THE UNIVERSITY OF HULL

Policing Internet Fraud in Saudi Arabia: The Mediation of Risk in a Theocratic Society

Being a Thesis Submitted for the Degree of Doctor of Philosophy in the University of Hull

By

Abdullah Faze Algarni

Bachelor in Security Sciences (1st in Cohort with 1st Class Honours), King Fahad Security College, 1995

Bachelor in Fundamentals of Religion (1st in Cohort with 1st Class Honours), Imam Mohammed Bin Saud Islamic University, 2000

MA Criminology, The University of Hull, 2005

Postgraduate Diploma in Research Training, The University of Hull, 2011

June 2012

Abstract

This thesis aims to contribute to current debates on the policing of Internet fraud by introducing the Saudi Arabian experience. Drawing on the findings of field research focusing on the capital city of Riyadh, this study assesses the extent to which the Saudi state response to Internet fraud fits in with contemporary debates on cybercrime control within a late-modern penal framework as theorised in Western literature. At the same time, the study provides a detailed micro-sociological account of how the policing of Internet fraud is carried out in different police units within the city in which the case study was conducted. This involves an in-depth investigation into both the organisational and operational dimensions of the Saudi police response to such criminal activity. In this respect, the thesis explores and analyses how this new aspect of policing activity fits in with not only the existing organisational practices, but also the occupational and individual concerns of frontline officers (McCahill, 2002). Moreover, the study considers the implications of the Arab, Islamic and specifically Saudi culture, social norms, values and political environment for police responses to Internet fraud.

An interpretive approach was adopted, employing a single case study strategy, which utilised two methods, i.e. participant observation and semi-structured interviews, to collect the required data. The observational data was generated from seven police departments that are directly involved in the policing of Internet fraud in Riyadh. Interviews were conducted with 41 participants, including representatives of both the managerial and operational levels at the units targeted in the observational work, officers from supporting departments and officers with key roles in planning, controlling and supervising the implementation of police policies and strategies in relation to Internet fraud, at both national and local levels.

The findings revealed that the only way in which Saudi control strategies in response to cybercrime can be aligned with those followed by Western authorities is in relation to the state's 'expressive gestures' (Garland, 1996, 2001). In this regard, evidence demonstrated that the legal and organisational innovations introduced by the Saudi state, ostensibly to address informational crimes, had serious limitations in achieving their declared purposes and were perceived by police participants as intended only to create and sustain a favourable global image. In contrast, the study failed to find a clear and wide application of plural policing of Internet fraud, which is characterised by networks of calculation through deploying instrumental ordering practices and risk management technologies. In addition to the limited relevance in an autocratic society such as Saudi Arabia of the ideological, socio-economic and political conditions that facilitated the emergence of the notion of plural policing in Western societies, the Saudi police organisation also appeared unready to engage in networked policing of Internet fraud.

Moreover, it was shown how the policing response to Internet fraud was shaped by specific moral principles and cultural values. The findings of this thesis emphasise not only the persistent influence of ‘old’ cultural traditions and moral principles on officers’ perception of risk in Internet fraud and, consequently, their decision to respond to incidents brought to their attention, but also how police commitment to these cultural and religious values can place limits on the ability of technological systems to facilitate preventive policing of online fraudulent activities. Based on these findings, it is argued that policing of Internet fraud in Saudi Arabia, and the extent to which it aligns with the principles of crime control in late modernity, can only be understood by examining and analysing how new policing modes and cultural traditions merge and integrate to shape police response to such a novel criminal phenomenon as Internet fraud.

Acknowledgements

As this chapter of my life comes to an end I praise Allah the Almighty for giving me the strength and perseverance I needed to accomplish this project. Thank you Lord for all the blessings you have bestowed upon me.

Initially, I would like to thank Professor David Wall and Professor Majid Yar for their kind acceptance to examine this thesis.

There are a number of people whose guidance, motivation, expertise and love made the completion of this research possible, and therefore expression of gratitude is due to each and every one of them.

First, I am deeply grateful to my parents for their support and prayers, which enlightened my way throughout this work.

I would like to express my deepest gratitude to my supervisor, Dr. Michael McCahill, for his enthusiastic supervision, insightful guidance and constructive criticism. His intellectual and practical support during all phases of this research, as well as his sincere endeavour to help me improve the quality of my work, are all highly appreciated. A good share of any strengths in my thesis can be traced to his influence. I should also acknowledge the support of Dr. Adam Calverley, who was my second supervisor during the last two years of my course.

My thanks extend to the Department of Social Sciences at the University of Hull for a truly friendly learning experience. I am especially grateful to the Head of the department, Professor Peter Young, and the secretaries for the excellent help I received throughout my PhD. The Graduate School's members of staff are also owed thanks for being handy and cooperative whenever they were needed.

A big thank you goes to all the many relatives, friends and colleagues who phoned me constantly to check on my well-being and to offer their support and best wishes. Their encouragement and caring words toward me and my family sustained me more than they know.

These acknowledgements would be incomplete without recognising the favour of King Fahad Security College in giving me the opportunity to continue my higher education, and also expressing a special note of gratitude to all the individuals who assisted with the fieldwork in Riyadh and were kind enough to share with me their experience and attitudes, which formed the core of this study.

Last but not least, I owe an enormous debt of gratitude to my beloved wife, Um Fahad, for her unwavering love, tireless caring, positive attitude and continuing encouragement. To her and to my lovely sons, Fahad, Naif and Nwaf, I say: thank you very much for picking me up when I was disheartened and for helping me to end my PhD journey successfully. I will eternally be thankful for the sacrifices each of you has made to make my dreams come true, and I will cherish the memories I had with you in the UK forever.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ACPO	Association of Chief Police Officers
ACPT	Australian Consumer Protection Taskforce
AHTCC	Australian Hi-tech Crime Centre
ARPA	Advanced Research Project Agency
ATM	Automated Teller Machine
AusCERT	Australia’s Computer Emergency Response Team
CA	Crime Analysis
CC	Consultative Council
CFR	Case Final Reports
CIPP	Commission of Investigation and Public Prosecution
CITC	Communications and Information Technology Commission
CM	Crime Mapping
DDI	Department of Detection and Intelligence
DFE	Department of Forensic Evidence
DFE/CCU	Department of Forensic Evidence’s Computer Crime Unit
DPS	Directorate of Public Security
DPS/DPD	DPS’s Department of Planning and Development
DT	Department of Training
FBI	Federal Bureau of Investigation
GCC	Gulf Cooperation Council
GDD	General Detective Directorate
GDD/CU	General Detective Directorate’s Cyberterrorism Unit
IC3	Internet Crime Complaint Centre
ICT	Information and Communications Technology
ICU	Informational Crime Unit
IP	Internet Protocol
ISPs	Internet Service Providers
IWF	Internet Watch Foundation
KACST	King Abdulaziz City for Science and Technology
KFSC	King Fahad Security College
KSA	Kingdom of Saudi Arabia
MCIT	Ministry of Communications and Information Technology

MDTs	Mobile Data Terminals
MoUs	Memoranda of Understanding
NCITP	National Communications and Information Technology Plan
NIC	National Information Centre
NW3C	National White Collar Crime Centre
NYECTF	New York Electronic Crimes Task Force
PCeU	Police Central e-crime Unit
POSs	Points of Sale
RP	Riyadh Police
SAMA	Saudi Arabian Monetary Agency
SCOT	Social Construction of Technology
SCUs	Specialist Cybercrime Units
TIA	Terrorism (originally ‘Total’) Information Awareness
WSIS	World Summit on Information Society
WTO	World Trade Organisation

Chapter One

Background and Overview of the Thesis

Chapter One: Background and Overview of the Thesis

1.1 Introduction

Historical evidence reveals that there have always been links between crime and technology and that ostensibly beneficial technological advances are often accompanied by the possibility of harm (Wall, 2008). In his analysis of the Victorian electric telegraph, Standage (1998: 199, quoted in Wall, 2008: 50) observed broadly that 'given a new invention, there will always be some people who see only its potential to do good, while others see new opportunities to commit crime or make money'. Standage suggests that we can expect exactly the same reactions to whatever new inventions appear in the present era of accelerating changes in information and telecommunications technologies. Whilst the innovations of the information age have brought tremendous advantages for human well-being, they have also given rise to new opportunities for criminals.

Fraudsters are argued to have always been among the quickest criminals to respond to, and take advantage of, new technologies (Wall, 2008; Yar, 2006). Fraudulent activities are rapidly evolving in step with technological developments. As they evolve they create new challenges for law enforcement. Various forms of fraud are proliferating rapidly in online environments. As one commentator puts it, the Internet 'can be viewed as a breeding ground for fraud' (Fried, 2001: 1). There has been a major transformation in the ways in which money is owned, stored and moved, as a result of which not only are we increasingly moving towards a cashless economy but opportunities are opened up to new, profitable low-risk criminal activities, particularly fraud (Wall, 2008). Crime today, as in the past, still tends to follow opportunity (Grabosky and Smith, 1998), but those opportunities have changed in scope. This has led Albanese (2007) to propose that in the same way that larceny characterised much of the twentieth century, fraud is likely to be the characteristic crime of the twenty-first century.

This risk is now becoming a source of concern in Saudi Arabia, where there has been a noticeable growth of Internet usage over the last decade or so. According to the Communications and Information Technology Commission (CITC) (2010: 24), the number of Internet users reached 11.4 million, representing approximately 41% of the population of the Kingdom of Saudi Arabia (KSA), by the beginning of 2010, compared with just 200,000 in 2000. Gazzaz (2006) reported use of users of the Internet in homes, workplaces, educational institutions and Internet cafes across the country. His survey findings are supported by Sait et al. (2007), who found that, despite the relative novelty of the Internet in Saudi Arabia, it is penetrating many segments of the Saudi population. Respondents to Sait et al.'s (2007) research admitted spending a considerable amount of time on Internet activities. This tremendous growth in Internet usage in Saudi society has been attributed to the impetus by government towards e-commerce and e-government, which are important catalysts for individual and organisational adoption of IT (Al-Gahtani 2004). For instance, the CITC's (2010: 23) Annual Report indicates that the Saudi government has invested heavily in the expansion of the communications infrastructure, enabling, inter alia, broadband subscriptions to increase exponentially from 64,000 in 2005 to over 4.4 million connections by the end of 2010. Al-Gahtani (2004) forecasted that such factors would further enhance the growth of Internet use in the Kingdom of Saudi Arabia.

The increasing spread of the Internet throughout Saudi society, as highlighted above, poses potential challenges of cybercrime and misuse of the Internet. As the use of information and communications technology (ICT) becomes more widespread, the potential increases for cybercrime generally, and particularly Internet fraud, so that large numbers of Saudis will be vulnerable to various forms of fraudulent activity from this source. The absence of official figures about the incidence of Internet fraud, due to the restrictions placed on publication of crime statistics, does not obscure the fact that responding to this type of crime has become an aspect of the Saudi police activity. This issue has been highlighted frequently in the Saudi press. However, the policing of Internet fraud, especially in the context of the public police, has not yet been the subject of systematic academic research. While the lack of scholarly attempts to investigate how Internet fraud is policed seems to be linked to the sensitive nature of such topics in the Saudi context, which makes gaining access to police settings relatively difficult, it might also be attributed to a lack of interest in this area of research amongst the academic community. Regardless of the reasons behind this gap, this research is an attempt that is hoped to inspire further contributions towards the development of an adequate understanding of the policing of Internet fraud in Saudi Arabia.

Thus, in this chapter, a preliminary context for raising the main argument and rationale for this thesis is developed, starting with a statement of the research problem. The research objectives and questions are outlined, and the significance of undertaking this study highlighted. The chapter also introduces the Saudi context, before it ends with an overview of the structure of the thesis.

First, though, it is important to define Internet fraud to ensure a clear understanding of what this term means in the context of the current thesis.

1.2 What is Internet Fraud?

From a legal perspective, fraud is ‘a false representation by means of a statement or conduct made knowingly or recklessly in order to gain material advantage’ (Martin, 2003: 211). Perpetrators deprive victims of their financial or other resources by the use of misinformation and deception. The deception may concern the true value of something offered for sale, whether it is genuine, who actually owns it, and so on. It is also possible to be misled as to the identity of the other party to a transaction, as fraudsters may adopt a false identity, claiming to represent a legitimate organisation or to hold a particular occupational or professional status. Such false representation is the essential means by which victims are persuaded voluntarily to hand over money or property, in contrast to the coercion employed in the case of crimes of force (Yar, 2006).

Internet fraud shares with the traditional form of fraud the characteristic of deception (Grazioli and Jarvenpaa, 2003) used to inflict financial loss on innocent people. However, despite the general similarity between Internet fraud and traditional fraud, it is essentially changed by taking place in cyberspace (Cohen, 2002). The nature of the change varies according to the specific features of the Internet utilised. The Internet offers potential both for the efficient conduct of ‘traditional’ crimes and for the perpetration of totally new forms of criminality (Grabosky, 2000). Unlike traditional fraud, Internet fraud is characterised by impersonality, anonymity, instantaneity, ease of access and convenience (Wall, 2008; Yar, 2005, 2006).

Although a wide variety of terms are used to connote fraud committed with the aid of computing technology[1], there has been little attempt to define Internet fraud as a specific form of cybercrime (Algarni, 2011). Usually, Internet fraud is defined within the general category of cybercrime. At the 10th United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop focusing on issues of

[1] There are numerous terms including computer abuse, computer-related fraud, high-tech fraud, Internet fraud, online fraud, as well as the more recent cyber-fraud (see, for example, Wall, 2001; 2002; 2003; 2008; McQuade, 2006; Yar, 2006; Berg, 2008; Cukier and Levin, 2008).

crimes involving computer networks, a broad definition was formulated as ‘any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network’ (United Nations, 2000: 5). According to Thomas and Loader (2000: 3), cybercrimes are ‘computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks’. Among the few specific definitions of Internet fraud is that of the US Federal Bureau of Investigation (FBI) (2003: unpaginated), according to which Internet fraud is:

> any fraudulent scheme in which one or more components of the Internet, such as websites, chat rooms, and e-mail, play a significant role in offering non-existent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims’ funds, access devices, or other items of value to the control of the scheme’s perpetrators.

Consistent with the above definition, the legal dictionary of The Free Dictionary website by Farlex[2], defines Internet fraud as:

> a crime in which the perpetrator develops a scheme using one or more elements of the Internet to deprive a person of property or any interest, estate, or right by a false representation of a matter of fact, whether by providing misleading information or by concealment of information.

Based on such narrow definitions of Internet fraud, existing literature tends to group different types of online deception into six categories, as follows: online auction frauds, investment frauds, deceptive advertisement of products and services, advanced fee frauds, phishing and spoofing, and card-not-present payment frauds. Online auction frauds refer to various forms of deception carried out via auction websites, including failure to deliver the items purchased; misrepresentation of goods offered on the auction site; the practice of ‘shill bidding’, in which false bids are placed in order to drive up the price of the item, so as to increase the payment that can be extracted from legitimate bidders; and ‘fee stacking’, in which the seller adds on additional fees after completion of the auction and so raises the price beyond that agreed (Wall, 2008, cited in Algarni, 2011: 3). Investment frauds are typically exemplified by ‘work at home’ and ‘stock investment’ scams as well as share market manipulation (Yar, 2006). Deceptive advertisement of products and services includes scams that attract victims by falsely claiming huge price reductions (Hall, 2005), advertisement of goods or services that fail to materialise, or misrepresentation of product quality (Grabosky et al., 2001). Another form exploits grey markets created by differences in price across jurisdictions or by

[2] See http://legal-dictionary.thefreedictionary.com/Internet+fraud.

legal arbitrage, where items that are banned or restricted in one jurisdiction are purchased from jurisdictions where they are legal (Granovsky, 2002). Internet advanced fee frauds are an online version of the famous 419 Nigerian scams, involving persuading the victim to part with money with the promise of a substantial gain later (Edelson, 2003; Holt and Graves, 2007; King and Thomas, 2008). 'Phishing' for information via e-mails and 'spoofing' via bogus versions of legitimate financial services websites are usually used in combination to persuade victims to voluntarily reveal passwords and other personal data, which perpetrators employ to access their bank and credit card accounts (Yar, 2006). Finally, card-not-present payment frauds are payment frauds using genuine credit cards obtained fraudulently via identity theft, account take-over, or fake cards obtained by counterfeiting or cloning information (Wall, 2008).

It seems that the previous definitions and the typification built on them narrowly portray Internet fraud as a crime driven solely by financial motivations. One of the limitations of these definitions is that they fail to consider online deceptive activities intended for non-financial purposes. Moreover, such a conceptualisation of Internet fraud ignores the important role of cultural and social factors in shaping the deception process. In this regard, existing definitions take no account of how the nature of a society and its culture facilitates the use of specific instruments for luring victims.

To avoid such limitations, Internet fraud is defined in this research as any act of dishonesty or deception carried out with the use of the Internet. This can be undertaken to achieve financial or non-financial goals, and the dominant culture and social characteristics of a society can shape the process of deception through the employment of specific fraudulent instruments and the targeting of certain social groups. This broad concept is supposed to be suitable for the current research due to its exploratory nature, which investigates the studied phenomenon within the wider political, social, cultural and economic aspects of the Saudi context.

1.3 The Research Problem

Given a scenario in which almost nothing is known about the policing of Internet fraud in Saudi Arabia, there is a need to conduct detailed research to explore how this new criminal phenomenon is controlled in this part of the world. To that extent, it is important to highlight the key aspects of the policing response to Internet fraud, both at the macro (the state) and micro (police organisation) levels.

The existing criminological literature on the policing of Internet fraud remains dominated by perspectives and experiences emanating from liberal, democratic countries, particularly the United States of America, Canada, the United Kingdom and Australia. In these societies, the states' response to the predicament created by the emergence of online criminal activities, such as Internet fraud, and the limitations of criminal justice agencies, particularly the police, in handling this novel social problem appears to straddle the two contradictory aspects of crime control in late modernity highlighted by Western writers such as Garland (1996, 2001). On the one hand, governments have adopted a sovereign state approach that seeks to reassert the state's power to control cybercrime through, for example, the establishment of Specialist Cybercrime Units (SCUs). However, at the same time, there has been an attempt to adapt to the state's limitations in respect of cybercrime control, and thus develop pragmatic strategies which emphasise partnership and prevention through deploying instrumental practices and risk management technologies.

However, as Pakes (2004: 178) points out, while globalisation is seen by some as diminishing diversities and increasing similarities in criminal justice systems around the world, 'one can remain sure that as long as cultures, languages, public opinions and social discourses differ, so will criminal justice systems and the way they operate'. Other writers argue that administration of justice is, after all, an institutional function, and therefore it is bound to reflect the nature and culture of a society (Fairchild and Dammer, 2001). Such comments indicate that the policing of Internet fraud needs to be investigated in Saudi Arabia taking into consideration the political, social and cultural characteristics of this society. This investigation needs also to be guided by the assumption that 'Islamic society conceives of crime and punishment in different ways to the Western outlook and to make value judgments about what constitutes the priorities in law enforcement might neglect the differing values of Saudi people' (Al-Saud, 2000: 8). In this way, the study can contribute towards better understanding of how Internet fraud is policed in a non-Western society by examining the potential impacts of the specific idiosyncrasies of the Saudi context in terms of shaping both the perceptions and practice of those involved in the policing of Internet fraud.

Taking the ‘late-modern penal framework’ as a foundation, this thesis explores and analyses empirically the policing of Internet fraud in Riyadh, the capital city of Saudi Arabia, as a case study that would provide insights into how this social control function is undertaken in the Kingdom. In this regard, the research addresses two issues in the policing response to Internet fraud in the Saudi context. It investigates the Saudi state’s response to Internet fraud by examining the extent of both the sovereign approach and adaptation in this response. Moreover, it looks at the operational process of responding to Internet fraud in different police settings.

Although the thesis focuses specifically on Internet fraud, at the request of the researcher’s employers (see § 1.4), the research findings and implications are potentially relevant for the wider study of policing cybercrime in Saudi Arabia. This is because Internet fraud, as one type of cybercrime, has many features in common with other cybercrimes, and so the police response is expected to be similar. Moreover, most of the factors found to shape the police response to Internet fraud, such as availability of technical equipment, and training, and the factors that shape the crime itself are similarly applicable to the policing of cybercrime more generally.

1.4 The Research Motivation and Objectives

The present researcher’s interest in the policing of Internet fraud has emerged from a general interest in cybercrime per se which began during the course of his Master’s degree almost a decade ago. However, a particular impetus for this study has been the observations and insights gained by the researcher as a result of attending one of the series of events held annually at King Fahad Security College (KFSC)[3] under the title ‘the Security and Society Forum’. This was the 2005 symposium, which was entitled ‘Electronic Crimes: Features and Dimensions’. Working papers presented during this symposium covered a wide range of areas concerning the emergence of this type of crime in Saudi society, including legal, psychological, sociological, technical and security issues. However, within the discussions and presentations which took place during the symposium, there was a noticeable lack of attention to the Saudi policing response to electronic crimes. Having highlighted this issue in the report that the researcher submitted to his academic department at KFSC on the proceedings of the

[3] King Fahad Security College is an educational/military institution that is responsible for educating and training candidate officers recruited every year to join the internal security forces under the Ministry of Interior.

symposium, he was encouraged, due to his ‘Fraud and Counterfeiting’ teaching specialism, to make investigating the policing of Internet fraud the focus of the research to be undertaken in his forthcoming PhD scholarship. Given the lack of relevant literature in the Saudi context and the sensitivity of the area of policing in Saudi society, which was expected to make access a problematic issue, embarking on such a study did not seem to be an easy undertaking. However, the researcher accepted the challenge and began to prepare himself for what was expected to be a significant but ‘troublesome’ project.

While it is important for the researcher to clarify personal reasons that ‘push’ him/her to be involved in academic study (Van Maanen, 1978: 314), personal motivation is not enough to justify carrying out academic research. Research is subject to academic criteria that need to be met. Accordingly, it is necessary to define the objectives that the researcher aims to achieve by conducting the study.

The current research attempts to contribute to an understanding of how the policing of Internet fraud is implemented in Saudi Arabia. It is intended to be an exploratory study that covers a broad range of issues in relation to the policing response to Internet fraud in the Saudi context. Consequently, by drawing on the findings of field research focusing on the capital city of Riyadh, the current study seeks to assess the extent to which the Saudi state response to Internet fraud fits in with contemporary debates, in the Western-dominated literature, on cybercrime control within a late-modern penal framework. At the same time, the thesis aims to provide a detailed micro-sociological account of how the policing of Internet fraud is carried out in different police units within the case city. In this respect, the thesis intends to explore and analyse how this new aspect of policing activity fits in with not only the existing organisational practices, but also the occupational and individual concerns of frontline officers (McCahill, 2002). Moreover, being undertaken in a non-Western setting, the study endeavours to highlight the implications of the Arab, Islamic and specifically Saudi culture, social norms, values and political environment for police responses to Internet fraud.

That said, however, it is important to be clear that this study is oriented towards ‘research *of* policy’ rather than ‘research *for* policy’. Thus, the research does not attempt to make specific recommendations concerning, nor does it intend to specifically and explicitly shape, decisions relating to future policy direction in the policing of Internet fraud in Saudi Arabia.

1.5 The Research Questions

According to the research problem and the study objectives, the following questions have been formulated and will be addressed in this study:

To what extent does the Saudi state response to Internet fraud mirror the features highlighted in Western literature of ‘crime control in late modernity’ in terms of emphasising the ‘sovereign state’ approach, with its ‘expressive gestures’, while at the same time attempting to develop new pragmatic ‘adaptive’ strategies that rely on ‘partnership’ and ‘prevention’? In this respect, to what extent does the policing of Internet fraud in Saudi Arabia reflect the notion of ‘plural policing’ in terms of the array of private and public actors involved? How is Internet fraud policed in practice? For example, how does the policing of Internet fraud fit in with the existing organisational practices? How is police response to Internet fraud shaped by the organisational, occupational and individual concerns of operative officers? To what extent is the policing of Internet fraud influenced and shaped by the wider social norms and cultural values of Saudi society?

1.6 The Significance of the Study

The main significance of this study lies in it being the first empirical study to investigate the policing of Internet fraud in Saudi Arabia. The absence of detailed research on how cybercrimes such as Internet fraud are policed in the Saudi context affords an opportunity for the present thesis to make a valuable contribution to the body of knowledge in two significant ways. First, the findings of this research can give a background for other researchers and encourage more research in this area of policing in Saudi Arabia. This will help to build a better understanding of the governance of cybercrime from a criminological perspective. Indeed, there is a shortage of empirical work on this field even in Western literature. As Nhan (2008) has pointed out recently, much of the research on the control of cybercrime has been conducted by industry trade groups interested in commercial solutions and by the computer sciences that focus mainly on technologies, but attempts to subject the policing response to this type of criminal activity to empirical scrutiny by criminologists remain very limited. Thus, this empirical and analytical study will expand the limited literature.

Secondly, this study will contribute to some insight into how far Western perspectives on crime control are applicable in a different cultural context. The researcher believes that criminology should be made a discipline that can shed light on ‘global’ trends rather than just a Western science, and this requires that criminological theories and concepts be tested in non-Western settings. While the present research is a case study, its importance springs from the endeavour made herein to put the Saudi experience into the general theoretical literature on contemporary crime control strategies and practices. The application of Western policing approaches and crime control concepts in a different environment might provide a new perspective. This might be particularly important in an autocratic, religious and traditional society such as Saudi Arabia. Consequently, much of the value of this study will emerge from its attempts to emphasise the significance of considering the Saudi context with its social norms, cultural values and religious attitudes, which might have an impact on the policing response to Internet fraud. In fact, admitting the context specificity into the generality of the study of the policing of Internet fraud is enormously important, since this might lead to rethinking some of the theoretical assumptions in the literature on policing and crime control. The results of the present research may, therefore, be a useful reference for researchers interested in studying this and other areas of policing, particularly in traditional societies.

1.7 Theoretical Framework

This thesis utilises Garland’s (1996, 2001) theoretical analysis of crime control in late modernity as a framework to understand the current practices and policy in the Saudi response to Internet fraud. According to Garland, crime control strategies in late modernity are characterised by their emphasis on the ‘sovereign state’ approach, with its ‘expressive gestures’, while at the same time attempting to develop new pragmatic ‘adaptive’ strategies that rely on ‘partnership’ and ‘prevention’. Garland set out his thesis on crime control in late modern society to explain states’ response, mainly in the United States and the United Kingdom, to the criminological predicament created by the normality of high crime rates and the limited capabilities of the sovereign state’s criminal justice agencies. However, Garland’s thesis has enormous implications for theorising issues relating to crime and social control in contemporary societies, because it presents a powerful argument about the rise of a crime control complex that is characteristic of late modernity (Owen, 2007). The considerable influence that Garland's late-modern penal framework has had on literature discussing recent developments in crime control strategies in Western societies can be illustrated, for example, by Norris and McCahill's (2006) use of this theoretical framework to analyse the growth of surveillance technologies, such as CCTV, in the United Kingdom.

Although aspects of Garland's thesis are not sustainable in Saudi Arabia, where it may appear that there are no limits to the 'autocratic' state, his work provides a useful lens through which current Saudi practices in relation to the policing of Internet fraud may be viewed. By applying the 'late-modern penal framework' in the analysis of the policing of Internet fraud in the Saudi context, there will be an opportunity to identify both parallels and points of divergence between Garland's work and contemporary developments in the social control system in a non-Western society. Since Garland acknowledges that his 'general analysis...is not a substitute for more detailed case-studies' (2001: 21), the current research is intended to be one such study.

1.8 Outline of Methodology

The present study is an exploratory description based on qualitative methods. The paucity of information about the policing of Internet fraud and the inherent sensitivity of such a topic in the Saudi context, along with the research's concern with investigating the process of the policing response rather than its outcomes, are issues which require the adoption of a qualitative approach that can provide in-depth focus and generate detailed, complex data. The research data were collected by means of two instruments: observation and semi-structured interviews.

Participant observation was selected to be the first stage in the process of data collection. During the research period, over 630 hours was spent in such observation, representing around 90 hours carried out over 15 days in each of the seven research sites. These included five police stations (one from each of the five geographical areas of the city of Riyadh), the Department of Detection and Intelligence (DDI) and the Informational Crime Unit (ICU). The observation in these settings enabled the researcher to collect detailed data on how Saudi police officers perceived and went about policing Internet fraud; which technologies were used in the various police departments to deal with Internet fraud and how; whether a proactive policing approach was used, and if so, how; ways of surveillance and intelligence gathering; handling of evidence and preparation of proofs; and whether and to what extent the cultural, organisational, occupational and individual concerns of the Saudi police officers shape their response to Internet fraud. Observations also elicited insights into the nature and extent of cooperation taking place between officers within and between police departments. This was gained by scrutiny of relationships among officers, or between them and managers, how joint tasks were conducted, approaches to exchange of information and intelligence, and so on. Moreover, to learn how the police cooperated with outsider agencies, their interactions and communications with entities such as banks, the CITC, and the CIPC, in relation to the policing of Internet fraud were observed. In such cases, attention was paid to the purpose, mechanism and outcome of such interaction. Moreover, during the observational fieldwork the researcher was able to obtain and analyse secondary unpublished data, which included, for example, police annual crime statistics for the years 2006, 2007 and 2008, the organisational structures of some departments, as well as police case files of Internet fraud incidents processed by police stations.

A total of 41 semi-structured interviews, on the other hand, were conducted with three groups of officers[4]. The first are officers from departments that are directly involved in the policing of Internet fraud in Riyadh, i.e. the police stations, the DDI and the ICU. The second group of officers are from supporting departments, i.e. the Department of Forensic Evidence (DFE) and Department of Training (DT), whose responsibilities affect the previous departments' handling of Internet fraud. The third group are senior officers from the highest level of management both in the Directorate of Public Security (DPS) (the Saudi police organisation) and the Riyadh Police, who have a key role in planning, controlling and implementing crime control strategies and also supervise the performance of all the concerned departments in Riyadh.

The research design and methodology will be discussed in more detail in Chapter Three.

[4] The word 'officer' in the Saudi military and security forces system is exclusively used to describe anyone with a rank ranging between Lieutenant and General. These are called *thubbat*, the plural of *thabit*. Personnel with lower ranks (the rank-and-file officers) are called *afrad*, and they usually perform clerical duties and are not assigned investigative tasks. Thus, they were not included in the interview sample.

1.9 The Research Context

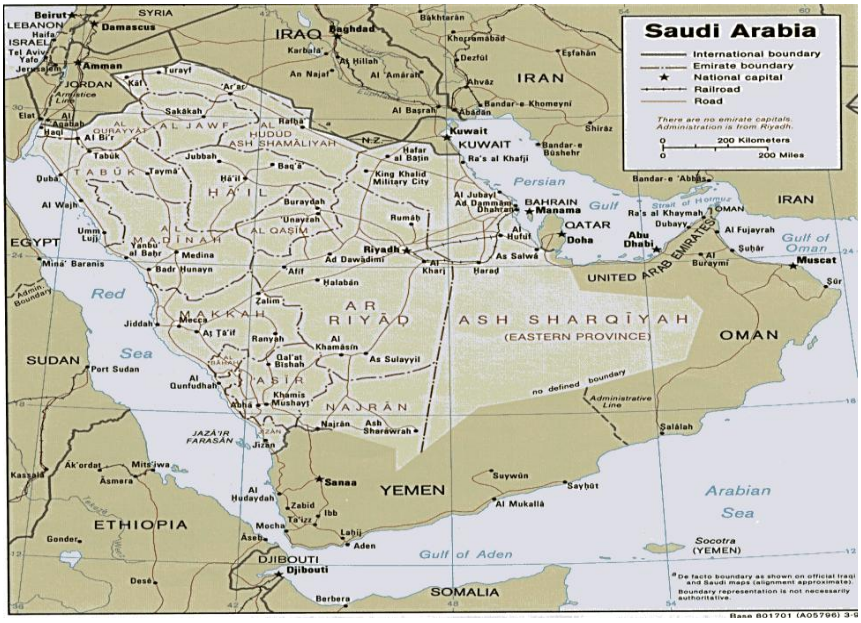
Given the importance of context for the current study, this section will present a brief introduction to Saudi Arabia. It will provide an overview of the country before it sheds more light on the Saudi policing system.

The Kingdom of Saudi Arabia[5], as it is officially known, is the product of battles and conquest of territories by the late King Abdulaziz Bin Abdulrahman Al-Saud, who formally proclaimed it in 1932, and from whom the country took its name. Before the formation of present day Saudi Arabia, ‘the Arabian Peninsula was politically unstable and in a state of chaos’ (Vasilliev, 2000: 50). A brief history of the political structure of the peninsula by Facey (1990) shows that it was pitifully poor and composed of separate emirates and warring tribes, with peace being a rare phenomenon. King Abdulaziz’s struggle to unify the kingdom began in 1902 with an attempt to restore the emirate of the house of Saud in Najd. The Al-Saud family has ruled the country ever since (see Rashid and Shaheen, 1987; Facey, 1990).

The Kingdom of Saudi Arabia occupies almost 80 per cent of the Arabian Peninsula, with an area of over 2,240,000 square kilometres (865,000 square miles) (Ministry of Planning, 1999). The total population of Saudi Arabia for the year 2009 was estimated at 25,370,000, including 6,380,000 non-Saudi nationals who work and reside in the kingdom (Ministry of Economy and Planning, 2010). Administratively, Saudi Arabia consists of 13 Administrative Provinces (*Mintaqah*). These are Riyadh (this province includes the capital city of Riyadh, where the study was conducted), Makkah, Al-Madinah, Al-Baha, Asir, Jazan, Najran, Al-Qasim, Hail, Tabuk, Al-Jawf, Ash Sharqiyah (the Eastern Province) and Al-Hudod Ash Shamaliyah (the Northern Border) (see Figure 1.1). These provinces are further divided into 178 municipalities.

[5] The Arabic pronunciation of the official name of Saudi Arabia is *Al-Mamlaka Al-Arabiya As-Saudiya*.

Figure 1.1 Administrative Provinces of the Kingdom of Saudi Arabia



The official and only religion of Saudi Arabia is Islam. Due to the fact that Saudi Arabia is regarded as the cradle of Islam and houses its two holy cities, Makkah and Al-Madinah, Islam is the main guide for the affairs of people and for the policies and functions of government (Al-Gheraibi, 1994; Wardak, 2005). The Qur'an (the holy book of Islam) and Sunnah (sayings and actions of the Prophet Mohammed) represent the constitution of the Kingdom. All political and legal action within the country is centred on various interpretations of *Shari'ah,* the Islamic Law. Arabic is the official language in Saudi Arabia and it exists in two forms: classical and colloquial. Classical Arabic is the language of the Qur'an and the means of formal communication, literary expression, poetry and oration.

The country has no political parties or elections; the monarch is the central institution of government, and he is the ultimate source of the state's judicial, executive and regulatory (legislative) powers (Al-Otaibi, 1995). Further, each province is ruled by an emir from the royal family. In 1993, the government established *majlis al shura*, the Consultative Council (CC). Members of the CC are selected, not elected, and they represent major professions in the country including writers, journalists, the armed forces, educationalists and the religious establishment. Initially, the CC acted as an advisory body to the Council of Ministers and it had no right of veto. However, in 2003, a royal decree expanded the duties of the members to include 'some' legislative functions (Kapiszewski, 2006).

King Abdulaziz and his successors have pursued a culturally oriented policy and maintained religion as the backbone of both the society and the state. Oil wealth enabled the development of business, health and education services. An elaborate welfare system was introduced, guaranteeing free health insurance and free education to Saudi citizens, especially to support people who did not benefit from business opportunities and social change (Al-Farsy, 2003; Kostiner, 1997; Vassiliev, 2000).

1.9.1 The Saudi Policing System

A number of writers (Alahmari, 1997; Alharthi, 1990; Alshalhoob, 2000; Alzahrani, 1999) trace the genesis of policing in the Arabian Peninsula to the Ottoman network of policing in the cities associated with pilgrimage in the Hejaz region: Makkah, Al-Madinah, Jeddah and Taif. These authorities were, however, independent from each other and unregulated, but were simply a tool for enforcing the will of the rulers. Elsewhere in the country, as Al-Shaygi (1992) indicates, the police role was performed by armed men (*Khweya*) associated to local governors (emirs) in cities, towns and villages, serving as their bodyguards and messengers.

As soon as King Abdulaziz assumed control of the Hejaz region in 1923, he brought the forces in the above mentioned cities under a centralised General Police Commission in Makkah. According to Fouad Hamza, a former royal advisor and Deputy Foreign Minister, policemen were few in number and of low educational attainment. Their activities were limited to investigation of major crimes, supervision of public morals and enforcement of traffic law. Planning, training, construction and facilities, and specialised units were all absent (Hamza, 1963).

