniors. *International Journal of Cyber Criminology*, *2*(2), 346–367.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory. *Deviant Behavior*, *31*(5), 381–410. https://doi.org/10.1080/01639620903004903

Markowitz, F. E., Bellair, P. E., Liska, A. E., & Liu, J. (2001). Extending Social Disorganization Theory: Modeling the Relationships Between Cohesion, Disorder, and Fear. *Criminology*, *39*(2), 293–319. https://doi.org/10.1111/j.1745-9125.2001.tb00924.x

Martin, J. (2011). Volunteer Police and the Production of Social Order in a Taiwanese Village. *Taiwan in Comparative Perspective*, *3*, 33–49.

Martinez, N. N., Lee, Y., Eck, J. E., & O, S. (2017). Ravenous Wolves Revisited: A Systematic Review of Offending Concentration. *Crime Science*, *6*(1), 10. https://doi.org/10.1186/s40163-017-0072-2

Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime Victimization and Problematic Social Media Use: Findings from a Nationally Representative Panel Study. *American Journal of Criminal Justice*. https://doi.org/10.1007/s12103-021-09665-2

Mattei, F., Liverani, S., Guida, F., Matrat, M., Cenée, S., Azizi, L., Menvielle, G., Sanchez, M., Pilorget, C., Lapôtre-Ledoux, B., Luce, D., Richardson, S., Stücker, I., & Group, I. S. (2016). Multidimensional Analysis of the Effect of Occupational Exposure to Organic Solvents on Lung Cancer Risk: The Icare Study. *Occupational and Environmental Medicine*, *73*(6), 368–377. https://doi.org/10.1136/oemed-2015-103177

Matthews, B., & Minton, J. (2017). Rethinking One of Criminology's 'brute Facts': The Age–Crime Curve and the Crime Drop in Scotland. *European Journal of Criminology*, 1477370817731706. https://doi.org/10.1177/1477370817731706

Matthews, B., & Minton, J. (2018). Rethinking One of Criminology's 'Brute Facts': The Age–Crime Curve and the Crime Drop in Scotland. *European Journal of Criminology*, *15*(3), 296–320. https://doi.org/10.1177/1477370817731706

Mawby, R. I. (2001). *Burglary*. Willan.

Maxfield, M. G. (1987). Lifestyle and Routine Activity Theories of Crime: Empirical Studies of Victimization, Delinquency, and Offender Decision-Making. *Journal of Quantitative Criminology*, *3*(4), 275–282. https://doi.org/10.1007/BF01066831

Maxfield, M. G., Lewis, D. A., & Szoc, R. (1980). Producing Official Crimes: Verified Crime Reports as Measures of Police Output. *Social Science Quarterly*, *61*(2), 221–236. https://doi.org/10.2307/42860716

Mayhew, P., & van Dijk, J. (2011). Assessing Crime Through International Victimization Surveys. In *The SAGE Handbook of Criminological Research Methods*. SAGE Publications Ltd.

McAfee. (2020). *What Is the Difference Between Malware and a Virus?* https://www.mcafee.com/enterprise/en-gb/security-awareness/ransomware/malware-vs-viruses.html

McGuinness, F. (2018). *Poverty in the UK: Statistics* (No. 7096; p. 43). House of Common Library. https://dera.ioe.ac.uk/32118/1/SN07096..pdf

McGuire, M., & Dowling, S. (2013). *Cyber Crime: A Review of the Evidence* (Research Report 75). Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Me, G., & Spagnoletti, P. (2005). Situational Crime Prevention and Cyber-Crime Investigation: The Online Pedo-Pornography Case Study. *EUROCON 2005 - The International Conference on 'Computer as a Tool'*, *2*, 1064–1067. https://doi.org/10.1109/EURCON.2005.1630133

Meier, R. F., & Miethe, T. D. (1993). Understanding Theories of Criminal Victimization. *Crime and Justice*, *17*, 459–499.

Menard, S. (2002). *Applied Logistic Regression Analysis*. SAGE Publications, Inc. https://doi.org/10.4135/9781412983433

Merseyside Police. (2001). *Operation Crystal Clear: In an Effort to Reduce Glass Related Street Violence, the Message Remains 'Crystal Clear'*. Merseyside Police. https://popcenter.asu.edu/sites/default/files/library/awards/tilley/2001/01-49(W-cdrc).pdf

Mesch, G. S. (2009). Parental Mediation, Online Activities, and Cyberbullying. *Cyberpsychology & Behavior*, *12*(4), 387–393.

Messner, S. F., & Blau, J. R. (1987). Routine Leisure Activities and Rates of Crime: A Macro-Level Analysis. *Social Forces*, *65*(4), 1035–1052. JSTOR. https://doi.org/10.2307/2579022

Miethe, T. D., & McDowall, D. (1993). Contextual Effects in Models of Criminal Victimization. *Social Forces*, *71*(3), 741.

Miethe, T. D., & Meier, R. F. (1990). Opportunity, Choice, and Criminal Victimization: A Test of a Theoretical Model. *Journal of Research in Crime and Delinquency*, *27*(3), 243–266. https://doi.org/10.1177/0022427890027003003

Miethe, T. D., Stafford, M. C., & Long, J. S. (1987). Social Differentiation in Criminal Victimization: A Test of Routine Activities/Lifestyle Theories. *American Sociological Review*, *52*(2), 184–194. https://doi.org/10.2307/2095447

Miethe, T. D., Stafford, M. C., & Sloane, D. (1990). Lifestyle Changes and Risks of Criminal Victimization. *Journal of Quantitative Criminology*, *6*(4), 357–376. https://doi.org/10.1007/BF01066676

min Park, S. (2015). A Study of Over-Dispersed Household Victimizations in South Korea: Zero-Inflated Negative Binomial Analysis of Korean National Crime Victimization Survey. *Asian Journal of Criminology*, *10*(1), 63–78. https://doi.org/10.1007/s11417-015-9206-1

Miniwatts Marketing Group. (2020). *World Internet Users Statistics and 2020 World Population Stats*. https://www.internetworldstats.com/stats.htm

Miniwatts Marketing Group. (2021, May 26). *Internet Usage Statistics: World Internet Users and 2021 Population Stats* [Internet World Stats]. https://www.internetworldstats.com/stats.htm

Mirrlees-Black, C., Budd, T., Partridge, S., & Mayhew, P. (1998). *The 1998 British Crime Survey* (Vol. 21/98). Home Office.