In 1926, all the police departments that had been established by that time in the Kingdom were united under the central command of the General Police Commission located in Makkah and an order issued to specify their duties and responsibilities. Not only were new police departments established, in Al-Ahsaa, Abha, Najran and Jazan, but the responsibilities of the police were also expanded to cover activities such as fire fighting, immigration and passports, price control, weights and measures, organising road traffic and preserving public social order (Alahmari, 1997; Al-Harbi, 2008).

In 1950, the General Police Commission was reorganised as the Directorate of Public Security (DPS) and extended by establishing the Police Academy and Fire Department (Siraj and Addas, 1969). For a number of writers, this marked a turning point in the history of police development in Saudi Arabia, with specification of the organisational charts of the national headquarters, the duties and obligations of the police, methods of conducting criminal investigation, and the rights of accused individuals (Alahmari, 1997; Al-Harbi, 2008). The following year, when King Abdulaziz announced the birth of the country's first central administrative body, 'The Council of Ministers', he branded the Ministry of Interior as one of the most important and principal offices of the state, responsible for maintenance of law, order and security throughout the Kingdom; protecting citizens' lives, honour and possessions; safeguarding public and private rights; fighting crime; drawing policies for internal security; and ensuring that judgements of *Shari'ah* judges were executed (Al-Bishr, 2000).

However, as Cordesman and Obaid (2005) point out, although the foundations for the development of the police, justice and internal security organisations were laid down in the early years of the state's establishment, the capability of the 'young' Saudi state to maintain effective control in the whole country remained inadequate, due to lack of experience and shortage of income. For this reason, the Saudi state pursued social control by means of traditional mechanisms and informal methods enacted through the tribal control structure. Under this system, the head (*shaikh*) of the tribe was responsible for upholding and enforcing religious, moral and traditional norms and values. These control structures and mechanisms were made possible by the close acquaintance and geographical proximity of members of the social group (Al-Ghamidi, 1981; Al-Sharidah, 1999).

In the past fifty years, Saudi Arabia has experienced a process of rapid modernisation. The exploitation of oil has enabled the funding of ambitious programmes of infrastructural development (Al-Farsy, 2003) while large-scale urbanisation, modern lifestyles and wider work and education opportunities stimulated internal migration to the new modern cities (Long, 2003). Urban dwellers were said to constitute 88 percent of population by 2004 (Ministry of Economy and Planning, 2006: 2-8). Modern towns sprang up as industrial, administrative and cultural centres. As an illustration, the area of Riyadh expanded almost 15-fold between 1968 and 1997, from 110 square kilometres to 1,600 square kilometres, while its population rose from 160,000 to 2 million (Vasilliev, 2000: 459). Between 1997 and 2010, the number of inhabitants grew dramatically and reached a total of 5,254,560 (Central Department of Statistics and Information, 2010: unpaginated).

Under these circumstances, the government began to introduce measures to replace traditional methods of social control based on tribal norms with a strengthened system of centralised formal control (Al-Ghamidi, 1981, cited in Alhadar and McCahill, 2011: 317) with the aim of controlling anonymity and community mobilisation. Al-Shaygi (1992) and Rajehi (1981) report a rapid restructuring of the police to cope with the prevailing social demands and the necessity of specialisation. Major developments included the placing of the DPS under the direct supervision of the Ministry of Interior, in 1962, and the issuance, in 1964, of a Royal Decree specifying precisely the roles the police were expected to play. The decree describes three major police functions. First, the administrative function. This requires the police to: maintain public order; handle emergencies; control traffic; ensure order and people's safety during the pilgrimage and festivity seasons; guard government buildings and institutions; know the topography of the area under their control as well as people in that area; and prevent crime. Second, the judicial function. Here, duties include: reporting all encountered incidents to the concerned police station; pursuing and apprehending criminals and offenders; gathering information from the crime scene (for example, statements from witnesses) and waiting for the inspector who is required to complete the investigation; and appearing in the court to give testimony (Siraj-Addin, 1969: 8).

In the light of increasing political and social demands, since the 1960s, many moves to restructure the DPS have been made. Nevertheless, as Rajehi (1981) points out, the DPS has frequently been subject to piecemeal restructuring by expanding old departments or fragmenting them to create new divisions or subdivisions, or separating some departments from the DPS to create independent departments then reincorporating them into the structure of the mother directorate at a later stage (Rajehi, 1981). Facilities and equipment have been constantly modernised and updated at substantial cost (Cordesman and Obaid, 2005), the numbers of recruits have steadily increased and the total number of uniformed police force in Saudi Arabia had jumped from 929 men in 1932 to reach approximately 135,000 policemen in 2005 (see Siraj-Addin, 1969; Rajehi, 1981; Ministry of Economy and Planning, 2006). What have not changed, however, are the hierarchical structures and core police functions. On this point, Kurian (1989) notes that the Saudi police force is highly centralised; regulations and procedures are identical throughout the country, and the Ministry of Interior directs, controls and finances all forces.

Currently, the DPS is located in the central administrative capital, Riyadh, and headed by a General Director appointed by the King. Operational control of the DPS is formally delegated to this General Director, who in turn, delegates some of his authority to the respective police department directors in the thirteen Administrative Provinces around the country. There is a two-tier structure below that of each provincial police department, with police sub-departments in each municipality and police stations in the cities and rural areas within that municipality. Again, the director of the provincial police department retains overall control of all aspects of police in the province but directly delegates authority to deal with day-to-day policing activities to the directors of municipal sub-departments and the managers of police stations respectively. Governors of the Administrative Provinces, who are all related to the Royal family but accountable to the Ministry of Interior, exert considerable influence on the administration and practices of police departments in their provinces. The organisational structure of the DPS is, to a large extent, replicated at a provincial police department level.

One of the distinctive characteristics of the police profession in Saudi Arabia is that police officers or chiefs are not politically selected or elected, but rise to their position through rank and seniority. Part 4, Section 1, Article 23 of the Uniformed Officers' Code makes seniority the basic condition for promotion. The Code, moreover, treats every officer in the country in the same way, regardless of the force with which they work. For example, all uniformed, commissioned officers (2nd Lieutenant and up) of each rank have the same basic monthly salary, basic monthly living expenses, basic yearly clothing allowance, basic yearly housing allowance, basic 45 days vacation a year, and must spend the same amount of time in each rank before promotion. There are, however, some extra fringe benefits for special types of jobs. For instance, pilots are given extra for flying, and officers who teach in training institutions and those with a Master's or PhD degree in any field receive special pay.

In Saudi Arabia, no officer may be commissioned, promoted or dismissed except by Royal Decree. Candidates for officer positions in the Saudi police must be graduates from King Fahad Security College (the police college) in Riyadh or from other accredited colleges and universities inside or outside the country and have entered the police as commissioned officers. It is worth mentioning that as a strategy for preventing police officers from displaying divided loyalties, candidates for training in the police college (that is, who eventually carry the prestigious 'officer' rank) are usually drawn from different areas, families and tribes of the country. It should be noted here that officers (who are also known as *thubat*) constitute only one category of the police personnel in Saudi Arabia. The other category is made up from regular policemen, who are usually referred to as *afrad* and of a lower rank than officers. These policemen are usually given a few weeks pre-service training in military discipline, self defence, conducting patrols, handling fire arms and making arrests. In general, regular policemen were initially drawn from among the poorer and uneducated sections of society. Lately, however, the minimum entry requirement for candidates for the lower ranks in the police, as well as other internal security forces, is becoming increasingly higher, and recently recruits have been drawn from university graduates.

Finally, the DPS, discussed above, is not the only police force responsible for enforcing the law and maintaining order in the country. Rather, there are also a number of distinct paramilitary forces that have their own hierarchies and are connected to the Ministry of Interior. These are a) the General Detective Directorate[6], which is responsible for national security in general; b) Special Security Forces. This is a specially trained force to be deployed in times of emergencies and crises; c) Directorate of Border and Coast Guards; d) Installations Security Forces; e) Directorate of Immigration and Passports; f) Directorate of Civil Defence. Each of these directorates has provincial branches, as is the case with the DPS. There is yet another kind of police agency in Saudi Arabia, the Commission for the Propagation of Virtue and the Prevention of Vice, better known locally as the *Alhai'a*. The *Alhai'a* is maintained to ensure the strict assertion of Islamic code of conduct throughout the nation.

1.10 Structure of the Thesis

Following from this introductory chapter, which has provided a background rationale for the research and set out its objectives, the thesis contains a further six chapters.

Chapter Two establishes the theoretical framework within which the findings of the research are discussed and analysed. Following an assessment of the implications of the advances in information and telecommunications technology associated with the information revolution for criminal activities, particularly those related to fraud and deception, the chapter moves on to situate the discussion of the policing of Internet fraud within the broader theoretical debates on crime control in late modern societies. In

[6] The General Detective Directorate is known locally as *Mabahith*.

doing so, the chapter examines critically some of the ideas found in this literature, mainly the notions of ‘plural’ and ‘risk-based’ policing, and evaluates their relevance for thinking about controlling Internet fraud by drawing on relevant empirical research. Attention in this chapter is particularly focused on highlighting and discussing the salience and limitations of theories and concepts developed in Western societies for analysing the policing of Internet fraud in Saudi Arabia, given the distinctive features of the Saudi political, cultural and social milieu.

Following the establishment of a theoretical framework in the second chapter, Chapter Three addresses the methodological issues involved in conducting an in-depth empirical investigation into the Saudi policing response to Internet fraud. Ontological and epistemological assumptions underpinning the research are explicated, and it is shown how this thinking was reflected in the development and execution of an inductive, qualitative case-study strategy encompassing participant observation and semi-structured interviewing techniques. The chapter also explains the data analysis procedures. Finally, access arrangements, ethical considerations and criteria for establishing the quality of the research are highlighted.

The research findings are interpreted thematically in three chapters, beginning in Chapter Four with an analysis of the Saudi state response to Internet fraud in the light of contemporary debates on crime control strategies that seek to assert and demonstrate state power while also adopting pragmatically to an erosion of that power. Within this framework, the chapter discusses the nature and prevalence of Internet fraud crimes in Saudi Arabia, critically analyses the relevant legislation, and considers the recently established Information Crime Unit (ICU) before drawing conclusions on the adaptive strategies employed by the Saudi authorities in response to this category of crime.

Chapters Five and Six represent a shift in focus, from the macro-level of state control strategies to the micro-level organisational and operational contexts of policing Internet fraud in Riyadh. Chapter Five begins by presenting the perceptions amongst members of the ICU and other participating police officers of its role in the policing of Internet fraud and its capability to fulfil its stated purpose. The chapter then addresses a variety of organisational issues emerging from the data collected in police stations and the Department of Detection and Intelligence (DDI), through which the police service on Internet fraud is predominantly delivered. These include organisational conflict, the extent to which an intelligence-led approach to policing Internet fraud is adopted, and the provision of specialist training in relation to handling online fraudulent activity.

The themes raised in Chapter Five are closely intertwined with those of Chapter Six, in which the day-to-day practices of Riyadh police with regard to Internet fraud are scrutinised. The chapter commences by examining police officers' orientation towards policing Internet fraud through providing a typology of officers in terms of their acceptance of both the organisational goals and the technological means of achieving these goals in the fight against Internet fraud activity. The chapter, then, focuses on police prioritisation of Internet fraud incidents, before it moves on to analyse the detection of incidents of this type of crime. The chapter also looks at the human mediation of technological systems and its impact on effecting a proactive policing of Internet fraud, and it concludes by shedding light on the issue of policing the police.

The various themes and arguments of the thesis are brought together in the concluding Chapter Seven, in which the theoretical implications of the research findings are explored. Attention is drawn to the contribution of the thesis in enriching and extending debate on Internet crime control in late modernity, showing how its insights on the impact of political, cultural and social context both highlight and address limitations in the existing Western-dominated discourses and offering new directions for future research.

Chapter Two

Crime Control in Late Modernity and the Policing of Internet Fraud

Chapter Two: Crime Control in Late Modernity and the Policing of Internet Fraud

2.1 Introduction

The policing of Internet fraud, and cybercrime more generally, has become the subject of a fairly substantial body of literature in recent years as attempts are increasingly made by researchers to explore and analyse this area of policing and its dimensions. Therefore, various perspectives and debates have emerged in an endeavour to understand this phenomenon, especially given the significant impact that Internet fraud is argued to have on e-commerce worldwide. However, most of the existing literature on the policing of Internet fraud is introduced by Western writers who tend to discuss the topic in relation to Western-based theoretical perspectives on policing and social control. Moreover, the vast majority of research on cybercrime, including Internet fraud, continues to be conducted in Western countries (particularly the US) and discussed within their wider social and cultural contexts and policing systems. When it comes to non-Western nations, such as Saudi Arabia, it appears that academic writing on this issue hardly exists. This might be attributed to researchers' inability to undertake such research due to the complexities involved, or perhaps it is because there is no real interest in studying the subject. The current thesis attempts to fill this lacuna in literature by exploring the policing of Internet fraud in Riyadh as a case study of a non-Western context.

Referring to theoretical and existing literature in Western countries may assist in understanding and analysing the dynamics of policing Internet fraud in non-Western nations, such as Saudi Arabia. Accordingly, although the policing of Internet fraud in Saudi Arabia may not be carried out in exactly the same way as in Western countries, the main themes of the literature will be identified and discussed in the present chapter in order to provide a basis for examining the state and its police's response to Internet fraud in Saudi Arabia and highlight to what extent it is consistent with the existing theoretical literature. In this regard, the importance of considering differences in cultural values and social sentiment in both understanding and analysing the policing of Internet fraud will be emphasised. Policing is very much shaped by officers' cultural, occupational and individual concerns (Manning, 1988), but these vary from one society to another and are influenced by the wider culture and social characteristics of a nation.

To achieve its aims, the present chapter begins by highlighting the advances in information and telecommunications technology that have taken place in the information revolution and exploring the impact of these developments upon criminal activities, especially those related to fraud and deception. From this point, the chapter moves on to situate the discussion of the policing of Internet fraud within the current theoretical debates on crime control in late modern societies. An attempt will be made to look critically at some of the ideas found in this literature and their relevance for thinking about controlling Internet fraud by drawing on relevant empirical research. Some important questions on the relevance of theories and concepts developed in Western societies for analysing the policing of Internet fraud in Saudi Arabia are raised throughout the discussion.

2.2 The Information Revolution and Cybercrime

The term ‘information revolution’, according to Rogers (1986), has been used to describe socioeconomic systems that exhibit high employment of information-related occupations and the wide diffusion of information technologies. The impressive advances in information and telecommunications technology that have taken place in the information revolution stand among the most notable achievements in human history. These developments and their relentless penetration deeply influence almost all aspects of life; they are bringing about major changes in the spheres of business, work, consumption, leisure and politics (Castells, 2002). However, the pace of technological advance has accelerated dramatically in the past two decades, making it almost impossible to predict how information and telecommunications technologies might develop in future (Newman and Clarke 2003).

As May (2002) points out, it is often argued that new information and communication technologies are best represented by the Internet, which is the most obvious embodiment of the concept of computers-as-communication. Ample documentary evidence records how the Internet and its associated information technologies developed from its military origins to its subsequent use for educational, commercial and, eventually, social purposes (Castells, 1997, 2000; Jordan, 1999; Bell, 2001; Webster, 2002; Rheingold, 1994)[7]. The main reason for the rapid spread of the Internet as a communication medium is the facility it affords users to send and receive, retrieve and store messages and information or data, and gain access to mass media entertainment content (Lin, 1998). In other words, the Internet is an intermediate channel that can be utilised for achieving interpersonal, organisational and mass communication purposes. In the past three decades, the Internet has spread to become a fact of life for people around the world, particularly those living in the Western industrialised countries. The Internet is perceived as part of the globalisation process that is widely thought to be replacing former realities and certainties, giving use to new opportunities and problems associated with living in an increasingly connected world (Yar, 2006).

Sandywell (2010: 42) argues that with the advent of new digital information technologies, such as MP3 players, iPod and multimedia cellular phones, 'we are increasingly moving into an era of ubiquitous, mobile, distributed multimedia information appliances that "wire" individuals to distant and anonymous networks (exemplified by the availability of free software such as Skype and Linux and the impact of "cloud computing" organised by such major players as Google and Microsoft)'. Sandywell goes on to observe that 'with the coming of digital communication networks we not only witness the creation of ubiquitous multimedia but also experience an explosion of online criminality' (2010: 42). Therefore, for Sandywell, the mutation of analogue to digital forms of deviance and crime on a global scale is closely associated with the transition from the analogue to the digital era, which has corresponded with, and to a certain extent facilitated, the development of a truly globalised world of corporate capitalism. In sociological terms, cybercrime as a social phenomenon presupposes the 'distributed universe of information infrastructures as its fundamental technical and material condition' (Sandywell, 2010: 42).

At this point, it would be as well, before progressing further, to clarify what we mean by cybercrime. In order to do so, it is necessary not only to identify its key features, but also to acknowledge some of the emergent characteristics of this recent

[7] The term 'Internet' is shorthand for 'Interconnecting Networks' (Klopfenstein, 2002). A key event in the evolution of computers-as-communication was the establishment of the Advanced Research Project Agency (ARPA) in the U.S. Department of Defence in the early 1960s, in response to the Soviet Union's technological success in orbiting Sputnik (Rogers, 2002). Rogers revealed that ARPA invested millions of dollars in the advancement of computer science, an ARPA programme managed by Licklider and then Taylor, who saw this responsibility as an opportunity to implement their conception of computers as tools for communication.

criminal phenomenon. Before attempting such a description, however, it would be useful to consider first the origins of the term ‘cybercrime’ with reference to the metaphorical notion of ‘cyberspace’. According to Wall (2008: 10), the term ‘cyberspace’ is a ‘descriptor of the mentally constructed virtual environment within which networked computer activity takes place’. For Sandywell (2010: 43), cyberspace can be defined as ‘the virtual topography created by the Internet as a system of interactive, multimedia websites’. Based on a perception of cyberspace as both a concept and a force of social reconfiguration and personal experience, Sandywell conceptualises the Internet in terms of its ability to constitute new modes of production, appropriation and transnational connectivity. This falls in line with Terranova’s (2004: 53-4) argument that:

> The Internet, in fact, is not just a global computer network, but a network of networks, the actualisation of a set of design principles entailing the interoperability of heterogeneous information systems. Not only, that is, is there no central control of the Internet (although there are many control centres), but the whole space of communication has been designed and conceived in terms of dynamic and variable relations between different communication networks.

Even viewing the Internet in purely technical terms, as a communication that transcends national borders, this ability to blur boundaries and defy control is perceived by many commentators as highly anarchic and fraught with risk (Jordan, 1998; Lyon, 1994; Sandywell, 2006).

The distinctive features of cybercrime

Wall (2008) points out that the term ‘cybercrime’ has come to symbolise insecurity and risk online and is used to broadly describe crimes that take place within cyberspace. However, as Wall himself acknowledges, there remains a lack of clarification as to what it is that is particularly ‘cyber’ about cybercrimes. Indeed, the question of the ‘newness’ of criminal activities perpetrated via computer networks is a matter of controversy among criminologists. Some contend that cyber-crime is essentially little different from non-virtual crime, except for the exploitation of some new tools; what Grabosky (2001) characterises as ‘old wine in new bottles’. In other words, cyber-crime is seen as nothing more than the migration of ‘real-world’ crimes into cyberspace (Brenner, 2007: 13). There are those, however, who are convinced that it represents a new form of crime that differs fundamentally from earlier kinds of ‘real world’ crimes (Capeller, 2001; Sandywell, 2010; Snyder, 2001; Wall, 2001, 2008; Yar, 2005, 2006). Among this latter group, many criminologists maintain that understanding this new criminal phenomenon requires new tools. Yar (2006) for example, questions the validity of established empirical assumptions and theoretical notions when applied to Internet crime, and argues that cybercrime faces criminologists and sociologists of deviance with challenges that necessitate considerable theoretical innovation.

However, instead of formulating a holistic theoretical approach towards understanding the phenomenon of what Sandywell (2010) called the ‘new criminality’, these scholars’ discussion of the novelty of cybercrimes has been focused upon the social-structural features of the environment in which such crimes occur. The result has been a concentration of attention on three distinct aspects of cybercrime which, nevertheless, constitute a starting point for understanding how the Internet has transformed fraudulent activity. The first focus of interest is on how the establishment of cyberspace in different ways transcends, expands, squeezes or shrinks the geographical and temporal constraints that govern interaction in the real world. Drawing on sociological discussion of globalisation as time-space compression (Harvey, 1989) and time-space distanciation (Giddens, 1990), commentators on the Internet argue that cyberspace enables almost instantaneous encounters and interactions between geographically dispersed participants, facilitating the constant evolution of different forms of association and exchanges (Shields, 1996). Yar (2006) highlights, from a criminological perspective, the implication of this for the ease with which those with criminal intent can reach their victims, unconstrained by physical distance. He suggests, moreover, that the Internet facilitates the targeting of individuals and property because with the aid of computer-mediated communication (CMC) a single individual can reach, interact with, and affect thousands of others simultaneously. From this perspective, the technology is seen as a power enhancer allowing individuals to perpetrate potentially enormous damage with few resources. As illustrations of this phenomenon, Yar cites the mass distribution of email ‘scams’ and dissemination of viruses.

Anonymity or ‘facelessness’ is the second characteristic of cybercrime. This feature is considered as ‘an effect of the deterritorialisation of social encounters and online relationships in cyberspace’ (Sandywell, 2010: 44). As has been pointed out by Poster (1990) and Turkle (1995), cyberspace interactions give individuals the capacity to reinvent themselves, adopting new virtual personae potentially far removed from their ‘real world’ identities. Sandywell (2010: 44) points out that ‘in media influenced by Web 2.0 platforms like MySpace, YouTube [and] Facebook, cyberspace identities are wholly constructed through the information that users provide....which can themselves be “mashed”, morphed and manipulated to create specific image profiles’. In criminological terms, this can be seen as a powerful means by which would-be offenders can commit crime, concealing their identity through disguise (Snyder, 2001; Joseph, 2003; Yar, 2006). Cyber-criminals can create a false identity for themselves, or steal the identity of an innocent person without their knowledge in order to perpetrate their offences; this is known as ‘identity theft’ (Smith, 2003; Cabinet Office, 2002; Gordon et al., 2004; Finch, 2007; Marron, 2008).

The third characteristic of cybercrime relates to the move from ‘linear’ and ‘hierarchical’ to ‘networked’ and ‘rhyzomatic’ relations between perpetrators and victims (Brenner, 2002; Sandywell, 2010, Wall, 2008). As Wall (2008) observes, the Internet has transformed the organisation of crime, enabling fraudulent activities to be organised in cyberspace through fragmented alliances of criminals instead of hierarchical structures. Brenner (2002: 1) explains this transition in criminal organisation online by pointing out that whereas the two hierarchical models of real-world criminal organisation, the gang style and the Mafia style, evolved largely in response to physical world opportunities and constraints, the essential absence of these factors in cyberspace enables criminal activity to be organised online in ‘transient, lateral and fluid’ forms. As a result of this development in criminal organisation, Wall (2008) highlights a concern that not only are Internet fraudsters likely to join each other online to conduct orchestrated fraud schemes that would yield higher returns, but they may also collaborate online with individuals from other offending groups, such as hackers, virus writers and spammers. These collaborations, according to Wall, will be situation-specific and maintained only for as long as it takes to achieve the purposes for which they came into existence.

However, although the above characterisation of criminal organisation in cyberspace seems feasible, there has been only scarce evidence to support the validity of this characterisation. In fact, apart from the findings presented from a small scale exploratory study of two Internet cracker newsgroups (Mann and Sutton, 1998), there has been to date no empirical research to substantiate the above-indicated predictions for online organised criminal activity. It should be noted, however, that the scarcity of evidence on the existence of the ‘swarming’ model of criminal organisation online (Brenner, 2002: 50) might be attributed to the difficulties associated with research on this phenomenon. For instance, access to criminal networks that operate on the Internet might be restricted by the ‘transient’ and ‘fluid’ (Brenner, 2002) nature of these networks, the anonymity of their members and the 'ephemeral relationships' (Wall, 2008: 41) between them. These features are expected to pose great challenges not only for any attempt by researchers to study online criminal organisations, but also, as Brenner (2002) suggests, for law enforcement agents' ability to infiltrate such groups and detect participants engaging in them.

Taken together, the characteristics of cybercrime discussed thus far demonstrate the profound impact of the recent advances in information and communication technology upon how social interactions, both licit and illicit, can take place. They also highlight the extent to which the Internet 'transforms the potential scope and scale of offending, inexorably altering the relationships between offenders and victims' (Yar, 2006: 11).

Internet fraud is often cited by cybercrime theorists as the obvious manifestation of the transformation introduced by the Internet on criminal activity in contemporary society. As Wall (2008) argues, the new communication medium has enabled fraud to be carried out more extensively, more efficiently, more quickly, with greater ease of concealment, and thus with greater difficulty of detection, not to mention with more profound impact in terms of the harm caused. The question now arises as to the potential for criminal justice systems, represented by police, to control this 'new' criminal phenomenon. Understanding of this issue requires considering the policing of Internet fraud in the context of contemporary debates on crime control in late modern Western societies. Therefore, an attempt will be made in what follows to map out a critical engagement with some of the ideas found in this literature and their relevance for thinking about the policing of fraud in the information age. This will include, first, looking at the argument about the limits of sovereign state-sponsored crime control and its relevance for the policing of Internet fraud. The second step will be to analyse the policing of Internet fraud in relation to the emerging notions of 'plurality' and 'risk paradigm', which have come to dominate the Western literature on contemporary policing.

2.3 The Limits of the Sovereign State

A number of theorists have noted the continuing influence of punitiveness in Western penal systems (Garland, 1996, 2001; Hallsworth, 2002; O'Malley,1992 ,1999; Pratt, 2000). For example, Garland (1996: 445) points out that 'the most visible and striking phenomenon of recent penal policy in Britain and the USA is the punitiveness which has come to characterise prominent aspects of government policy and political rhetoric'. Garland argues that while this display of punitiveness 'may pose as a symbol of strength', it should, nevertheless, be seen as evidence of 'weak authority and inadequate controls' (1996: 445). Indeed, despite acknowledging the increase in incarceration, Garland maintains that the sovereign state has reached its limits in terms of crime control and points to various indicators that the state is abdicating its responsibilities in this arena. He argues that the state is following a 'responsibilisation' strategy (O'Malley, 1992), looking to devolve crime control obligations to citizen groups or private agencies. Shearing (1992) similarly ascribes the rise of private security to an erosion of the state's position as the sole holder and user of coercive force, executed via the public police (Bittner, 1970). The state, then, by surrendering responsibility for security and devolving its tasks to the community and to private agencies, seems to recognise its limitations and work within them, a situation which suggests, from Garland's point of view, the erosion of:

> one of the foundational myths of modern societies: namely, the myth that the sovereign state is capable of providing security, law and order, and crime control within its territorial boundaries. This challenge to the state's law and order mythology is all the more effective, and all the more undeniable, because it occurs at a time when the wider notion of 'state sovereignty' is already under attack on a number of fronts (1996: 448).

Thus, for Garland, current crime control trends apparently represent yet another manifestation of the increasing impotence of the nation-state. Once-powerful, territorial sovereigns are finding it increasingly difficult to exert control over dynamics within their jurisdiction. Just as the free flow of capital undermines state economic policy, in the same way, rising crime rates and public cynicism diminish the capacity of the state to coercively dominate the maintenance of internal social control (Garland, 1996, 2001).

Garland goes on in his argument to point out that at the same time that government authorities recognise 'the need to withdraw their claim to be the primary and effective provider of security and crime control', they also fear the likely disastrous political consequences of such a move (2001: 110). This 'predicament' explains, in Garland's view, why alongside the adaptive strategies taken by governments, such as 'commercialisation of justice', 'rationalisation of justice' and a 'redistribution' of the responsibility for crime control (2001: 113), there has been a recurring attempt by politicians to evade its terms altogether. Such an attempt, according to Garland, is a politicised reaction that is manifested in forceful 'denials' of the predicament and reassertion of the power of sovereign command, but it also takes the form of an 'expressive' mode 'that is concerned not so much with controlling crime as with expressing the anger and outrage that crime provokes' (2001: 110). Crime control and criminal justice in the late modern period have, therefore, been shaped by 'a remarkably volatile and ambivalent pattern of policy development' (Garland, 1996: 449).

According to Johnson and Post (1996), nowhere is the incompetence of the sovereign state's crime control more obvious than in the case of regulating cyberspace. These writers have argued that the growth of cyber-society and the potential it offers for communications that transcend national borders are gradually eroding the ability of the state to exercise control over social activity, including crime. As they put it:

> The rise of the global computer network is destroying the link between geographical location and...the *power* of local governments to assert control over online behaviour... [and]...the *legitimacy* of the efforts of a local sovereign to enforce rules applicable to global phenomena (1996: 1370 emphasis in original).

Johnson and Post draw attention to the efforts of authorities to police and prevent illegal online activity through, for example, filtering mechanisms and the establishment of electronic barriers, but suggest that the effectiveness of such protective schemes is limited, since it is possible for perpetrators to reconfigure their connection, giving a false impression as to their location, and so evade such strategies.

The above thesis about the 'fluidity' of cyberspace and its implications in terms of reducing the sovereign state's authority over online criminal activity was advanced by Herbert (1999). He suggests that the notions of 'jurisdiction' and 'territoriality' in policing, which constitute the fundamental prerequisites for the exercise of state power over criminal behaviour, are eroding in cyberspace. Herbert's argument will be discussed in detail, but the importance of spatial/geographical perceptions in police work needs to be considered first. As Herbert himself has noted in an earlier work, police work has strong traditional connotations, starting from officers' front allocation to divisional districts, their assignment to a particular patrol 'beat' and the tailoring of means or methods of conducting patrol to the characteristics of the territory (Herbert, 1997). With reference to police work in inner cities, McCormick and Visano (1992) note the extent to which officers' time is consumed in patrolling the streets with the aim of controlling public space. Similarly, Huey (2002: 245) argues that 'police officers come to understand, and perhaps to identify with the neighbourhoods that they patrol, to get a feel for the space'.

Ericson and Haggerty (1997) describe a variety of other ways in which policing is governed by physical space and spatial arrangements and the role played by technical policing solutions in this respect, for example, the use by Canadian police organisations of computerised mapping systems that enable the further breakdown of geographical territories. By this means, they report, patrol officers can pinpoint a small target area and obtain details of all officially recorded criminal activities within its perimeter. They record the comment of an interviewed officer concerning the benefit to a community officer of being able to identify prime locations for prostitution or sexual assault, for example. Similarly, police video surveillance, as well as placing the public under an electronic gaze (Lyon, 1994) helps officers to relate risks to territories (Ericson and Haggerty, 1997).

As Herbert (1999) points out, the emphasis on territoriality and jurisdiction in policing is based on the premise that community and geography are intertwined. For Herbert, it is because of this jurisdictional assumption that individuals are locatable in space, that law enforcement agencies are granted authority over bounded, mappable communities. As he explains, ‘communities are defined as boundable and mappable entities, and law enforcement agencies are given jurisdiction for the bounded areas...[and] respond to individuals based upon their physical presence and actions within that bounded space’ (1999: 160). However, these demarcatable boundaries, as Herbert observes, are unlikely ‘to hold in the more fluid “space” of cyberspace’, which raises serious questions not only as to the way in which ‘virtual’ communities can be bounded and dealt with by law enforcement agencies, but also about defining responsibility for monitoring and policing wrongdoing in non-physical space (Herbert, 1999: 159-160). Echoing the perspectives of several other commentators (Branscomb, 1995; Johnson and Post, 1996; Meyerson, 1994), Herbert suggests that addressing these issues requires that the police and other state criminal justice systems engage in a re-conceptualisation of ‘territory’ in order to accommodate more abstract notions of space.

Herbert, in his attempt to demonstrate the erosion of state-sponsored crime control by the growth of telecommunication technologies, moves on from the issue of ‘jurisdiction’ to consider the notion of ‘territoriality’ in policing. In this regard, he points out that the police traditionally depend on their capacities to locate and contain individuals in physical space, using an exquisite technology that, as Bittner (1967: 706) has suggested, involves ‘special facilities and procedures of sleuthing’ and ‘builds upon those socially structured features of everyday life that render persons findable in the first place’. Having located suspect or undesirable individuals, they can then implement various control techniques so as to carry out an arrest or to restore order (Herbert, 1997).

However, as Herbert maintains, the conditions which render suspects findable in the physical world do not apply in cyberspace. According to Herbert, locating and identifying individuals in cyberspace can be far more difficult and complex than in the real world for a number of reasons, which were also highlighted by Reitinger (2000). First, because via the Internet crime can be committed at a distance, knowing the location of the victim gives no clue to the whereabouts of the offender. Second, in contrast to the real world, where a criminal almost always leaves some physical trace or means of identification, such as CCTV images or voice identification, cybercrime can easily be committed without any such traces being apparent. ‘An email, for example, purportedly from me could in reality be from anyone, as the recipient cannot hear my voice or see my signature’ (Reitinger, 2000: 137). Third, because crime on networks is based on communications, attempting to determine the identity of network criminals involves tracing the relevant communications to their source. However, ‘those who make use of anonymous remailers, or who construct pseudonyms, make detection [of the source of information] even more troublesome’ (Herbert, 1999: 161). Herbert concludes that as a result of the elusiveness of suspects, most online criminal activity proceeds undetected and unpunished.

The challenges facing the police in controlling online criminal behaviour are undeniable and immediately apparent. What is questionable, however, is the premise around which the above discussed claims about the reduced capacity of state-sponsored security efforts to regulate cybercrime were primarily built, i.e. the notion of ‘non-physicality’ of cyberspace. Does cyberspace represent an abstract form of space? Are online activities really free of traditional and terrestrial constraints? This issue was tackled by Huey (2002), who argues that characterisation of cyberspace as being fundamentally different or abstract and thus not a space where normal policing strategies are easily applied is inadequate. Huey tries to demonstrate that contrary to this perceived compatibility, cyberspace is an entity that is not completely devoid of links to traditional understandings of what constitutes the physical. To illustrate the physicality of cyberspace, he notes that all computer and network activities are bounded by space and time in the sense that they inevitably leave traces, for however short a period, on a piece of physical equipment, in some place, at some point in time:

> For example, data exists physically on hard drives, on diskettes, on tapes, on the cylinders of direct access storage devices (DASD), on paper, in the jottings and scribbling of users and creators, and as electronic impulses travelling across wires (Huey, 2002: 247).

For Huey, the existence of computer data in such physical forms, and the variety of ways in which they can be stored, increases rather than restricts the police's opportunities to investigate cybercrimes successfully, as evidence of such activities is usually easy both to discover and obtain from various sources, such as Internet Service Providers (ISPs), webmasters and so on. He also adds that while the anonymity of the Internet may enable criminals to disguise themselves, it also provides the police in many cases with a covert means of gathering evidence of criminal activity. Having disputed what he perceives as the 'overblown claim that cyberspace represents...an abstract form of the social' (2002: 243), Huey concludes by arguing that there is nothing to suggest that Internet criminal activity is problematic for public policing.

Aside from the debate on whether the capacity of criminal justice agencies is diminished in relation to controlling Internet crimes, we are reminded by Garland (2001: 133) that state authorities, driven by fear of potential political disastrous costs, are always inclined towards finding popular and expressive measures that are intended to 'demonstrate that the state is in control and is willing to use its powers to uphold "law and order" and to protect the law-abiding public'. Perhaps, it is in this context of persistent invocation of 'the deeply rooted and politically potent myth of the penal sovereign and its "law and order" powers' (Garland, 1996: 450), that the emerging phenomenon of Specialist Cybercrime Units (SCU) within police forces might be understood.

In the United Kingdom, for example, Jewkes and Yar (2008) report that several SCUs have been established with varying names and operational remits. At a national level, Jewkes (2010: 541) points out that the Metropolitan Police Service-based Police Central e-crime Unit (PCeU) is the latest policing cybercrime initiative, which was created in 2009 'in response to calls by the Association of Chief Police Officers (ACPO) for increasing capacity and capability within the police service to get to grips with modern forms of Internet crime'. Most local police forces, according to Jewkes (2010), also have at least one SCU, with some departments containing numerous SCUs with overlapping responsibilities. A similar trend was also observed in the United States by several writers, including McQuade (2006), Murff (2007) and Nhan (2008). The latter, for instance, suggests that almost every state has an electronic or cybercrimes department. Drawing on his research on the policing of cybercrimes in the state of California, Nhan reports that ‘industry lobbying and an increasing number of individual victims’ placed the police under great pressure to respond to ‘a growing demand for specialised policing services’ by the formation of a specialist electronic crime unit (2008: 65).

Wall (2008) appears cautious about the effectiveness of such units. He points out that while the establishment of SCUs constitutes a visible response that reflects the perceived threat of cybercrimes, it tends to marginalise the problem it sets out to solve. In other words, Wall seems to suggest that rather than being driven by real concern to tackle cybercrimes, the police, as ‘symbolic expressions of state sovereignty’ (2008: 160), might have formed SCUs only as, to use Garland’s (2001: 134) terms, ‘expressive...gestures intended to reassure a worried public and accord with commonsense, however poorly these gestures are adapted to dealing with the underlying problem’. In Wall’s view, restricting the policing of cybercrimes to these units ‘runs the risk of preventing the broader accumulation of organisational and professional experience across the force in dealing with the issue at hand’ (2008: 160). He contends that what determines the success of the organisational and occupational response to new public concerns is not just the existence of a relevant body of specialist expertise within a police force, but also the wider presence of knowledge about it amongst other officers.