Mishna, F., Cook, C., Saini, M., Wu, M.-J., & MacFadden, R. (2011). Interventions to Prevent and Reduce Cyber Abuse of Youth: A Systematic Review. *Research on Social Work Practice*, *21*(1), 5–14. https://doi.org/10.1177/1049731509351988

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007). Online Requests for Sexual

Pictures from Youth: Risk Factors and Incident Characteristics. *Journal of Adolescent Health*, *41*(2), 196–203. https://doi.org/10.1016/j.jadohealth.2007.03.013

Mitchell, K. J., Segura, A., Jones, L. M., & Turner, H. A. (2018). Poly-Victimization and Peer Harassment Involvement in a Technological World. *Journal of Interpersonal Violence*, *33*(5), 762–788. https://doi.org/10.1177/0886260517744846

Mohler, G., Brantingham, P. J., Carter, J., & Short, M. B. (2019). Reducing Bias in Estimates for the Law of Crime Concentration. *Journal of Quantitative Criminology*, *35*(4), 747–765. https://doi.org/10.1007/s10940-019-09404-1

Moineddin, R., Matheson, F. I., & Glazier, R. H. (2007). A Simulation Study of Sample Size for Multilevel Logistic Regression Models. *BMC Medical Research Methodology*, *7*, 34. https://doi.org/10.1186/1471-2288-7-34

Molitor, J., Papathomas, M., Jerrett, M., & Richardson, S. (2010). Bayesian Profile Regression with an Application to the National Survey of Children’s Health. *Biostatistics*, *11*(3), 484–498. https://doi.org/10.1093/biostatistics/kxq013

Morgan, N. (2014). *The Heroin Epidemic of the 1980s and 1990s and Its Effect on Crime Trends – Then and Now: Technical Report*. Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/332963/horr79tr.pdf

Mosher, C. J., Miethe, T. D., & Hart, T. C. (2011). *The Mismeasure of Crime* (2nd ed.). SAGE Publications, Inc. http://dx.doi.org/10.4135/9781483349497

Mueller-Johnson, K., Eisner, M. P., & Obsuth, I. (2014). Sexual Victimization of Youth With a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors. *Journal of Interpersonal Violence*, *29*(17), 3180–3206. https://doi.org/10.1177/0886260514534529

Murphy, K., & Barkworth, J. (2014). Victim Willingness to Report Crime to Police: Does Procedural Justice or Outcome Matter Most? *Victims & Offenders*, *9*(2), 178–204. https://doi.org/10.1080/15564886.2013.872744

Mustaine, E. E., & Tewksbury, R. (1998). Predicting Risks of Larceny Theft Victimization: A Routine Activity Analysis Using Refined Lifestyle Measures. *Criminology*, *36*(4), 829–858. https://doi.org/10.1111/j.1745-9125.1998.tb01267.x

Näsi, M., Danielsson, P., & Kaakinen, M. (2021). Cybercrime Victimisation and Polyvictimisation in Finland—Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*. https://doi.org/10.1007/s10610-021-09497-0

National Police Agency. (2019a). *Yearly Statistics of Police Administration: Republic of China*. National Police Agency, Ministry of the Interior. https://www.npa.gov.tw/static/ebook/Y108/mobile/index.html

National Police Agency. (2019b). *Weekly Report of Statistics (Jingzheng Tongji Tongbao): Year 2019 Week 48*. National Police Agency.

https://www.npa.gov.tw/ch/app/data/list?module=wg057&id=2218

National Police Agency. (2020, December 9). *Report List of Statistics (Jingzheng Tongji Tongbao)* [Text/html]. National Police Agency, Ministry of the Interior, Republic of China (Taiwan). https://www.npa.gov.tw/ch/app/data/list?module=wg057&id=2218

National Statistics. (2018, October 30). *R.O.C - Composite Index and Related Indicators*. Statistic from Statistical Bureau. https://eng.stat.gov.tw/ct.asp?xItem=25280&ctNode=6032&mp=5

Navarro, J. N., & Jasinski, J. L. (2012). Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences. *Sociological Spectrum*, *32*, 81–94.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An Examination of Individual and Situational Level Factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.

Nickels, E. L. (2007). A Note on the Status of Discretion in Police Research. *Journal of Criminal Justice*, *35*(5), 570–578. https://doi.org/10.1016/j.jcrimjus.2007.07.009

Nixon, M., Thomas, S. D. M., Daffern, M., & Ogloff, J. R. P. (2017). Estimating the Risk of Crime and Victimisation in People with Intellectual Disability: A Data-Linkage Study. *Social Psychiatry and Psychiatric Epidemiology*, *52*(5), 617–626. https://doi.org/10.1007/s00127-017-1371-3

NortonLifeLock Inc. (2020). *The Risks of Public Wi-Fi*. https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html

O, S., Martinez, N. N., Lee, Y., & Eck, J. E. (2017). How Concentrated Is Crime Among Victims? A Systematic Review from 1977 to 2014. *Crime Science*, *6*, 9. https://doi.org/10.1186/s40163-017-0071-3

Office for National Statistics. (2016). *Consultation: Response to the ONS Consultation on the Methodology for Addressing High-Frequency Repeat Victimisation in Crime Survey for England and Wales Estimates*.

Office for National Statistics. (2017, August 3). *Internet Access – Households and Individuals, Great Britain*. https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2017

Office for National Statistics. (2018). *Overview of Fraud and Computer Misuse Statistics for England and Wales*. Office for National Statistics. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25/pdf

Office for National Statistics. (2019, January 24). *Improving Victimisation Estimates Derived from the Crime Survey for England and Wales*. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/improvingvictimisationestimatesderivedfromthecrimesurveyforenglandandwales/2019-01-24

Office for National Statistics. (2020, March 19). *Nature of Fraud and*

Computer Misuse in England and Wales: Year Ending March 2019. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019

Office for National Statistics. (2021a, February 3). *Crime in England and Wales QMI*. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/methodologies/crimeinenglandandwalesqmi

Office for National Statistics. (2021b). *Crime in England and Wales, Year Ending December 2020—Appendix Tables*. https://www.ons.gov.uk/file?uri=%2fpeoplepopulationandcommunity%2fcrimeandjustice%2fdatasets%2fcrimeinenglandandwalesappendixtables%2fyearendingdecember2020/appendixtablesfinalv2.xlsx

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology*, *13*(2), 309–325.

Onah, N., & Nche, G. C. (2014). The Moral Implication of Social Media Phenomenon in Nigeria. *Mediterranean Journal of Social Sciences*, *5*(20), 2231–2237.

Osborn, D. R., & Tseloni, A. (1998). The Distribution of Household Property Crimes. *Journal of Quantitative Criminology*, *14*(3), 307–330. https://doi.org/10.1023/A:1023086530548

Papathomas, M., Molitor, J., Hoggart, C., Hastie, D., & Richardson, S. (2012). Exploring Data From Genetic Association Studies Using Bayesian Variable Selection and the Dirichlet Process: Application to Searching for Gene × Gene Patterns. *Genetic Epidemiology*, *36*(6), 663–674. https://doi.org/10.1002/gepi.21661

Paquet-Clouston, M., Décary-Hétu, D., & Bilodeau, O. (2018). Cybercrime Is Whose Responsibility? A Case Study of an Online Behaviour System in Crime. *Global Crime*, *19*(1), 1–21. https://doi.org/10.1080/17440572.2017.
1411807

Patchin, J. W., & Hinduja, S. (2006). Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying. *Youth Violence and Juvenile Justice*, *4*(2), 148–169. https://doi.org/10.1177/1541204006286288

Patterson, B. H., Dayton, C. M., & Graubard, B. I. (2002). Latent Class Analysis of Complex Sample Survey Data. *Journal of the American Statistical Association*, *97*(459), 721–741. https://doi.org/10.1198/016214502388618465

Patterson, E. B. (1991). Poverty, Income Inequality, and Community Crime Rates. *Criminology*, *29*(4), 755–776. https://doi.org/10.1111/j.1745-9125.1991.tb01087.x

Pease, K. (1998). *Repeat Victimisation: Tacking Stock* (Paper 90; Crime Detection and Prevention Series). Home Office.

Pease, K., Ignatans, D., & Batty, L. (2018). Whatever Happened to Repeat Victimisation? *Crime Prevention and Community Safety*, *20*(4), 256–267. https://doi.org/10.1057/s41300-018-0051-x

Pease, K., & Tseloni, A. (2014). *Using Modeling to Predict and Prevent*

Victimization (1st ed., Vol. 13). Springer International Publishing. https://doi.org/10.1007/978-3-319-03185-9

Peng, C.-Y., & So, T.-S. (2002). Modeling Strategies In Logistic Regression With SAS, SPSS, Systat, BMDP, Minitab, And STATA. *Journal of Modern Applied Statistical Methods*, *1*(1), 147–156. https://doi.org/10.22237/jmasm/1020255720

Petersilia, J. R. (2001). Crime Victims with Developmental Disabilities: A Review Essay. *Criminal Justice and Behavior*, *28*(6), 655–694. https://doi.org/10.1177/009385480102800601

Pittaro, M. L. (2007). Cyber Stalking: An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology*, *1*(2), 180–197.

Polvi, N., Looman, T., Humphries, C., & Pease, K. (1990). Repeat Break-and-Enter Victimization: Time Course and Crime Prevention Opportunity. *Journal of Police Science and Administration*, *17*(1), 8–11.

Polvi, N., Looman, T., Humphries, C., & Pease, K. (1991). The Time Course of Repeat Burglary Victimization. *The British Journal of Criminology*, *31*(4), 411–414. https://doi.org/10.1093/oxfordjournals.bjc.a048138

Pooley, K., & Ferguson, C. E. (2017). Using Environmental Criminology Theories to Compare 'Youth Misuse of Fire' Across Age Groups in New South Wales. *Australian & New Zealand Journal of Criminology*, *50*(1), 100–122. https://doi.org/10.1177/0004865815596794

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296. https://doi.org/10.1177/0022427810365903

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and Routine Activity Theories Revisited: The Importance of "Risk" to the Study of Victimization. *Victims & Offenders*, *11*(3), 335–354. https://doi.org/10.1080/15564886.2015.1057351

Prendergast, L. A., & Staudte, R. G. (2016). Quantile Versions of the Lorenz Curve. *Electronic Journal of Statistics*, *10*(2), 1896–1926. https://doi.org/10.1214/16-EJS1154

Raftery, A. E. (1995). Bayesian Model Selection in Social Research. *Sociological Methodology*, *25*, 111. https://doi.org/10.2307/271063

Ratcliffe, J. H. (2010). The Spatial Dependency of Crime Increase Dispersion. *Security Journal*, *23*(1), 18–36. https://doi.org/10.1057/sj.2009.16

Ratcliffe, J., & Rengert, G. (2008). Near-Repeat Patterns in Philadelphia Shooting. *Security Journal*, *21*, 58–76. https://doi.org/10.1057/palgrave.sj.8350068

Read, B. (2012). *Roots of the State: Neighborhood Organization and Social Networks in Beijing and Taipei*. Stanford University Press.

Rege, A. (2014). A Criminological Perspective on Power Grid Cyber attacks: Using Routine Activities Theory to Rational Choice Perspective to Explore Adversarial Decision-Making. *Journal of Homeland Security and Emergency Management*, *11*(4), 463–487. https://doi.org/10.1515/jhsem-2013-0061

Reisig, M. D., Tankebe, J., & Mesko, G. (2012). Procedural Justice, Police Legitimacy, and Public Cooperation with the Police Among Young Slovene Adults. *Journal of Criminal Justice and Security*, *14*(2), 147–164.

Reiss, A. J. (1980). Indicators of Crime and Criminal Justice: Quantitative Studies. In S. E. Fienberg & A. J. Reiss (Eds.), *Victim Proneness in Repeat Victimization by Type of Crime* (pp. 41–53). Bureau of Justice Statistics, U.S. Department of Justice. https://www.jstor.org/stable/2288382?origin=crossref

Rengert, G. F., & Groff, E. (2011). *Residential Burglary: How the Urban Environment and Our Lifestyles Play a Contributing Role* (3 edition). Charles C Thomas Pub Ltd.

Reynald, D. M. (2009). Guardianship in Action: Developing a New Tool for Measurement. *Crime Prevention and Community Safety*, *11*(1), 1–20. https://doi.org/10.1057/cpcs.2008.19

Reynald, D. M., Moir, E., Cook, A., & Vakhitova, Z. (2018). Changing Perspectives on Guardianship Against Crime: An Examination of the Importance of Micro-Level Factors. *Crime Prevention and Community Safety; London*, *20*(4), 268–283. http://dx.doi.org.libproxy.ucl.ac.uk/10.1057/s41300-018-0049-4

Reyns, B. W. (2010). A Situational Crime Prevention Approach to Cyberstalking Victimization: Preventive Tactics for Internet Users and Online Place Managers. *Crime Prevention and Community Safety; London*, *12*(2), 99–118. http://dx.doi.org.libproxy.ucl.ac.uk/10.1057/cpcs.2009.22

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238. http://dx.doi.org.libproxy.ucl.ac.uk/10.1177/0022427811425539

Reyns, B. W. (2017). Routine Activity Theory and Cybercrime: A Theoretical Appraisal and Literature Review. In K. F. Steinmetz & M. R. Nobles (Eds.), *Technocrime and Criminological Theory* (1st ed., pp. 35–54). Routledge. https://doi.org/10.4324/9781315117249-3

Reyns, B. W., & Henson, B. (2016). The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119–1139. https://doi.org/10.1177/0306624X15572861

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Reyns, B. W., Henson, B., & Fisher, B. S. (2016). Guardians of the Cyber Galaxy: An Empirical and Theoretical Analysis of the Guardianship Concept From Routine Activity Theory as It Applies to Online Forms of Victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 148–168. https://doi.org/10.1177/1043986215621378

Robinson, M. B. (1998). Burglary Revictimization: The Time Period of Heightened Risk. *British Journal of Criminology*, *38*(1), 78–87.

Robinson, M. B. (1999). Lifestyles, Routine Activities, and Residential Burglary Victimization. *Journal of Crime and Justice*, *22*(1), 27–56. https://doi.org/10.1080/0735648X.1999.9721081

Robinson, M. B., & Robinson, C. E. (1997). Environmental Characteristics Associated with Residential Burglaries of Student Apartment Complexes. *Environment and Behavior*, *29*(5), 657–675. https://doi.org/10.1177/001391659729500

Roh, S., Kim, E., & Yun, M. (2010). Criminal Victimization in South Korea: A Multilevel Approach. *Journal of Criminal Justice*, *38*(3), 301–310. https://doi.org/10.1016/j.jcrimjus.2010.03.004

Rose, C. A., Monda-Amaya, L. E., & Espelage, D. L. (2011). Bullying Perpetration and Victimization in Special Education: A Review of the Literature. *Remedial and Special Education*, *32*(2), 114–130. https://doi.org/10.1177/0741932510361247

Rose, C. A., Simpson, C. G., & Moss, A. (2015). The Bullying Dynamic: Prevalence of Involvement Among a Large-Scale Sample of Middle and High School Youth with and Without Disabilities. *Psychology in the Schools*, *52*(5), 515–531. https://doi.org/10.1002/pits.21840

Rossmo, D. K. (1999). *Geographic Profiling* (1 edition). CRC Press.