Jewkes and Yar (2008: 581) highlight another issue when they warn that while the establishment of SCUs:

> may seem attractive to those who are alarmed by recent moral panics concerning the apparent expansion and increased visibility of cybercrimes,...expectations of these kinds of organisations can be widely ambitious and unrealistic, at least within the context of the finite resources within which they must operate.

Although it might be difficult to argue against the views proposed by these authors on the purpose and effectiveness of the SCUs, they fail, like Wall, to cite empirical evidence to justify their concerns on this issue, which seem to be based on merely theoretical assumptions. This might be attributed to the absence of a mature body of research that focuses on such units, due to their relatively recent engagement with the policing of cybercrimes. Without subjecting a SCU to empirical investigation, as the current study intends to do in relation to the Saudi Informational Crime Unit, ascertaining whether it is intended as an 'expressive gesture' by the state or a real response to an acknowledged cybercrime problem remains problematic.

Nevertheless, one could presume that the issue of symbolic demonstration of cyber-security is as highly significant in Saudi Arabia as in Western countries. The significance of displaying the state's power, capability and willingness to maintain law and order and protect the online environment in the Saudi context can be linked to the government's growing efforts to attract increased direct foreign investment into the Kingdom. The ability to attract growing quantities of foreign direct investment has over the past decade emerged as one of the major economic goals of the Saudi government. Recognising the vulnerability of the traditional reliance on oil revenues, Saudi Arabia is seeking to strengthen its economy and diversify the country's income stream by encouraging local and foreign private investors across a wide variety of sectors (Brimson and Al-Ghazzawi, 2010). According to the last two 5-year Development Plans, i.e. the Eighth (2005-2009) and Ninth (2010-2014) Development Plans, while every type of investment in all economic sectors is welcomed, the focus seems to be more on attracting a massive influx of foreign investment into areas that have the greatest linkages with the global economy. In this regard, information technology, finance and insurance services are considered to be investment areas of prime importance. Moreover, Saudi Arabia's accession to the World Trade Organisation (WTO), which was completed by the agreement with the United States in 2005, is hoped to open more prospects for larger foreign direct investment flows (Ministry of Economy and Planning, 2005, 2010).

However, for the growth of foreign direct investment, experience has shown that there needs to be a conducive business and investment climate, including an appropriate legal and regulatory framework and the rule of law (Hajela, 2005). As Hajela (2005) points out, preventative approaches to address cybercrime to ensure a secure information society with respect to ICT application services, such as electronic commerce and other e-services, are critical for building trust in information networks, which primarily and directly contributes to the broader commercial market. This issue has been highlighted in the recommendations of The Cyber Security Forum (2011: 21) which emphasise that 'confidence in cyber security measures will increase confidence in business success; this will increase productivity and inward investment'. The promotion of the country's investment environment as an investor-friendly one is therefore given special attention in the Saudi government's current initiatives and plans to place the Kingdom among the most competitive economies in the world. For instance, the Eighth Development Plan highlights Saudi policy-makers' awareness that traditional factors such as large markets and geographical locations are not enough to attract foreign investment, and that the country has to embrace institutional as well as legislative changes in order to provide assurance to potential investors about the protection of their capital and profits (Ministry of Economy and Planning, 2005). One would plausibly assume that such measures would include demonstrating the sovereign state's competence to ensure a secure environment for electronic commerce and other e-services, and to align the country with international best practices in this regard. Accordingly, the state's desire to construct and maintain a global image of cyber-security appears to be an important factor that cannot be underestimated or ignored when analysing any developments in the Saudi context in relation to the regulation of cybercrime.

The issue that needs to be considered, nevertheless, is Wall's (2000, 2003, 2008) argument that the scope, scale and structure of the Internet and the jurisdictional variations in different countries combine to ensure that the policing of Internet fraud and other forms of cybercrime outstrips the capacity of any single enforcement or regulatory body. Understanding of this situation, as Jewkes and Yar (2008) note, facilitates more realistic expectations of the role of the police, who themselves are becoming part of a more diverse assortment of bodies that undertake the monitoring, regulation, protection and enforcement related to cybercrime (Jewkes, 2010; Jewkes and Yar, 2008; Wall, 2000, 2003, 2008, Yar, 2008, 2010). As Jewkes and Yar (2008: 582) summarise it, 'just as the policing of terrestrial space has demanded a "joined-up approach" between individual citizens, private sector agencies and the police, so too has the policing of cybercrime become a pluralistic endeavour'.

Considered from the perspective of Garland (1996, 2001), these developments might be seen to exemplify a late-modern crime control situation in which the state is no longer the primary guarantor of security. As Garland points out, crime control strategies become diffused, as moves are made to 'embed controls in the fabric of normal interaction, rather than suspend them above it in the form of sovereign command' (1996: 451). Garland suggests that as a result of the reconfiguration of the field of crime control, a new criminological discourse (what he termed *the new criminologies of everyday life*) has emerged, which seeks to make a 'distinction between the *punishment of criminals*, which remains the business of the state...and the *control of crime*, which is increasingly deemed to be "beyond the state" in significant respects' (Garland, 2001: 120 emphasis in original).

With this suggestion we move now to the next part of our discussion, which attempts to situate the policing of Internet fraud within the ongoing debate amongst Western criminologists on the idea that contemporary crime control systems are witnessing a 'paradigm shift' towards 'pluralistic' and 'risk-based' strategies of policing.

2.4 Plural Policing of Internet Fraud

As noted above, the move to plural policing is portrayed by Garland (1996, 2001) as an outcome of a responsibilisation strategy adopted by Western states as an adaptive response to insecurities, control problems and risks accompanying 'late modernity', a concept he used to refer to the distinctive pattern of social, economic and cultural relations that emerged in America and Great Britain in the last third of the twentieth century. Garland (2001) identifies the relocation and redefining of crime control responsibilities as a set of pragmatic activities prompted by pressures and opportunities within or outside the crime control organisations, and appears to suggest that these trends were specific and unique to the late modern period. However, to characterise plural policing solely as a response to the late modern criminological predicament is misleading, as it fails to take account of the existence of forms of private policing or private participation in order maintenance and crime control in earlier periods. According to historical research (Zedner, 2006), the private security industry has been operating on a less visible and sizable scale for over a hundred years. Zedner points out that as early as the nineteenth century, large corporations often administered formal social control over their workers by employing in-house security staff, and she identifies other early antecedents of contemporary crime control, including thief-takers, prosecution associations and communal self-help. Thus, privatisation, in broader terms pluralisation, processes in Western contexts are not as novel as they may seem (Crawford, 2008).

However, as Crawford (2008) has argued, while plural policing has been around for some time, recent decades have witnessed a further shift in emphasis, with a greater focus on private participation, resulting in a breaking of the state monopoly and the development of a plural approach to policing, involving diverse bodies (Crawford, 2008). A prominent argument in the ongoing criminological debate about the extent and nature of contemporary changes in the delivery, practice and orientations of policing in Western societies claims a gradual erosion, or ‘hollowing out’ (Rhodes, 1994), of public police authorities’ hegemonic presence that may pose serious challenges to the condition of the police (McLaughlin and Murji, 1999). Reiner (1992: 779) characterises state crime control through the operation of a professional police organisation as a feature of the ‘modern’ period and questions its continued relevance in the ‘post-modern’ configuration of social structure and culture. Other authors have taken such arguments further by forecasting radical transformations in policing. Bayley and Shearing (1996: 585) go as far as to argue that democratic countries ‘have reached a watershed in the evolutions of their systems of crime control and law enforcement. Future generations will look back on our era as a time when one system of policing ended and another took its place’. They suggest the occurrence of a seismic upheaval in which the government monopoly of the crime control function has been dissolved:

> Policing has become a responsibility explicitly shared between governments and its citizens, sometimes mediated through commercial markets, sometimes arising spontaneously. Policing has become pluralised. Police are no longer the primary crime-deterrent presence in society; they have been supplanted by more numerous private providers of security. (Bayley and Shearing, 1996: 588)

Such a view resonates with wider debates about trends in policing. For example, scholars have commented on transnational pressures and changing global relations, with governments no longer having sole control over their territory but sharing surveillance and regulatory functions with (commercial) policing institutions operating within and across national borders (Johnston, 2000a, 2006; Sheptycki, 2002; Walker, 2003; Marenin, 2005). Writers on neoliberal ideology (O’Malley, 1997), post-Keynesian states (O’Malley and Palmer, 1996), new regulatory states (Braithwaite, 2000) and commodified policing (Loader, 1999) have drawn attention to the importation into public police organisations of business-like management techniques, including the devolution of functions through public-private partnerships and downsising government. In addition, authors have linked increased reliance on private security to fashions in information technology (Marx, 2005) and a move toward information-intensive preventative policing strategies, whereby police forces are increasingly sharing their duties with a range of specialist agencies outside state parameters (Ericson and Haggerty, 1997).

In a far more radical argument, however, Bayley and Shearing (1996, 2001) asserted that the growth of non-state security services extends beyond the increasing number of providers, to the emergence of entities that control their own policing. This phenomenon can be seen notably in the growing importance of private governments (Macaulay, 1986) with the power even to decide the concept of order to be upheld (Shearing, 1996, 2006). These trends imply a ‘pluralisation’ or ‘mulilateralisation’ process that markedly changes the privileged status of state police organisations (Bayley and Shearing, 2001).

Not surprisingly from the above perspective, transformation theorists refrain from assigning a privileged position to dominant auspices and/or security providers. Whilst not suggesting that public police forces have collapsed altogether, they do not take for granted that these forces should play the dominant role in social control. In this respect, Shearing (2001, 2005) and others (e.g. Johnston, 2006) have introduced a new morphology of security governance that stresses the emergence of polycentric or nodal networks (Johnston and Shearing, 2003) of security arrangements that may be public, private or amorphous. Within these networks, policing is neither unquestionably state led, nor is the state exclusively preoccupied with crime fighting and reactive law enforcement. Rather, it focuses also on preventative strategies while devolving to private organisations an increasing share of tasks that were once the sole preserve of the state’s police force. Shearing and his colleagues seem to promote the idea that this pluralised, networked mode of policing, notwithstanding the dangers of unconstrained expansion of private governance serving the interests of privileged (corporate) entities, could support the interests of less advantaged groups (Shearing and Wood, 2003). They suggest that state-led security provision is not well-placed to perform such a role because of a tendency toward bureaucracy, inefficiency and even oppression. Thus, they propose that locally designed and organised interventions might better serve communities’ needs for accountable and democratic policing.

The debate concerning the emergence of a fragmented and pluralised network of policing has parallels with Wall’s (2008) notion of an ‘Internet’s order-maintenance assemblage’. Influenced by Haggerty and Ericson’s (2000: 605) ‘surveillant assemblage’ thesis, Wall has proposed that cyberspace is currently policed by multiple policing actors. These include Internet users and user groups, online virtual environment managers and security, Internet Service Providers (ISPs), corporate organisations/corporate security organisations, nongovernment/non-police organisations, governmental non-police organisations and public police organisations (Wall, 2008: 167-177). These entities constitute the nodes of networked Internet governance because ‘new technologies have accelerated the growing tendency towards networking sources of security’ (Wall, 2008: 167). They are referred to as an assemblage because they ‘work as a functional entity across the network, but do not necessarily have any other unity’ (2008: 167). Within this assemblage, Wall distinguishes between ‘auspices’ and ‘providers’ of governance. According to him, entities that authorise governance are ‘auspices’ and entities that shape behaviours are ‘providers’.

Moreover, Wall’s emphasis on ‘order-maintenance’ in his model reflects his critical view of the debates over the policing of the Internet, in which he sees ‘a replication of the terrestrial reassurance policing debate (Crawford and Lister, 2004), though with a slight twist’ (Wall, 2008: 178). He contends that whereas the reassurance policing debate takes for granted that the police cannot win the fight against crime nor meet the public’s insatiable demand for a visible policing presence, when shifted into cyberspace, the debate still acknowledges the police’s incapacity, but nevertheless demands a more visible policing presence. From the viewpoint of Wall, ‘the rather conflicting messages emerging in the debate over policing the Internet’ are a consequence of ‘the replication of the bifurcation found in terrestrial policing between the maintenance of order and the enforcement of law’ (2008: 177-78). Separating the two, Wall claims, ‘helps to unravel the apparently rather tangled role of the public police’ (2008: 178).

According to a number of writers, nowhere can the emergence of a pluralised and differentiated patchwork of policing be observed more obviously than in the context of policing cyberspace criminal behaviour in general and Internet fraud in particular (Chung, 2008; Nhan, 2008; McKenzie, 2006; Wall, 2008; Yar, 2010). In the US, Nhan (2008: 65) reports that the plural policing of Internet fraud can be exemplified by the formation of task forces, which are ‘temporary ad hoc assemblies of separate security entities functioning to focus on a defined problem or activity’. For instance, the New York Electronic Crimes Task Force (NYECTF) consists of 50 law enforcement agencies, 200 corporations and 12 universities. Similarly, the High Tech Crimes Advisory Committee, whose formation was mandated by California Penal Code 13848.6, includes representatives from the computer software, banking, film, music and other industries. Nhan (2008: 68) indicates that ‘the law enforcement’s investigations-oriented security capital’ embedded in a task force ‘appeals to industries in need of digital forensics’. He also adds that the task force model serves to streamline jurisdictional issues in the cyber environment. Alongside these formally established plural policing entities, Nhan (2008) observes the existence of another form of security alliances that are formed through informal means, using personal referrals rather than structured arrangements.

In the Australian context, McKenzie (2006) has noted that in addition to police forces, Internet fraud is policed by a variety of private entities. For instance, McKenzie points out that Australia’s Computer Emergency Response Team (AusCERT), which was formed in 1993, is an independent subscription-based, not-for-profit team of 20 security professionals that offers incident management services, operates e-mail subscription service that warns users about network threats and provides an incident reporting scheme. Moreover, the CERT network permits AusCERT to act against fraudulent sites overseas and thereby mitigate the impact of incidents. According to McKenzie, AusCERT handled over 700 incidents in 2005, while the number of cases dealt with in 2006 rose to over 2000 (2006: 42). McKenzie also states that there has been a growth in small to mid-size firms offering forensic services, and that private fraud investigators are becoming more commonplace in the financial, IT, telecommunications and government sectors. According to McKenzie, partnership, including with private agencies, is emphasised by Australia’s Electronic Crime Strategy as one of the five focus areas that the police need to address. ‘Recognising an increasing array of providers of policing services’, the strategy is guided by a principle of ‘private sector leadership and self-regulation wherever possible, and practical regulation wherever necessary, complemented by effective and mutually beneficial partnerships with the police’ (McKenzie, 2006: 48).

In the UK’s Cybercrime Strategy, working closely with private sector partners is singled out as one of the most important ways in which the Government can respond effectively to financial crimes on the Internet (The Home Office, 2010). However, examples of plural policing of Internet fraud within the UK context appear only rarely in the available literature. In the work of a leading British cybercrime researcher such as Wall (2008), the ‘Internet’s order maintenance assemblage’ model, which he has proposed as a plural framework for policing Internet fraud and other cybercrimes, was exemplified mostly by initiatives from the US. The only example provided by Wall for the UK is the Internet Watch Foundation (IWF). The IWF, according to Wall, is a hybrid public/private arrangement that contributes towards cybercrime prevention and public awareness. Formed in December 1996 with the endorsement of the Metropolitan Police, Department of Trade and Industry (DTI), Home Office and associations of IPs, such as the Internet Service Providers Association and the London Internet Exchange, the IWF functions to bring any illegal activity reported to its hotline to the attention of ISPs, or, if serious enough and within the UK, it may pass on details of a website directly to the police (Wall, 2008). As Wall notes, 'the standing of the IWF has increased and it has become the quasi-public face of Internet regulation in the UK, more notably since its relaunch in 2000' (2008: 173).

In non-Western contexts, a study conducted by Chung (2008) in South Korea has shown that the monopoly of state-funded organisations over the policing of Internet fraud has been largely eroded by the increasing role of private actors in this arena. As Chung notes, Internet fraud is dealt with not only by the public police, but also by a variety of private and semi-private agencies, which participate in the same policing activities, though under the banner of 'private security' as 'it is unthinkable for the private sector to use the word "policing"' (2008: 146). Chung also indicates that while the concept of policing Internet fraud by the private sector in Korea is mainly associated with preventive IT security activities by financial institutions, such as banks, credit-card companies and stock companies, there is also a growing number of private agencies that have in-house investigative capabilities. Moreover, Chung argues that the rise of new forms of hybrid policing which blur the boundaries between public and private policing of Internet fraud is epitomised by the emergence of 'a very unique group called "CONCERT" which...was founded in June 2005 as an organisation of security power, merging public and private security for collective benefit' (2008: 149). Consisting predominantly of private companies related to Internet security, such as SamsungS DS, SK Telecom, LG CNS, KT, Naver, Daum, KTF, Shinhan Bank, SIEMENS. SK C&C, LG Telecom, Posco, Korea Amway, Dacom, Koscom, 'the CONCERT's major objective is to share information and to respond to any threatening attempts to penetrate the Korean telecommunication infrastructure' (Chung, 2008: 149). Chung (2008: 158) suggests that 'recently, private and public sectors of policing have realised that they have to cooperate with each other in response to increasing fraud incidents in cyberspace'.

In his 'Internet's order-maintenance assemblage' proposal, Wall (2008) argues that within the broader network of security that constitutes the policing of cyberspace, the public police role is comparatively minor, with other actors playing the larger role in policing and regulating Internet fraud and other online criminal activity. By outlining various challenges with regard to offending online, he suggests that 'the police are in fact fairly ill-equipped organisationally, occupationally and culturally to deal with it' (2008: 179). Nhan (2008: 24-25) provides a similar view as he argues that while the police are still distinguished as the sanctioned punitive body, power in the 'nodal governance of the Internet' is distributed to a 'shifting network of alliances' and no longer concentrated in the state.

However, in a society such as that of Saudi Arabia, which is characterised by the dominance of the state power and its central authority in people's life, the question that needs to be raised is to what extent the policing of Internet fraud in this society mirrors the 'plural policing' notion in terms of the array of public and private actors. The key point in pluralistic notions, such as Wall's (2008) 'Internet's order-maintenance assemblage', relates to the transformation in the field of security in Western contexts, from vertical hierarchical structures to horizontal networks. The formation of security networks and the adaptive strategies deployed by public institutions to adjust to networked governance need to be understood in the light of the democratic political structure and the capitalist economic process in Western societies. In these societies, the private sector has been allowed to exercise policing practices for commercial purposes as a requirement of capitalist ideology and a competitive market (Rose, 1993). Moreover, the pluralisation of the governance of security is bound up with the spread of neoliberal-inspired reforms that have sought to rearticulate the relationship between state, market and civil society (Crawford, 2008). As several writers have pointed out, neoliberal approaches to governance have led to growing separation of the functions of governance, such that while the state continues to retain the responsibility for establishing the norms of governance, the responsibility for implementing these norms and securing compliance with them is increasingly devolved to non-state auspices (Barry et al., 1996; Rose, 1996; Harvey, 2005). Thus, in accordance with these neoliberal strategies of 'rule-at-distance' (Rose and Miller, 1992) in order better to demarcate 'steering' functions from 'rowing' ones (Osborne and Gaebler, 1993), Western governments have employed privatisation policies to devolve some 'peripheral' security functions to the commercial sector, leaving 'core' functions in the hands of state police (Cope et al., 1995). Such privatisation is part of a much broader responsibilisation process that activates citizens and organisations to take responsibility for crime prevention and crime control (Garland, 1996, 2001). In the UK, for instance, 'where once citizens were told to "leave it to the professionals", they are now enlisted as "partners in crime prevention" in a new corporate approach [that aims] to encourage and entrench a diversification of policing functions at a local level' (Crawford, 2003a: 141).

The capitalist and neoliberal principles which have served as the basis for the developments toward plural policing in Western countries, however, have limited relevance in Saudi Arabia, where the state has sought to enhance its central role in the lives of all citizens by arrogating to itself the main responsibility for social welfare and service provision, including (as explicitly stated in Article 36 of the Kingdom's Basic Law of Governance[8]) ensuring the security of all citizens and residents of the country. So entrenched is the state's functional monopoly, in both thinking and practice, that even advocates of reform have stopped short of proposing transfer of policing functions to private sector agencies. Al-Harbi (2008), for example, accepted that some forms of plural policing, such as community policing, might be appropriate in Saudi Arabia, but he did not go as far as to suggest private sector involvement. This might be taken to reflect an implicit recognition that the state's monopoly over the performance of the policing function is jealously guarded, and any devolution of roles in this respect, which might appear to pose a challenge to the state's dominant power, is unlikely to win favour.

A further potential obstacle to the concept of plural policing as it has developed in Western societies can be seen in the history and demographic composition of the Kingdom. Before unification of the Kingdom, the territory now known as Saudi Arabia was occupied by rival tribes, competing for resources and in constant conflict. Stability was brought to the region by the uniting of these tribes under a single strong, central ruler, and under the banner of Islam. Nevertheless, Saudi society remains strongly tribal and it may be suggested that in such a context, the fragmentation and pluralisation of social control functions could be problematic. A potential danger exists that, if the gates were opened to the formation of private security organisations, as has happened in the West, the result might be the formation of ideological and tribal security groups which may not coexist easily with each other or with government entities. Such groups would be likely to recruit from their own limited pool, and might be tempted to operate in a manner favouring the interests of that group at the expense of others. Mackey (1987: 278) plausibly suggests that the danger of such factionalism is a key factor in the Saudi state's preference to retain a centralised model of policing:

[8] A full translation of the Saudi Basic Law of Governance is available at: http://www.saudinf.com/main/c541f.htm.

> Always cognisant of the divisiveness within its kingdom, the House of Saud from the beginning centralised control of the police. Consequently, municipalities neither hire nor command their own police forces. Every policeman who patrols the streets works directly for and is answerable to the Ministry of Interior.

Perhaps the only noticeable development since the above comments were made is the rise in recent years of private manned guarding services. The core business of the guarding companies is the controlling of mass private properties, such as shopping centres and leisure parks (see Alhadar and McCahill, 2011), and the protection of commercial bank branches (see De Jong, 2002), although their services have also extended to guarding the buildings of some government civil organisations. Nevertheless, the state's obsession with preventing the potential danger of factional power amassment remains implied not only in the fact that the private guards are both licensed and strictly supervised by the Ministry of Interior, but also in the restrictions imposed on their policing powers, in terms of not allowing them, for example, to use even non-lethal equipment such as batons and handcuffs.

Thus, it can be seen from the above that in Saudi Arabia, not only do the forces that have led to dispersal of government security responsibilities have less relevance, but there are ideological, political and social factors that render such developments problematic and, to many, undesirable. In addition to a marked reluctance to transfer power from government hands to non-government entities, there is a strongly centralised and hierarchical structure which limits the scope for devolution even within the police force itself. This is not to say that no form of plural policing of Internet fraud would be possible in Saudi Arabia, but it seems that the scope for such a development would be very limited compared with the functional and structural changes that have been witnessed in Western societies.

However, even in those societies where plural policing has emerged and has been discussed in criminological literature, writers have rarely addressed the relationship between public and private entities. Thus, many questions arise as to the relative power of different kinds of agency, the division of responsibilities between them, communication channels, cooperation mechanisms and the like. Whereas Garland (1996, 2001) has proclaimed a 'culture of control' based on personal reflections on the emergence of forms of private policing and involvement of private actors, nevertheless, he did not attempt to unravel the entanglement of the functions of state and non-state policing bodies. Exploring how public police officers and private security personnel operate together is important because it should throw light on the consequences of increased private security for the sovereignty of state police forces. A possible explanation for this omission is that Garland's discussion was purely theoretical; his comments were not based on any empirical investigation. Nonetheless, Garland does assert that at the same time as the devolution of crime-control responsibilities to non-state actors:

> the state agencies [...] take on a new set of co-ordinating and activating roles, which, in time, develop into new structures of support, funding, information exchange or co-operation. Where it works [...] the responsibilisation strategy leaves the centralised state machine more powerful than before, with an extended capacity for action and influence (Garland, 1996: 454).

Similarly, other writers have maintained that it would be naive to argue that state agencies are simply on a par with actors in the private sector (Stenson, 2005, cited in Coleman and McCahill, 2011: 88). As Crawford (2006) points out, state agencies still possess the ultimate power, and are advantaged in terms of access to resources and information, and their claims to legitimacy. In this situation, their role in the security network should not be underestimated (Stenson, 2005). As Crawford and Lister (2004: 426) have shown in relation to the British context, 'the reality, at the moment at least, is that the crime and disorder partnerships remain state-dominated institutions'. Thus, we should not be surprised to find, as will be suggested in the following subsection, that while 'security systems' introduced by private institutions to respond to Internet fraud may be driven by 'beyond-the-state' interests of loss prevention and commercial image, these systems 'can be easily and routinely co-opted for "traditional" policing' (McCahill, 2008: 216) of the same phenomenon.

2.4.1 Police Co-option of 'Non-sate' Policing Systems

As Coleman and McCahill (2011), citing Shearing and Stenning (1983), have argued, the strategic focus of private security systems tends to be on the objectives of 'private justice' and the prevention of loss, more than the apprehension and sanction of identified criminals. Noting the time and expense involved in pursuing offenders through the courts (Wakefield, 2005, cited in Coleman and McCahill, 2011: 78), they suggest that private agencies tend to prefer the more cost-effective strategy of anticipating and pre-empting offending. Moreover, when attacks on a private organisation's system do take place, these are likely to be dealt with 'internally' by private security arrangements rather than by criminal prosecution to avoid 'negative publicity' and future loss of revenue (Chung, 2008; Nhan, 2008; Wall, 2008; Jewkes and Yar, 2008). Credit card companies and banks, for instance, have independently operated fraud prevention measures, installing special monitoring software into their servers to detect any unusual events occurring to the accounts or credit cards of their customers (Chung, 2008). These institutions also use risk management computer programs to monitor customers' behaviour, such as excessive withdrawals of cash or excessive use of credit cards (McKenzie, 2006). Meanwhile, network infrastructure providers, fearful of any negative publicity that might affect their strategic position in the communications networks, employ a range of software solutions to reduce deceptive behaviour online (Wall, 2008). Most typical of these are robust security systems accompanied by sophisticated professional spam filters (Wall, 2008; Yar, 2006). In addition, corporate security firms provide a wide variety of goods and policing services that are aimed at 'the goal of protecting profits and minimising losses' from network fraudulent activities (Nhan and Huey, 2008: 77; see also Yar, 2010).

The 1990s witnessed an increasing role of the public police in providing information to a range of external bodies, for the purpose of monitoring compliance with laws and regulations (Ericson and Haggerty, 1997). However, as Crawford (2003a, cited in Coleman and McCahill, 2011: 79) has pointed out, knowledge exchange between plural policing bodies is by no means a unidirectional flow from police to private security. Indeed, research on the policing of Internet fraud has shown that the information produced and security systems used by private agencies can be extremely useful for the state police. For instance, computer forensic software is increasingly employed by corporate organisations to identify and investigate abnormal patterns of their client behaviour (Wall, 2008) and this can prove useful for criminal investigations conducted by the public police. In one case study, it was reported how private investigators saw that making their computer forensics subservient to the demands of the police 'was their butter and bread' (McKenzie, 2006: 208). A respondent representing the private sector investigators in the above mentioned study commented on what he described as an 'evidence packaging' trend by saying, 'you've got to box it all up with a lovely bow on top for them. That's what you've got to do. That's why I exist, to do that for them' (2006: 208). Moreover, McKenzie highlighted that 'there was a strong belief that private investigators who could not produce evidence packages of sufficient quality for police would get squeezed out of the market place informally as police would refuse to accept their jobs' (2006: 212). In addition to receiving 'packaged evidence', several police officers reported going outside Victoria Police to conduct evidence analysis using the resources, namely, the EnCase systems, of a third party investigation firm hired by the complainant company (2006: 252). McKenzie, while indicating that the clear benefit of this process for police was a reduction in their workload, notes its implication in terms of prolonging the police limitations in this area.

Another clear example of police 'co-option' of non-state policing systems, according to McKenzie (2006: 308), is the strategy of 'secondment of bank investigators to law enforcement'. As McKenzie notes, secondment agreements are formalised through Memoranda of Understanding (MoUs) between the Australian Hi-tech Crime Centre (AHTCC) and each external organisation. Highlighting that these MoUs and agreements focus on information sharing, McKenzie asserts that secondment of banks' private investigators into police forces 'offers a means for bi-directional learning and practice' (2006: 310). However, as one police respondent revealed, 'police still call the shots in these joint investigations, because if it's a police matter, it's a police matter' (McKenzie, 2006: 312).

Internet Service Providers (ISPs) play an important role in the regulation of online behaviour through their capacities to locate the Internet Protocol (IP) addresses of their subscribers, which enable the monitoring of online risky activities and thus restricting the subscription of the users involved in them (Wall, 2008). However, these capabilities can also be utilised by the police to obtain the actual physical address of the suspect computer in an Internet crime (Nhan, 2008). The investigators interviewed in Nhan's study explained that using the victim's last received email from the offender, they obtain the IP address from the ISP, who also possesses registered subscriber information such as home addresses and telephone numbers. Having obtained the subscriber's information, investigators 'can then do a subscriber search using the phone number to find the exact address of the person and issue and get a search warrant' (Nhan, 2008: 77). Similar practices have also been recorded by McKenzie's (2006) study, which reported that ISPs' backup data have been used by the police, without even search warrants, to obtain evidence of Internet fraud and other e-crimes. As one ISP respondent stated, 'we contacted the police and we provided them logs of connection usage, which gives phone numbers. This enabled the police to locate the offender. No agreements, no pack drill, just getting on with the job of solving the crime' (McKenzie, 2006: 239). As Wall (2008) indicates, the ISPs are subject to contractual governance through the terms and conditions laid down in their own contracts with the telecommunications providers who host their Internet services. Consequently, 'the fear of civil sanctions encourages ISPs' compliance with the regulatory demands made of them by the police and other state bodies [and] they are fairly responsive to police requests for cooperation' (Wall, 2008: 170-171).

Coleman and McCahill (2011: 80), citing Johnston (2000b: 70), note that neoliberal projects of 'responsibilisation' encompassed the privatisation of state entities such as the police and moves to devolve governmental functions to communities through projects such as '"community policing", "community education", "community justice" [and] "punishment in the community"'. Against this background, encouraging the 'active citizen' or 'communities' themselves to take responsibility for the prevention of crime has been a recurring theme in public pronouncements from politicians in the UK and elsewhere in Western societies in recent years (Coleman and McCahill, 2011). In the context of policing Internet fraud, 'non-state actors are encouraged to protect themselves against the threat of online criminal victimisation via market mechanisms, such that they become consumers of IT security goods and services, rather than citizens who have the right to expect protection from the state as part of social contract' (Bowling and Foster, 2002: 981-982, cited in Yar, 2010: 553). Equally though, as Johnston and Shearing (2003: 74) have observed, 'responsibilisation' strategies also focus on 'mobilising citizens as informers so as to facilitate bandit-catching'. The deployment of the 'active citizen' in the policing of Internet fraud might be seen in relation to the establishment in recent years of Internet reporting systems designed to encourage Internet users to report illegal behaviour online to law enforcement agencies. The Internet Crime Complaint Centre (IC3) (formerly known as the Internet Fraud Complaint Centre), which is an organisational collaboration between the FBI and the National White Collar Crime Centre (NW3C) in the US, may be viewed as a model for such systems (Yar, 2006). According to Yar (2006), the IC3 model is used to enable law enforcement agencies to investigate the reported frauds and catch offenders.

As Wall (2008) has shown, government-initiated responsibilisation strategies have also mobilised the policing and surveillance activities of other organisations and individuals in the virtual community. Wall points out that most virtual environments, including online role playing/game playing, chat rooms, discussion lists, e-auction rooms, cyberworlds, now employ 'trained, police-vetted' security managers to police the behaviour of their online community (2008: 168). Wall argues that in some respects these actors could be viewed as acting on behalf of law enforcement agencies in monitoring their community members for any illegal or harmful activities. The sanctions that virtual environment managers can invoke when ‘community norms or laws are transgressed’ include ‘temporary removal of access rights if the offending is minor, or permanent exclusion from the environment if it is serious’ (Wall, 2008: 170). However, when the offending behaviour ‘crosses the line into more serious offending’, the concern becomes about the legal responsibilities of the virtual environment owner, which require reporting to the police (Wall, 2008: 170).

As the above developments show, ‘below-the-state’ policing networks in the virtual community are being used by the state to control cyberspace, with the aim of identifying, apprehending and punishing perpetrators of Internet fraud and other cybercrimes. Therefore, it could be argued, following McCahill (2008: 216), that in reacting to the ‘cybercrime control’ requirements of central state organisations, private security actors have added the goals of ‘crime fighting’ and ‘law enforcement’ to their central concerns of ‘private justice’ and ‘loss prevention’.

Nevertheless, the extent to which the potential for employing non-state capabilities in traditional policing of Internet fraud exists or is exploited depends on the specific concerns and interests of the individuals and agencies involved, and on the nature of relations among them. This is an aspect of plural policing or partnership arrangements that is neglected by Garland (1996, 2001). He appears to favour greater involvement of civil society in crime prevention and control, seeing it as both an answer to the political reality of weakened state power and a means of exploiting the capabilities of non-state actors in a democratic model of local governance. However, a serious omission in Garland’s argument is his apparent failure to address the potential instabilities or problems that can limit the feasibility or effectiveness of police-civil partnerships. Competing organisational goals and cultural ethos can create conflict among the actors involved in ‘plural policing’ of Internet fraud. As Wall (2001: 147) points out:

> Traditionally, the tensions between the commercial and public actors arise because the primary function of the former is to police their own ‘private’ interests. In so doing, they pursue a ‘private model’ of justice that does not expose publicly their organisation’s weakness and thereby maintains the confidence of the market. The public criminal justice model, on the other hand, is public and the prosecution of offenders is carried out in the public interest and in the public gaze – not a model of criminal justice that many corporate entities want.

Tensions between public police and private actors in the policing of Internet fraud have been reported by several studies (Chung, 2008; McKenzie, 2006; Nhan, 2008). For instance, Nhan’s (2008) research in the state of California has found that the technology sector's relations with law enforcement were viewed by respondents as significantly weakened as a result of divergent goals. One computer security expert explained that 'corporations enforce their laws as standards and policy. This is only a means to an end; for law enforcement, the enforcement is the end' (2008: 121). Moreover, Nhan reports that because some companies perceive state agencies as competitors instead of security partners, they are often reluctant to share with these agencies information and technologies that they 'use to make a buck' (2008: 128).

Similarly, McKenzie (2006) demonstrates through examination of various investigative partnership mechanisms in the Australian state of Victoria that attempts to integrate public and private policing response to e-crime remain constrained by strained relations between them. One of the tensions that existed between the two sectors emanated, according to McKenzie, from the police's policy of 'evidence packages', which contributed to underreporting of e-crime to the public police. The responses of some potential partners to either underreport or direct reports to where it suits them represents in McKenzie's view 'marginalisation of public police' (2006: 351). McKenzie's findings also highlighted the existence of a feeling of imbalance of power in the investigation of Internet fraud which seemed to create frustration amongst some private investigators and limit their cooperation with their police counterparts. This situation led McKenzie (2006: 239-240) to suggest that the relationship between the police and private security actors in Victoria 'could be characterised as falling somewhere between stage two (grudging recognition) and three (open hostility)' of Stenning's (1989) five-stage model for the interactions and level of cooperation between police and private security.

As these reports indicate, it has been recognised in the literature that police co-option of non-state systems in the policing of Internet fraud is far from straightforward, and that it should be taken into consideration 'that the aims and intentions of dominant state forces and elites will not always be realised in practice'(McCahill, 2008: 199). However, such accounts of tensions and conflict between the police and private security personnel in the context of policing cybercrime appear so far to have focused largely on the private actors' perspective, that is, on reasons why they may be reluctant to cooperate with the police. What has been neglected, by comparison, is the effect of police organisation and culture in constraining the potential for cooperation. Traditionally, police forces are hierarchical organisations, with a strict chain of command, which might limit the flexibility for horizontal and networked communications. Burns et al. (2004) draw attention to the importance of considering this issue in the context of policing Internet fraud by highlighting the research conducted by researchers, such as Maguire et al. (2003), which suggested that the inflexibility of bureaucratic organisation inhibited some large American police agencies' engagement in transition toward a community policing philosophy as proposed by community policing reformers. Moreover, state policing agencies tend to be characterised by a conservative, isolated culture, marked by cynicism, if not suspicion, towards 'outsiders' (Reiner, 2000a), characteristics not conducive to cooperation with external, private agencies. In his study of six CCTV schemes in the Southern region of England, Goold (2004: 138) reported that while the development of good working relationships in police-led schemes was enabled by the fact that police and private operators worked in the same station and shared similar backgrounds, the lack of such factors in local authority-led schemes made police officers less willing to seek help from, or exchange information and intelligence with, private operators, perceiving them 'as "outsiders" and not part of the local "police team"'.