Roth, J. J., & Trecki, V. L. (2017). Burglary Expertise: Comparing Burglars to Other Offenders. *Deviant Behavior*, *38*(2), 188–207. https://doi.org/10.1080/01639625.2016.1196972

Rountree, P. W., Land, K. C., & Miethe, T. D. (1994). Macro-Micro Integration in the Study of Victimization: A Hierarchical Logistic Model Analysis Across Seattle Neighborhoods. *Criminology*, *32*(3), 387–414. https://doi.org/10.1111/j.1745-9125.1994.tb01159.x

Sallavaci, O. (2018). Crime and Social Media: Legal Responses to Offensive Online Communications and Abuse. In H. Jahankhani (Ed.), *Cyber Criminology* (pp. 3–23). Springer International Publishing. https://doi.org/10.1007/978-3-319-97181-0_1

Salmivalli, C., & Pöyhönen, V. (2012). Cyberbullying in Finland. In Q. Li, D. Cross, & P. K. Smith (Eds.), *Cyberbullying in the Global Playground: Research from International Perspectives* (1st ed.). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119954484

Sampson, R., Eck, J. E., & Dunham, J. (2010). Super Controllers and Crime Prevention: A Routine Activity Explanation of Crime Prevention Success and Failure. *Security Journal; London*, *23*(1), 37–51. http://dx.doi.org.libproxy.ucl.ac.uk/10.1057/sj.2009.17

Sampson, R. J. (2002). Studying Modern Chicago. *City & Community*, *1*(1), 45–48. https://doi.org/10.1111/1540-6040.00005

Sampson, R. J., & Groves, W. B. (1989). Community Structure and Crime: Testing Social-Disorganization Theory. *American Journal of Sociology*, *94*(4), 774–802. JSTOR.

Sampson, R. J., & Lauritsen, J. L. (1990). Deviant Lifestyles, Proximity to Crime, and the Offender-Victim Link in Personal Violence. *Journal of Research in Crime and Delinquency*, *27*(2), 110–139.

https://doi.org/10.1177/0022427890027002002

Sampson, R. J., Morenoff, J. D., & Gannon-Rowley, T. (2002). Assessing 'Neighborhood Effects': Social Processes and New Directions in Research. *Annual Review of Sociology; Palo Alto*, *28*, 443–478.

Sampson, R. J., & Raudenbush, S. W. (1999). Systematic Social Observation of Public Spaces: A New Look at Disorder in Urban Neighborhoods. *American Journal of Sociology*, *105*(3), 603–651. https://doi.org/10.1086/210356

Sampson, R. J., Raudenbush, S. W., & Earls, F. (1997). Neighborhoods and Violent Crime: A Multilevel Study of Collective Efficacy. *Science*, *277*(5328), 918–924. https://doi.org/10.1126/science.277.5328.918

Sampson, R. J., & Wikström, P.-O. H. (2008). The Social Order of Violence in Chicago and Stockholm Neighborhoods: A Comparative Inquiry. In S. N. Kalyvas, I. Shapiro, & T. Masoud (Eds.), *Order, Conflict, and Violence* (pp. 97–119). Cambridge University Press. https://doi.org/10.1017/CBO9780511755903.006

Sampson, R. J., & Wooldredge, J. D. (1987). Linking the Micro- and Macro-Level Dimensions of Lifestyle-Routine Activity and Opportunity Models of Predatory Victimization. *Journal of Quantitative Criminology*, *3*(4), 371–393. https://doi.org/10.1007/BF01066837

Sampson, R., & Scott, M. S. (1999). *Tackling Crime and Other Public-Safety Problems: Case Studies in Problem-Solving*. U.S. Department of Justice, Office of Community, Oriented Policing Services. https://popcenter.asu.edu/sites/default/files/library/reading/PDFs/1Tackling.pdf

Schaefer, J. D., Moffitt, T. E., Arseneault, L., Danese, A., Fisher, H. L., Houts, R., Sheridan, M. A., Wertz, J., & Caspi, A. (2018). Adolescent Victimization and Early-Adult Psychopathology: Approaching Causal Inference Using a Longitudinal Twin Study to Rule Out Noncausal Explanations. *Clinical Psychological Science*, *6*(3), 352–371. https://doi.org/10.1177/2167702617741381

Schreiber, J. B. (2017). Latent Class Analysis: An Example for Reporting Results. *Research in Social and Administrative Pharmacy*, *13*(6), 1196–1201. https://doi.org/10.1016/j.sapharm.2016.11.011

Schroeder, J. H., Cappadocia, M. C., Bebko, J. M., Pepler, D. J., & Weiss, J. A. (2014). Shedding Light on a Pervasive Problem: A Review of Research on Bullying Experiences Among Children with Autism Spectrum Disorders. *Journal of Autism and Developmental Disorders*, *44*(7), 1520–1534. https://doi.org/10.1007/s10803-013-2011-8

Sharkey, P., Besbris, M., & Friedson, M. (2017). *Poverty and Crime* (D. Brady & L. M. Burton, Eds.; Vol. 1). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199914050.013.28

Shaw, C. R., & McKay, H. D. (1942). *Juvenile Delinquency and Urban Areas*. University of Chicago Press.

Shaw, C. R., & McKay, H. D. (1969). *Juvenile Delinquency and Urban Areas, a Study of Rates of Delinquents in Relation to Differential Characteristics of Local Communities in American Cities*. The University of Chicago Press.

Shaw, M., & Pease, K. (2000). *Research on Repeat Victimisation in Scotland*. Scottish Executive Central Research Unit. http://docs.scie-socialcareonline.org.uk/fulltext/rptvictim.pdf

Sheu, C.-J., Wu, Y.-X., Chung, Y.-C., & Chen, Y.-S. (2018). Family, Opportunity, and Delinquency. *Journal of Research in Delinquency and Prevention*, *9*(2), 57–117.

Sidebottom, A. (2013). *Understanding and Preventing Crime in Malawi: An Opportunity Perspective* [Doctoral dissertation, University College London]. https://discovery.ucl.ac.uk/id/eprint/1388179/1/Sidebottom%20Final%20Thesis%20March%202013%20e-submission.pdf

Sidebottom, A., Kuo, T., Mori, T., Li, J., & Farrell, G. (2018). The East Asian Crime Drop? *Crime Science*, *7*(1), 6. https://doi.org/10.1186/s40163-018-0080-x

Sidebottom, A., Tompson, L., Thornton, A., Bullock, K., Tilley, N., Bowers, K. J., & Johnson, S. D. (2018). Gating Alleys to Reduce Crime: A Meta-Analysis and Realist Synthesis. *Justice Quarterly*, *35*(1), 55–86. https://doi.org/10.1080/07418825.2017.1293135

Silver, E., Arseneault, L., Langley, J., Caspi, A., & Moffitt, T. E. (2005). Mental Disorder and Violent Victimization in a Total Birth Cohort. *American Journal of Public Health*, *95*(11), 2015–2021. https://doi.org/10.2105/AJPH.2003.021436

Skogan, W. G. (1975). Easurement Problems in Official and Survey Crime Rates. *Journal of Criminal Justice*, *3*, 17–32.

Skogan, W. G. (2012). Disorder and Crime. In B. C. Welsh & D. P. Farrington (Eds.), *The Oxford Handbook of Crime Prevention* (pp. 173–188). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780195398823.013.0009

Slonje, R., Smith, P. K., & Frisén, A. (2013). The Nature of Cyberbullying, and Strategies for Prevention. *Computers in Human Behavior*, *29*(1), 26–32. https://doi.org/10.1016/j.chb.2012.05.024

SmartWater Group. (2021). *Smartwater Technology*. The SmartWater Group. https://www.smartwater.com/our-brands/

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its Nature and Impact in Secondary School Pupils. *Journal of Child Psychology and Psychiatry*, *49*(4), 376–385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Smyth, S. M., & Carleton, R. (2011). *Measuring the Extent of Cyber-Fraud: A Discussion Paper on Potential Methods and Data Sources* (Public Safety Canada Working Paper No. 20). Social Science Research Network. https://doi.org/10.2139/ssrn.2020637

Soler, L., Paretilla, C., Kirchner, T., & Forns, M. (2012). Effects of Poly-Victimization on Self-Esteem and Post-Traumatic Stress Symptoms in Spanish Adolescents. *European Child & Adolescent Psychiatry*, *21*(11), 645–653. https://doi.org/10.1007/s00787-012-0301-x

Sommet, N., & Davide, M. (2017). Keep Calm and Learn Multilevel Logistic Modeling: A Simplified Three-Step Procedure Using Stata, R, Mplus, and SPSS. *International Review of Social Psychology*, *30*, 203–218. https://doi.org/10.5334/irsp.90

Sommet, N., & Morselli, D. (2017). Correction: Keep Calm and Learn Multilevel Logistic Modeling: A Simplified Three-Step Procedure Using Stata, R, Mplus, and SPSS. *International Review of Social Psychology*, *30*(1). https://doi.org/10.5334/irsp.162

Sourander, A., Klomek, A. B., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., Ristkari, T., & Helenius, H. (2010). Psychosocial Risk Factors Associated With Cyberbullying Among Adolescents: A Population-Based Study. *Archives of General Psychiatry*, *67*(7), 720–728. https://doi.org/10.1001/archgenpsychiatry.2010.79

Sparks, R. F. (1981). Multiple Victimization: Evidence, Theory, and Future Research Criminology: Symposium on Victimization and Victimology. *Journal of Criminal Law and Criminology*, *72*(2), 762–778.

Steenbeek, W., & Weisburd, D. (2016). Where the Action is in Crime? An Examination of Variability of Crime Across Different Spatial Units in The Hague, 2001–2009. *Journal of Quantitative Criminology*, *32*(3), 449–469. https://doi.org/10.1007/s10940-015-9276-3

Steffensmeier, D., Zhong, H., & Lu, Y. (2017). Age and Its Relation to Crime in Taiwan and the United States: Invariant, or Does Cultural Context Matter?. *Criminology*, *55*(2), 377–404. https://doi.org/10.1111/1745-9125.12139

Stockman, M. (2014). Insider Hacking: Applying Situational Crime Prevention to a New White-Collar Crime. *Proceedings of the 3rd Annual Conference on Research in Information Technology*, 53–56. https://doi.org/10.1145/2656434.2656436

Stokes, N., & Clare, J. (2019). Preventing Near-Repeat Residential Burglary Through Cocooning: Post Hoc Evaluation of a Targeted Police-Led Pilot Intervention. *Security Journal*, *32*(1), 45–62. https://doi.org/10.1057/s41284-018-0144-3

Sunshine, J., & Tyler, T. R. (2003). The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing. *Law & Society Review*, *37*(3), 513–548. https://doi.org/10.1111/1540-5893.3703002

Swaminathan, H., Rogers, H. J., & Sen, R. (2011). Research Methodology for Decision-Making in School Psychology. *The Oxford Handbook of School Psychology*. https://doi.org/10.1093/oxfordhb/9780195369809.013.0038

Sweney, M. (2020, April 26). UK Traffic to Film and TV Piracy Sites up Nearly 60% in Lockdown. *The Guardian*. https://www.theguardian.com/media/2020/apr/26/uk-traffic-to-film-and-tv-piracy-sites-up-nearly-60-in-lockdown

Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, *22*(6), 664–670. https://doi.org/10.2307/2089195

Tade, O., & Aliyu, I. (2011). Social Organization of Internet Fraud among University Undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2), 860–875.

Tankebe, J. (2013). Viewing Things Differently: The Dimensions of Public Perceptions of Police Legitimacy. *Criminology*, *51*(1), 103–135.

https://doi.org/10.1111/j.1745-9125.2012.00291.x

Tanksley, P. T., Barnes, J. C., Boutwell, B. B., Arseneault, L., Caspi, A., Danese, A., Fisher, H. L., & Moffitt, T. E. (2020). Identifying Psychological Pathways to Polyvictimization: Evidence from a Longitudinal Cohort Study of Twins from the Uk. *Journal of Experimental Criminology*, *16*(3), 431–461. https://doi.org/10.1007/s11292-020-09422-1

Taoyuan City Government. (2020). *Taoyuan City—Statistical Yearbook*. Taoyuan City; Taoyuan City. https://www.tycg.gov.tw/eng/home.jsp?id=78&parentpath=0,1,75&mcustomize=onemessages_view.jsp&dataserno=201706160005&aplistdn=ou=data,ou=statistic,ou=entycg,ou=ap_root,o=tycg,c=tw&toolsflag=Y

Terry, K. J., & Ackerman, A. (2008). Child Sexual Abuse in the Catholic Church: How Situational Crime Prevention Strategies Can Help Create Safe Environments. *Criminal Justice and Behavior*, *35*(5), 643–657. https://doi.org/10.1177/0093854808314469

Tewksbury, R., & Mustaine, E. E. (2003). College Students' Lifestyles and Self-Protective Behaviors: Further Considerations of the Guardianship Concept in Routine Activity Theory. *Criminal Justice and Behavior*, *30*(3), 302–327. https://doi.org/10.1177/0093854803030003003

Tewksbury, R., & Mustaine, E. E. (2010). Cohen, Lawrence E., and Marcus K. Felson: Routine Activity Theory. In F. Cullen & P. Wilcox (Eds.), *Encyclopedia of Criminological Theory* (pp. 187–193). SAGE Publications, Inc. https://doi.org/10.4135/9781412959193.n52

Thompson, R., Tseloni, A., Tilley, N., Farrell, G., & Pease, K. (2018). Which Security Devices Reduce Burglary? In A. Tseloni, R. Thompson, & N. Tilley (Eds.), *Reducing Burglary* (pp. 77–105). Springer International Publishing. https://doi.org/10.1007/978-3-319-99942-5_4

Thornberry, T. P., & Krohn, M. D. (2000). The Self-Report Method for Measuring Delinquency and Crime. *Criminal Justice*, *4*, 33–83.

Tilley, N., Thompson, R., Farrell, G., Grove, L. E., & Tseloni, A. (2015). Do Burglar Alarms Increase Burglary Risk? A Counter-Intuitive Finding and Possible Explanations. *Crime Prevention and Community Safety*, *17*(1), 1–19. https://doi.org/10.1057/cpcs.2014.17

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. https://doi.org/10.1057/sj.2010.2

Tillyer, M. S., & Kennedy, D. M. (2008). Locating Focused Deterrence Approaches within a Situational Crime Prevention Framework. *Crime Prevention and Community Safety*, *10*(2), 75–84. https://doi.org/10.1057/cpcs.2008.5

Tippett, N., & Kwak, K. (2012). Cyberbullying in South Korea. In Q. Li, D. Cross, & P. K. Smith (Eds.), *Cyberbullying in the Global Playground: Research from International Perspectives* (1st ed.). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119954484

Titus, R. M. (2001). Personal Fraud and Its Victims. In N. Shover & J. P.