Such considerations are particularly salient in the Saudi context for two reasons. The first is the highly centralised structure and rigid bureaucracy of the police organisation. On this point, Kurian (1989) notes that not only are regulations, uniform and procedures identical throughout the country, but the Ministry of Interior has the authority to direct, control and finance the police force. The second reason why police cooperation with private agencies may be difficult stems from the nature of Saudi police training, which is essentially a military training. For example, Annual Training Plans[9] circulated by the DPS Training Department for the years 2007, 2008 and 2009 emphasise military discipline, obedience, combat techniques, weapon handling, target shooting, body building and fitness, and the commander-commanded relationship. This tends to embed and perpetuate a culture of 'separateness' and secrecy, which again is not conducive to multi-party, networked operations that demand openness, trust and willingness to share both information and functions. Evidence also shows that training focuses on issues and activities directly related to traditional policing functions, such as traffic control, patrol techniques, investigation, law enforcement strategies and administration. However, no reference was found in any of the training plans to computer and Internet-related crimes, or indeed to computer skills more generally.

[9] The DPS's Annual Training Plans were obtained from the DPS Training Department during the field-work by personal request.

Given these limitations, police officers may well lack both the awareness of the potential of computer technologies, and the practical skills in their use, necessary for a networked, cooperative approach to policing.

Apart from the complexity involved in the relationship between public and private actors, Johnston and Shearing (2003) have argued that one of the consequences of the rise of 'plurality' in the context of policing is the mix of state and corporate mentalities. On the one hand, the activities of private sector agencies reflect their growing engagement with the law-enforcement role formerly assigned exclusively to the public police. On the other hand, state police forces are increasingly adopting the risk-based approach more traditionally associated with corporate security, whereby the focus turns from reactive applications of sanctions after the event, to analytical assessment of criminal potential and proactive measures to reduce risk (Johnston and Shearing, 2003; Ericson and Haggerty, 1997). Against this background, the discussion turns now to examine this notion of a paradigm shift in policing strategies from 'crime-fighting' to 'risk-management' in the context of policing Internet fraud, taking into account the empirical complexity involved in this issue as highlighted by relevant police research.

2.5 Surveillance, Risk and Pre-emption in the Policing of Internet Fraud

The previous section concluded by drawing attention to an increasing emphasis on a risk-based approach to policing in the West, which, according to Johnston and Shearing (2003), reflects a more general trend toward instrumental forms of governance that focus attention less on the past and more on the future. In the criminal justice context, such a trend was observed almost three decades ago, when Cohen (1985) noted a 'master shift' from a cognitive to a physical focus in social control; thus, attention turned away from issues of motivation and intention, towards a focus on observed behaviour. Thus the emphasis was less on changing the criminal, and more on manipulating the physical environment to reduce the opportunity for crime. This 'master shift' has also given rise to strategies of social control which, instead of reacting to violations of rules, aim to proactively predict and prevent potential dangers (Cohen, 1994; Marx, 1988). More recently, several writers have expressed a similar notion of a paradigm shift in the criminal justice process. For instance, Feely and Simon (1994) have argued that the 'old' penology, which focuses on deterrence and punishment, was being superseded by the 'new' penology, which adopts a more proactive approach, targeting the prevention of future risk.

Thus, crime control policy in Western societies has become guided by 'techniques of identifying, classifying and managing groups assorted by levels of dangerousness' (Feely and Simon, 1994: 180). According to Castel (1991: 288), the trend of social control is moving towards what, in a reference to Foucault, he refers to as a 'post-disciplinary' mode, which pays less attention to changing people (the focus of Foucault's notion of normalisation). Instead, the emphasis is shifting towards the exercise of surveillance with the intention of anticipating how and where threat and deviance could occur and the elevation of suspicion to the status of risk assessment (Castel, 1991). These developments, as Coleman and McCahill (2011: 69) note, 'have given rise to "actuarial justice", whereby criminal justice interventions have become increasingly based on risk assessment, rather than on the identification of specific criminal behaviour'. This new actuarial mentality called for surveillance and preventative measures to be targeted at groups assessed as posing potential risk identified by statistically derived profiles (Weber, 2007).

In the context of policing, Coleman and McCahill (2011) note that 'risk-based', 'pre-emptive' approaches in industrial societies are not new; drawing on Zender (2006), they point out the focus on prevention among early commentators on social control, such as Chadwick, Colquhoun and Fielding, and the much later dominance of the reactive actions of arrest and prosecution. Nevertheless, there are those who argue that in the late modern period, a renewed emphasis on risk-based policing has been prompted by certain social developments. Among these, Johnston (2000b) notes the New Public Management (NPM) movement, whereby public sector agencies, the police included, were increasingly called upon to espouse the values and practices of the private sector. Citing Broder (1999), he argues that police organisations have experienced a melding of public and private-sector mind-sets, characterised by increasing preoccupation with the identification and assessment of risk, and with acting to avert the risk, or at least minimise consequential damage.

Ericson and Haggerty (1997: 222) argue that 'raising awareness' of circumstances of risk, so that people can take action on their own to prevent them, exemplifies trends in policing risk society, in which 'risk management knowledge is exchanged within a framework of preventive loss reduction'. Ericson and Haggerty built this argument on findings from the electronic data security branch examined in their study, which showed that it ‘played a major educational role’ through, for example, publishing ‘a data protection bulletin that had a print run of 20,000 copies and was circulated internationally’ (1997: 221). Moreover, the branch’s staff served as ‘both investigative experts and preventive security advisors to government and private sector organisations’, including providing training to government department security coordinators responsible for safeguarding computerised knowledge (1997: 220).

However, there has been a heated debate among criminologists, as well as researchers from other related disciplines, about the need for awareness-raising campaigns by regulatory agencies, mainly the police, to warn Internet users of the misleading and deceptive practices that exist in the online environment. Such a preventative approach is dismissed by some writers, such as Levi (2001), on the basis that it is unlikely to have much impact on reducing the consequences of online frauds and that it may – by exaggerating ‘fear of crime’ – result in consumers being reluctant to take up new technology and producers being reluctant to develop it. Nevertheless, it has been highlighted by many researchers as an effective method for reducing victimisation (see, for example, Grabosky and Smith, 1998; Grabosky et al., 2001; Smith, 2007; Mckenna, 2008). For instance, Smith (2007) reports that, in Australia, many consumers are assisted by the information provided by the Australian Consumer Protection Taskforce (ACPT) to help reduce the risks posed by the perpetrators of scams. Collins and Mansell (2005) have a broader perspective on the issue and view the importance of raising the public’s awareness of the risks that exist in the online environment to cyberspace crime prevention as lying beyond its contribution to reducing victimisation. These authors emphasise that the extent to which people are likely to accept government intervention or controls over their behaviour in cyberspace depends upon whether they are informed about the potential risks of cyberspace and whether they perceive themselves to be at risk.

It is argued that the renewed focus on risk management in social control provides further impetus for police use of ‘new surveillance’ technologies, in order to produce the information on potentially dangerous people and places necessary for effective risk assessment and proactive risk avoidance or reduction strategies (Johnston, 2000b). Historically, the development of surveillance has taken shape around the visual monitoring of physical persons as they move and act in a variety of terrestrial settings (the street, the workplace, the shop, the transit area, public transport, and so on).

However, with the appearance of networked electronic communications, it has become possible for individuals to engage in a variety of behaviours and exchanges in space in which they are not physically present. Surveillance in this arena consequently takes a rather different form from its terrestrial counterparts. As Yar (2006: 142) notes, 'rather than monitoring the physical presence and bodily actions of subjects, Internet surveillance observes and collects the digital footprints that all online activities leave in their wake'. Anyone who uses the web leaves, albeit unwittingly, a data trail; for instance, 'the electronic record of their mouse clicks and key-strokes, the websites they have visited, the searches they have run, the personal information they have entered, the words and images they have sent via email, and so on' (Yar, 2006: 142). From such 'dataveillance' (Clarke, 1988), a 'data-double' (Haggerty and Ericson, 2000) or simulation of an individual and his/her activities can be compiled, without the need for physical observation (Bogard, 1996; Poster, 1990). Clearly, this situation illustrates Ogura's (2006: 276) argument that, in the information age, 'human beings, or at least their bodies, are reduced to digital data or information'.

By means of networked technologies, it is possible to create and store informational data records of all Internet users' activities, thereby increasing the level of informational surveillance in such a way that, as Wall (2008) suggests, no-one can evade the 'electronic gaze'. For this reason, he argues, the popular view that the Internet is anonymous is mistaken. Rather, he claims, networked technologies have the opposite effect, leading to the experience of what Haggerty and Ericson (2000: 619) described as the 'disappearance of disappearance'.

Katyal (2003: 2268) argues that proactive solutions to Internet fraud and other forms of cybercrime should seek to make effective use of 'the natural surveillance' afforded by the Internet and the potential it offers for online control, without detriment to the openness that is its key characteristic. This argument is advanced by Wall (2008) who suggests that the 'surveillant qualities' of networked technologies can be utilised to enable both the monitoring and prevention of Internet criminal activities in a number of ways. As Wall points out, these characteristics can be used to generate a range of automated active policing tools that seek to identify wrongdoing. In this respect, Wall points to 'Honeynets', which are fake websites designed to 'socially engineer offenders to access the site and indicate wilfully their intent, before they eventually find themselves facing a law enforcement message and a notice that their details will be recorded or, in cases where intent is clear, subsequently become the subject of the investigation' (2008: 190). The purpose of Honeynets, according to Wall (2008), is to obtain intelligence about criminality, but also simultaneously to create a preventative effect through the awareness of being surveilled, which can inhibit the actions of fraudsters, spammers and hackers. In a sense then, as Wall (2008) points out, Honeynets exploit the discipline of Foucault's panopticon to become the 'electronic' (Lyon, 1994) panopticon.

A second and more important way of exerting 'risk-based' crime control of Internet fraud and other forms of cybercrime through utilising the 'natural surveillance' of networked technologies is 'data-mining'. As Wall (2008: 189) states, data-mining refers to 'the analysis of collected and retained Internet traffic data which records every Internet transaction'. The Internet's 'fine-grained distributed systems' are linked to 'every part of social life' (Lessig, 1999: 1) and offer the means of online monitoring and also the exploitation of records of network traffic (Wall, 2008). The potential exists for the use of data-mining to anticipate future behaviour; knowledge of customer behaviour, for example, can be used to lucrative effect by commercial enterprises (Gandy, 2003). Similarly, as Levi and Maguire (2004) point out, data records can be monitored in real-time to spot potentially criminal anomalies of behaviour, rather like the way in which financial institutions currently monitor transactions to detect money laundering, payment card fraud and other offences.

The data-mining principle has been the basis for a number of recently proposed dragnet intelligence systems in Western contexts. As Wall (2008) points out, these systems are based on the concept of linkage and analysis of various databases created by networked information technologies to detect a variety of criminal intentions. For instance, the Terrorism (originally 'Total') Information Awareness (TIA) system was proposed in the US after September 11 specifically to link all important national databases together to 'drain the swamp to catch the snake' (Levi and Wall, 2004: 207). In the UK, Ballard (2006) reported that a firm that produces surveillance software used by numerous British police forces was looking for one of them to test its latest invention, a programme called Nice Inform. According to Ballard, the manufacturers of the Nice software, which can be used by one user from one desk in a control room to scrutinise conversations, email communications and CCTV footage, claim that their new system can analyse different multimedia intelligence sources to detect abnormal behavioural patterns that it identifies as a possible sign of illegal activity.

These developments seem to illustrate Ericson and Haggerty's (1997) argument that policing 'the risk society' is increasingly about information brokering and that interaction among policing bodies is increasingly concerned with negotiating the exchange of information. In this case, the exchange is of Internet traffic data, which can be exploited more broadly to observe deviant online behaviour (Walker and Akdeniz, 2003). These interactions create formal and informal relationships that facilitate the networks of security discussed in the previous section.

In summary, as Wall (2008) points out, information obtained by means of online surveillance enables the construction of profiles that facilitate the identification of risks in cyberspace prior to their occurrence and, hence, the initiation of pre-emptive action.

The notion of what constitutes 'risk', however, is a problematic issue in identifying the nature and symptoms of risk and shaping the policing response to it. It appears that the ideology and nature of a society would play an important role in this regard. For example, in capitalist societies, the perception and treatment of risk seem to be linked to and influenced by capitalist principles and rational thought that emphasises economic concerns shaped by the values of loss prevention and profit. The impact of these factors on how risk is viewed and dealt with by police in the context of Internet fraud in capitalist societies has been documented by previous studies, which suggest that risk was understood in terms of financial loss (Murff, 2007) or of the cost incurred in investigation (McKenzie, 2006). This reflects Garland's (2001) argument that, in Western nations, social disorder comes to be viewed and addressed from an economic perspective and based on capitalist administrative principles.

In non-Western contexts, however, the issue of risk in the policing of Internet fraud has not been examined. It can be argued, nevertheless, that in a conservative society like Saudi Arabia, where Arab cultural traditions, adherence to strict Islamic values and mass participation in collective shared cultural and religious activities represent the major elements of the nation's identity (Helms, 1981; Niblock, 1982), it might be expected that such factors would influence police conceptualisation of and response to risk. Despite the rapid process of modernisation, beliefs, principles and traditional values are resistant to change. Although the Kingdom has undergone rapid socio-economic development, large-scale urban migration and the influx of foreign workers with different beliefs and customs, Saudi sociologists such as Al-Joware (1983), Al-Omary (1984), Abdraboh (1986) and Alsaggaf (2004), cited by Alhadar and

McCahill (2011: 317), point out that traditional Saudi values and religious principles remain unchanged, and continue to govern day-to-day life. Thus, modern Saudi society still revolves around the dogma of adherence to the commands of God, and even at the individual and interpersonal level, Saudi culture is heavily disciplined, with rigid moral codes and highly valued customs and rituals (Abo-Hasirah, 1998; Al-Harbi, 2008; Al-Romaih, 1993; Al-Sharidah, 1999; Wardak, 2005). The most influential cultural norms are those linked to Islam, such as defernce towards elders, a concern with morality and chastity, and the importance attached to honour (*sharaf*), at individual, family and tribal levels (Souryal, 1987, 1988; Mackey, 1987). As Wardak (2005) points out, the persistence of these values can be attributed to the near universal enforcement of them by Saudi educational, cultural, religious and justice institutions, as well as through the extended family. In addition, the consolidation of Islamic and Arab traditions among Saudis has also been strengthened by the ways the Kingdom and its population are perceived by its neighbours and the Muslim world as a whole. As Wardak (2005) argues, the concern among both the rulers and people of the Kingdom to meet the expectations of millions of Muslims around the world about Saudi Arabia as the cradle of Islam and home of its two holy cities, and as the symbol of the first Islamic community that was led by the Prophet of Islam and his followers, has played an important role in shaping the religio-cultural identity of Saudi society.

The key issue is not how much Saudi society has changed, but rather, how the society has been resilient in the face of change. It seems that there is a deep influence of cultural and normative social values in Saudi society. They are, therefore, expected to have a bearing on police perception of and response to risk in Internet fraud activity.

The issue of the impact of social norms and cultural values on police mediation of risk is also important in the debate concerning police adoption of risk-prediction technologies in the policing of cybercrime, since the operation and effects of these technologies are strongly dependant on those individuals who use them. Although the question of whether and to what extent new technologies and computerised surveillance databases are incorporated into existing police intelligence systems to effect a 'risk-based' crime control of Internet fraud has not been addressed empirically by research published to-date, we might gain some useful insights by reviewing some of the literature on policing and information technology. As will become clear in the following subsection, the findings of the reviewed empirical studies suggest that the use of computer-based surveillance technologies for 'proactive' policing relies on the individual concerns of police officers.

2.5.1 Police Culture and the Mediation of Risk-Prediction Technology

The introduction of computer-centred surveillance technologies has been seen by some writers as fitting neatly with the 'risk mentality' by allowing interventions to be made by the police before any deviant act has taken place (Graham, 1998). However, as McCahill and Norris (2002) have observed, much of the writing on information and telecommunication technologies in the policing arena is characterised by a 'technological determinism' which takes as given the way new technologies are applied in practice. They quote Lyon (1994: 9) as arguing that the problem with technological determinism is that 'it underestimates both the role of social factors in shaping the technology in the first place, and also the variety of social contexts that mediate its use' (2002: 4). Following Lyon, as McCahill and Norris point out, 'a number of researchers have drawn on the Social Construction of Technology (SCOT) approach to show that the way new technologies are applied in practice depends upon how they fit in with existing social relations, political practices and cultural traditions in different locales and institutional settings' (2002: 4-5). As Graham and Marvin (1996: 104) point out, the SCOT approach rejects the notion that technological systems 'have some autonomous "logic" which "impacts" on cities as an external force'. Instead, it aims to show how 'individuals, social groups and institutions...have some degree of choice in shaping the design, development and application of technologies in specific cases' (Graham and Marvin, 1996: 105, quoted in McCahill and Norris, 2002: 5). From this perspective, information technology may enable pre-emptive or risk-based policing, but police officers have the ability to 'adapt, bend, shape, develop, subvert, misuse or otherwise manipulate technological specifications for various purposes' (Ackroyd et al., 1992: 11).

Indeed, evidence found by studies in a variety of Western contexts shows, as highlighted by Coleman and McCahill (2011: 75-78), how police use of new technologies is shaped by the concerns and interests of the individual officers involved, often with the result that these technologies and resources are used as much in the service of 'old paradigm' law-enforcement policing as in the 'new' pre-emptive approach. Ericson and Haggerty's (1997) research in Canada, for example, showed that Computer-Aided Dispatch systems in police cars were commonly used in the routine patrolling context to check vehicle licensing information. Meehan (1998: 232), in the

United States, found that officers of the small force that was the focus of his case study favoured the use of mobile data terminals (MDTs) in police vehicles to run checks on licence plates and offenders with ‘outstanding warrants’. The proactive checking of plates in the car parks of establishments habitually used by drug dealers and other criminals featured strongly in investigative work and often led to arrests.

In Australia, Chan (2001, 2003) has reported similar findings in terms of the continuities, rather than changes, that the introduction of information and communications technologies into public police organisations often leaves in the habitus of policing. Citing also Sheptycki’s (2003) research outcomes regarding detectives’ tendency to limit intelligence gathering to the collection and evaluation of evidence for investigative purposes, rather than analysing crime trends and patterns to inform pre-emptive action, Chan (2003: 576) argues that:

> in spite of their vital role in the communication of risk knowledge, police organisations themselves have not yet become active and willing participants in the risk management enterprise [because] officers are most enthusiastic about technologies that advance traditional law enforcement objectives of arrest and conviction.

Chan (2003) has also observed the role of the competing cultures of police and civilian analysts in inhibiting the adoption of a more analytical and problem-oriented approach to crime.

A more recent study in the United States (Manning, 2008a) provides further evidence of how the organisational, occupational and individual concerns of frontline officers shape and often constrain the use of new technologies. Manning’s research focused on the introduction of Crime Mapping (CM) and Crime Analysis (CA) in the Boston, Washington and Western Police Departments. Although the CM/CA was designed to support pre-emptive policing by the provision of information on time, location and social factors, the data collected in Boston revealed that the system in practice was used simply for reactive, incident-based database queries, with no attempt to pre-empt crime by analysing and manipulating the temporal, spatial and social factors creating motivations or opportunities for crime. In Western Police Department, the system was operated by a retired clerk and a close-to-retirement officer who used it for personal purposes – tracking investments and checking email. In the light of such evidence, Manning (2008a) calls into question the notion of the police as a proactive, risk-focused, information-based organisation and concludes that it is still essentially reactive in nature, focusing on ‘the pragmatic, here-and-now, short-term-results approach to policing based on controlling known incidents after they take place' (2008a: 129).

The findings reviewed above are particularly relevant when considering the possibility of using computer-based technologies to gather and analyse intelligence from multiple sources in order to assess the risk of online fraud and take pre-emptive action. This is because the adoption of such technologies in the policing of Internet fraud is likely to be mediated by the normative, organisational, occupational and individual concerns of frontline practitioners.

However, previous researchers have focused predominantly on the organisational and occupational concerns of frontline officers, paying no attention to the impact of the wider cultural and social circumstances on officers' perceptions and operation of technologies, although McCahill (2002) asserts the influence of local cultural traditions in an English city on the use of new surveillance technologies by private security officers. Again, given the nature of Saudi culture and the importance of religion in that context, we may anticipate that these factors are likely to shape police officers' attitude toward and use of technology. It is essential, therefore, to take the cultural influences seriously into consideration when studying the way the policing of Internet fraud is carried out in practice. Hence, two key empirical questions will be raised and explored in this research. Firstly, examination of Saudi police response to Internet fraud will be directed to ask to what extent does policing this digital type of crime undermine 'old' forms of social control based on social conformity and a reactive approach, in favour of the concept of suspicion, potential risk and technological inspection that are embedded in a proactive control style? Secondly, to what extent can cultural values and social norms, especially in societies regulated by cultural rules and traditional norms such as the Saudi one, affect police response to Internet fraud by shaping officers' attitudes and operational paradigms? These questions are addressed by examining available official documents and government policies and studying the practical policing of Internet fraud in different police settings.

2.7 Summary

Starting from the frequently-voiced premise that the explosion of online criminality consequent upon development of the Internet constitutes a new phenomenon, requiring new approaches, this chapter has explored perceptions of and responses to the limited capability of the sovereign state to exercise control in late modernity. Some authors take the view that cybercrime, with its transcendence of spatial and temporal constraints, anonymity, and networked organisation, poses new challenges to 'public' policing, which has traditionally been dominated by physical space and spatial arrangements. Others question the 'non-physicality' of cyberspace, arguing that cybercrime leaves, however temporarily, a physical trail that increases the opportunities for investigation.

In the Western context, the policing of Internet fraud can be seen to reflect a dual transition between 'old' and 'new' penology in crime control strategies in late-modern communities. In this regard, the state's response to Internet fraud and other cybercrimes by setting up SCUs is seen by some critics as no more than 'expressive gestures' to reassure the public, as this is accompanied by an increasing trend towards 'responsibilisation' of citizens reflected in public-private partnerships and networks in the policing of Internet fraud, something which fits easily the new penology. However, from the perspective of the old penology, the 'pluralisation' of the policing of Internet fraud through the involvement of private actors seems to extend rather than reduce the central state's control, since private security systems, which may be driven by commercial concerns with 'loss prevention', can be, and frequently are, employed to assist the state in 'traditional' policing. This, nevertheless, appears to be dependent upon the interrelations between actors in local partnerships. Furthermore, the policing of Internet fraud may also reflect the 'risk mentality' with which the new penology is characterised. In this regard, the potential for proactive targeting of online fraudsters is increased by using 'risk-prediction' technologies, whereby Internet traffic data can be analysed to anticipate possible future fraudulent activities. However, how far this potential is exploited depends, as research on policing and information technology suggests, on the organisational, occupational and individual concerns of operatives.

Attention was given, however, throughout the discussion to highlighting the extent to which the Saudi state and its police's response to Internet fraud may mirror aspects of the late-modern crime control framework that appears to shape the policing of this crime in Western countries. Thus, while the possible manifestation of some of the Western strategies in this regard, particularly those intended for 'expressive gestures', in the Saudi state response to Internet fraud was acknowledged, caution was sounded about the applicability of other policing approaches in the Saudi context. Moreover, it was noted that theories developed on police and policing in Western contexts, reflecting their rational culture and economic concerns, may not explain attitudes and practices toward the policing of Internet fraud in Saudi Arabia, a society undergoing rapid socio-economic development, yet still solidly rooted in traditional religious values and cultural norms. Questions were accordingly posed as to the relevance of ‘plural policing’ in an autocratic state; the compatibility of proactive, risk-based policing with the traditional paradigm of control based on social and cultural values; and the possible impact of traditional norms and values on police officers’ attitudes and operations.

In the following chapter, the methodology adopted to guide the empirical investigation of the policing of Internet fraud in Riyadh will be explained and justified.

Chapter Three

Research Design and Methodology

Chapter Three: Research Design and Methodology

3.1 Introduction

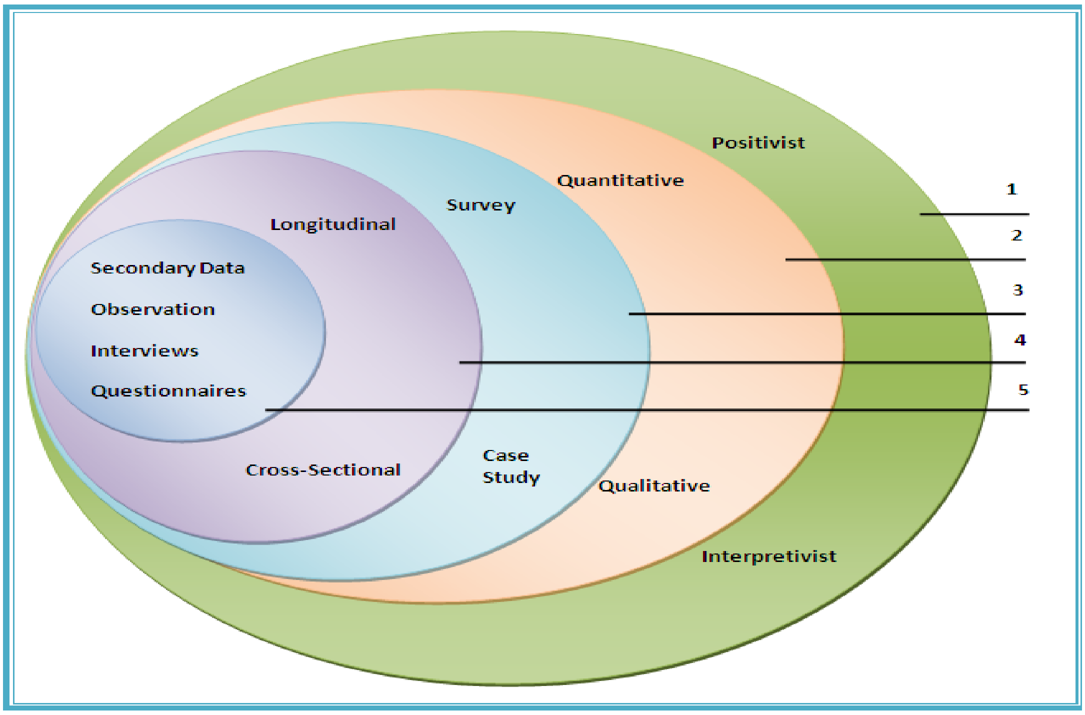
The purpose of this study is to understand how Internet fraud is policed in Saudi Arabia. This involves an in-depth investigation into both the organisational and operational dimensions of the Saudi police response to such criminal activity. In the preceding chapters, the relevant literature was reviewed to establish a theoretical framework for understanding the policing of Internet fraud in the Saudi context and provide a direction for empirical research. The present chapter sets out the methodology that guided data collection and interpretation. Initially, the chapter highlights epistemological issues and related issues in research design. Subsequently, it outlines how data collection and analysis methods were applied, emphasising the advantages and limitations of the selected methods. Other important methodological issues, such as access arrangements, ethical considerations as well as the validity, reliability and generalisability of the research findings, are also considered.

3.2 Process of Research Design

Yin (2009: 26), a well-known authority on case study, defines research design as 'the logical sequence that connects the empirical data to a study's initial research questions and, ultimately, to its conclusions'. He describes research design as an action plan for bridging the gap between the research questions and the answers to them. It consists of a set of decisions and actions to be undertaken, among them the collection and analysis of required data. Bryman (2008), too, views research design as a framework or structure for the research undertaking, which constitutes a blueprint for gathering and processing data.

It is important to recognise that research design should not be seen solely in terms of data collection method(s) as this restricts the concept unduly (De Vaus, 2001; Yin, 2009). Whilst data collection methods are indeed central, research design is a broader concept, extending over the whole course of a project. This view is captured by Saunders et al. (2003) in their 'onion' diagram, which illustrates research design as a series of successive layers, each entailing a specific decision to be made, which should be mutually consistent. Only after peeling these layers is the central point, the research methods, reached (see Figure 3.1).

Figure 3.1 The Research Design Process



Adapted from Saunders et al. (2003: 83)

1: Researcher's epistemological position 2: Research approach 3: Research strategy 4: Time horizon 5: Data collection methods

The first layer concerns the research paradigm or philosophy; the view (epistemological position) taken by the researcher regarding the nature of the social world and what constitutes valid knowledge. This leads to selection of the research approach and in turn, the main strategy to be followed. The fourth layer identifies the research as longitudinal or cross-sectional. Once all these layers have been peeled away, the heart of the process is reached – the selection of suitable data collection and analysis methods. This model was followed in the present research, aiming to ensure that the research was consistently and appropriately designed and conducted.

3.3 Researcher's Epistemological Position

The epistemological position a researcher adopts is the way he/she sees the world, which inevitably has implications for the research conduct. A basic distinction is generally made between positivist and interpretivist paradigms (Bryman, 2008; Guba and Lincoln, 1989; Lincoln and Guba, 1985; Saunders et al., 2003; Seale, 1999; Travers 2001). Whilst positivists see social phenomena as having objective existence, irrespective of human perception, interpretivists view 'knowledge' of the social world as subjectively constructed through individuals' values, culture and experience. Therefore, the researcher's task is to gain understanding of how particular individuals and communities perceive and experience the world (Walsh, 2001). Hence the researcher in the interpretivist paradigm is a key factor in the research process, as he/she determines its perspective and scope.

In the current study, the phenomenon of Internet fraud in Saudi society is considered to be socially constructed; each Saudi police officer can perceive, understand and respond to Internet fraud incidents in different ways. For this reason, the researcher adopted the interpretivist paradigm and was fundamentally concerned with meanings more than facts. He sought to understand the Saudi police subjective perceptions and experience of the policing of Internet fraud and the related situations in which they find themselves. For the same reason, the principles and approaches of the natural sciences, which are adopted by most positivists and focus on fact rather than meaning, were considered to be inappropriate. As Travers (2001) explains, when these principles are transferred to the social science context, researchers seek to describe the social world objectively, adopting a scientific perspective, ignoring the subjective differences between people. Partington (2002), for example, illustrates how such assumptions might be applied to the use of established terminologies, concepts and theories, so the research is homogenised and no account is taken of individuals' different perceptions of their environment and experiences.

Moreover, the requirement imposed by positivism that the researcher remain independent and isolated from the phenomenon under investigation (Saunders et al., 2003) was inappropriate in the current research. Bryman (2008) suggests that while this neutral stance is considered desirable in the natural sciences, it may be less appropriate for the social sciences, since people and organisations concerns are of a different kind, requiring a different approach, more suited to the distinct nature of the human and social world. From this perspective, social science must take account of individual differences, and the researcher must engage with the people being studied and explore events in the social world from their perspective. This is because, as McNeill (1990) argues, human beings are active, conscious agents, whose actions, thoughts and decisions are influenced by their perceptions of the context and circumstances. Thus, ‘it is the researcher’s task to “get inside their heads” until it is possible to see their world as they do’ (McNeill, 1990: 70).

For this reason, the current study involved interaction with Saudi police officers, to understand their experience of policing Internet fraud, rather than being independent in measuring the performance of those officers. Interacting with Saudi police officers in different units also provided a means to understand how the officers work, communicate and deal with each other and with their ‘clients’, and how Saudi culture impacts upon their response to Internet fraud. The adoption of the interpretivist paradigm is not to claim that it is ‘better’ than others, but it meets certain needs of the research and provides an overarching framework which needs to be considered to ensure coherence and consistency in the research design process.

3.4 Research Approach

The contrast between the positivist and interpretivist paradigms has implications for selection of the research approach; as Cassell and Symon (1994) comment, these different epistemological perspectives are widely invoked to account for the distinction between qualitative and quantitative approaches. Qualitative approaches are associated with the interpretivist paradigm, while quantitative approaches are underpinned by positivism. Thus, whilst the former approach tends to be defined as one that involves the meaning, concepts, definitions, characteristics, metaphors, symbols, and description of things, the latter is often regarded as one that involves measuring traits, characteristics, or attributes of things (Bieger and Gerlach, 1996). A further factor in the choice of approach is the nature of the issue under investigation (Bryman, 2008; Ghauri and Gronhaug, 2005; Saunders et al., 2003). Saunders et al. (2003), for example, suggest that when the research topic is one of which little is known and exploration is required, a qualitative approach may facilitate the collection and analysis of information, leading to the generation of theory.

In the present study, given the researcher's interpretive stance and the nature of the research topic (i.e. Saudi policing of Internet fraud), a qualitative approach was considered to be the most appropriate. Such an approach enabled the researcher to gain access to the understandings and perceptions of others and to explore the meanings they attach to their experiences (Berg, 2001).

Epistemological considerations have already been addressed. In what follows, therefore, the focus is on how the nature of the research problem influenced the choice of the qualitative approach.

A little known topic

Due to the lack of detailed empirical research, the policing of Internet fraud in Saudi Arabia is still an ambiguous, vague and little known topic. In fact, policing and police practice, not only with regard to Internet fraud, but more generally, is still an under-researched subject in Saudi Arabia. Most of the writing about Saudi police is descriptive; it describes the police organisation and set-up and so on. However, as explained in the introduction chapter of this thesis, no systematic research on the policing of cybercrimes, such as Internet fraud, is available. Thus, exploratory endeavours are needed to understand how Saudi police deal with Internet fraud, how the policing of this type of crime is experienced by officers and the implications of police practice. Developing such an understanding is considered to be one of the main strengths of a qualitative approach. Cassell and Symon (1994: 4) suggest that for exploratory studies, a qualitative approach offers advantages, because the 'researcher is less driven by very specific hypotheses and categorical frameworks and more concerned with emergent themes and ideological descriptions'. Padgett (1998) also argues that when little is known about the research topic, a qualitative approach offers greater flexibility to collect and analyse data simultaneously, so collection is informed by emerging insights. Bryman (2008) similarly believes that the flexibility of the qualitative approach enables the researcher to pursue alternative directions of enquiry and perspectives, which can facilitate deeper understanding of what is happening in the research setting.

A sensitive issue

The current research is concerned with exploring police activity in dealing with Internet fraud cases. However, police activity is a sensitive issue, the researching of which can be seen as posing what Lee (1993) calls ‘a political threat’. This is because the researcher deals with the ‘vested interests’ of the powerful in society and risks encroaching into areas of social conflict (Brewer, 1993; Westmarland, 2001). Additionally, this sensitivity is inherent not only in the policing of Internet fraud itself, but also in the relationship between this activity and the context within which it is carried out. In Saudi society, for instance, criticism of the police as a national establishment is taken to suggest a lack of commitment to the organisation. In turn, this is often misinterpreted as an indication of a lack of patriotism and loyalty to the nation. In fact, this sensitivity provided a challenging context for the research. Getting access (as will be discussed later) was very difficult, and many Saudi police officers refused to participate in the study. Those who participated were hesitant when answering particular questions, and sometimes were less than frank. This, as Lee (1993) points out, can be attributed to the potential consequences or implications that may threaten the participants in such sensitive research.

This provides further support for adopting a qualitative approach. Many research theorists consider qualitative approaches to have advantages over quantitative approaches when the research issue is a sensitive one (e. g. Lee, 1993; McCall and Simmons, 1969; Padgett, 1998). Padgett (1998), for example, argues that such approaches offer greater flexibility to explore sensitive topics and obtain detailed information than is offered by the standardised and closed-ended questions that typify quantitative approaches. Moreover, qualitative approaches reap the benefit of the researcher’s engagement with participants, enabling him/her to get close to them and win their trust (McCall and Simmons, 1969). Such relationships are especially important when investigating sensitive topics. Indeed, the qualitative approach allowed the researcher not only to build trusting relationships with Saudi police officers, but also to understand much better the context in which they carried out their activity. In this regard, spending time socialising with officers inside and outside their immediate work environment, as will be explained when discussing the observation stage of the research, proved to be an extremely useful technique. This personalised approach was conducive to greater accuracy of the data collected than would have been likely with a depersonalised approach such as a questionnaire, given the sensitivity of the topic. Previous researchers have claimed questionnaires are not taken seriously in Saudi Arabia and Saudi workers have little interest in participating in survey research (Al-Trawnah and Al-Lawzi, 1995; Nyambegera et al., 2000). Although this may be due to the unwillingness, as pointed out by Saunders et al. (2003), to spend time providing written answers, especially if the questions are open-ended or if there is any ambiguity in the questions, it can also be attributed to the reluctance of participants to fill in a questionnaire that they feel seeks sensitive information – a reason that is more relevant to this study.