Wright (Eds.), *Crimes of Privilege: Readings in White-Collar Crime* (pp. 57–74). Oxford University Press. https://global.oup.com/ushe/product/crimes-of-privilege-9780195136210?cc=gb&lang=en&

Tokunaga, R. S. (2010). Following You Home from School: A Critical Review and Synthesis of Research on Cyberbullying Victimization. *Computers in Human Behavior*, *26*, 277–287. https://doi.org/10.1016/j.chb.2009.11.014

Tompson, L., Belur, J., Thornton, A., Bowers, K. J., Johnson, S. D., Sidebottom, A., Tilley, N., & Laycock, G. (2021). How Strong is the Evidence-Base for Crime Reduction Professionals? *Justice Evaluation Journal*, *4*(1), 68–97. https://doi.org/10.1080/24751979.2020.1818275

Topçu, Ç., Erdur-Baker, Ö., & Çapa-Aydin, Y. (2008). Examination of Cyberbullying Experiences among Turkish Students from Different School Types. *Cyberpsychology Behav. Soc. Netw.* https://doi.org/10.1089/cpb.2007.0161

Townsley, M. (2008). Visualising Space Time Patterns in Crime: The Hotspot Plot. *Crime Patterns and Analysis*, *1*(1), 61–74.

Townsley, M., Birks, D., Bernasco, W., Ruiter, S., Johnson, S. D., White, G., & Baum, S. (2015). Burglar Target Selection: A Cross-National Comparison. *Journal of Research in Crime and Delinquency*, *52*(1), 3–31. https://doi.org/10.1177/0022427814541447

Townsley, M., Homel, R., & Chaseling, J. (2000). Repeat Burglary Victimisation: Spatial and Temporal Patterns. *Australian & New Zealand Journal of Criminology*, *33*(1), 37–63. https://doi.org/10.1177/000486580003300104

Townsley, M., Homel, R., & Chaseling, J. (2003). Infectious Burglaries: A Test of the Near Repeat Hypothesis. *The British Journal of Criminology*, *43*(3), 615–633. https://doi.org/10.1093/bjc/43.3.615

Townsley, M., & Sidebottom, A. (2010). All Offenders Are Equal, but Some Are More Equal Than Others: Variation in Journeys to Crime Between Offenders. *Criminology*, *48*(3), 897–917. https://doi.org/10.1111/j.1745-9125.2010.00205.x

Tseloni, A. (2006). Multilevel Modelling of the Number of Property Crimes: Household and Area Effects. *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, *169*(2), 205–233. https://doi.org/10.1111/j.1467-985X.2005.00388.x

Tseloni, A., & Pease, K. (2005). Population Inequality: The Case of Repeat Crime Victimization. *International Review of Victimology*, *12*(1), 75–90. https://doi.org/10.1177/026975800501200105

Tseloni, A., Thompson, R., Grove, L. E., Tilley, N., & Farrell, G. (2017). The Effectiveness of Burglary Security Devices. *Security Journal*, *30*(2), 646–664. https://doi.org/10.1057/sj.2014.30

Tseloni, A., Wittebrood, K., Farrell, G., & Pease, K. (2004). Burglary Victimization in England and Wales, the United States and the Netherlands: A Cross-National Comparative Test of Routine Activities and Lifestyle Theories. *British Journal of Criminology*, *44*(1), 66–91. https://doi.org/10.1093/bjc/44.1.66

Tseng, Y. H. (2014). *Using Optimal Foraging Theory to Analyze the Spatial Moving Patterns of Serial Burglars* [National Taiwan University]. https://hdl.handle.net/11296/tev47p

Tsigebrhan, R., Shibre, T., Medhin, G., Fekadu, A., & Hanlon, C. (2014). Violence and Violent Victimization in People with Severe Mental Illness in a Rural Low-Income Country Setting: A Comparative Cross-Sectional Community Study. *Schizophrenia Research*, *152*(1), 275–282. https://doi.org/10.1016/j.schres.2013.10.032

Turner, H. A., Shattuck, A., Finkelhor, D., & Hamby, S. (2017). Effects of Poly-Victimization on Adolescent Social Support, Self-Concept, and Psychological Distress. *Journal of Interpersonal Violence*, *32*(5), 755–780. https://doi.org/10.1177/0886260515586376

Twigg, L., Taylor, J., & Mohan, J. (2010). Diversity or Disadvantage? Putnam, Goodhart, Ethnic Heterogeneity, and Collective Efficacy. *Environment and Planning A: Economy and Space*, *42*(6), 1421–1438. https://doi.org/10.1068/a42287

Tyler, T. R., & Fagan, J. (2008). Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in Their Communities. *Ohio State Journal of Criminal Law*, *6*, 231.

United Nations Development Programme. (2018). *Human Development Indices and Indicators* (2018 Statistical Update). United Nations Development Programme. http://hdr.undp.org/en/2018-update

United States Census Bureau. (2015). *Census Tracts*. https://www2.census.gov/geo/pdfs/education/CensusTracts.pdf

Vakhitova, Z. I., Alston-Knox, C. L., Reynald, D. M., Townsley, M., & Webster, J. L. (2019). Lifestyles and Routine Activities: Do They Enable Different Types of Cyber Abuse? *Computers in Human Behavior*, *101*, 225–237. https://doi.org/10.1016/j.chb.2019.07.012

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 169–188. https://doi.org/10.1177/1043986215621379

van de Mortel, T. F. (2008). Faking It: Social Desirability Response Bias in Self-report Research. *Australian Journal of Advanced Nursing*, *25*(4), 40–48.

van de Weijer, S. G. A., Leukfeldt, E. R., & Bernasco, W. (2019). Determinants of Reporting Cybercrime: A Comparison Between Identity Theft, Consumer Fraud, and Hacking. *European Journal of Criminology*, *16*(4), 486–508. https://doi.org/10.1177/1477370818773610

van Dijk, J. (2008). *The World of Crime*. SAGE Publications, Inc. https://uk.sagepub.com/en-gb/eur/the-world-of-crime/book231814

van Dijk, J., Tseloni, A., & Farrell, G. (2012). *The International Crime Drop: New Directions in Research*. Springer.

van Kesteren, J., van Dijk, J., & Mayhew, P. (2014). The International Crime Victims Surveys: A Retrospective. *International Review of*

Victimology, *20*(1), 49–69. https://doi.org/10.1177/0269758013511742

van Wilsem, J. (2011). Worlds Tied Together? Online and Non-Domestic Routine Activities and Their Impact on Digital and Traditional Threat Victimization. *European Journal of Criminology*, *8*(2), 115–127.

van Wilsem, J. (2013a). Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization. *Oxford Journals*, 168–178.

van Wilsem, J. (2013b). Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437–453.

Vandeviver, C., Neirynck, E., & Bernasco, W. (2021). The Foraging Perspective in Criminology: A Review of Research Literature. *European Journal of Criminology*, 1–27. https://doi.org/10.1177/14773708211025864

Varano, S. P., Schafer, J. A., Cancino, J. M., & Swatt, M. L. (2009). Constructing Crime: Neighborhood Characteristics and Police Recording Behavior. *Journal of Criminal Justice*, *37*(6), 553–563. https://doi.org/10.1016/j.jcrimjus.2009.09.004

Vermunt, J. K. (2003). Multilevel Latent Class Models. *Sociological Methodology; Washington*, *33*, 213–239.

Vézina, J., Hébert, M., Poulin, F., Lavoie, F., Vitaro, F., & Tremblay, R. E. (2011). Risky Lifestyle as a Mediator of the Relationship Between Deviant Peer Affiliation and Dating Violence Victimization Among Adolescent Girls. *Journal of Youth and Adolescence*, *40*(7), 814–824. https://doi.org/10.1007/s10964-010-9602-x

Wang, H. C. (2015). *A Study on the Cause of Burglary Victim and the Reaction of Burglary Victim* [Master's thesis, Central Police University]. https://ndltd.ncl.edu.tw/cgi-bin/gs32/gsweb.cgi/login?o=dnclcdr&s=id=%22103CPU05102011%22.&searchmode=basic

Wang, J., Iannotti, R. J., & Nansel, T. R. (2009). School Bullying Among Adolescents in the United States: Physical, Verbal, Relational, and Cyber | Elsevier Enhanced Reader. *Journal of Adolescent Health*, *45*, 368–375. https://doi.org/10.1016/j.jadohealth.2009.03.021

Wang, S.-N., & Jensen, G. F. (2011). Explaining Delinquency in Taiwan: A Test of Social Learning Theory. In R. L. Akers & G. F. Jensen (Eds.), *Social Learning Theory and the Explanation of Crime* (pp. 65–83). Transaction Publishers.

Wang, Z., & Liu, X. (2017). Analysis of Burglary Hot Spots and Near-Repeat Victimization in a Large Chinese City. *ISPRS International Journal of Geo-Information*, *6*(5), 148. https://doi.org/10.3390/ijgi6050148

Warner, B. D. (1997). Community Characteristics and the Recording of Crime: Police Recording of Citizens' Complaints of Burglary and Assault. *Justice Quarterly*, *14*(4), 631–650. https://doi.org/10.1080/07418829700093531

Warner, B. D., & Pierce, G. L. (1993). Reexamining Social Disorganization Theory Using Calls to the Police as a Measure of Crime*. *Criminology*, *31*(4), 493–517. https://doi.org/10.1111/j.1745-

9125.1993.tb01139.x

Weisburd, D. (2015). The Law of Crime Concentration and the Criminology of Place. *Criminology*, *53*(2), 133–157. https://doi.org/10.1111/1745-9125.12070

Weisel, D. L. (2005). *Analyzing Repeat Victimization*. U.S. Department of Justice, Office of Community Oriented Policing Services. https://popcenter.asu.edu/sites/default/files/analyzing_repeat_victimization.pdf

Welsh, B. C., & Farrington, D. P. (2009). Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis. *Justice Quarterly*, *26*(4), 716–745. https://doi.org/10.1080/07418820802506206

Wetzels, P., Ohlemacher, T., Pfeiffer, C., & Strobl, R. (1994). Victimization Surveys: Recent Developments and Perspectives. *European Journal on Criminal Policy and Research*, *2*(4), 14–35. https://doi.org/10.1007/BF02249437

Wilcox, P., Madensen, T. D., & Tillyer, M. S. (2007). Guardianship in Context: Implications for Burglary Victimization Risk and Prevention. *Criminology*, *45*(4), 771–803. https://doi.org/10.1111/j.1745-9125.2007.00094.x

Williams, J. (2016). *Reporting Victimisation in the Crime Survey for England & Wales*. TNS BMRB.

Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *The British Journal of Criminology*, *56*(1), 21–48. https://doi.org/10.1093/bjc/azv011

Williams, M. L., & Burnap, P. (2016). Cyberhate on Social Media in the Aftermath of Woolwich: A Case Study in Computational Criminology and Big Data. *British Journal of Criminology*, *56*(2), 211–238. https://doi.org/10.1093/bjc/azv059

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. *Deviant Behavior*, *40*(9), 1119–1131. https://doi.org/10.1080/01639625.2018.1461786

Williams, M. L., & Pearson, O. (2016). *Hate Crime and Bullying in the Age of Social Media*. https://orca.cardiff.ac.uk/88865/1/Cyber-Hate-and-Bullying-Post-Conference-Report_English_pdf.pdf

Willison, R., & Siponen, M. (2009). Overcoming the Insider: Reducing Employee Computer Crime Through Situational Crime Prevention. *Communications of the ACM*, *52*(9), 133–137. https://doi.org/10.1145/1562164.1562198

Wilson, C., & Brewer, N. (1992). The Incidence of Criminal Victimisation of Individuals With an Intellectual Disability. *Australian Psychologist*, *27*(2), 114–117. https://doi.org/10.1080/00050069208257591

Wilson, C., Nettelbeck, T., Potter, R., & Perry, C. (1996). *Intellectual Disability and Criminal Victimisation* (No. 60; Trends and Issues in Crime and Criminal Justice). Australian Institute of Criminology.

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.511.5467&rep=rep1&type=pdf

Wittebrood, K., & Nieuwbeerta, P. (2000). Criminal Victimization During One's Life Course: The Effects of Previous Victimization and Patterns of Routine Activities. *Journal of Research in Crime and Delinquency*, *37*(1), 91–122. https://doi.org/10.1177/0022427800037001004

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2007). Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts. *Journal of Adolescent Health*, *41*(6, Supplement), S51–S58. https://doi.org/10.1016/j.jadohealth.2007.08.019

Wolke, D., Lee, K., & Guy, A. (2017). Cyberbullying: A Storm in a Teacup? *European Child & Adolescent Psychiatry*, *26*(8), 899–908. https://doi.org/10.1007/s00787-017-0954-6

Wooldridge, J. M. (2012). *Introductory Econometrics: A Modern Approach* (5th ed.). South-Western Cengage Learning.

Wortley, R. (2001). A Classification of Techniques for Controlling Situational Precipitators of Crime. *Security Journal*, *14*(4), 63–82. https://doi.org/10.1057/palgrave.sj.8340098

Wortley, R. (2010). Critiques of Situational Crime Prevention. In B. S. Fisher & S. P. Lab (Eds.), *Encyclopedia of Victimology and Crime Prevention* (pp. 885–887). Sage. https://doi.org/10.4135/9781412979993

Wortley, R., & Smallbone, S. (Eds.). (2006). *Situational Prevention of Child Sexual Abuse*. Criminal Justice Press, Willan. https://www.ojp.gov/ncjrs/virtual-library/abstracts/situational-prevention-child-sexual-abuse

Wortley, R., & Townsley, M. (2016). Environmental Criminology and Crime Analysis: Situating the Theory, Analytic Approach and Application. In R. Wortley & M. Townsley (Eds.), *Environmental Criminology and Crime Analysis* (2nd Edition, pp. 1–25). Routledge.

Wu, L., Xu, X., Ye, X., & Zhu, X. (2015). Repeat and Near-Repeat Burglaries and Offender Involvement in a Large Chinese City. *Cartography and Geographic Information Science*, *42*(2), 178–189. https://doi.org/10.1080/15230406.2014.991426

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society* (3rd ed.). SAGE.