Despite the trusting relationships built during the research, however, having read what has been written about police culture, the researcher remained careful throughout the course of the fieldwork not to assume that he would in any sense become a total police 'insider' within a few short months. Police researchers are reminded by Reiner (2000b) that even with observational work, the trust of the subjects of the research is unlikely to ever be complete. Being aware of this issue from the outset enabled the researcher to remain cautious about what he was told, and to continue to work hard to maintain a good working relationship with the police right up to the end of the research.

Process rather than outcome

As was explained at the beginning of this thesis, evaluating and measuring the outcomes of the Saudi police response to Internet fraud incidents in terms of solving or reducing such incidents has not been the primary concern of the present research. Rather, it is the process of policing Internet fraud (the ways that officers think, behave and act when dealing with Internet fraud incidents) that this study set out to explore. We know that online fraudulent activity is a novel area of deviant behaviour that the Saudi police have to deal with. However, we do not know how the introduction of the policing of this emergent type of criminality into the activity of the Saudi police fits in within their existing organisational, occupational and individual concerns. In addition, police response to a given criminal phenomenon is influenced and shaped by the legal framework, political practices and cultural traditions of the society in which it takes place. Again, we need to know how and to what extent these issues guide the Saudi police response to Internet fraud.

Such questions made qualitative approaches particularly suitable in the current study, as they facilitate development of in-depth understanding of the research phenomenon and context before drawing conclusions. Qualitative approaches are also more suitable for understanding dynamic situations. As Cassell and Symon (1994) point out, whilst quantitative approaches may reveal that a change has taken place over time, they do not explain the mechanism or reason for the change. Qualitative approaches, on the other hand, enable a detailed analysis of change. They also, according to Bryman (2008), facilitate understanding of how the various components of a social system interconnect, and thereby help to uncover the processes at work in the social world.

To summarise, the researcher's interpretive stance and the nature of the research subject made a qualitative approach the most suitable for this research. This, in turn, influenced the choice of research strategy.

3.5 Research Strategy

Research strategy is what connects the researcher's assumptions about the nature of the social world and of knowledge and the means of collecting empirical data (Denzin and Lincoln, 2000; Saunders et al., 2003). It constitutes a general plan for gathering the data needed in order to address the research question(s). Saunders et al. (2003) describe the research strategy as rooted in clear objectives based on the research questions, encompassing an indication of the sort of data needed and the sources from which it can be obtained, an estimation of how long it will take to collect the data, and by what means it can be appropriately gathered and analysed. According to Yin (2009), there are three factors that differentiate research strategies: (a) the nature of the research question posed, (b) the degree to which the researcher is able to manipulate actual behavioural events, (c) and the extent to which the concern is with contemporary as opposed to historical events. On this basis he identifies five strategies: archival analysis, case study, experiment, history and survey.

Following these criteria, a case study strategy was selected as the most appropriate to answer the current research questions, as the following subsections explain.

3.5.1 Case Study Strategy

Policing Internet fraud is a social process inextricably linked to the context in which it occurs. Thus, gaining an in-depth understanding of the process of Saudi police response to Internet fraud within its real-life context (i.e. the Saudi society and Saudi police organisations) was an essential and imperative condition that gave a case study strategy priority in the current research.

According to Denscombe (2007: 38), the case study strategy ‘lends itself to the study of processes and relationships within a setting’. He asserts the advantage of a case study strategy when the research objectives include not simply describing outcomes, but also explaining the mechanisms and reasons underlying them. In comparison, other strategies such as surveys, he claims, are more limited in their ability to address the details of relationships and processes. Gummesson (2000) similarly argues that case studies offer opportunities for understanding formal and informal processes in organisations. As Cassell and Symon (1994) comment, they are extensively used in studies of organisational behaviour for the potential insight they provide into evolving social processes, which can be seen in their organisational and environmental context. This strength of case study strategies supported its selection in the present study. Since it was anticipated that the policing of Internet fraud might be influenced by the wider culture of Saudi society as well as organisational culture within the concerned police departments and units, there was a need to observe and understand everyday practices, which could best be met by a case study strategy. There was also a need to understand how the phenomenon of Internet fraud is conceptualised by the Saudi police. In fact, adopting the case study strategy contributed to elucidating what Internet fraud meant to Saudi police officers in different departments, and how that was reflected in their response to it, which a survey strategy, for example, would not have uncovered.

Another important strength of case study strategies is their holistic approach to the case being studied. Policing Internet fraud, as a police activity, is a multi-dimensional process, involving social, organisational and legal variables and factors over which the researcher has no control. This reinforced the need for a case study strategy to facilitate the understanding of interacting effects among elements of the case (Denscombe, 2007) and maintain the unity and integrity of the case (Punch, 2005).

In short, the case study strategy was selected in order to study the phenomenon of policing Internet fraud holistically within its natural environment (i.e. Saudi police departments), and to gain a deep understanding of the meaning of actions involved in this process. Below, the choice between single and multiple cases is discussed, prior to explaining case selection.

3.5.2 Type of Case Study Employed

Case studies may explore single or multiple cases (Bryman, 2008; Denzin and Lincoln, 2000; De Vaus, 2001; Hakim, 2000; Punch, 2005; Yin, 2009). The decision as to how many cases to examine is a crucial one. Yin (2009) argues that a single case study is more appropriate when a particular case offers all the required conditions to confirm, challenge or extend an established theory; when a single case is rare or unique; when a single case is typical of a wider group of cases; and when a single case offers the opportunity to observe and study a phenomenon that was previously not accessible. Multiple case studies, however, offer the possibility of replication of a single type of incident in different settings, or comparison across cases. Like several other writers (De Vaus, 2001; Johnston et al., 2001), Yin views multiple case strategies as generally more powerful and convincing in the insights they provide. Hakim (2000) similarly suggests that multiple cases add to the credibility of the research.

However, based on the objectives and circumstances of the current research, the multiple case study strategy was considered less appropriate. This is because the present research was not comparative in nature. Rather it was a revelatory study which aimed primarily to explore an area of policing in Saudi Arabia which had never been studied before. According to Ghauri and Gronhaug (2005), a single case rather than multiple cases approach is preferable for an exploratory research, which can pave the way for a subsequent, more comprehensive study. Moreover, as Yin (2009) points out, a multiple case study research requires extensive resources and time. In the present study, time and resources were limited, thus making examination of multiple cases in different regions of a country with the vast area of Saudi Arabia impractical. Access to cases was another issue which influenced the selection of single case study. As will be discussed later on in this chapter, inaccessibility of research sites is a limitation frequently raised by researchers conducting police-focused studies. The situation was no different in the present study, as access was only possible to one case (i.e. the Riyadh Police). Additionally, given the concern to contextualise insights from the case study, and in accordance with the advice of Dyer and Wilkins (1991), a single case study is the optimal form of case study research for this purpose.

The single case studied in this research was what Yin (2009) labels a ‘typical case’. As has been explained in Chapter One of this thesis, the Saudi police organisation, known as the Directorate of Public Security (DPS), is highly centralised, and therefore regulations and procedures are identical in all the provincial branches of the DPS throughout the country. Thus, the chosen case (i.e. the Riyadh Police) seems to be typical among the DPS's branches in the thirteen administrative provinces of the Kingdom, which suggests the possibility of generalising findings to other Provincial Polices. This is not to deny, however, that further investigation may be needed to confirm the extent of generalisability to police departments in other parts of Saudi Arabia. Among other things, unity of Saudi culture should not be taken for granted, and acknowledgement of the probability of cultural diversity and subcultures among and within different Saudi regions and police forces would entail using multiple cases to examine and compare these issues and their influence on the policing of Internet fraud.

Having determined the suitability of a single case, the next step was to choose between a single holistic case study with only one unit of analysis and an embedded single case study involving a number of embedded sub-units. According to Yin (2009), a holistic design would logically only be used when it is impossible to identify sub-units, and when the relevant theory underlying the case study itself is of a holistic nature. In our research, the case study had neither of the above characteristics. In addition to being informed by multiple theoretical perspectives, the case study included a main unit and many sub-units. Indeed, police response to Internet fraud in Riyadh is a complex phenomenon and involves many actors on different levels. Therefore, our research strategy in its entirety was the single embedded case study, with Riyadh being the main unit of analysis, and the police departments involved in the policing of Internet fraud in that setting (as will be explained in the following subsection) the sub-units. Through taking this strategy, and by combining multiple sources of data, the research looked for consistent patterns of evidence across units, but within a case. Such a strategy, according to Eisenhardt (1989), can ensure appropriate analytic generalisability of the research conducted. Now, let us see how the case and its subunits were selected.

3.5.3 The Selection of the Case and its Units of Analysis

Given the aim of this research, it follows that the Saudi police force is the study population. Evidently, investigating every police branch in the Kingdom is impossible, due the constraints of time, resources and access. Consequently, choosing an ideal geographical area to become a representative case study remained the only alternative. Such a practice is supported by Fletcher and Plakoyiannaki's (2008) assertion that since case studies are defined by their degree of focus, a case may be a geographically defined entity, such as a country, city or state.

The city of Riyadh was deemed to be an informationally (as opposed to statistically) representative case (Sandelowski, 2011) for studying the policing of Internet fraud in Saudi Arabian, for a number of reasons. Riyadh is the capital city of Saudi Arabia and is located in the heart and centre of the nation. All the ministries and the headquarters of the government institutions are situated there. Thus, the city has important functions as a political, administrative, cultural, commercial, financial and transportation centre for the whole country. Riyadh has also the largest population concentration in the country, with 5,797971 persons, exceeding the rest of the Saudi regions by at least three hundred thousand. In addition, the number of non-Saudis living in Riyadh is 973,079, which means that it has the largest portion of foreigners living in the kingdom (Ministry of Economy and Planning, 2006: 13-21). These factors may explain the fact that more than one third of the police forces are assigned to Riyadh (The High Commission for the Development of Riyadh, 2006: 11). The headquarters of the Saudi police organisation, the DPS, is based in Riyadh, as is the Department of Forensic Evidence (DFE) with its Computer Crime Unit (CCU), a central laboratory to which materials relating to Internet fraud cases from all over the country are brought to be examined. More importantly, Riyadh hosts the Informational Crime Unit (ICU), which has been established recently to deal with technology-related crimes, including those involving online fraud and deception.

For purely administrative purposes, Riyadh is divided into twenty three geographical zones that vary considerably in size (depending upon the available landmarks such as main roads). Each zone has a police station with a workforce of between 80 and 100 employees, depending on the number of residents and level of crime in the zone. In turn, each zone is divided into a number of neighbourhoods that vary very little in social composition. In other words, people of different nationalities, races and social classes live side by side, and no neighbourhood is restricted exclusively to any particular social group. However, variation in economic conditions is more evident amongst these neighbourhoods, with some being more affluent than others. Police stations are usually run by mid-ranking officers who receive orders from their superiors at the Riyadh Police (RP). Also under the direct control of the RP is the Department of Detection and Intelligence (DDI). The primary function of the DDI is to assist in solving crimes whose perpetrators could not be identified by police stations' conventional means of criminal investigation. This involves, inter alia, undertaking undercover operations of information gathering. Moreover, as has been indicated above, Riyadh contains the headquarters of both the DFE/CCU and the ICU. However, in contrast to the police stations and the DDI, both of which report to the Riyadh Police Director, the DFE/CCU and the ICU function under the supervision of the DPS and receive referrals from all over the country.

Within Riyadh, the police stations, the DDI and the ICU constitute the agencies through which police service in relation to Internet fraud is delivered. They, therefore, formed the embedded units on which empirical data in the case study were collected. Each of these units was observed in its entirety except for the police stations, of which only five out of the twenty-three were included. That was necessary to capture depth and richness, which can only be ensured if the number of selected cases is kept at a minimum (Ghauri and Gronhaug, 2005; Yin, 2009). The selected police stations represented the five geographical areas (i.e. south, north, east, west and centre) of Riyadh. The stations were also chosen on the basis of variations in their demographics, size and workload, in the anticipation of capturing as many relevant variables as possible

Having highlighted the type of case study adopted and the way the case and its units were selected, it is important now to discuss the time horizons of the study, justifying the selection of cross-sectional research.

3.6 Time Horizons

The current project is an exploratory study, which aimed to investigate in detail how the Saudi police respond to fraudulent activities conducted online. For such studies, ideally a longitudinal design is preferable as it has the capacity to examine events over an extended period (Dantzker and Hunter, 2006). Indeed, longitudinal research could be useful, as it could facilitate comparisons on the development of the policing of Internet fraud in Saudi Arabia over time. However, the opportunities to conduct longitudinal research were limited in the present study. First, due to topic sensitivity, it was not easy to have access for a sustained period of time, especially as strict bureaucracy and legislation in the Saudi police inhibit access. Second, longitudinal study is time consuming, and limited time was available for the fieldwork of this PhD due to the strict regulations of the Saudi government, represented by the Cultural Bureau, regarding the period of time an overseas scholarship-holder may spend away from his institution of study. A period of three months is allowed for fieldwork. On the research supervisor's recommendation, a request was made for 12 months' fieldwork leave, but refused. The researcher therefore took his 3-month fieldwork entitlement and extended it by a further month by using his holiday allowance. Bryman (2008) and Saunders et al. (2003) advocate a cross-sectional design when time is constrained. Hence, a cross-sectional study was conducted, providing a 'snapshot' of the situation prevailing within a defined period, June to September 2009.

The selection of consistent and coherent epistemological position, approach, strategy, and time horizons in turn made possible an appropriate choice of data collection methods (i.e. participant observation and interviews). These are explained in the following section.

3.7 Data Collection Methods

Participant observation and semi-structured interviews were selected as the most appropriate methods to collect the required data, and were applied sequentially; the first stage (participant observation) constituting the foundation for the second (interviews). In the following subsections, the rationale underlying the selection of these two methods and their implementation are discussed in more detail.

3.7.1 Participant Observation (First Stage)

As a data collection method, participant observation is defined as:

> a method in which the observer participates in the daily life of the people under study, either openly in the role of researcher or covertly in some disguised role, observing things that happen, listening to what is said, and questioning people, over some length of time (Becker and Geer, 1967: 322).

This method has the particular merit of enabling the researcher to get close to the research setting studied and, consequently, facilitates a comprehensive and balanced view of the day-to-day life of participants. Waddington (1986) comments on the advantage of this method for researchers seeking to understand people's thoughts, emotions, behaviour and experiences, and to uncover new concepts, meanings or dimensions that may not be accessible in other ways. In the context of studying the police, Goold (2004: 55) cites Holdaway (1983) as arguing, based on his experience of researching the British police, that 'ethnography's methodological commitment to the value of empathy and the importance of understanding actors within their specific context makes it particularly well suited to studying the police'. Moreover, as Padgett (1998) suggests, participant observation is invaluable for collection of raw data that can subsequently be followed up in more detail by other means, such as interviewing. In addition to this advantage, Becker and Geer (1967) draw attention to the usefulness of participant observation as a means of evaluating interview data, based on their experience in a medical context, in which they found discrepancies between what respondents said in interview, and the behaviours observed. Based on this experience, they suggest that advance participant observation can help researchers to recognise possible bias and misinformation in interviews.

Another advantage of participant observation is the opportunity it affords to gain informal access to the most appropriate participants (in the present case, operational officers). As Bryman (2008) argues, even when access is granted by top management, success of the research may depend on obtaining acceptance and cooperation from lower levels in the organisation studied. Formal or official access alone may not be sufficient to obtain information needed from all levels. Indeed, as Miller (1952) found out in a trade union leadership study, the practice of gaining formal access, through the leaders and becoming close to them could actually alienate him from those at the grass-roots levels, and could constitute an impediment to gathering information from them.

With these advantages in mind, participant observation was selected to be the first stage in the process of data collection. During the course of the study, over 630 hours of observation was conducted, which amounted to approximately 90 hours of observation undertaken over a period of 15 days at each of the seven research sites (i.e. the ICU, the DDI, and the five police stations). In these observational episodes, all days of the week were covered. Although covering all times of the day would have been preferable, this was practically not feasible. The decision on which times of the day to observe was influenced by the fact that the sample police departments for the observation were fully staffed during the period between 07:30 and 14:30 (Saturday-Wednesday), which is the official working hours in Saudi Arabia, while duty out of these hours was undertaken only by a small team of 'full-day duty' officer and assistant officers. As it was evident that most of the police activity was carried out during the official working hours, a large proportion of the observational work had to be focused on this period. However, an effort was made not only to include a reasonable number of evening, night, and early morning hours, but also to extend the observation of the police work to weekends (Thursday and Friday) at different times of the day in order to ensure that the time-frame in which the data were being collected was sufficiently broad.

The observations focused on how officers carried out their daily work, but they concentrated more specifically on issues relating to the policing of Internet fraud. This included, for example, observing the processes by which Internet fraud crimes came to the police attention; how the Saudi police officers perceived and went about policing Internet fraud; which and how technologies were used in the various police departments to deal with Internet fraud; whether and how a proactive policing approach was used; ways of surveillance and intelligence gathering; handling of evidence and preparation of proofs; and whether and to what extent the cultural, organisational, occupational and individual concerns of the Saudi police officers shaped their response to Internet fraud. The observational work also concentrated on data that would enable the researcher to describe the nature and extent of cooperation between officers within and across police departments by monitoring, for example, officer/officer and officer/manager relationships, how officers worked together in times of joint tasks, exchange of information and intelligence, and so on. Moreover, to gain insights into police/non-police cooperation, the observation involved watching how the police interacted and communicated with non-police bodies, such as banks, the CITC, and the CIPC, in relation to the policing of Internet fraud, including the purpose, mechanism and outcome of such interaction. Close attention was also paid to the actual words employed by the police personnel, which constituted what Hammersley and Atkinson (2007: 145) call ‘situated vocabularies’. These offered vital clues as to how the officers perceived the world, and also they contributed to reveal the formal, organisational goals of the police stations and DDI in response to Internet fraud and the informal, occupational concerns of individual officers.

The participant observations provided a useful basis for the subsequent interview stage in various ways, not least of which was facilitating identification of suitable participants for the interviews. In this regard, an effort was made from the beginning of the observation process not only to gather personal information about such participants, but, more importantly, to build trusting relationships with them, which encouraged a smooth flow of information during the interviews. Moreover, the participant observations also afforded opportunity to socialise with the participants, including participating in their collective breakfasts and out of work meetings in the *el-Istraha* (rest place), which made it easier to discuss issues affecting the policing of

Internet fraud. In this way, many important themes and questions were raised, which were explored more deeply during the interviews. For example, the conflict between some police stations' officers and their counterparts in the DDI emerged as an issue (see § 5.3), as did officers' personal interest in training (see § 5.5). Although considered politically sensitive matters in the Saudi police organisation, officers were prepared to speak openly about management/employees relationship, resources and bureaucratic procedures. They also talked comfortably about their views on investigating types of Internet fraud and their attitude towards offenders and victims, within a friendly relationship with the researcher.

The participant observations were also useful in that they provided opportunities for group discussions. On a number of occasions during the observational work stage, conversations between the researcher and a number of officers proved to be very useful; by subtly directing the topics covered, the researcher was able to obtain some interesting data about how the officers viewed their tasks. Having three or more officers reflecting upon their work and debating aspects of it was highly illuminating in relation to how officers as knowledgeable actors construct their social world.

Finally, the participant observations also enhanced the validity of the research, as data collected from the interviews and observations were complementary and mutually supportive (the validity of the research will be discussed in more detail in section 3.11). Worthy of noting here is the fact that the material obtained from the observational work and the informal interviewing of frontline officers integrated within it served to counteract the management's accounts of the police approach to Internet fraud investigations, which tended to provide an organisational gloss.

The role of the researcher

Researchers can adopt a variety of roles towards their subjects, with consequent implications for the generation of data (Bryman, 2008; Sarantakos, 1998; Waddington, 1986). Possible roles can be distinguished according to the level of involvement with, and detachment from, those being studied. On this basis, Gold (1958) identified four roles that researchers adopt during participant observation, arranged on a continuum from complete participant to complete observer. The former is usually a covert observer, who tries to participate fully in the activities of the members of the research setting, without revealing his/her true identity and purpose. In contrast, the complete observer, while similarly conducting observation in an unobtrusive way, does so without engaging socially with informants. Between these two extremes are the participant-as-observer, who participates alongside the research subjects but is open about his/her identity and purpose, and the observer-as-participant, whose status as a researcher is overt, but who has less involvement and participation in the activities of those researched.

In the current study, the first two roles (i.e. the complete participant and the complete observer) were rejected for three main reasons. Firstly, whilst a covert role avoids the need for permission to gain entry to the research setting, access may become a serious problem if the target population belongs to a corporation, institution or organisation like the police, unless the researcher is already a member of that organisation. Holdaway (1982), for example, was able to carry out a covert study of a police force because he was a police sergeant. A further consideration was that adopting a covert role would prevent him from carrying out interviews in a later stage of the research, and doing so was considered essential in order to answer the research questions. Thirdly and crucially, whilst a covert approach can reduce the risk of bias introduced as a result of research participants modifying their behaviours when they are aware of being observed (Bryman, 2008; May, 2001; Padgett 1998), there are ethical problems with such a role. Saunders et al. (2003) characterise covert observation as tantamount to ‘spying’, which is unacceptable.

Participant-as-observer and observer-as-participant roles were selected, and adopted interchangeably as circumstances allowed. An advantage of these roles for the present study was that openness as to the researcher’s identity and purpose helped to allay suspicion and encourage participants’ trust, which in turn made them comfortable to display their natural feelings, attitudes and behaviour in his presence. A similar experience was reported by Punch (2005) in his study of police work in Amsterdam. In the present study, the researcher’s overt identity conferred both social legitimacy and academic credibility, and enabled him to benefit from interactions with participants outside the scope of formal semi-structured interviews. In those informal conversations, the researcher’s overt role enabled him to ask ‘naive’ questions in a way that would otherwise have been impossible, thereby gaining invaluable insights.

Choosing to conduct these types of observation also enabled the researcher to focus on the research problem, practically and mentally. At the practical level, the researcher and the participants understood that the researcher's main task in the setting was his research work. The researcher was also relieved of tension or anxiety about his status being detected. Bryman (2008) similarly notes the potential stress involved in participant observation which can be exacerbated by concerns about detection. In the current study, the researcher found that his overt role allowed him to act more naturally and to ask questions, conduct informal interviews and take field notes with relative ease and freedom.

Human sources

Participant observation gives rise to complex sampling issues (Spradley, 1980; Bryman, 2008). During the observation process, differences emerged in the quality of interactions with participants. Although initially the researcher engaged with everybody equally, experience in the field soon led him to identify 'key informants' (Ericson et al., 1987) – that is, those individual officers most closely involved with Internet fraud investigations. For example, in the early stages of the research, it became evident that one particular officer in the Southern Police Station had become renowned across the Riyadh police force for his success in solving a number of Internet fraud-related cases, and that his success had resulted from personal interest, enhanced by self-education. It made sense, therefore, to focus attention on this officer when covering the Southern Station. Frequent recourse was had to those key informants, sometimes to test ideas about the nature of policing online fraud, and sometimes for clarification of issues of organisational policy and practice. On the one hand, the prolonged engagement with some officers may have enhanced their trust in and rapport with the researcher (Hobbs, 2000), contributing to a more frank discussion of the policing process. On the other hand, care had to be taken not to bias the research by over-privileging the views of a few particularly helpful and co-operative participants. With this in mind, every effort was made to include a representative range of rank, position and work experience.

It was also important to be aware of political sensitivities, in the sense of making all the research participants feel that their ideas and information were valued and important. Hence, although some officers were clearly better placed than others to provide useful insights into particular operations, efforts were made to maintain contact with all officers and sustain a professional and mutually co-operative ethos. The positive relationships so maintained were enormously valuable in facilitating further access to operational procedures, sensitive information and the processes and practices of policing online frauds.

Documentary sources

As Atkinson and Coffey (2004) point out, in today's literate societies, much of what people do and think in organisational or other settings is recorded and stored in documentary form, and such documents are a valuable resource to ethnographers seeking to understand how organisations and their members work. For this reason, 19 case files of Internet fraud-related incidents were scrutinised in detail, with the aim of enhancing understanding of the complexities involved in the policing of Internet fraud, and providing a firm basis for any conclusions. These files record not only the results of the investigation, but the whole investigation process, and their examination enabled the identification of key issues within each investigation. The files therefore proved invaluable for the detailed insights they afforded into the nature of incidents investigated and the processes, practices and protocols employed by the police in their response to them.

The use of the case files was predominately to confirm or assist in interpreting issues that emerged from data obtained by other means. Examples appear in the accounts of the research findings in Chapters Four to Six. For example, in interpreting crime statistics, it was useful to observe how fraud incidents involving Internet use had been recorded in case files; this information, together with officers' remarks in interviews, revealed the failure, on many occasions, to distinguish Internet crime as a separate category of offence, and supported the researcher's interpretation of the officers' subjective definition of crimes. In another example, reported in section 6.3, the procedures logged in the case files indicated which complaints had been investigated and which merely recorded and transferred to an external agency, thereby providing evidence that supported the impression of a hierarchy of response according to the nature of the complaint.

However, while case files provided useful information on the product of the police investigative activity and accounts of the process by which this product was produced, they could not be viewed uncritically. It was important to remain aware of the fact that these files are deliberately constructed texts, created to serve a particular purpose.

Field notes

Field notes play a crucial role in participant observation (May, 2001; Seale, 1999). They refer to brief written notes made by the researcher during the course of observation, to assist subsequent recall. A notepad was used for this purpose when the situation permitted. As detailed note-taking was not always possible, Fielding's (2002: 152) 'jotted notes' technique, in which the observer noted only key words, phrases and quotations, was useful. These jottings, which represented more extensive chunks of verbal and non-verbal behaviour, stimulated the memory when the researcher had time and opportunity to reconstruct the events in more detail. The time saved by using this technique enabled more attention to be paid to the ongoing activity in the setting.

Although it is not necessary to hide the jotted notes in overt observations, it was nevertheless preferred to be as discrete and unobtrusive as possible in note-taking, in order to allow the group to forget that they were being observed and therefore behave naturally. This was consistent with the warning of Nachmias and Nachmias (1996) that recording in the presence of research participants may influence their behaviour and also constrain the researcher's participation in the group's activities. In order to avoid drawing attention to his note-taking, the researcher made notes in private settings, including toilets (see also Reiner 2000b).

Since, as Hammersley and Atkinson (2007) note, a time delay between observation and recording can result in loss of recall, the full field notes were written up immediately at the end of each round of observation. In so doing, in line with Fielding's (2002) advice, a system of notation was adopted, in which full quotation marks (") denoted verbatim quotation, while single quotation marks (') indicated a précis of what was said. The field notes were also written reflexively to include the researcher's feelings and responses toward the events described. Among other things, such information helps compensate for shifts in perspective (Fielding, 2002), and can highlight matters for future investigation.

When conducting the observations, it was apparent that it was impossible to attempt to record everything. Hence, the observations were guided by the study framework, and were more focused on matters clearly pertinent to the research questions, as was explained earlier in this section (see p. 83). In this regard, while the priority was to make note of the main observations, conversations, and informal interviews that occurred in each of the research sites, attention was also paid to making what Burgess (1982) calls ‘methodological field-notes’, which described the context in which the observations were made and the researcher’s own perceptions of situations and subjects. This record included assessments of the likely reliability of participants, the impact of the researcher’s presence, and the ‘mood’ and ‘feel’ of the setting. In hindsight, however, it was realised that keeping a daily fieldwork diary that records the researcher’s general feelings and impressions as to how the work progressed would have served to remind the researcher of the various problems faced when collecting the data, enriching the process of data analysis (Goold, 2004)

Limitations

Despite the advantages of undertaking participant observation in this field, there is a danger that the participant observer wittingly or unwittingly influences the setting and participants (Bryman, 2008; Denzin and Lincoln, 2000). Indeed, this problem was experienced in the early stages of the fieldwork. The researcher’s purpose was evidentially a matter of concern to some participants and they did not always act naturally. However, acquaintance with many of them predating the research, together with engagement with the participants in informal and social activities helped to overcome suspicion and to win participants’ confidence, which lessened the distortive impact of his presence. It was also helpful to obtain official permission to conduct the research, as this contributed to allay participants’ worries. In these ways, this potential limitation of participant observation was overcome.

Another limitation of participant observation is that it is very time-consuming. As Seale (1999) comments, a few seconds or moments interviewing may reveal a wide range of attitudes and behaviours that could take many weeks to uncover via observation. Whilst the researcher acknowledges this feature, it was in many respects counterbalanced by his familiarity with the national and organisational context of the research, which eliminated many cultural, linguistic and systemic obstacles, facilitating interpretation with less need for prolonged participant observation. This experience is consistent with the arguments of Nachmias and Nachmias (1996) and Vidich (1955) that participant observation in one’s own society is easier because communication is facilitated by a common language and symbolic system.

Participant observation is also marked by its subjectivity, since as Jupp (1998) points out, the findings presented are the researcher's interpretation of what has been observed. Hence, the researcher's role is an inextricable part of the data collection process. This problem, however, can be alleviated by training, as Lincoln and Guba (1985) argue. With this in mind, the researcher attended a course on ethnographic research, which broadened his understanding of the importance of considering how observers' subject positions might influence their accounts of the observed situations. It was learned from that course that researchers can relatively address the problem of subjectivity by being reflexive throughout the process of their observation, thus giving their audience the opportunity to evaluate them as active participants in the process of meaning creation. This reflexivity skill was further enhanced by the outcomes of the ethnographic exercise that the researcher had to undertake during the course, including comments and feedback provided on the reflexive essay that he produced on his experience in that exercise. Participants in the course were also trained on observational skills, such as note-taking, data recording, data coding and communication skills in the field.

Finally, the difficulty of gaining access is the most significant limitation of participant observation noted by methodologists (Bailey, 1996; Bryman 2008; Saunders et al., 2003). Such difficulty, as expected, was encountered in the current study. Initially, some departments refused to allow the observation. However, once official permission had been granted, participant observation proved very helpful in facilitating informal access, which in turn enhanced the officers' participation and cooperation in the later interviews

Whilst every effort was exerted to overcome the potential problems associated with observations, the researcher was, nevertheless, conscious that the use of another complementary and supplementary means of data collection would balance the subjectivity of the observation and increase credibility. For this reason, semi-structured interviews were conducted with a number of people involved in the policing of Internet fraud.

3.7.2 Interviews (Second Stage)

Interviewing is a popular and widespread method in qualitative research (Bryman, 2008; Fontana and Frey, 2000; Punch, 2005), and Yin (2009) views it as a major source of data in case study. Its popularity lies in the opportunity it affords for gaining insight into human behaviour, attitudes and meanings. In this research, interviewing was employed in the second phase as a means of exploring in detail the issues surrounding the policing of Internet fraud in Saudi Arabia, from the perspective of those charged with this task, namely, Saudi police officers in both managerial and operational positions. King (1994) and Punch (2005) both regard interviewing as an effective way of finding out how people perceive situations and the meanings they ascribe to their experiences, leading to an authentic and accurate understanding of the situation.

Moreover, in studying a sensitive topic like policing, where respondents seemed reluctant to divulge information about the nature of their work, as they regarded this as a national security issue that should be hidden, interviewing proved to be a particularly suitable method. This is because it offered official people the opportunity to provide information orally rather than in a written form, which they wanted to avoid, as they feared that it could be considered as an official statement. Another advantage of interviewing was the opportunity it afforded for the researcher to probe or to clarify the meaning of questions as required (Neuman, 2000; Babbie, 2001).

Interviews can take several forms and perform various functions. The majority of methodologists identify three main interview forms, namely, structured, semi-structured and unstructured (Fontana and Frey, 2000). Semi-structured interviews were employed in this study, for reasons explained below.

Semi-structured Interviews

Semi-structured interviews were considered appropriate in this study because of the potential to balance the strengths and drawbacks of the structured and unstructured forms of interview. Structured interviewing, with a standard, prearranged schedule, offers greater objectivity and comparability, but may be unable to take account of individual differences and contextual factors. Doherty and Perry (2001) acknowledged this limitation in their study of organisational culture in the UK financial services sector. Whilst structured interviews facilitated direct comparisons between the opinions of different participants, their focus on content at the expense of context resulted in loss of awareness of the differences between respondents. At the other end of the scale, unstructured interviewing leaves greater flexibility and freedom for respondents to express their views in their own way, affords scope for reflection, and can provide a wider range and greater depth of information (Ghauri and Gronhaug, 2005; King, 1994; Saunders et al., 2003), but the lack of structure and standardisation is not conducive to comparability and/or replication (Fontana and Frey, 2000).

Semi-structured interviews provided both flexibility and the possibility of comparison in the present study as an embedded single-case study with multiple units of analysis. Indeed, the interview guide, as will be discussed below, was designed in such a manner as to provide a structure for comparability between units of analysis within the case, but this does not mean that the interview questions were standardised and inflexible. Ample scope was left for following-up emergent issues, recognising differences between respondents, and appreciating the influence of social context. Questions were added, omitted or rephrased as appropriate, and question order was also varied, as the natural flow of the conversation demanded.

Semi-structured interviews make use of a topic guide consisting of 'a list of topic headings and possibly key questions to ask under these headings', along with 'a set of associated prompts' (Robson, 2002: 278). Accordingly, a number of themes and questions related to the policing of Internet fraud were incorporated into a set of interview schedules; one for use in the police stations and DDI (the main schedule) and adapted versions for use with the ICU, senior officers in the DPS and Riyadh Police, officers in the DFE/CCU, and members of the Training Department (see Appendix A). In developing his interview schedules, the researcher was guided and influenced by the literature he consulted. Extensive discussions were also held with the supervisor of the research who, before giving his approval of the final versions of the interview schedule, provided invaluable comments and suggestions which resulted in substantial changes in question topics, wording/prompts and sequence. Colleagues and police professionals back in Saudi Arabia were also consulted to ensure that interviews would cover all important points. Telephone interviews were then conducted with one police manager and two investigating officers as well as with a specialised member of teaching staff at King Fahad Security College. The results of those interviews were positive, and hardly any changes were made to the original schedules.

For the sake of brevity, only the main schedule, the one designed for use in police stations and the DDI, will be described in detail here. The interview questions were classified into five main sections. The first section was introductory and consisted of open-ended questions designed to have the respondent’s general perception on the extent and nature of Internet fraud in the research setting. The second section dealt with the organisational context of the policing of Internet fraud. At the beginning of the section, an indirect question was presented to the interviewee about whether there have been any changes in the Saudi police organisation in reaction to the emergence of Internet fraud. Subsequent questions addressed issues such as the existence of specialist units and investigators, specialist equipment to deal with Internet fraud cases, training of officers in this field of policing, and the priority Internet fraud is assigned in the interviewee’s department. The policing of Internet fraud in practice was the focus of the third section of the interview guide. The aim was to find out respondents’ daily activities and experience in this area of policing. Therefore, questions contained in this section were designed to obtain sufficient and detailed information on how the police handle online fraudulent activity, including exploring how, why, when, and by whom incidents come to the attention of the police; reactivity versus proactivity in police response to Internet fraud; strategies and methods used to monitor and police digital personae; and the way in which Internet fraud cases involving a cross-border dimension are tackled. Cross-agency cooperation in the policing of Internet fraud was another issue that the third set of questions in the interview schedule sought to examine before concluding with a question on the degree of success achieved by the police in solving Internet fraud cases as perceived by the respondent. In the fourth section, respondents were asked to offer their opinion on the future of the policing of Internet fraud and the changes that could make the police response to this problem more effective. Finally, the interviews were closed by asking demographic information about the respondent using a mixture of closed and open-ended questions. Since the interviews aimed to elicit information on a sensitive topic, it was thought that starting with personal details may produce a negative attitude in the respondents and thus influence the validity of their answers (Oppenheim, 2005).

Adapted schedules for use with the other groups and departments mentioned above were developed on the same principles as the main schedule, but with the addition or removal of questions or sections, or modification of wording as appropriate to tailor each schedule to the responsibilities and experience of the relevant group of respondents.

The Sample

Before explaining the sampling procedure followed in the interviews, an important point is worthy of clarifying first. As has been highlighted when explaining the organisation and structure of the Saudi police (see Chapter One), the departments investigated in the current study consisted of two groups of sworn personnel. The first group comprised those who occupy the prestigious ‘officer’ position, also known as *thabit* (the singular of *thubbat),* which is associated with those who carry the rank of lieutenant and above. They represent the core team in each department as they are the ones who carry out the investigative work. The second group represents regular policemen or assistant officers, who are known as *afrad* (those who carry the rank of staff sergeant or below). They usually perform clerical duties and are not assigned investigative tasks. The absence of any investigative duties amongst the responsibilities of the assistant officers (*afrad*) meant that it is unlikely that inclusion of representatives from this category of personnel in the sample of the current research would have any significant substantive influence on its outcomes. Thus interviews were conducted only with a sample of the officers (*thubbat*).