Ye, X., Xu, X., Lee, J., Zhu, X., & Wu, L. (2015). Space–Time Interaction of Residential Burglaries in Wuhan, China. *Applied Geography*, *60*, 210–216. https://doi.org/10.1016/j.apgeog.2014.11.022

Yu, O., & Zhang, L. (1999). The Under-Recording of Crime by Police in China: A Case Study. *Policing: An International Journal of Police Strategies & Management*, *22*(3), 252–264. https://doi.org/10.1108/13639519910285035

Yucedal, B. (2010). *Victimization in Cyberspace: An Application of Routine*

Activity and Lifestyle Exposure Theories [Kent State University]. https://etd.ohiolink.edu/pg_10?0::NO:10:P10_ACCESSION_NUM:kent1279290984

Zhang, L., Messner, S. F., & Liu, J. (2007). A Multilevel Analysis of the Risk of Household Burglary in the City of Tianjin, China. *The British Journal of Criminology*, *47*(6), 918–937. JSTOR.

Zhang, L., Messner, S. F., & Zhang, S. (2017). Neighborhood Social Control and Perceptions of Crime and Disorder in Contemporary Urban China. *Criminology*, *55*(3), 631–663. https://doi.org/10.1111/1745-9125.12142

Zhang, Y., Zhao, J., Ren, L., & Hoover, L. (2015). Space–Time Clustering of Crime Events and Neighborhood Characteristics in Houston. *Criminal Justice Review*, *40*(3), 340–360. https://doi.org/10.1177/0734016815573309

Appendix

Table A.1 Near-repeat analysis of burglary risk using police recorded burglary data from Taoyuan city, Taiwan, 2015-2018 (n = 506) (999 iterations)

Spatial unit (m)	Temporal unit (day)													
	0 to < 7	7 to < 14	14 to < 21	21 to < 28	28 to < 35	35 to < 42	42 to < 49	49 to < 56	56 to < 63	63 to < 70	70 to < 77	77 to < 84	84 to < 91	91 to < 98
Same location	__32.00**__	__4.00**__	__4.00**__	0.00	0.00	0.00	n.s.	0.00	0.00	n.s.	n.s.	n.s.	n.s.	n.s.
0.1 to <100	2.00	0.00	0.00	0.00	0.00	2.00	0.00	2.00	2.00	0.00	0.00	2.00	0.00	0.00
100 to <200	__4.00**__	__3.00*__	2.00	1.00	0.00	1.00	0.00	1.00	1.00	2.00	2.00	__4.00*__	__6.00**__	0.00
200 to <300	__5.33**__	2.00	2.00	1.00	1.00	0.00	1.00	0.00	0.00	1.00	0.00	2.00	0.00	1.00
300 to <400	__4.00**__	1.33	0.67	0.00	2.00	0.67	0.67	0.00	__2.00*__	0.67	0.67	1.00	0.67	0.00
400 to <500	0.00	__5.33**__	0.67	0.00	0.00	0.67	1.33	1.33	0.67	__3.33**__	0.67	1.33	0.67	1.00
500 to <600	1.20	0.80	1.00	1.00	1.50	0.50	0.50	1.00	0.50	1.50	1.50	1.50	0.00	1.50
600 to <700	1.67	__3.20**__	0.40	0.40	1.60	1.00	0.50	1.50	__3.00**__	__2.50*__	__2.50**__	1.50	1.00	0.50
700 to <800	0.67	1.60	0.50	0.40	__2.50*__	1.00	2.00	2.00	0.00	0.50	__2.50*__	__3.00**__	1.50	0.00
800 to <900	__2.29**__	1.14	0.67	1.33	1.00	__2.00*__	1.20	0.80	1.20	1.60	__2.40**__	0.40	__2.00*__	1.20
900 to <1000	1.25	__2.29**__	0.00	1.14	0.67	0.33	1.33	1.33	__2.33**__	0.00	1.67	0.00	1.33	0.00
1000 to <1100	1.43	__2.67**__	1.33	1.67	1.60	1.20	1.20	0.80	1.33	0.80	0.80	0.40	0.40	0.40
1100 to <1200	0.57	0.57	0.67	1.00	__2.33**__	1.60	1.60	1.60	0.33	0.40	0.80	1.20	1.20	1.20
1200 to <1300	0.67	1.00	0.57	1.71	0.67	__2.67**__	1.33	1.00	1.67	1.67	1.67	0.67	0.67	0.67
1300 to <1400	0.00	0.67	__1.67*__	0.00	0.40	__2.00*__	1.60	1.20	0.40	1.20	1.20	__2.00*__	1.20	0.50
1400 to <1500	0.50	1.43	0.00	1.43	__2.00*__	0.33	1.33	1.67	1.67	1.33	1.00	1.20	__3.00**__	0.80
1500 to <1600	1.11	1.00	__1.71*__	__2.57**__	1.14	1.00	0.67	0.67	__1.71*__	1.33	1.00	1.33	1.33	__1.67*__

(continued)

Table A.1. *(continued)*

Spatial unit (m)	Temporal unit (day)													
	0 to < 7	7 to <14	14 to < 21	21 to < 28	28 to < 35	35 to < 42	42 to < 49	49 to < 56	56 to < 63	63 to < 70	70 to < 77	77 to < 84	84 to < 91	91 to < 98
1600 to <1700	1.11	0.75	0.86	0.29	__2.00**__	1.00	1.33	1.33	__2.29**__	0.00	0.67	0.67	0.33	1.67
1700 to <1800	0.40	0.44	1.00	1.50	1.43	0.57	1.71	1.14	1.25	1.43	1.71	0.57	0.00	1.43
1800 to <1900	0.80	1.33	1.50	1.50	__1.75*__	0.29	1.14	0.29	0.00	0.86	0.57	0.86	0.86	0.29
1900 to <2000	0.18	__1.80**__	__1.78*__	1.33	1.33	1.25	1.00	1.25	0.50	0.25	__1.75**__	1.43	1.25	1.43
2000 to <2100	0.55	0.80	0.89	0.89	__1.75*__	1.75	0.25	1.25	1.00	0.75	__1.75*__	1.75	1.00	1.43
2100 to <2200	1.27	1.33	0.25	0.44	__3.25**__	0.50	1.43	1.43	0.00	1.25	1.00	1.14	0.50	0.86
2200 to <2300	1.20	1.33	1.25	1.25	0.50	0.86	1.43	0.86	0.50	1.43	0.86	__2.00**__	0.86	0.29
2300 to <2400	__2.00**__	0.40	1.00	1.33	0.25	1.00	1.14	__2.50**__	0.75	1.71	1.00	0.57	0.57	0.57
2400 to <2500	0.91	1.20	__2.00*__	0.89	1.25	1.00	1.00	0.75	0.89	0.25	__2.00**__	0.86	1.25	1.43
2500 to <2600	__2.00**__	__1.78*__	1.25	1.25	1.25	0.57	0.57	1.14	1.43	1.14	__2.00**__	0.57	0.86	0.86
2600 to <2700	0.92	0.55	1.40	1.27	1.11	0.89	0.89	0.44	0.89	0.67	1.11	0.44	0.89	__1.75*__
2700 to <2800	1.08	1.27	1.00	__1.8**__	0.89	0.44	0.89	0.22	1.11	1.33	1.33	1.00	0.22	__1.75*__
2800 to <2900	0.67	0.73	0.80	0.40	1.00	0.67	0.44	1.11	0.80	0.89	0.89	1.25	1.11	__1.56*__
2900 to <3000	1.17	0.73	__1.60*__	0.73	0.67	1.33	0.44	0.67	0.67	__1.56*__	0.67	0.25	0.44	__2.00**__

Note *Significant at $p < 0.05$. **Significant at $p < 0.01$. n.s. indicated expected counts of zero in that cell.