Forty one semi-structured interviews were conducted. Interviews were selected purposively (Bryman, 2008), to include a variety of positions and occupations. As can be seen in Table 3.1, in the seven organisations covered in the case study participants from the managerial level (the head or the deputy head of the department) as well as from the operational level took part in the interviews, providing rich data from different sources. The Informational Crime Unit (ICU), in particular, was considered the most relevant body in the policing of Internet fraud; it was, at the time of the fieldwork, only four months old. Thus, in contrast to the other departments where only a representative sample was sought, all the ICU’s officers were interviewed, including the manager and other four officers. The interviews included also representatives from the DPS’s Department of Training (DT) and Department of Forensic Evidence’s Computer Crime Unit (DFE/CCU), whose responsibilities affect the previous departments’ handling of Internet fraud. Training of the DPS staff is organised in this department through two main sections; one deals with home-based training programmes, while the other arranges the enrolment of staff members in programmes held outside the Kingdom. A leading officer from each of these two sections was interviewed. Interviews in the DFE/CCU were conducted with a manager and two members of the analytic team. In addition, three high ranking officers, two from the top management of the DPS and one representing that of the Riyadh Police, were interviewed. They were selected because of their key role in planning, controlling and implementing crime control strategies, and because they supervise the performance of all the investigated departments.

Table 3.1: Distribution of the Interviews within the Case Study

Departments	Occupational Level of Participants		Total
	Managerial Level	Operational Level	
5 Police Stations in Riyadh	5	20	**25**
The Department of Detection and Intelligence in Riyadh	1	4	**5**
The Informational Crime Unit	1	4	**5**
The Department of Forensic Evidence/Computer Crime Unit	1	2	**3**
Subtotal	8	30	**38**
The DPS's Department of Training			**2**
Top Management of the DPS			**2**
Top Management of the Riyadh Police			**1**
Total			**41**

This selection of interviewees from different organisational and occupational categories was essential. It enabled comparisons to be drawn across categories, providing an insight on cultural and organisational differences, behaviours, relationships and practices within the research setting.

That said, whilst the dominant sampling technique was purposive, there were also elements of snowball sampling. According to Oliver and Jupp (2006: 281), snowball sampling is:

> a form of non-probability sampling in which the researcher begins by indentifying an individual perceived to be an appropriate respondent. This respondent is then asked to identify another potential respondent.

Within the context of this research, snowball sampling was most apparent when senior officers recommended members of their team on the basis of notable experience, responsibilities or involvement within a specific investigation. The snowball sampling strategy also helped in identifying the key players involved in the construction of the ICU, and an interview was held with one of them. This was a senior officer from the DPS's top management who participated in the committee formed to draw the plans for the structure and policy of the new unit and to supervise their implementation.

Conducting and Recording the Interviews

It is argued in the methodology literature that successful interviewing requires a diverse and challenging range of communication skills which require practice (Robson, 2002). Before commencing the current study, the researcher had the opportunity to familiarise himself with interviewing skills and techniques through attending an intensive course on research interview at the University of Hull. Among the issues covered in this course were techniques that are supposed to be beneficial in building rapport, such as giving good eye contact a well as using posture and facial expressions to show interest and a sympathetic attitude to probe participants' responses. The course also involved practical sessions, in which the researcher, along with other students, conducted several interview exercises on all types of interviewing. Performance in these exercises and reflexive accounts on them were assessed by the module leader, who also provided some useful feedback. It is believed by the researcher that the lessons learned and experiences gained from taking part in the aforementioned course enabled him to carry out his field interviews in a way that served to achieve the purpose of their use.

Observing the work of the participants over a period of time prior to the interviewees provided an opportunity for a degree of familiarity and trust to build between the researcher and the interviewees, which was required in order to develop a greater degree of confidence to provide accurate and open responses. Before conducting the interviews, arranging the right times and places for the interviews was given considerable attention. With the exception of one investigating officer who wished to be interviewed at a hotel lounge, all participants were interviewed in their offices or place of work.

During the course of each interview, the researcher observed participants' body language and apparent comfort, and broke off the discussion when participants so requested. Leading questions were avoided. Questions were open-ended questions, followed if necessary by probes encouraging the interviewee to clarify vague statements, to give examples, or to further elaborate on brief comments. Use was made of the techniques advocated by Willig (2001) of expressing ignorance to encourage participants to answer in detail and to express implicit assumptions and otherwise 'obvious' information. Another technique employed that facilitated the generation of the required information was to confront the respondent with what the researcher already knew from previous interviews. This technique, referred to by McCahill (2002) as ‘directive’ questioning, was often successful in encouraging the interviewees to talk more freely about sensitive issues.

Interviewing style was varied to gain optimal outcomes and rigid adherence to the interview framework was avoided. This meant that emergent themes directly pertinent to the policing of Internet fraud in Saudi Arabia could be pursued freely, thereby enriching collected data with additional dimensions.

Consideration also had to be given to the recording of information imported during the interviews. Criminal justice practitioners have been known to view recording instruments with suspicion (Noaks and Wincup, 2004) and there is a risk that interviewees will withhold information when an interview is being recorded. However, most of the participants in this study appeared relatively unworried about the recording of their interview and in consequence the majority of interviews were digitally recorded, with the interviewee’s permission. Only six participants expressed unwillingness to be recorded, purportedly for fear of identification, despite being given assurances of anonymity and confidentiality. In these cases, responses were recorded in note form. Before starting the interviews, it was explained that the recorder could be turned off whenever they wished, and the machine was so positioned as to give control to the interviewee. On one occasion, an officer turned off the recorder revealing information which, whilst of interest for the insight it afforded into the inner working of operational procedures and individual officers’ minds, it would have been inappropriate to report in this thesis. Difficulties in recording sometimes occurred due to acoustic problems, particularly with some very softly spoken participants. Repeatedly asking such individuals to speak up was disruptive and stressful for both parties. In such cases, the researcher accepted the loss of some of the interviewee’s words rather than make such requests too frequently, particularly as the main points were also being noted in writing.

During the interviews, which lasted between one and three hours, the researcher listened attentively, recorded the responses (with the exception of six cases), and noted key phrases and major points made by the respondents as well as non-verbal behaviour, using a system of abbreviation and informed shorthand. In so doing, in order to avoid interrupting the flow of important parts of the conversation, it was sometimes necessary to remember points or sentences for some minutes and write one thing while discussing something else (Maguire, 2008). Soon after every interview, notes about the setting and the conduct of the interviewee were added, which assisted in recall of the interview context during analysis. The interviews were transcribed, with the researcher's comments, immediately after each interview.

Limitations

Although semi-structured interviews have many strengths, commentators warn of the potential for bias arising from the respondent's reaction to the interviewer, for his/her remarks, tone, appearance, gestures and expressions, which can influence how interviewees respond (Saunders et al., 2003). There is also a risk of interviewees presenting a distorted account of their experiences, either because of their awareness of an ultimate audience for their responses, or through an impulse to tell the researcher what they think he/she wants to hear. Al-Nimir and Palmer (1982) reported such an experience in their study of bureaucracy in the Saudi public sector. This sort of distortion can undermine the validity and reliability of the research (Saunders et al., 2003). In this study, as has been mentioned above, this risk was reduced by the researcher's prior training on interviewing, which enabled him to guard against interviewer bias. Furthermore, combining the interview with participant observation, as was done here, provided a means of cross-checking information and interpretation, which increased reliability of the findings.

Limitations with semi- and unstructured interviews have also been identified pertaining to the analysis stage, one reason for choosing structured interviews often being that standardisation facilitates comparison (May, 2001). There are also issues of time and cost when the sample to be covered is large (Bryman, 2008; Sarantakos, 1998). These last two limitations were to some extent overcome by simultaneous collection and analysis of data. As well as being time-saving, this encouraged feedback from participants, which contributed in validation of the findings.

3.8 Data Analysis

Before discussing the analytical procedures followed in the present research, it is important first to describe how the collected data were transcribed. It was decided that recorded interviews and observational field-notes would be transcribed in the Arabic language. This provided a means to discover practical understandings of meanings and actions. It was not easy to translate from Arabic to English since some nuances cannot be fully expressed in other languages. Arabic is often described as a language with vast vocabulary, and many Arabic concepts may not have an English equivalent. For example, the Arabic word '*thubat*' is exclusively associated with those military or police officers carrying the rank of lieutenant and above, while '*afrad*' are used to refer to all officers from the rank of Staff Sergeant and below. Suffice to say that the researcher was faced with great difficulties in conveying concepts from Arabic into English. Therefore, translation was conducted only for the interview quotations and observational extracts that were selected to be included in the final document of the research. The translation was carried out first by the researcher. However, to ensure a high accuracy of translation, a specialist in English translation was approached for a second opinion. A few alterations were made in the translation based on the suggestions provided by the linguist. Having explained the transcription of the collected data, let us now consider how they were actually analysed.

According to Merriam (2009), it is preferable for analysis of qualitative data to proceed simultaneously with data collection, to enable data collection to be guided by emergent understandings. 'Without ongoing analysis, the data can be unfocused, repetitious, and overwhelming in the sheer volume of material that needs to be processed' (Merriam, 2009: 171). With this suggestion in mind, and following the advice of the research supervisor, it was decided to begin data analysis early during the data collection phase. Accordingly, initial analysis took place in the field, involving careful analysis of interview transcripts, observational field-notes and documents on a daily basis, to ensure reflective research practice and systematic progress through further contact and subsequent investigations. The researcher read and reread each set of data, making notes capturing his reflections, tentative themes, ideas, and things to pursue when collecting the next set of data that were derived from the previous ones. This 'simultaneous and recursive process' (Ruona, 2005: 237) of data collection and mini-analysis continued throughout the fieldwork in a cyclical development.

However, as Merriam (2009) reminds us, to say that data collection and analysis is a simultaneous and recursive process does not mean that analysis is finished when all the data have been collected. Quite the opposite; analysis becomes more intensive once all the data are in (Merriam, 2009). Thus, following the completion of fieldwork, the data were scrutinised in a more detached way and this stage constituted the main analysis. This involved a three-fold approach which Coffey and Atkinson (1996) summarise as a) coding and categorising; b) retrieving and exploring; and c) displaying.

Coding and categorising is a process of reducing the data by dividing it into categories each of which might encompass several subthemes, assigning chunks of data to the appropriate sub-themes and categories (Merriam, 2009). Initially, the researcher thought of using an Nvivo 7 program to achieve the management of coding and categorising. However, it was not used due to the fact that, as Wincup (1997: 69) stated, a 'software package consumes too much time for sorting and retrieving data at the expense of writing'. Instead, the data were categorised manually using traditional index cards. Extracts from transcripts were printed out, labelled and assigned to the relevant category. Colour markers were used to code similar categories. This procedure helped in identifying relationships in the data at an early stage, as well as encouraging constant comparison of data in order to assign extracts appropriately and check whether new categories were necessary. During this process, a key role was played by writing memos that recorded the development of categories and the relationships between them. This helped to ensure that ideas, comments and intentions that emerged during the process were not lost, and provided material for further reflection as the analysis proceeded.

The coding and categorisation phase concluded with a reorganisation and re-evaluation of all categories and subcategories, and the formation of initial, tentative theoretical conclusions which, were subsequently developed, integrated and verified by returning to the field notes and interview transcripts, as well as discussions with other academics. In this way, conclusions were formulated in relation to the research questions and emergent themes.

The second phase of analysis was retrieval and review of the reduced and categorised data, to see if there were similarities and differences between respondents, and if appropriate to discover and develop any new concepts, themes or sub-themes. The last step was to display the data (e. g. concepts, themes, similarities, and differences) in a meaningful way. By displaying information on a single page rather than in extended form, it became easier to recognise relationships and patterns, to uncover new ideas, and so draw and verify conclusions (Miles and Huberman, 1994). The concept of data display was used from the beginning of the analysis process to ensure that the themes and concepts generated were interpreted and linked together in the light of the previous theoretical discussion. As mentioned above, these three steps were repeated iteratively, resulting in many fruitful and interesting discoveries.

3.9 Access

As Reiner (2000b) notes, the problems of access and trust, which typically arise in social science research, are intensified in police research. Respondents may be suspicious of the researcher's motives and have a vested interest in secrecy. Numerous previous researchers have reported the difficulties of gaining access to the police organisation and the fundamental challenges of conducting research in this context (Fox and Lundman 1974; Holdaway 1983; Punch 1989; Young 1991). Moreover, as Cassell (1988) points out, 'getting in' in the sense of obtaining formal access by no means guarantees the accomplishment of social access on an everyday, interpersonal level with members of the research setting.

In the current research, gaining formal access was facilitated by a number of procedures. As a starting step, the researcher obtained a letter from the University of Hull that contained information about the researcher and the purpose of his project and the importance of cooperation for the success of the study. That was followed by acquiring another letter from the Saudi Cultural Bureau in London, to serve the same purpose. In Saudi Arabia, two letters were produced by the Director General of King Fahad Security College. One of these letters was addressed to the Director of Riyadh Police (Appendix B.3), requesting access to the study sites lying within his limits of control, including the DDI and the five police stations. The other letter (Appendix B.2), which was addressed to the DPS's Director General's Assistant for Security Affairs, was intended to assist the researcher in gaining access to those police departments in Riyadh access to which could not be granted by the Riyadh Police, namely, the ICU and the DFE/CCU. Each of these letters, in addition to the above information, stated that the researcher was sponsored by the college to undertake this study and had permission to collect the required data. To ensure quick response, the researcher decided to present the letters and explain the objectives and methodology of the research in person. Initial introductions were held with the DPS's Director General's Assistant for Security Affairs and one of the deputies of the Director of Riyadh Police. While no misgivings about the research were overtly expressed, it was clear that the two senior officers were concerned with the dissemination of the findings. However, many of these fears were soon laid to rest after a full explanation was provided by the researcher, and access to the targeted police units, relevant individuals therein, and related information was agreed.

While formal access had been approved at the top of the organisation, the researcher was aware that a whole new process of negotiation was required in order to gain the acceptance of operational officers. Reiner (2000b) warns that there is more to gaining access than obtaining formal permission from the authorities; more important is subsequently eliciting the trust and genuine cooperation of the people in the research site itself. Fox and Lundman (1974) make the same point with regard to police organisations, referring to two ‘gates’, senior managers and the ordinary members of the force, both of whom affect access.

Initially, the researcher was met with suspicion and cynicism, especially from the sample departments’ managers, and it was therefore necessary to engage in a delicate process of negotiation. Some managers appeared extremely concerned about the nature of the research, and the potential repercussions that it might pose for them. Their suspicion was exacerbated by the fact that the research was undertaken in a period which witnessed a wave, within the Ministry of Interior, of early relieving of officers from their duty across the security forces. There was an apparent fear amongst these managers that allowing an outsider researcher who would potentially publicise negative research findings on their departments would somehow contribute to them being the new ‘victims’ of the forced retirement movement. Moreover, while every effort was made to clarify the objectives of the study, for example, by providing copies of the interview schedule as well as information sheets which explained the nature of the research and plans for dissemination of the findings, a few managers still mistakenly perceived the research as an evaluation of their unit’s performance. Hence, further effort had to be expended to dispel those misperceptions and make clear the exact purpose of the research.

Moreover, fears and concerns about the research were expressed by ordinary officers also, since they perceived the researcher as an ‘outsider’; a research position which can have significant implications for the type of data and material that is accessed (Reiner 2000b; Ericson 1982; Brown 1996). While reflecting the general suspicion that the police have towards outside researchers, the concerns shared by officers fundamentally related to the Saudi Police’s unfamiliarity with qualitative research methods such as participant observation. Some officers feared that individual officers might be identifiable from the thesis, exposing those who disclosed ‘sensitive’ information to the risk of being ‘called up to the headquarters’ about their conduct.

While these officers later expressed interest in the research, their initial reactions reflected their entrenched distrust of ‘outsiders’.

Despite the initial concerns, the researcher succeeded in establishing and maintaining a good rapport with police officers in the research sites. The fact that he has worked and taught in KFSC, the institution in which Saudi police officers are trained, was advantageous in this regard. The population of his ex-students within the police force has grown to the extent that he was already known to at least two of the officers in each site he visited for the purpose of this research. Such officers played an important role in introducing the researcher to the rest of their colleagues with whom he had no previous acquaintance, mainly because they graduated before he joined the College. Therefore, for the most part, there was no overt hostility or resistance towards the researcher or the project. On the contrary, once officers became more familiar with him, the researcher was able to access much of the ‘unspoken agenda’ of operational police work (Young 1991). And while it is problematic to suggest that a researcher can gain access to all areas of police life (Ericson 1982), the current researcher feels that a number of incidents demonstrated officers’ willingness to accept him. That he was able to gain the trust of at least some of the officers that he was observing, was apparent on the occasions where he was introduced to members of the public as a ‘colleague’, or when he was invited to in and out-of-work social occasions, such as collective breakfast and *el-Istraha* (rest place) meetings. Furthermore, although the researcher took care to emphasise his neutrality, many officers also seemed to appreciate the opportunity to voice their concerns about unfavourable work conditions, such as work overload, staff shortages and insufficiency of equipment.

It is impossible, however, to ascertain exactly what impact the researcher’s presence had on the ‘natural’ behaviour of those officers who participated in this study. Nonetheless, other researchers in similar situations have suggested that the police would not expose themselves to ‘embarrassment’ (Reiner, 2000b: 220) or to the possibility of reprimand from senior officers unless they had to a great extent accepted the researcher (see Norris, 1987). Several incidents could be cited in support of this claim, but two themes in particular stand out. First, officers were open in expressing dissatisfaction (and sometimes strong criticism) regarding their immediate bosses and those in the DPS and the Ministry of Interior, which leads the researcher to infer that he had won their confidence to some degree. Second, there were instances in which he observed officers exhibiting disdain and disrespect towards members of the public. It is unlikely that these behaviours would have been manifested, had participants felt constrained by the researcher's presence.

3.10 Ethical Considerations

All research poses ethical issues that must be addressed from the outset. According to Sumner (2006: 96), ethics in social research is a 'field of moral philosophy dealing with the standards by which behaviour should be regulated'. Academic associations, like the American Sociological Association and the British Society of Criminology, have published codes of conduct for both qualitative and quantitative research. The researcher has followed the guidelines of the British Society of Criminology's (2006) Code of Ethics for Researchers in the Field of Criminology, which focuses upon two central principles: professional integrity and responsibility towards research subjects and towards colleagues.

Professional integrity

A risk attached to the participant as observer role is that of 'going native', a phrase used to denote ethnographers becoming excessively embroiled in the context they are investigating (Bryman, 2008: 302). Hobbs (2006) reports that ethnographers have sometimes been criticised for letting their participant role overshadow their objectives and obligations as researchers. Hobbs points out the danger posed by such a stance, as it removes the element of objectivity necessary for the generation of valid theoretical inferences.

During the fieldwork, it was very difficult to remain detached in social interactions, without being drawn in to forming real friendships. The researcher availed himself of opportunities to engage in various elements of police culture to which he was afforded access, and participated in several social events. Such activities contributed to the researcher's social legitimacy and academic credibility, helping to establish him as a familiar and accepted figure in the research setting. At times, during such social events, police officers evidently supposed the researcher to be 'off duty', and discussed information and opinions that, despite their interest and the insights into police work they provided, could not be reported in this thesis. It was therefore necessary to be constantly vigilant regarding possible tensions between formal and informal disclosure made as part of the research process, and informal disclosures emerging as part of peripheral conversations. Maintaining the identity of researcher is important in all participant observation because it is also part of the process of eventual detachment from the research setting.

Responsibility towards research subjects

Since this research involved data collected from participants involved in the policing of Internet fraud, it was possible that harm to a respondent could ensue from information obtained. This possibility gave rise to potential problems related to informed consent, anonymity and confidentiality, and dissemination.

According to the British Society of Criminology (2006), participants in criminological research should be engaged in the study voluntarily, having given informed consent. This means that participants must be informed of and understand the nature and purposes of the research, and that, based on such understanding, they can freely agree to take part in the research. For this research, at an early stage, an open agreement was obtained from higher-level managers for the conduct of the research and collection of all the required data. Moreover, the researcher presented himself and his role in a manner that was understandable and acceptable to the participants. He took care that participants should not be harmed by participation in this research and accepted responsibility to safeguard their physical, social and psychological well-being. The cooperation of each interviewee was secured individually and their involvement was voluntary. Interviewees were not placed under any compulsion to attend and were assured of their right to withdraw at any stage.

However, while the principle of informed consent was followed with the police, no attempt was made to seek the permission of members of the public with whom the researcher came into contact, for pragmatic reasons. It appeared likely that to explain the reason for the researcher’s presence would create problems of ‘observer effect’. Generally, therefore, the researcher remained silent about his role, although this was occasionally raised by police officers. When that happened, the researcher was introduced as ‘a colleague’ undertaking a PhD research project.

Another two important principles of ethical practice are anonymity and confidentiality. First of all, as the current study is a case study research, the researcher was faced with the challenge of choosing between anonymising and disclosing the identity of the case. According to Yin (2009), anonymity of the entire case is undesirable because it entails omission of important background information, and also deprives the reader of the opportunity to connect the study with any other previous information he or she may have learned about the same case, whether acquired from previous research or other sources, in interpreting the case study's findings. With this in mind, a decision was taken to make the identity of the case explicit, especially as the case study is not on a controversial topic, nor is the issuance of its final report expected to affect the subsequent actions of those that were studied – the only two situations in which anonymity can be justified (Yin, 2009).

Anonymity was, however, guaranteed to all those who participated in the case study. It was agreed that all transcripts would be made anonymous and that individuals who participated in the study would not be identifiable from the way in which the findings were presented. Furthermore, assurance was provided that documents containing extremely sensitive data, such as case files, names, addresses and profiles of victims and offenders, were collected only for research purposes and would never be disclosed. Also, the data collected and stored will be secured until the thesis is approved by the viva examination. After the viva, all data will be disposed of securely.

Whilst codes of conduct advocate assurance of respondents' anonymity and confidentiality, methodologists warn that where the research sample is small, individuals may be recognisable to those who know them. This issue posed a great dilemma in the current study, since some of the targeted units (i.e. ICU, the DDI and the DFE/CCU) could not be anonymised, due to their singularity within the case. Indeed, unlike the police stations where multiplicity of this type of police component in the case enabled the anonymisation of the selected units without affecting the quality of the research, hiding the names of these units would have rendered any discussion of the findings relating to them meaningless. In an attempt to overcome this dilemma, additional measures were taken to protect the confidentiality of the participants in those units in reporting of the findings. These included, as Yin (2009) has advised, reporting only a cross-unit analysis and avoiding attributing any particular point of view or comment to a single individual or providing a full insight into officers' practice.

Finally, Bulmer (2002) points out that publication of the research is an issue of ethical concern, and participants should be informed in advance how and to whom materials will be disseminated. Taking this into account, it was agreed early in the fieldwork that the materials and data collected would be used for academic purposes and published in an academic thesis.

Having discussed how ethics were carefully addressed throughout the research, let us now conclude this chapter by discussing some important issues in research methodology. These are validity, reliability and generalisability.

3.11 Validity, Reliability and Generalisability

The case study strategy has enhanced the validity of the current study, helping to understand the phenomenon of the Saudi policing of Internet fraud as a whole within its real-life context. The high level of internal or ecological validity of case study, in the sense of its ability to capture authentically people's experiences, perceptions, beliefs and knowledge, is an advantage of this strategy as compared to, for example, experiments and surveys, according to Bryman (2008). Other strategies such as survey, whilst having high technical validity, may be far from reflecting the reality of experience in a natural context. Yin (2009) similarly asserts the high internal validity possible with case study.

The use of two data collection methods, observation and interview, further contributed to the validity of this research. Both methods provided deep, contextualised data that greatly enriched our understanding of how online fraud is policed in Saudi Arabia and in particular the way it is subjectively perceived and interpreted by officers in specific circumstances. The combining of methods also enhanced the accuracy of the data since each method helped to reinforce, explain and occasionally correct information and interpretations obtained via the other.

Nevertheless, it must be acknowledged that, like other qualitative methods, case studies have been challenged in terms of external validity, reliability or generalisability. External validity concerns the extent to which a study's findings can be generalised (Yin, 2009), and it is often said that, however deep an understanding is obtained of a particular case, this is not a satisfactory basis for generalising more widely. Punch (1998) similarly draws attention to the difficulty of generalising results based on the study of only one or a small number of cases. A response to such criticism is that case research does not aim at generalisation, but at understanding of the cases investigated in context (Punch, 2005; Stake, 1995). Further, they argue that excessive concern with generalisation may distract the researcher’s attention from features that are critical to illuminate the case itself (Denzin and Lincoln, 2000).

Despite focusing on one phenomenon (i.e. policing Internet fraud in Saudi Arabia), using one case (Riyadh), the findings of the current study can be generalised. This is because generalisation in case study research is of a different kind from that in survey research. Whereas the latter might seek generalisation from statistical samples, this is not the only generalisation, and is not universally applicable (Gummesson, 2000). ‘Statistical generalisation’ needs to be distinguished from ‘analytic or theoretical generalisation’ (Blaikie, 2000; De Vaus, 2001; Yin 2009). Statistical generalisation involves drawing conclusions about a population based on empirical data collected about a sample. This type of generalisation is the usual approach in surveys or analysis of archive data, but it is not appropriate for case study strategies, since cases differ from sampling units (Blaikie, 2000; Cassell and Symon, 1994; Yin, 2009).

The other approach to generalisation is to generalise from a study to a theory (Punch, 2005; Yin, 2009). Instead of drawing inferences about the wider population, as in statistical generalisation, a researcher is aiming to relate a particular set of results to some broader theory. In Punch’s (2005) view, this can be done in two main ways. One is by conceptualising, the other is by developing theoretical propositions. He maintains that for identifying the important aspects of a new research topic, developing an understanding of them, and conceptualising them for further case study is often the most effective strategy.

Based on the above discussion, it is not the purpose of the current study to generalise to other police organisations in different parts of Saudi Arabia (statistical generalisation). The case (i.e. Riyadh police) was not considered to be a representative sampling unit, as in surveys. Rather, it was selected to provide a real-life context to examine and understand the policing of Internet fraud in Saudi Arabia and therefore achieve the study aims and objectives. However, as the study contributed to an intensive examination of police response to online fraud as a new topic in Saudi Arabia, to capture a deep understanding of it within its real-life context, and to develop new concepts that will help to explain some of its aspects, it has the potential to inform future research on this area of policing in different regions of the Kingdom and in other similar contexts (theoretical generalisation).

3.12 Summary

As Punch (2005) points out, the coherence of the components of a research design is important for validity. The onion metaphor was therefore employed as a guide to decision making, and in this way integrity and consistency were maintained among its components. An interpretative epistemological position was adopted consistent with the exploratory nature of the research questions and objectives. This was implemented by a qualitative approach that focused on eliciting meaning rather than facts, and deep insights into Saudi police officers' attitudes and behaviour in relation to Internet fraud were obtained by means of an embedded single-case study strategy, in which the research phenomenon was viewed within its real-life context. Consistent with this epistemological position, approach and strategy, participant observation and semi-structured interviews were employed to collect the required data. The information gathered was analysed and interpreted in an iterative process, generating significant and interesting findings. Finally, due consideration was given to access and ethical issues throughout the research.

The research methodology adopted for the present study enabled the researcher to develop a rounded picture of the policing system applied by the police in a Saudi Arabian city for dealing with Internet fraud. The next three chapters report the empirical findings of the research before discussing, in the final chapter, their implications for both theory and policy.

Chapter Four

Saudi State Response to Internet Fraud: Symbolic Gestures or Adaptive Strategies?

Chapter Four: Saudi State Response to Internet Fraud: Symbolic Gestures or Adaptive Strategies?

4.1 Introduction

The literature reviewed in Chapter Two of this thesis suggests that states' response to the predicament created by the emergence of cybercrimes, such as Internet fraud, and the limitations of criminal justice agencies, particularly the police, in handling this novel form of criminality straddles the two contradictory aspects of crime control in late modernity highlighted by Western writers, such as Garland (1996, 2001). On the one hand, governments have adopted a sovereign state approach that seeks to reassert the state's power to control cybercrime through, for example, the establishment of specialist police units dedicated to responding to computer crimes. However, at the same time, there has been an attempt to adapt to the state's limitations in respect of cybercrime control, and thus develop pragmatic strategies which emphasise prevention and partnership.

Drawing on the data collected for the current research, this chapter seeks to assess the extent to which the Saudi state response to Internet fraud fits in with contemporary debates, in the Western-dominated literature, on cybercrime control within a late-modern penal framework. To achieve this aim, the chapter starts with an examination of the scope of the problem of Internet fraud in Saudi society, followed by a detailed analysis of the law – the Anti-Cybercrime Law – introduced recently to address Internet fraud as well as other forms of information technology-related illicit activity. Next, the introduction of the Informational Crime Unit, as a sovereign state approach in the Saudi government response to cybercrime, is explored. Finally, the chapter provides an account of the extent and nature of adaptive strategies in the policing of Internet fraud.

4.2 A Response to a Growing Internet Fraud Problem?

The Ministry of Communications and Information Technology (MCIT) reporting to the 2003 World Summit on Information Society (WSIS) indicates the enthusiasm of successive Saudi governments to modernise the country and promote the use of new technologies. Evidence includes the considerable attention to information technology development in its development plans, the restructuring of the Telecommunications Authority, and the introduction of several electronic information interchange projects, such as the e-Government Project, the Smart Card Project, and the Omrah Project for streamlining the process of issuing visas electronically (MCIT, 2003). The flourishing computer industry that has developed in the Kingdom of Saudi Arabia can be seen, then, as a reflection of its government's policy to promote the adoption of information technology in all facets of life. It has been suggested that 40 per cent of all computers sold in the Middle East ended up in Saudi Arabia (*The Independent*, 17th June 2001, cited in Gazzaz, 2006: 93).

As a consequence of all the above mentioned developments, there has been a monumental growth of Internet usage in Saudi society. The 2007 census estimated that 41.30 per cent of all Saudi households had members who used the Internet (Ministry of Economy and Planning, 2007). According to Gazzaz (2006), the Internet has transformed lifestyles in Saudi Arabia in areas such as Internet shopping and social interaction through online chatting. Moreover, he found that Saudis interacted not only with local Internet contents but also with those originating from different countries and different cultures. Locations of Internet use include homes, places of work, universities and Internet cafes. Sait et al. (2007) support the findings of Gazzaz (2006). They reported that, despite being a relatively new phenomenon in Saudi Arabia, the Internet is spreading across a broad spectrum of the Saudi population. They also documented that the respondents of their research spent a considerable amount of time on Internet activities.

The exponential growth of the Internet in the Saudi society, as observed by Gazzaz (2006) and Sait et al. (2007), raises concern about cybercrime and misuse of the Internet. This proliferation of Saudi communications infrastructure will widen usage, not only by innocent users, but also by criminals. It is also likely to expose a large section of the Saudi population to the risks of various forms of fraudulent activity emanating from cyberspace.

However, with the Internet in its early stages in Saudi Arabia, active online fraud in the Kingdom has not been extensively covered in official statistics or academic research. It is thus extremely difficult to assess the extent and nature of this form of cyber-criminality in the Saudi context. There has been, at the time of writing, only one empirical study which aimed to measure the pervasiveness of cybercriminal activities in the Kingdom. The study, titled *Internet Crimes in the Saudi Society*, was carried out by Alminshawi (2003), who used a web-based survey distributed via King Abdulaziz City for Science and Technology (KACST). Evidence gathered in Alminshawi's research suggested that there was only minimal fraudulent activity within, or propagated outwardly from, Saudi Arabia. The study showed, for instance, that 186 participants (5.3 per cent), of whom 82 per cent were Saudis, claimed to have been subject to deceptive attempts via the Internet (Alminshawi, 2003: 189-207).

It should be noted, however, that Alminshawi's research, whose data were collected over the period from January until April 2002, was undertaken when Internet usage was still in its infancy in the Saudi society and the numbers of users accessing the new technology were, therefore, limited. Saudi Arabia is now, however, entering a new era in which a large proportion of the Saudi population, encouraged by the increasing availability of broadband connections and the decrease in subscription fees, are becoming regular users of the Internet. Consequently, the potential for Internet-related criminal activities, mainly online fraud and deception, in the kingdom is even greater (El-Guindy, 2008).

However, while there is as yet not enough reliable data available to compare the progress of Internet users and Internet fraud in Saudi society, concerns have been voiced, particularly in the press, about an increase in Internet fraud incidents. For example, on 24th October 2005, *Asharq Al Awsat* newspaper reported a warning which had been issued by the Saudi Ministry of Trade and Industry to Saudi citizens about a dramatic increase in cases of Internet fraud. The report indicated that officials issued the warning after a rise in complaints from Saudis about online scams. Saudi officials were said to have attributed the increase to lack of knowledge about information technology (*Asharq Al Awsat,* October 24th, 2005).

Moreover, El-Guindy (2008) claims that Saudi Arabia is ranked as the leading country in the Middle East as the target and source of malicious activities online and ranked number 38 worldwide. Also, Saudi Arabia is alleged by El-Guindy to be the number one source of malicious attacks in the Gulf Cooperation Council (GCC). This was confirmed by an official at the Saudi Ministry of Interior, who noted that a large number of Saudis were involved in hacking. In a press statement published on the 24th of September 2007, the official, who is the adviser for information technology (IT) security at the ministry, said that financial crimes with the use of technology, including Internet fraud, are costing Saudi Arabia millions of dollars annually (Al-Hakeem, 2007).

According to *Al-Ryiadh* daily, reports of e-payment frauds have been commonplace in Saudi Arabia, accompanying the expansion of e-banking services in the Kingdom and the dramatic growth of users of these services over the past few years. A banking expert was quoted as stating that phishing scams, in the form of e-mails purporting to be from the customer's bank, have been successful in trapping many customers of banks in Saudi Arabia into revealing confidential information, such as account number or PIN. In consequence, substantial losses have been suffered by both customers and banks. He also pointed out that although the losses are estimated to be millions of SA Riyals, exact figures are yet to be published by the affected banks as they fear that this could shake customers' confidence in the security of their e-banking services (*Al-Ryiadh Daily*, 10th October, 2007).

Undeniably, the press reports outlined above signify a concern in Saudi society about Internet fraud. However, a judgement that Internet fraud is in the ascendency cannot be based solely on journalistic sources. As Reiner (2002) points out, there has been an endless debate in the literature on whether the extent to which crimes are featured in news represent their incidence in society, and the media have often been accused of amplifying the crime problem in order to generate support for repressive solutions (see for example Carrabine et al. 2002; Brown 2003; Jewkes 2004; Greer 2005). To measure the extent of Internet fraud, official sources, such as data produced by the police, as well as unofficial methods, such as self-report crime and victimisation surveys, are needed. These, however, are currently unavailable in the Saudi context. Crime statistics in Saudi Arabia, unlike in the UK and most other countries, are considered classified data. They are, therefore, accessible only by officials and policymakers within the government and not available to a wider audience, such as the news media, academics and other researchers. Moreover, attempts made by some researchers to conduct crime surveys have also been blocked by the Saudi authorities. For example, Souryal (1988) reports an attempt to conduct a mail survey or an opinion poll with the aim of validating the Saudi official data presented in the report of the United Nations' Secretary General on crime prevention in 1977, but adds that his attempt 'was shunned by the officials on the grounds of stirring public doubts' (1988: 11).

Similarly in the current research, the task of reviewing police crime statistics proved to be very problematic. Despite the painstaking efforts exerted to achieve such an objective, access was granted to crime data for Riyadh only and not for the entire Kingdom, thanks to the cooperation of the Riyadh Police management who, unlike the DPS's Statistics Department, showed an understanding of the importance of such data for the research objectives. This access was not, however, without restrictions, as permission was given to view crime statistics covering only the last three years prior to the research. Moreover, the researcher was requested to sign a written undertaking that only the figures pertaining to the crime in question, i.e. Internet fraud, be published in the thesis.

Given the difficulties encountered, as explained above, in building a wider picture of the scope of online fraudulent activity in Saudi society at large, the focus will be narrowed in the remainder of this section to concentrate on the situation in Riyadh. To this end, the extent of Internet fraud in Riyadh as viewed by police officers will be discussed, providing a contrasting base for the analysis of the representation of this type of criminal behaviour in the police-compiled data obtained for the Riyadh area.

4.2.1 Extent of Internet Fraud in Riyadh as Viewed by Police Officers

Police officers spoken to in the current research were significantly divided in their perceptions of the extent of the problem of Internet fraud. Over half (57.5 % N=23) of the participating officers saw online fraudulent activity as a growing phenomenon, affecting an increasing number of people from different categories of Saudi society. Some respondents asserted that the incidence of Internet fraud has exceeded that of many other forms of criminality. One senior officer at the Riyadh Police headquarters went so far as to claim that incidents in which complainants reported falling victim to an Internet scam have come to constitute half of all the crimes reported to the police stations in the city. This view of Internet fraud as an increasing problem was corroborated by officers in three of the five participating police stations. These officers indicated a noticeable rise in complaints about Internet fraud, especially in the two years prior to the research. For example, the Chief Investigator in a city-centre location said:

> Previously, complaints brought to us about Internet fraud used to be quite rare. But since the beginning of 2007, they have started to increase and we have begun to receive between 5 and 8 cases a month. In the last month, the number jumped suddenly and we received 10 complaints in one week alone (PS7).

In another site, the head of the station voiced a similar concern about the increasing frequency with which Internet fraud incidents were being reported to his station. He mentioned that he was so worried about the extent of this crime that he had written a report to the higher authorities to draw their attention to the problem and suggested setting up a media campaign to raise awareness among citizens regarding this type of criminal activity.

In contrast, a similar perception of Internet fraud as a growing problem was not echoed by respondents in two of the participating police stations. Officers in these sites, although believing that Internet fraud represented a considerable challenge for them qualitatively, were not unduly concerned about it from a quantitative perspective. Rather, they thought that Internet-related crimes, including cyber-fraud, were encountered less frequently than other forms of criminal behaviour. Internet fraud incidents were very often described by such officers as being ‘few’ or ‘of a limited number’. ‘It is a once-a-month crime’ is another phrase which was also used by an officer working in a station located on the western side of the city (PS24) to indicate that Internet fraud was experienced only intermittently and not on a scale comparable to that of other crimes. Officers from the other police station reported an even lower rate of Internet fraud incidents being brought to their attention. For example, one officer, who did not seem to be particularly worried about the current level of online fraudulent activity, said:

> Thankfully, we do not usually have many complaints regarding Internet fraud at our station. The last case we received here was more than three months ago. The level of Internet fraud has never been as much a concern for us as have those of crimes like burglary, physical assaults or crimes against morality (PS4).

An observation worthy of highlighting, however, is that some officers, while reporting limited experience of dealing with Internet fraud incidents in their daily work at their station, still believed that other stations might have been encountering larger numbers of such criminal acts. They ascribed the apparent low rate of cases reported to their stations to the demographics of the areas covered by these stations, namely, the eastern and southern districts. They largely perceived these as populated predominantly by communities whose economic situation and level of education would not be conducive to intensive usage of the Internet. This, the officers thought, reduced the likelihood of their being exposed to online fraudulent activity, in comparison to those living in other more affluent neighbourhoods. The quotations provided below are characteristic of these officers’ explicit remarks on the supposed connection between the level of Internet fraud incidents received at the police stations in these areas and the social stratification of their population:

> You know the kind of people living in [the neighbourhood lying within the jurisdiction of the police station]. They are mostly Bedouin and poor, and therefore they don't have the luxury to possess computers or use the Internet. It is not like, for example, the North or the Centre, where even children have their own laptops and Internet [access] (PS3).
>
> Perhaps the only advantage of working in a station located in an area such as this is that you don't get as much high-tech crime, because most people here are not used to using technology (PS4).

Clearly, the officers who made the previous comments seemed to be convinced that the low incidence of victimisations by Internet fraud reported within their jurisdictions was merely a reflection of a digital divide between different parts of the city, with the areas where they worked being on the disadvantaged side of this divide.

The view held by officers interviewed in the stations of the eastern and western sides of the city that Internet fraud cases were being more widely encountered in stations located in more affluent neighbourhoods appeared to be founded on hearsay, based on conversations with colleagues from those stations in their off-duty meetings. As one respondent explained:

> I meet colleagues from [two more developed districts] stations nearly every evening in *El-Istiraha* and they've often told me that they get complaints from victims of this crime very often, some of them even twice or three times a week (PS5).

'*El-Istiraha*' referred to by this officer is a place of relaxation, usually built on the outskirts of the city and provided with leisure facilities. It has become a common practice in Saudi society in recent years for a group of people with a particular affinity, such as relatives, friends or people from the same profession, to rent such a place (though it can sometimes be owned, individually, by one member of the group who shares it with the others, or collectively by all or some members of the group) to meet on a daily, weekly or monthly basis to spend their free time. Obviously, such meetings have become important social events, in which people, inter alia, exchange experiences on different aspects of life. These social contacts provided opportunities for police officers to develop a general knowledge, informally, of what is going on in each other's departments and, by implication, form a perception of the extent of any criminal activity, including Internet fraud, even beyond the boundaries of their jurisdictions.

A widespread view, frequently expressed by the research participants, is that Internet fraud would be a far more visible problem, if everyone who fell victim to it acknowledged their victimisation and approached the police to request their assistance. Thirty one (77.5%) of the officers interviewed were insistent that most of those victimised by Internet fraud will be unwilling to report it to the police because of embarrassment, especially when the reporting is likely to reveal the immorality of the victim, or because they do not want to be stigmatised as being stupid. This assumption is emphasised in the following quotation with regard to one particular form of Internet fraud:

> When a person gets defrauded as a result of getting involved in an indecent relationship on the Internet, where he or she has been tricked into sending obscene photos of him or herself to the fraudster and gets blackmailed, would you expect that person to come to the police and tell them about both the obscenity and his/her foolishness? Absolutely not. As long as they have the money, they will continue to pay the fraudster to buy their reputation. It’s only when they can no longer pay that victims proceed to us to report the fraud (DDI2).

Reluctance to report victimisation of Internet fraud is not restricted, according to respondents, to private individuals, but also applies to corporate businesses who may be inhibited from admitting their victimisation for fear of adverse publicity or damage to their reputation. In this respect, many officers pointed specifically to the banking sector. They stated, based on stories told to them by inside sources, that many banks have recently been subject to fraudulent hacking on numerous occasions. However, the police were never involved and the banks addressed the matter simply by indemnifying customers against the losses that resulted from the frauds. In the opinion of these officers, the victimised banks did not involve the police because they were fearful that publicising their systems’ vulnerabilities might deter clients from adopting the Internet banking services which they (and other Saudi banks) are currently promoting as part of their strategies to cut costs and meet competitive challenges, among other objectives. Several narratives described this approach by banks; the following is a typical example:

> I have a friend who works in Al…. Bank. He told me that last month the bank had an incident in which a hacker managed to infiltrate the *Mahafid* [online financial wallets] of five of the bank’s clients, sell their stocks and transfer the money to an account outside the country. When these clients realised that their *Mahafid* had been emptied of both shares and money, they came one after another to complain to the bank. Apparently, the bank found that a loophole in their control system had enabled the hacking to take place. They then covered it up. The clients were reimbursed a total of SR3.5 million. The police were never informed. The bank did so because if other clients knew about it they would lose confidence in the security of the bank’s electronic share trading system and probably begin to look for other banks with stronger security systems (PS11).

It seems that, in order to examine the dark figure of online fraudulent activity that escapes the attention of the police, independent research, which can be designed to capture patterns of crime reporting behaviour among individual as well as corporate victims of Internet fraud, needs to be conducted. Self-reporting victimisation surveys are the best-known instruments that can be used to serve such a purpose. The issue of reporting Internet fraud will be returned to later in Chapter Six, with more focus on the police crime reporting system in the studied area and its role in encouraging, or otherwise, victims of Internet fraud to report their victimisation.

The evidence documented so far demonstrates that despite the relative newness of this type of high-tech deviance in the Saudi context, Internet fraud has been perceived by police officers (whether based on actual or vicarious experience) as a phenomenon that is increasing in prevalence and scope. It is not clear, however, whether the respondents' views on the extent of Internet fraudulent activities reflect their actual incidence. Nevertheless, we can at least say that this is how the problem presented itself to police officers and examine the data further in this light. At this point, it is interesting that the perceptions from the officers tally with police records. Thus, the manifestation of Internet fraud in the police official crime data will be considered in what follows.

4.2.2 Internet Fraud in Riyadh Police Official Statistics

Before proceeding to analyse the statistics, an important methodological issue which was encountered with these statistics should be highlighted. The data afforded to the researcher had been prepared based on the *Hijri*[10] calendar, with no mention of the corresponding dates in the Gregorian calendar. Therefore, since the thesis is prepared and presented in a Western country (the UK), a date conversion had to be performed to specify the Gregorian dates corresponding to the period covered by the statistics obtained from the Statistics Unit. A special date convertor software on the Internet was used for this purpose. This showed that the years 1427, 1428 and 1429 in the *Hijri* calendar coincided almost exactly with the Gregorian years of 2006, 2007 and 2008 respectively, as it was found that the first day of 1427 happened to be January 31th, 2006, while the last day of 1429 corresponded with December 28th, 2008. Hence, it is only the Gregorian years – 2006, 2007 and 2008 – which will be used in the following discussion of the crime statistics.

[10] The *Hijri* date is the Islamic calendar. It started in the lunar year in which Prophet Mohamed (peace and blessings be upon him) migrated from Makkah to Al-Madinah.

Crimes in the Riyadh Police's official statistics were classified into ten major categories. These were: murder and assault; immorality crimes; property crimes; intoxicant crimes; faith desecration and crimes against religion; crimes against public order; terrorism; arson; administrative contravention; and riots[11]. While fraud in general was listed under the major category of Property Crime in the crime reports, Internet fraud was not included as one of the index crimes in these reports. This suggests that incidents of this form of fraud may have been recorded under the sub-category of general fraud. However, in 2008, an amendment was made to the crime classification in the recording system, creating a new category for high-tech crime to reflect the introduction of the Anti-Cybercrime Law. The new category was meant to encompass all types of criminal activity relating to the illegal use of computer and the Internet. Online fraudulent activity is one such, and thus Internet fraud incidents are supposed to have been recorded under this category. The review of the crime statistics below will consider general fraud first, and then move to the recorded high-tech crimes.

Table 4.1 illustrates the incidents of all types of fraud committed in Riyadh, the number of cases in which offenders were identified and the nationality of the known offenders over the three years from 2006-2008. From this table, it can be observed that the rate of fraud in Riyadh is rising. While, in 2006, fraud accounted for about 0.6 per cent of the total number of recorded crime, the number of fraud events and their ratio to the total crime figure increased steadily over the following two years. The same table reveals that offenders were identified in almost two thirds of the cases recorded in 2006; the number was slightly lower, however, in subsequent years, as the data show that only over half the cases were registered with known offenders in both 2007 and 2008. Moreover, among known offenders, the percentage of native offenders exceeded that of non-Saudi in all three years. Interestingly, when we compare the number of events in which the police were able to establish the identity of the offender(s) with the number of these known offenders, we find that there are noticeable differences, with the number of offenders being significantly bigger in each of the three years. This phenomenon may suggest that the frauds were committed not only by individuals but also by criminal groups.

[11] This crime classification is standardised by the Central Statistics Department at the DPS and implemented by all Provincial Police Departments across the Kingdom of Saudi Arabia.

Table 4.1 Fraud crimes recorded by police in Riyadh (2006-2008)

Year	N.	% (of total crime)	Offender(s) known		Offender(s) unknown		Nationality of known offender(s)			
			N.	%	N.	%	Saudi		Non-Saudi	
							N.	%	N.	%
2006	168	0.598	108	64.28	60	35.72	85	61.59	53	38.41
2007	180	0.667	99	55	81	45	72	66.05	37	33.95
2008	199	0.694	119	59.79	80	40.21	108	72.48	41	27.52
Total	547	1.959	326	179.07	221	120.93	265	200.12	131	99.88

Source: obtained by the researcher from the Riyadh Police/Criminal Statistics Unit by a personal request.

However, the absence of any reference, in the above data, to the modus operandi of the crime in regard to the role of computers and the Internet prevents identification of Internet-related incidents from recorded fraud statistics. Description of Internet fraud offending is submerged beneath aggregate fraud offending statistics. Moreover, the data are not informative about such factors as age, sex, nationality and occupation of offenders – factors known to be related to crime rates. Nor do they take into account the location of the incident by indicating where it was discovered or reported. Further to this, information on victims is completely absent in these data, which also do not cover the values (monies lost or at risk from being lost) of the cases of reported fraud. Instead of illuminating the problem, police records are thus contributing to the invisibility surrounding Internet fraud offending.

Contrary to our expectations, some respondents in the current study appeared not to lament the omission of details on the modus operandi of the crime from the data provided in the crime reports. For instance, one senior officer from the Riyadh Police, while confirming that such details are recorded in the case file, said:

> It is really difficult to make categories for crime based on the method used for its commission. For instance murder could be committed by too many means, such as strangling, burning, shooting, etc. If murder is going to be categorised based on the method used this will require a tome. The same applies to fraud, and so such a categorisation is practically impossible in the crime statistics (SO2).

It is evident from the above that police's concern in crime data is reduced to providing counts of crime and criminals, limiting the utility of such data for solving crime and informing public policy.

Turning now to focus more specifically on high-tech crime, statistics show that in 2008, the year in which the recording system were redefined to include an independent category for crimes involving the use of computer and the Internet, five events were recorded as high-tech crime, representing less than one percent (0.016%) of the total crime figure. Data also show that in none of all the recorded high-tech crime incidents did the offender(s) become known to investigators.

Once again, detailed data are lacking in this report to check which of the events recorded as high-tech crime related directly to Internet fraud. Nevertheless, even if all the incidents of high-tech crimes recorded in that year were to be considered Internet fraud, this figure appears to be substantially at odds with police officers' actual experience of incidents of this type of criminality as reported earlier in this chapter. As we have already seen, the overall picture depicted by respondents for the scale of Internet fraud incidents appears to suggest that they were being encountered at rates much higher than the above-illustrated numbers might signify. The mismatch between estimates of Internet fraud in the two data sources indicate that there has been a recording shortfall.

A finding which emanated from analysis of case files might account for some of the discrepancy. This finding shows that officers' subjective definition of the crime may have influenced their crime recording practice, with the result that many Internet fraud incidents were not recorded in accordance with the newly implemented reclassification of crime categories. Examining crime details recorded on case file for a sample of fraud incidents investigated during 2008 revealed a number of instances where the Internet was used in the commission of the fraud, but the incident was recorded as a conventional fraud. This prevented it from being counted in police crime statistics as a high-tech crime. During a conversation with several officers from one of the stations in which the mentioned case files were checked, the author queried why such cases were recorded as (plain) fraud although the Internet was used in performing the deception. It was the consensus of the attending officers that *fraud remains fraud, however it is committed*. This indicates that despite changes in legislation, represented by the enactment of the Anti-Cybercrime Law, and the police response to them by creating a new category in their recording system for high-tech crime, some officers continue to take a technology-neutral approach to offences.

At this point, we can see from the evidence detailed in the preceding analysis that the representation of Internet fraud in the crime records produced by the Riyadh Police is misleading. This supports the claims made in the criminological literature that police-generated data tend to be too unreliable a source to gain accurate counts of criminal events brought to the attention of the police (see, e.g., Sellin and Wolfgang, 1964; Bottomley and Coleman, 1981; O'Brien, 1985; Bottomley and Pease, 1986; Biderman and Lynch, 1991; Hope, 2005).

It seems, then, that the incidence of Internet fraud is likely to have been underrepresented in the statistics produced by the government agency. Evidence from Riyadh police district showed that in some departments, at least, Internet fraud was perceived to be a growing problem. Nevertheless, whether due to misclassification or any other reason, official statistics do not reflect this phenomenon as experienced by officers on the ground. Since official data do not present a picture of a serious and escalating crime problem, it may be doubted whether the Saudi state's action towards such crime can be explained in these terms. What seems more likely is that, as will be elaborated in forthcoming discussion, strategic political and economic objectives related to protecting the Kingdom's image in the eyes of the international community, and especially potential investors, provided reasons why a prompt and visible response was required. These, rather than fears induced by a manifest and acknowledged crime wave, seem to be more plausible explanations for the legal and organisational measures introduced by the Saudi state and its social control agencies in relation to Internet fraud.

4.3 A New Cybercrime Law

Issued under the Council of Ministers resolution No. (74) dated 05/01/1428H (corresponding to 12/03/2007) and approved pursuant to the Royal Decree No. (M/12) dated 12/01/1428H (corresponding to 26/03/2007), the Anti-Cybercrime Law is the Kingdom's first set of laws designed to combat cybercrimes. Prior to the introduction of this resolution, judgement in cybercrime cases heard in the General Courts, which are ruled by Islamic law, was left to the judge's discretion. The law, which was drawn up by the Kingdom's Commission for Telecommunications and Information Technology, was first passed by Saudi Arabia's legislative body, the *Shoura* (consultative) Council.

Many Saudi experts have expressed favourable comments about the new law, hoping that it will bridge the legal gap in this area and put a curb on cybercrime. Their optimism, they argue, stems from the law's apparent efficiency in deterring cybercriminals with its tough punishments, as well as its potential ability to intercept future cybercrimes not yet discovered (*Al-Riyadh Daily*, 14th February, 2008). Such statements reflect an assumption among those experts, at least, which interprets the enactment of the new law as merely a step that has been taken by the Saudi state towards combating Internet fraud and other forms of cybercrimes, after recognising the growing threat that such criminal behaviours pose to Saudi society. However, the validity of such an assumption becomes questionable when considering the National Communications and Information Technology Plan (NCITP), which was drawn up by the Ministry of Communications and Information Technology (MCIT) in 2005. The NCITP, which represents the framework within which ICT can be managed, planned for, and utilised, sets out the Saudi government's vision towards the information society and states its general objectives in this area. The details of projects and mechanisms for realising these objectives are also described in the NCITP. The second general objective of the NCITP long-term vision seeks 'to regulate the ICT sector in a form that guarantees impartiality, stimulates and attracts investments', and 'formulating a regulation for ICT crimes' is pinpointed as one of the projects for implementing this objective (MCIT, 2005: 39-40). In this context, it is apparent that, by introducing the Anti-Cybercrime Law, the Saudi state is concerned not so much with controlling cybercrime as with achieving economic development through implementing policies that provide reassurance of safety and security to investors.

The purposes behind its creation aside, let us now consider the Anti-Cybercrime Law[12]. In brief, the Law consists of sixteen articles, of which the first defines the terms used in the Law and the second expresses the objectives underlying its enactment. The Law is said to be intended to provide legal and regulatory standards to combat information, computer and Internet crimes by identifying such crimes and specifying the penalty for each, in order to: 1) maintain information security; 2) safeguard the rights associated with legitimate use of computers and computer networks; 3) protect the public interest, morals, and communal values; and 4) develop and safeguard the National Economy (CITC, 2007a).

Articles 3 to 13 address the determination of punishable cybercrimes and specification of the relevant sanctions. The last three articles define the duties of the law enforcement agencies in respect of the Law.

The Anti-Cybercrime Law contains no specific definitions of Internet fraud, although it is encompassed in the broad definition of cybercrime contained in Article 1

[12] A full, official translation of the Saudi Anti-Cybercrime Act is available at: http://www.citc.gov.sa/English/RulesandSystems/CITCSyste/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf

(8) as ‘any action which involves the use of computers or computer networks, in violation of the provisions of this Law’ (CITC, 2007a: unpaginated). The breadth and inclusivity of this definition also provide the flexibility to embrace any new forms of cybercrime that might emerge in the future (Algarni, 2011).

The criticism could, nevertheless, be raised that by referring to certain forms of cybercrime, the Law could potentially cause confusion as to whether it covers forms of Internet fraud not mentioned (Algarni, 2011). The specifically mentioned violations are:

> 1. Acquisition of movable property or bonds for oneself or others or signing such bonds through fraud or use of false name or identity.
>
> 2. Illegally accessing bank or credit data, or data pertaining to ownership of securities with the intention of obtaining data, information, funds or services offered (Article 4) (CITC, 2007a: unpaginated).

As Algarni (2011) points out, this constitutes a weakness in the law and leaves scope for possible misinterpretation. The inadequacy of the Anti-Cybercrime Law in respect of Internet fraud was emphasised in an examination by the Saudi Communication and Information Technology Commission (CITC) of the way the issue of spam is addressed in current enactments. It was pointed out that spam messages are not fully addressed in the Law, and attention was drawn to significant lacunae in the Law’s handling of this and other forms of Internet fraud. For example, although the Law prohibits certain types of content in electronic messages, it does not explicitly concern itself with unsolicited commercial messages, although these are a major form of spam. The CITC criticises the Law for not explicitly defining spam and unsolicited commercial advertisements, clarifying what consent is required, and setting out criteria for legitimate messaging (CITC, 2007b, cited in Algarni, 2011: 10). Asserting the nuisance of spam and the threat it poses to Internet and communications infrastructure, applications, computer users in general and users of the Internet in particular, the report notes that in the Kingdom of Saudi Arabia itself, spam has been used for malicious purposes including phishing, spreading viruses and fraud.

As Algarni (2011) points out, such problems have been recognised and addressed in a variety of regional and international laws, such as the recent reform of the UK Fraud Act 2006. The revision incorporates a provision intended to clarify existing laws, covering phishing attacks. In order to reinforce the existing law and make prosecution easier, the new provision makes the act of sending such emails, without the need for any proof of deception or obtaining of any property, liable to prosecution (Savirimuthu and Savirimuthu, 2007, cited in Algarni, 2011: 10).

The United States of America introduced the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, which imposed limitations and set out sanctions regarding the sending of unsolicited commercial electronic mail via the Internet. In Section Four of the Act, Chapter 47 of Title 18, United States Code, was amended by the addition of Section 1037, whereby the use of a protected computer for the distribution of multiple commercial electronic mail messages while intentionally misleading recipients, or service providers, as to their origins is punishable with a fine and/or imprisonment. Another example is Pakistan's Prevention of Electronic Crimes Ordinance, 2007, which contains a provision explicitly defining the offence of spamming, which covers the transmission of multiple misleading or unsolicited electronic messages without the express permission of the recipient (Article Fourteen, Subsection One) and goes on in the following subsection to specify a penalty of a fine of up to fifty thousand rupees for a first offence and of three months imprisonment and/or a fine for subsequent offences (Algarni, 2011: 10).

In contrast to these examples, the Saudi Anti-Cybercrime Law does not deal directly with spamming and related matters; it contains no definition of spamming or clarity whether unsolicited commercial messages fall into this category. Nor does it set out basic criteria for the legitimacy of commercial messages, such as the option for users to request the sender to cease sending such messages. No punishments are specified for the transmission of unsolicited commercial messages, should this be held to constitute a spamming offence (CITC, 2007, cited in Algarni, 2011: 11).

In a previous work (Algarni, 2011), the author has identified three types of penalties imposed by the Saudi Anti-Cybercrime Law for perpetrators of Internet fraud: imprisonment, fines and confiscation. The first two are set out in Article 4, which renders the perpetration of any of the offences referred to in the article liable to either or both a prison term of up to three years and a fine of up to SR two million, payable to the treasury. It is noteworthy that, while maximum penalties are specified, no minimum is stipulated, which can be considered a serious weakness of the Law. Failure to make such a determination, thereby bringing the matter within the personal discretion of the judge, could result in disproportion between sentences and the seriousness of the offence. The third of the identified types of penalty, confiscation, is provided for in

Article 13, which provides for the seizure, in all cases, of all hardware, software and other means employed in commission of specified offences and confiscation of the money earned as a result of such crimes. The article also provides for permanent or temporary closure of a site or project whose owner used or allowed it to be used for the relevant crimes.

Particular reference is made in the Law to Internet crimes involving criminal organisations. According to Article 8, commission of any of the offences specified in the Law through a criminal organisation is punishable by no less than half of the relevant maximum imprisonment term and/or fine stated. A similar penalty is provided for those who commit such an offence during the performance of a public job, exploit minors, or have been indicted, locally or internationally, for similar offences. Article 10 provides that an offender apprehended after initiation, but before completion of an offence stipulated in the Law, is liable to not more than half the maximum penalty for the crime in question. Article 11 of the Law empowers the relevant court with discretion to waive the stipulated penalty for offenders who inform the responsible authorities about the crime before they become aware of it, and before the harm occurs. In the event of such reporting taking place after the crime has come to the attention of the authorities, an exemption can be given only if the offender’s evidence is instrumental in capturing other criminals, if multiple offenders are involved, or in enabling equipment used in the crime to be seized.

A significant shortcoming of the Anti-Cybercrime Law is the absence of clearly specified enforcement mechanisms. It merely contains a provision that ‘the Communications and Information Technology Commission, pursuant to its powers, shall provide the assistance and technical support to competent security agencies during the Investigation stages of such crimes and during trial’ (Article 14) (CITC, 2007a: unpaginated). However, it can be argued (Algarni, 2001; CITC, 2007b) that in the absence of formal coordination mechanisms between relevant regulatory bodies, such as the Ministry of Interior, represented by the police, and the CITC, and given that the relevant authorities are not provided with cybercrime investigation specialists, the control of Internet fraud and other cybercrimes could be seriously hampered. The Law made no provision for the creation of a specialised agency with trained professionals and experts, despite purporting to address specialised types of offence. These weaknesses in respect of enforcement can be attributed to the composition of the body that drafted the Law, which was confined to lawyers and ICT advisors. The absence of members of the police community resulted in the lack of a law enforcement perspective in the drafting of the new law (Interview with the DPS's senior management representative).

A final limitation worth noting is that the Law addresses only offences originating within Saudi Arabia. Consequently, it shares with other similar laws the weakness that it will be ineffective with regard to fraudulent activities that originated in another country. Global cybercrime experts agree that effectively tackling cybercrime necessitates harmonisation of laws and law enforcement practices among states. This point is made by Phil Williams, who argues that:

> Harmonisation is necessary for both substantive and procedural laws. All countries have to reappraise and revise rules of evidence, search and seizure, electronic eavesdropping, and the like to cover digitised information, modern computer and communication systems, and the global nature of the Internet. Greater coordination of procedural laws, therefore, would facilitate cooperation in investigations that cover multiple jurisdictions (2001: unpaginated, quoted in Algarni, 2011: 12)

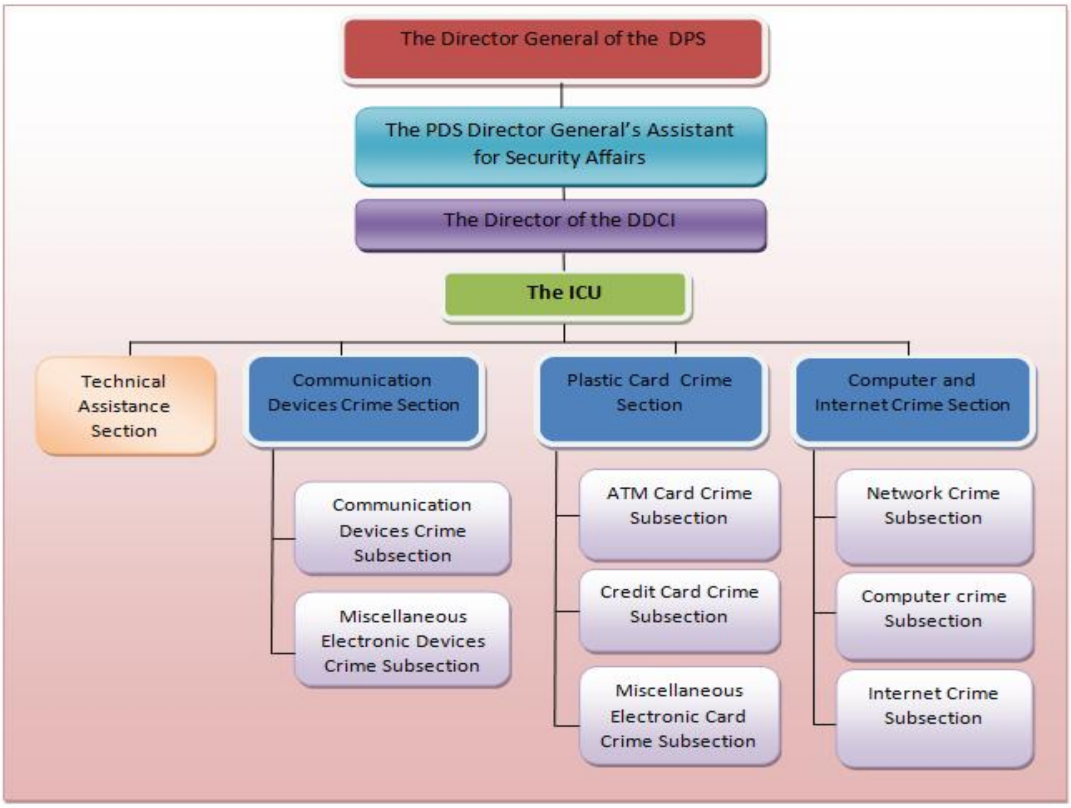
Harmonisation of global and local administrative procedural laws is an essential requirement that was overlooked by the drafters of the Saudi Anti-Cybercrime Law, which did not even refer to examples of local and international administrative policy and procedural issues already set out in the Saudi Criminal Procedural Code and the Convention on Cybercrime respectively.

From this analysis, the conclusion is inescapable that despite its status as the main legal reference for controlling Internet fraud in Saudi Arabia, the Anti-Cybercrime Law is far from comprehensive and indeed is deficient in relation to many aspects of Internet fraud. There are, clearly, also significant omissions in the Law in relation to jurisdiction and provision for enforcement. The impression is of a law that was introduced hurriedly, without sufficient prior research and forethought, and without the participation of those who could bring real experience and expertise to bear. Such a rushed and uninformed legislation process raises serious doubts as to whether tackling cybercrime was in fact the primary reason for the introduction of this law. Certainly, it can be said that until such lacunae are filled, the potential of the Law to effectively control deceptive and damaging Internet activities in Saudi Arabia will be severely constrained.

4.4 The Sovereign State Approach and the Formation of the Informational Crime Unit: Expressive Gestures to Reassure Investors?

The latest version of the DPS Organisation and Functions Guide, prepared by the DPS's Department of Planning and Development (DPS/DPD) (2009), indicates that a new department, called *The Informational Crime Unit* (ICU), has been created within the structure of the DPS. The ICU is hosted administratively by the Department of Detection and Criminal Intelligence (DDCI), which in turn is positioned under the direct supervision of the DPS General Director's Assistant for Security Affairs. The ICU comprises three main sections and an ancillary section, with each of the main sections having subsections (DPS/DPD, 2009). The organisational chart of the ICU is illustrated in Figure 4.1 below.

Figure 4.1 The ICU Organisational Structure and Its Position within the DPS


The Director General of the DPS
The PDS Director General's Assistant for Security Affairs
The Director of the DDCI
The ICU
Technical Assistance Section
Communication Devices Crime Section
Plastic Card Crime Section
Computer and Internet Crime Section
Communication Devices Crime Subsection
Miscellaneous Electronic Devices Crime Subsection
ATM Card Crime Subsection
Credit Card Crime Subsection
Miscellaneous Electronic Card Crime Subsection
Network Crime Subsection
Computer crime Subsection
Internet Crime Subsection

Source: Adapted from the DPS Organisation and Functions Guide prepared by the DPS's Department of Planning and Development (DPS/DPD) (2009).

In a statement made in May 2009 to announce that his administration was in the process of forming the ICU, the Director General of the DPS asserted that, as part of a national crackdown on cybercrimes, including Internet fraud, there needed to be a 'specialised department for policing electronic crime'. He went on to state that 'because web-related crime was posing a threat to public security, authorities needed to act to fight back'. The new unit, according to the Director General, would monitor computer crimes and explore means of pursuing those attempting to exploit technology for criminal purposes, such as blackmail, cyber threats, electronic theft and financial robbery. Specialists would be used to detect and arrest cyber criminals, he added, and the latest equipment would be used to find evidence and prosecute offenders (*Al-Watan Daily*, May 9th, 2009).

Clearly, this pronouncement by the DPS's Director General represents the type of rhetoric used by state actors in their attempts to reclaim the power of sovereign command. However, the evidence obtained for the current research suggests that while the formation of the ICU might be seen as a populist measure, designed to send a message to the public that the government was doing something about the cybercrime problem, it is also intended to boost the country's global image. Indeed, a dominant view amongst participating officers was that the reasons behind the decision to create the ICU and the timing of that decision should be seen as part of Saudi Arabia's strategy to expand its income sources by opening up business opportunities for foreign investment. For the advocates of this view, the formation of a policing unit specialised in electronic crime was meant to contribute to establishing a secure environment that would attract international investors to the Kingdom. The following quotation is representative of this view:

> As you know, the Kingdom has joined the World Trade Organisation recently, and by creating the ICU the MOI is implementing the Government's policy to show that our country is electronically a safe environment for investment, so that international banks would be encouraged to open branches here (ICU1).

Such an interpretation is supported by the NCITP, discussed in section 4.3, in which the stimulation and attraction of investment is explicitly stated to be among the purposes of the government's long-term vision for managing ICT, including the regulation of cybercrime (MCIT, 2005).

Another opinion, which was linked with the one stated above, perceived the establishment of the ICU as a reaction to the enactment of the Anti-Cybercrime Law. It was seen that there was a need for a body to enforce the provisions of the new law, which would 'give assurance to foreign investors that their businesses are protected against electronic crime by the existence of both a criminalising legislation and enforcement agency' (ICU3).

There were officers, however, who viewed the issue from a slightly different angle, although converging with the previous opinions on emphasising the influence of non-domestic concerns on the Saudi state's decision to create the ICU. For instance, one respondent insisted:

> The idea of setting up a specialist computer crime department might have been around for some time, but the MOI had to speed up the introduction of the ICU only to comply with the requirements of the Arab treaty that it has signed recently (ICU2).

The treaty alluded to in the above quotation is the Arab Treaty on Fighting Crimes of Information Technology, which was prepared and ratified, in 2006, by the Joint Council of Arab Interior and Justice Ministers. This treaty requires each member state to 'ensure the existence of a specialist body that is available 24/7 to provide instant assistance for investigations or procedures related to information technology, or for the collection of evidence in its electronic format in a particular crime' (Article 43).

4.4 Adaptive Strategies

So far, we have seen how concerns with enhancing the sovereignty of the state have shaped the Saudi government's approach towards responding to Internet fraud, through the introduction of a new cybercrime law and the formation of the ICU. This approach reflects the Saudi state's interest in old penology, as the emphasis in the new measures taken in 'the fight' against Internet fraud and other cybercrimes seems to be on managing past crime. However, alongside this emphasis on the old penal tools, has there been any scope for the actuarial techniques promoted by the new penology in the Saudi state's response to the emergence of Internet fraud? In this section, the researcher draws on the data collected in the case study of Riyadh police response to Internet fraud to show the limited extent to which the Saudi government has sought to reconfigure its strategies and adapt them to the conditions of late modernity. In particular, it will be demonstrated that the two prominent principles of 'the new criminologies of everyday life' (Garland, 1996, 2001), i.e. public-private partnerships and preventative policing and risk management, are far from being fully translated into the Saudi government policy on policing Internet fraud.

4.4.1 Public-private Partnerships

The existence of private policing in Saudi Arabia is still confined to private security firms which employ security guards and patrol personnel. Those private security companies operate mainly in privately owned spaces, such as retail areas and shopping malls, but their services have also begun to be relied upon by some government institutions. Apart from these limited security functions, the Saudi law still does not permit the private sector to undertake other aspects of police work, such as crime investigation and apprehension as well as forensic examination. As these policing activities are owned exclusively by the sovereign state, partnership policing of Internet fraud in the manner described in the existing Western literature does not formally exist in Saudi Arabia. Unlike Western nations, Saudi society appears to be far from ready to implement the licensing of private investigators and detectives, whether online or offline. The issue is highly political and, therefore, the majority of police officers interviewed were opposed to the idea of a private model of policing Internet fraud, even though they recognised its efficiency and effectiveness. The following quotation is representative of this dominant view (n= 34/ 85%) among the police participants:

> You can privatise communications, education, sports, electricity, healthcare, and many other services that are provided by the government, but not policing and investigation of crime. What is left for the state to do then? If the police and crime investigation is privatised, we would be in a mess. Yes the private sector might have better technology and resources, but having business companies to run crime investigation is just unacceptable, and I wouldn't imagine our government go that route (PS6).

Respondents also suggested that if Saudi Arabia were to witness the birth of licensed private crime investigation, the delegation of policing Internet fraud to private investigators would not be a simple task, since the Saudi policing system has maintained a centralised national police force. As one station manager pointed out:

> The Saudi policing system is not fragmented; it's concentrated in the DPS. So before policing Internet fraud can be handed over to the private sector, the policing system needs to be adjusted, I mean there should be an innovative restructure of policing division of labour (PS18).

We can see here, therefore, that there is no inclination for any form of criminal investigation of Internet fraud to be allowed to take place 'beyond-the-state'. However, even the scope for cooperation between the police and private sector for the purpose of controlling Internet fraud also appeared to be very limited. It was evident during the research that private sector entities were not always perceived by the police organisation as reliable partners in crime control. For example, it emerged that despite a number of proposals which had been repeatedly passed to the DPS's senior management for borrowing experts from the information technology sector to assist in police investigations of high-tech crimes, the idea was always rejected. The DPS's negative attitude towards such a form of partnership with the private sector was explained by one respondent thus:

> Inviting outsiders to participate in investigations in one way or another means that they would ultimately access sensitive information about citizens and about the system as a whole, and of course the police would not be happy to get such information disclosed beyond the official circle (PS12).

This, however, did not stop some officers from seeking informal avenues of cooperation with members of ICT companies:

> I do not know what happens in other departments, but I personally have begun to take advantage of my relationships with some computer specialists to gain more knowledge about the Internet, hackers, chat rooms, forums, and so forth, which should help me in my job (DDI3).

In Riyadh, what can be described as real public-private cooperation in policing Internet fraud was only observed in police liaison with two groups of private sector entities: banks and Internet Service Providers (ISPs). The former were consulted with regard to obtaining bank account details for individuals involved in cases under investigation, and the latter when the police sought to identify suspects' IP addresses or other telecommunications details. However, the effectiveness of this liaison, usually initiated by the police, appeared to be hindered by rigid bureaucratic rules and procedures, which allow formal communication to be conducted only vertically through a long chain of bureaucratic layers rather than horizontally and directly between the immediately concerned parties. The following quotation provides an example of the problems encountered by officers in this regard:

> In an Internet fraud case, the first thing you need to know is the location of the offender by locating their IP address. Here you need to write a request to the CCIT [the Commission of Communications and Information Technology]. The request must be endorsed by the Chief Investigator then signed by the head of station. It goes then to the Director of the Riyadh Police and from him to the Governor of Riyadh who sends it down to the President of the CCIT. I don't know how many people it has to be seen by afterwards in the CCIT. But it takes no less than 15 to 20 days before we have the answer from them, and sometimes even more. They would probably send the request back to us asking for further detail. Here you would be looking at approximately 30 days. Would the offender be waiting in his place all this time?! Why can't that be made shorter? I mean from the head of the police station to the concerned department in the CCIT (PS5).

While the respondent quoted above was talking specifically about difficulties experienced in communicating with the ISPs, a similar situation of undesirable delays in response was also reported by respondents in relation to banks, which cannot offer any form of cooperation in criminal investigations except through the channel of the Saudi Arabian Monetary Agency (SAMA). This disjuncture in communication between the police and their private sector partners undermines the development of sustained collaborative relations necessary for effective policing of Internet fraud. Therefore, informal channels of cooperation through personal relationships with individuals from the industry remain for some investigators the only way of securing speedy and effective cooperation. As one officer commented:

> Sometimes personal relationships help in obtaining the information I need from banks. If I have a good relationship with the head of the security department at the bank, I would be able to get, for instance, details of transactions carried out on a specific account or footages from the CCTV at the ATMs. Most people want to help out, most individuals in organisations want to help, but they'll have their corporate rules and regulations (DDI3).

Moreover, conflicting organisational interests impacted on police-private cooperation in policing Internet fraud. For instance, there was a dominant view amongst police participants that instead of enforcement of law, banks' collaboration with the police is based on the evaluation of potential benefits and harm. As explained by one investigator, who at the time of the research had led two investigations of security breaches that resulted in acquiring their customers' banking information and eventually stealing their accounts:

> Arrests of criminals and successful prosecutions are important to accomplish the goal of the public security. But deterrence and prevention while ensuring uninterrupted business activities is better for the banks than the arrest of offenders. So, it really was a challenge to get any information. They don't share their audit findings; don't want to share about weaknesses (PS8).

The divergence in the desired outcomes of policing Internet fraud seems to further divide the police and the banks, as the following quotation implies:

> The banks have often used an investigation process as a fraud control strategy. They think, you know, that if fraudsters knew that an investigation has taken place, they may not continue their criminal activities. So, we have sometimes felt unmoved to assist with cases reported by banks (PS2).

As the current research has been concerned specifically with the Saudi public police response to Internet fraud, it is hard to gain full understanding of public-private partnership in the policing of online fraudulent activity, as this would require examining the issue from the viewpoint of both sides of the partnership. What the data presented above indicates, however, is that the plural policing models suggested by Western writers, such as Wall (2008) and Nhan and Huey (2008), for controlling criminal activities in cyberspace, are far from being fully adopted in Saudi society, at least in relation to Internet fraud.

4.4.2 Pre-emptive Policing and Risk Management

The lack highlighted in the previous discussion of a public-private partnership culture which promotes collaboration and information sharing between the police and the private sector for the prevention of cybercrime has apparently limited the scope for risk-based and pre-emptive policing of Internet fraud. Thus, the Saudi policing system remains a reactive system that responds to a committed crime and is incapable of accommodating the change to a proactive and decentralised policing model. As one officer rather bluntly put it:

> I would be lying to you if I said we do anything more than wait for a crime to be committed, and then conduct an investigation and try to trace back to the perpetrator and provide evidence for prosecution. We haven’t yet become capable of intervening to prevent a fraudulent act before it takes place on the Internet; that is beyond our ability at the moment (PS15).

Officers spoken to in this research insisted that in order for the police to get control at effective points for policing intervention, they need either to acquire the technological capabilities for gaining access to operational intelligence prior to the commitment of the crime or to have readily available cooperation from the private sector entities that possess such capabilities. However, they complained that neither was in their hands. With regard to the former, officers in all the departments studied were very critical of the absence of even the basic equipment for online policing, let alone the more sophisticated technologies that would shift the initiative from the criminal to the police. The following is a telling remark that was made in this regard:

> We’re here like soldiers who are sent to the battle field to defeat the enemy without weapons. Frankly speaking, I don’t think we can talk about pre-emption of fraudsters’ activity on the Internet when we can’t even access the Internet at work (DDI4).

The lack of technological capabilities was combined with the inherently very limited familiarity of most police officers, particularly in the police stations and the DDI, with information technology in general, but the Internet more specifically, due to shortage of training. ‘Most of us don’t know anything about the Internet apart from sending e-mails and browsing web pages’, stated one officer (DDI5).

Interestingly, some investigating officers tended to compare the modest capabilities of their departments in relation to preventative policing of Internet fraud to what they viewed as the superiority of the General Detective Directorate's Cyberterrorism Unit (GDD/CU):

> [The GDD/CU] is much more sophisticated than you think. It has a huge budget, highly qualified experts and more advanced technology to monitor terrorists' activities on the Internet. Because of all that, they have been able to intercept terrorists' communications and infiltrate their plotting websites, which helped foil many planned attacks in recent years. For them to have all that, that's fine. But shouldn't the police's know-how and resources have been built up in the same manner for the purpose of protecting the public from Internet fraud, which is ultimately a protection of the national security? (PS11).

The low level of attention given by the Ministry of Interior to the problem of Internet fraud, implicitly alluded to in the previous quotation, seems to be influenced, to a great extent, by the apparent underrepresentation of Internet fraud in police records pointed out earlier in this chapter. This issue was raised by one officer, who argued:

> I think you won't see the kind of change you're talking about unless it [Internet fraud] is perceived by the decision maker in the MOI as a widespread problem. So far, this doesn't seem to be the case (PS23).

However, apart from being technologically inadequately prepared for carrying out proactive tactics of online policing, officers also felt that the way the relationship between the police and ISPs – who are also the telecommunications companies – was currently organised made very little room for pre-emptive policing of Internet fraud. As explained in the previous subsection, police communications with ISPs are mediated through an extended chain of governmental and non-governmental bodies, which means delayed response to requests for cooperation. Moreover, there was a complaint from officers that IPSs had always been hesitant to respond to their demands thoroughly and with complete information, as the following quotation indicates:

> We never got complete answers from telecommunications companies. Maybe they are concerned with the confidentiality of the information of their customers. But that shouldn't be exercised with us, because we are entrusted with people's lives, property and honour (PS17).

Based on such experiences of limited collaboration, some respondents expressed doubts about the possibility of any forthcoming cooperation from ISPs for preventative policing and real-time interventions, which would involve, for example, carrying out interceptions or collecting and producing communications traffic records:

> The maximum STC [Saudi Telecom Company], Mobily or any of the other telecommunications companies would probably give us is something like IP address or telephone numbers. Nothing more than that (PS19).

A number of officers also noted that the ISPs were distancing themselves from the police because they perceived no gains in partnering with them. The following is one of the remarks made on this issue:

> Why would they cooperate with us if there are no reciprocal benefits out of such cooperation? We are always dependent on them but they rarely need us. If they have problems, even criminal ones, they have their own solutions (PS22).

Although the Anti-cybercrime Law provided a legal obligation for the CCIT to assist in criminal investigations of informational crimes, officers believed that the ISPs, as part of the CCIT framework, are still under no pressure from the MOI to offer effective and genuine assistance to the police. 'There is nothing at the moment that compels them to be cooperative with us just as they are with the GDD/CU' (PS16).

While the research failed to observe police-initiated actions taken by police in the departments visited to predict and eventually prevent potential online fraudulent acts, their policing of Internet fraud was not completely devoid of risk management practices. This was particularly obvious in the DDI, whose activities included sharing information with the Saudi Monetary Agency (SAMA), via the Ministry of Interior, that would help banks to prevent future risks of fraud by, for instance, addressing security loopholes or taking extra preventative measures. An example of this approach to risk management occurred when a number of complaints had been received from victims deceived into disclosing critical banking details as a result of responding to phone calls (as will be explained later in Chapter Six) from fraudsters purporting to be bank agents providing instructions on how to avoid termination of accounts:

> We wrote to SAMA and informed them about this kind of tricks. We said, 'The banks should do this, this and this to prevent this from happening to other customers. Send warning SMSs or e-mails to customers, put that on ATM screens for customers to read'. The banks actually did so, and you must have received SMSs from your bank warning not to respond to this kind of calls, or have noticed the warnings that pop up on all ATM screens. They also introduced another measure. Now you can't use the same password every time. You've got to have your mobile registered and every time you try to log on to your account online, you would be texted a password that you can use only once (DDI3).

As the above quotation shows, the police appear to perceive banks as an effective channel for providing risk information to the public. Consequently, direct communication with the public to educate them on how to protect themselves against online fraud was less accentuated in the police risk management approach. It depended largely on issuing press releases announcing arrests of criminals in some Internet fraud cases, but without providing useful information for preventing future victimisations, such as details of offender's modus operandi and deceptive ploys:

> Arrests news you see every now and then in newspapers are mostly for show-off. With the big boss's photo next to the news, they would claim 'The police used advanced technologies to trace the offender'. Come on! What advanced technologies? We haven't seen them. These arrests were probably the fruits of diligent work of investigators with a bit of luck. Well, to highlight your success, I have no problems with that, but also give people advice on how not to become the next victim (PS25).

Another investigator acknowledged:

> People are using the Internet without realising the dangers it can involve. They are not educated enough to be conscious of the pitfalls of the technology. We have the Public Relations Department, but I think they aren't doing enough in this area. I mean online fraudsters' deceptive tactics we come across in incidents we investigate should be conveyed to the public to tell them to be cautious about them (PS20).

4.5 Summary

This chapter has endeavoured to examine the Saudi state response to Internet fraud. This required, first, addressing the question of whether the Saudi state has been faced with a growing Internet fraud problem. At first sight, the rapid expansion of Internet usage may seem to bolster anecdotal media claims that online fraudulent activities are increasing. However, obtaining a well founded understanding of the extent of Internet fraud was hindered by the lack of substantiated evidence, whether from official statistics or academic research. Therefore, extrapolating from the situation of Riyadh to the Kingdom of Saudi Arabia as a whole remained the only alternative. In the case of Riyadh, the underrepresentation of Internet fraud in police statistics, which stood at odds with officers' perceptions on its incidence, raises questions as to any assumption that the Saudi state response to this criminal phenomenon has been driven by a concern about a serious crime problem that is on the increase. Indeed, the analysis of the recently enacted Anti-Cybercrime Law and of the creation of the Informational Crime Unit highlights the importance given to the concern for global image in the introduction of these legal and organisational innovations. The data also shows that while the Saudi government acknowledged the limitations of the sovereign state in winning the battle against terrorism and began, therefore, to pay more attention to pre-emptive policing and partnership with the private sector, the scope for such pragmatic adaptive strategies in its response to a non-state threatening cybercriminal activity like Internet fraud remains very limited.

In sum, the existing literature presents the policing of cybercrime as bearing the contradictory characteristics of a late-modern crime control framework, in which expressive gestures, which seek to demonstrate visibly that the sovereign state is doing something about crime, sit alongside pragmatism and adaptation, with their emphasis on prevention and partnerships. However, the analysis presented in this chapter suggests that the Saudi state response to Internet fraud fits with the former more easily than the latter. Questions now arise as to how the policing of Internet fraud fits in with the existing political and cultural traditions, how it is carried out in practice and how it is shaped by the existing organisational, occupational and individual concerns of the Saudi police. These issues were investigated in this research, and the outcomes concerning them are presented in the following two chapters, beginning in Chapter Five with an exploration of the organisational context of the Saudi police response to Internet fraud.

Chapter Five

Police Response to Internet Fraud: the Organisational Context

Chapter Five: Police Response to Internet Fraud: the Organisational Context

5.1 Introduction

The previous chapter presented a discussion of the Saudi state response to Internet fraud at the macro level. In the present chapter and in Chapter Six, the focus turns to the micro level, represented by the police organisational entities involved in addressing cybercrime issues. This chapter uses the empirical data gathered in our case study to provide an account of the organisational context of the police response to Internet fraud. It begins with a consideration of the newly launched Informational Crime Unit (ICU) in terms of its role in the policing of Internet fraud, how this role is perceived by its members and the wider police community, and the extent to which the ICU has been enabled to fulfil its declared purpose. The chapter then moves to discuss a number of organisational issues which emerged from the research on the departments through which the police service on Internet fraud is predominantly delivered, i.e. the police stations and the Department of Detection and Intelligence (the DDI). Amongst the issues examined is organisational conflict and the impact it has on the policing of Internet fraud. The chapter also assesses the extent to which an intelligence-led approach to policing Internet fraud is adopted and explores the determinants of such an approach. Finally, the provision of specialist training to officers in relation to handling online fraudulent activity is analysed.

The themes of this and the next chapter are not mutually exclusive; they blend and blur into each other, and they underlie and reinforce each other. The decision has been made to analyse them in two separate chapters for the purpose of clarity, but in the process of analysis, their interrelation will become evident.

5.2 The ICU – a Unit without a Purpose?

Although the introduction of the ICU has been hailed by the Saudi law enforcement community as a significant step towards specialisation in combating cybercrime, it would be hard to argue anything other than that the role of the newly established unit in the policing of Internet fraud and other forms of informational crime is still only nominal. To begin with, the ICU did not have a formal definition of the crimes falling within its area of responsibility, nor were there in place written policies and procedures concerning its operations. The absence of documentation in those areas has major implications for determining the types of Internet fraud which the ICU is supposed to handle as well as for understanding when and how the unit should be involved when an incident relating to this criminal activity occurs. Respondents always maintained that, currently, the ICU used informal procedures with no specific guidelines to instruct its members on how they go about their work. ‘To be honest with you, we don’t have a vision of a work mechanism for our unit yet’, commented one respondent (ICU4). In particular, respondents appeared very critical of the vagueness that still surrounded the tasks and jurisdiction of the ICU and its DFE-hosted evidence analysis division. One interviewee summed up this dilemma by saying:

> We are told that our job here is to provide technical support for the investigation, but the forensics section is also about providing technical support, you see. There is just no clear distinction between ours and their job, meaning when and how each of us should step in is not clear yet (ICU2).

Despite the ambiguity surrounding the ICU work mechanism, officers tended to consider the responsibility of their unit to be akin to that of the traditional Department of Detection and Intelligence (DDI), in that:

> This unit is required to assist in incidents where the police station’s investigations could not determine the identity of the offender/s, by gathering intelligence and collecting information that would lead to their identification. What distinguishes our job from that of the DDI is that they look for intelligence in the physical world, whereas we look for it in the cyber world (ICU1).

However, apart from information collection and intelligence gathering, ICU members were adamant that they have no responsibilty for undertaking other operational functions. They maintained that standard policing activities, such as reception of complaints, search and seizure, as well as arresting and interviewing suspects, remain the duties of police stations. Explaining what happens if potential victims of Internet fraud contacted the ICU directly, one officer indicated:

> We don’t like to take our victims and tell them to go places, but things must come through the proper channels. But we try and make it as easy as possible for them. We’ll call the station and have them interview the victim, and if they feel at a certain point that they need us then eventually we do get it through the Provincial DDI (ICU3)

In other words, the ICU will not handle an Internet fraud incident without it having been processed at a police station level and determined not to be capable of solution using the station’s investigative resources.

Interestingly, the existence of the ICU was found to still be widely unknown to the sample police stations' and DDI's officers, which reflects a serious organisational failure of the centralised management of the DPS to achieve synergy between its divisions. Twenty-seven (90%) out of the thirty respondents spoken to in those sites reported having no idea about the new unit, while the other three (10%) said they had heard about it from the media, but had not been informed formally about its role and location. Not only that, but there were some police station respondents who viewed the ICU as a cybercrime complaint centre, where victims can report their experience of Internet criminal activities, including fraud. The following is a telling remark that was made by one of the participants who held such a perception:

> The role of the guys of this unit [the ICU] is just to take a piece of paper in one hand and pass it by the other to another agency. A passing bridge only. We don't need this, what we need is a department with branches spread across the country to carry out the investigation of Internet crimes (PS3).

Apparently, this ignorance amongst the officers in the police stations and the DDI about the existence and role of the newly launched specialist department greatly reduced the number of potential Internet fraud incidents that might have been referred to the ICU, and it was unsurprising, then, to observe that the ICU detectives were not struggling to cope with a heavy workload. By the time the fieldwork was completed, the ICU had been assigned only a few cases, of which only two involved Internet fraud. One of these two cases, which came to the ICU through Interpol, concerned a phishing website which was allegedly hosted on an IP address located in Saudi Arabia and had been used to intrude into a number of Internet banking accounts in South Africa in the summer of 2008. The South African authorities requested the cooperation of the Saudi police in their investigations of the fraudulent scheme by identifying and arresting those responsible for setting up the fraudulent website. The other case was based on a complaint made by a female victim to the Minister of Interior's Assistant for Security Affairs, claiming that she had lost SAR950,000 as a result of responding to advanced fee e-mails purporting to be from UK-based senders. The DPS was directed to process the complaint and the ICU was chosen to undertake the investigation.

In describing the challenge he was faced with, the officer who was charged with the handling of the above mentioned Internet fraud cases expressed:

> The cases were sent down to me because I'm supposed to represent the Computer and Internet Crime Section. But the problem is we still don't have the capacity to handle such cases. We don't have the equipment. I don't mind even if I'm not trained enough, I will eventually learn on the job. But don't give me jobs

> when I still have bare offices. We contacted the DTA to provide us with the details of the IP address owner in the South African bank case, and it has been around six weeks since the communication was made, and still we haven't got their response. The CCIT are more cooperative. But you need to speak to them directly to get all the things you need from them, and that is not possible. We asked them if they could monitor the e-mails used in the woman's case and their answer was in the negative. You need Internet surveillance and unless you grab the technology at your place you can't do that (ICU2).

As the previous quotation indicates, the picture we obtained of the evidence gathered in this research concerning current ICU capability shows that inadequate material resources have been made available for officers to handle the Internet fraud cases they have begun to receive. This does not bode well for the hopes that have been pinned on the ICU as an agency created to achieve what one Saudi commentator once called 'the highest mode of fighting crimes in cyberspace' (Beer, 2007: unpaginated). As one officer asserted, 'an impressive organisational structure does not amount to much unless sufficient resources are in place to make it work effectively' (ICU5). Officers insisted that it was impossible for them to be successful in processing any case referred to their unit by relying merely on computers and restricted access to the Internet. This led some of those interviewed at the ICU headquarters to raise the possibility of seeking more professional expertise for help with assignments pending completion of the technical equipment of their department, despite awareness of the managerial obstacles to such an approach. Exemplifying the remarks made in this regard, one respondent suggested:

> *Al-Mabahith's* Internet unit [General Detective Directorate's Cyber-terrorism Unit] and the MOI's Department of Technical Affairs have their own in-house investigative capability, and I know that there is a similar unit in the CCIT [Computer Emergency Response Team]. They all have the capability, and they could help us. But would the management let that happen? That is the big question. I don't think they would, because everybody is holding tight to their resources (ICU1).

The lack of any systematic planning and provision of training for officers was another issue which renders questionable the ICU's pronounced purpose as an instrument for effective handling of cybercrimes. For instance, it was found that the search for potential areas of cybercrime training, and for institutions that could provide specialised training in those areas, depended on the individual endeavours of two volunteering officers, who used the Internet and other information resources to undertake this task. The exploration of training availability carried out by the above mentioned two officers seems to have contributed in one of them being the first amongst the ICU officers to receive cybercrime-related training, as he was sent to attend a training programme that he identified and applied for. The programme, which was titled ‘Basic Data and Analysis’ and held in the US, was a course in recovering data from computers and lasted for one month. The rest of the ICU’s working officers were still awaiting their first opportunity to receive specialised cybercrime-related training.

As has become clear from the previous analysis, the ICU existed only in name in the DPS’s organisational structure, but remained virtually non-existent in operational terms. Thus, the onus of investigating Internet fraud remains on police traditional investigative units, that is, the police stations aided by Departments of Detection and Intelligence (DDI). However, as we shall see in the remainder of this chapter, a number of organisational issues had a major impact on the way Internet fraud was responded to in the sample police stations and DDI.

5.3 Organisational Conflict and the Limits of Cooperation

One of the most important determinants of police response to Internet fraud in the police stations studied in the current research was the level of conflict within the organisation. Conflict between the investigating officers and the management, for example, was intense in four out of the five stations. On a number of occasions during the research period, officers had problems with the manager of the station, which often resulted in disciplinary actions, such as the issuance of written warnings, referal to the Follow-up Department[13], and after-work-hours station detention. Reasons for such problems included, for instance, repeated mispresentation of Case Final Reports (CFR), delay in taking over full-day duty and disputes over nomination for training or approval of summer vacation times. The following statement illustrates the general mood amongst the officers in those stations as a result of the tensions that existed between them and their managers:

> *Extract from field-notes*: I did everything you can imagine to get transferred to this station. But now I regret it. We have an arrogant manager here. He doesn’t care about us. He’s always let us down when we needed his support. Nobody is immune from mistakes, you know. But he doesn’t forgive even a small mistake. So why should anyone be bothered to work extraordinarily? You talk about

[13] The Follow-up Department is positioned in the headquarters of the Riyadh Police and responsible for monitoring the progress of investigation. An officer can be either summoned to the FD or referred to it by their station manager to be questioned about what is perceived as a failure to do what ought to be done. Reasons include, inter alia, delay in processing cases (particularly those where a suspect(s) is held in custody pending the investigation, inaccuracy of reports and complaints by the public. A disciplinary action against the concerned officer may follow.

> investigating Internet fraud. This requires working beyond our means. But with such an atmosphere, no one is prepared to work beyond his means.

In another station, a similar comment was made by an investigating officer who was extremely dissatisfied with what he perceived as the influence of *Wastah* (patronage) on the manager's decision on the nomination for a Criminal Investigation Course, which went to a non-investigating officer instead of him:

> *Extract from field-notes*: You just work hard and think that if you make all the efforts, you would gain the appreciation of your manager, but in reality everything depends on *Wastah*. If you don't have a strong *Wastah*, don't aspire too much. In this station, one like me should perform his work in a manner that pleases Allah first and foremost and pleases his conscience. Don't compromise your duties, but at the same time stay within the limits of the means provided by the organisation.

As the previous statements imply, the hostile environment in the police station generated by the high level of organisational conflict between managers and investigating officers leaves the latter less enthusiastic to be innovative in investigating Internet fraud, offsetting the lack of material capabilities. In other words, disillusioned and demoralised officers were unwilling to make extra efforts and work beyond the availabale means to solve Internet fraud cases.

In addition to internal organisational conflict within the police station team, tensions also existed between the police stations and the DDI. The existence of a degree of frustration, jealousy and negative feeling directed towards the DDI was evident amongst police station officers, as the following extract from the field-notes illustrates:

> *Extract from field-notes*: We [the stations' officers] are always in an unfavourable position compared to the DDI guys. They get the leads, they get the suspects, and they get the evidence off the station's officer. We do all the hard work and they step in and take all the credit for the job. Compared to station officers their workload is really small and yet we still do most of the work for them. But they get the salary bonuses, they get the medals, they get the cars....They consider themselves the elites of the police.

Indeed, the DDI officers were perceived by their colleagues in the police stations as reaping the benefits of investigative successes that could not have been achieved without their significant contribution. Moreover, some police stations' officers had experienced work-related problems with the DDI. For instance, one officer, who is the head of a police station's Criminal Intelligence Unit, was annoyed about the treatment he received when he participated in a meeting in the DDI:

> *Extract from Field-notes*: I went the other day to the DDI to attend a meeting with [a DDI senior officer] about [a joint operation]. When I arrived

> there along with other heads of criminal intelligence units of some Riyadh police stations, I wasn't shown any respect. They didn't even allow me to park my car in their shaded parking area, and I struggled to find a parking space nearby. I also had to wait at Reception for about twenty minutes, and I got checked before I was let in. Worse than that, they didn't give us even a glass of water or a cup of tea. We entered the meeting room, and every one of us was so annoyed that we were looking forward to the moment the meeting ended. They didn't treat us as colleagues who work under the same umbrella.

In theory, the DDI's role is supplementary to that of police stations in that they work jointly towards resolving complex crimes, with the emphasis being on surveillance and intelligence gathering by the DDI (DPS/DPD, 2009). However, the on-going tensions between the police stations and the DDI often minimised the extent to which cooperation in the policing of Internet fraud occurred. In fact it was argued that genuine police station-DDI cooperation only happened when there was a joint investigation committee, giving common focus to a particular Internet fraud case:

> Everybody has got to put their conflict and grudges aside and work cooperatively towards resolving the case, because if the committee succeeds, the credit of the success will go to every member. And likewise everybody will be accountable for failure (PS11).

Organisational conflict between the police stations officers and the DDI team was also having an impact on operational procedures. For instance, the DDI officers expressed considerable frustration about the manner in which Internet fraud cases were forwarded to them by the police stations. From the point of view of the DDI officers, the unsatisfactory quality and detail of the police stations' initial investigations often necessitated going back to the beginning with an investigation. One DDI officer summed up the views of his colleagues:

> Sometimes there isn't much information you begin with in cases passed on by the police stations, and I would say this is even more so in Internet fraud cases. You see how big this case file is. When I got it from [one police station] it was only two pieces of paper, and that was the complainant's written statement. They did nothing else. They sent the case straightaway to us. So I had to do what they were supposed to do. I interviewed the complainant again, and I contacted the bank to get information from them. I also had to be in touch with CCIT as we needed their help in knowing whose email had been used in the fraud. So it's me who has built up this case from scratch (DDI3).

The impacts of organisational conflict have been pointed out, in terms of limiting cross-agency cooperation, particularly between police stations and the DDI, in the policing of Internet fraud. This should not be taken, however, to imply that cooperation did not exist between officers who worked together in the same organisation. Unlike the tension, and to some extent hostility, which surrounded management/officers relationships on the whole, a general sense of solidarity and internal cooperation was observed amongst officers in each department at the operational level. One officer highlighted this situation by saying:

> I would describe the way that we work with each other as working as comrades and brothers, helping and supporting each other. But our relationship with the management has its ups and downs. It isn't always alright (PS22).

Rather than being driven by 'the need to present a united front in the face of external attacks' (Reiner, 2000a: 92), brotherhood and supportive relationships that existed among some officers in the police departments examined in this research can be attributed to the tribal origins of those officers. In tribal communities, social rules dictate that everyone should support and appreciate those who live or work with him. Brotherly relationships might also be enhanced by the common social events and activities in Saudi society, such as welcoming parties, wedding ceremonies and gathering in off-work rest places (locally known as *el-Istraha*). The collectivistic values and meanings of such social events and activities extend to the organisations, shaping work values, relationships and behaviours with a sense of solidarity, cooperation and working as one family. Thus, this kind of relationship was built upon camaraderie and its consequences for the policing of Internet fraud emerged in numerous cases during the observational period. For instance, on some occasions, the researcher observed that an officer approached a colleague to seek assistance and advice on certain issues and procedures in the process of an Internet fraud investigation. In other instances, some officers volunteered to take over investigations of Internet fraud cases. The aim of some of these officers was to ease the workload of a colleague, while others intervened to replace officers who lacked the technological sophistication to deal with this type of incident.

5.4 Intelligence-led Policing?

Before discussing the extent to which an intelligence-led policing approach was adopted in police response to Internet fraud in Riyadh, a definition of the concept of 'intelligence-led policing' is needed. Ratcliffe (2008) has pointed out that although there is a growing literature on intelligence-led policing, it has been generally assumed that the term speaks for itself, and definitions are rare. According to Ratcliffe, despite the absence of a universally accepted definition, the crux of intelligence-led policing is an emphasis on the collection and analysis of information to guide police operations. A report which was published by the UK House of Lords' European Union Committee described intelligence-led policing as:

> An approach to crime reduction that moved resources away from retrospective crime investigations into pre-emptive operations based on analysed intelligence. Rather than reacting to events as they happen, intelligence-led policing uses the knowledge already acquired to determine crime trends and patterns, and criminal activities in progress, and uses that body of information to influence the directions the police go in targeting particular individuals, activities, geographical locations and the like (House of Lords, 2008: 26).

This policing approach, as Zinn (2010: 27) indicates, 'emphasises information gathering through the extensive use of confidential informants, offender interviews, analysis of recorded crime and calls for service, surveillance of suspects, and community sources of information'.

Resourcing issues (human and other) affect police frontline units' (i.e. the police stations and the DDI) response to Internet fraud in a number of different ways, not least in the field of intelligence-led policing. With regard to the issue of staffing, the entire group of officers representing police stations (n=25) were united in stressing that their departments were seriously understaffed. Those respondents noted a need for more personnel to meet the huge and ever-increasing demand by the public for police services. To quote one officer:

> …The number of officers in our stations is too little compared to the enormous quantity of cases we receive every day. And I think you would hear the same in other stations…. At this point with our current workload even a 100% increase in our strength would be absorbed very quickly (PS4).

Another station's officer added, though with more dissatisfaction:

> We [the police stations] are left to fight crime and criminals with the very, very minimum capacity. Police stations must be prioritised over any other department in the DPS, and officers who are just idling here and there in the headquarters without real jobs should be sent down to fill the huge gaps in stations (PS7).

A similar perception of inadequate staffing was also found to be prevalent among respondents from the DDI, including those from a managerial level, as the following statement suggests:

> We serve the entire Riyadh Province, with a total population of over 6 million people. And we only have a workforce of 32 personnel, of whom only 21can be deployed. I don't want to criticise anybody but this isn't reasonable. Even double or triple our current force would still be far below what this department needs (DDI5).

An inevitable consequence of the shortage of personnel, particularly in police stations, was the exceptionally and constantly high workload. This issue was particularly pertinent at the time of the study, when each station was managing this situation with at least three staff absences, some of which were likely to be long-term. One head of station explained:

> I think that the whole station here is under so much pressure that it is at breaking point. I mean I've got two officers off sick at the minute. And so I couldn't let any of the officers have the full 45-day summer holiday. I had to divide it between them, each one 3 weeks only. Otherwise there would be literally only two officers to take the full-day duty, and it is impossible to let it go that way (PS12).

Furthermore, the officers interviewed unanimously shared the view that the emergence of Internet fraud and the growing number of reported incidents of this form of criminality added to their already high workload. As one investigator stated:

> Fewer and fewer people are asked to do more and more. The number of crimes has never come down. Theft is increasing, burglary is increasing, assault as well, sexual assault…oh, awful. And now come Internet fraud, mobile phone theft and all the technology-related crimes (PS3).

The issue of staffing in terms of managing workload as explained above inevitably impacted on the availability of officers to engage in intelligence-led policing of Internet fraud. For instance, the use of informants, particularly by the police stations' Intelligence Units, to obtain information relating to Internet fraudulent activity was somewhat rare, with officers stating that their workload often precluded them from undertaking such tasks, as the following comments indicate:

> We are always overloaded. We don't have enough time to manage the huge amounts of information and the administrative work we have got, let alone to receive additional information from informants (PS13).

> Using informants is a part of our work, but only in serious cases. Murder, rape, big burglary, things like that. But not in an Internet fraud case, no, unless you've got something serious in that as well, like...I mean something that has a big, big loss in it, or when there is a sexual exploitation involved. It should be happening and we should have the ability to employ three or four guys out there to give us information about these cases, but you don't know how time consuming recruiting and handling informants is. So I have to save my time for the most important things. And there is no support from the management. If you succeeded in identifying the perpetrator they would say 'Well done', but no one is going to ask you what you have done or how much money you have spent from your own pocket. Okay, I have a good salary, but the people who work with me need money sometimes. I give money to them and I buy things for them from my own pocket, but that money is never going to be paid back to me by the management (PS5).

However, a further pertinent resource issue that became evident throughout the course of the study was the lack of technical equipment available to police officers for intelligence operations. In the police stations visited for the purpose of this research, there were only a small number of computers offered to officers. Many of these computers were brought in and owned by individual officers and not supplied by their employer. Most importantly, access to the Internet was never available to staff in any of the entire sample of police stations. Not only was connection to the World Wide Web not provided by the police organisation in those locations, but officers were also prevented from providing their own access to the Internet. To this end, network disabling equipment was installed in some stations to prevent use of broadband Internet devices. Lack of trust and the highly conflictual relationships prevailing appeared to be major contributing factors to managers' decision not to allow officers to access the Internet at work, as the following extract from a conversation with one station manager illustrates:

> I do not permit the Internet in here because it will be misused by officers. If they have the Internet, they will be abandoning their duty and they will be sticking instead to the computer screen to watch stock prices and undertake online sale or purchase transactions. This is what the Internet will be used for. So the Internet will be an element of distraction for staff rather than a facilitating tool (PS1).

The vital need for using the Internet to obtain intelligence to aid Internet fraud investigations was widely recognised by the Intelligence Units' officers of police stations. This is evident in statements such as the one below:

> When you are trying to fight Internet fraud, you have to invest in human intelligence. It's not just about knowing what the Internet means, it's about somebody sitting in the chat rooms or the forums, things like that, gathering intelligence, understanding the culture, understanding the way they're moving, what they're thinking, what they're doing. You know, also being able to infiltrate some organised hacking groups. So if you can build up human intelligence from the Internet, you can get a lot further in your investigation. It's not all just knowing what IPs means and things like that. It's knowing what is motivating these people and where to find these people (PS8).

The situation in the DDI was not very different from that affecting the stations. However, the lack of information and computer technologies was perceived as being particularly problematic in the DDI, whose role is to collect and analyse criminal information to assist other divisions of the Riyadh Police with those investigations that it is not practical for them to handle by virtue of their normal operations. The following is an example of the remarks made in this regard:

> Our department is meant to fight crime, Internet fraud and other, through intelligence, but the truth is we haven't got the means to collect all sorts of intelligence. We're expected to solve mysterious crimes like Internet crimes without even being able to access the Internet, let alone to utilise proper technological tools like those used by police in many other countries, including neighbouring ones (DDI3).

As a result of ICT shortages, the work of the DDI, like that of the police stations' Intelligence Units, is wholly dependent on human-based intelligence gathering through the deployment of undercover operators. When digital intelligence (e.g. a suspect's IP address or details relating to identified phone numbers) is needed, the DDI has to rely on outside help from telecommunication companies, either directly using informal personal contacts whenever possible or via the Commission of Communications and Information Technology (CCIT). An exception to the general situation of shortage of electronic resources is the computer terminals connected to the National Information Centre (NIC) network, which are available in both the police stations and the DDI for information inputting into and outputting from the national database. However, these were not used effectively, for reasons which will be discussed in Chapter Six (see § 6.5).

Despite their significant impact on the departments investigated in this research, resourcing issues were not the only obstacle to an intelligence-based police response to Internet fraud. Equally challenging also was the inefficiency of the formal structure of intelligence sharing between the DDI and the police stations' Intelligence Units in terms of processes of information exchange. Due to the inexistence of an inter-agency IT system that supports intelligence sharing between the DDI and the police stations (which is a direct consequence of the above discussed deficiencies with IT infrastructure of the police), it is impossible for an intelligence officer working in one organisation to search for relevant information in a different agency. Instead, they are reliant on making requests for information that may not always be processed in a timely or accurate manner for a variety of reasons. One of these reasons is the high level of organisational conflict, often fuelled by fierce competition ownership of success of investigation, which existed between the police stations and the DDI, as the following conversation between the head of a police station's Intelligence Unit and one of his staff reveals:

> *Extract from field-notes*: At 10:40 Lieutenant K (the second officer in the station's Intelligence Unit) has been discussing with Sergeant S what is going to be done with the individuals and material captured yesterday in a raid on a group dealing fake sexual dysfunction drugs. Captain A (the head of unit) comes in and interrupts the conversation. He asks Lieutenant K 'What's happened to the

> request we've sent to the DDI regarding [a name of person] case? Did they reply with any information about similar cases, similar modus operandi'? Captain A was inquiring about a case in which a man was arrested after it was discovered that his bank account was amongst those to which SR50,000, which an elderly man had reported as missing from his bank account, was transferred online. The arrested man has denied any involvement in the theft and claimed that all he did was he had met someone at an ATM who persuaded him that he had lost his *Sarraf* (debit) card and was in urgent need of SR5,000. So the arrested man allowed the stranger to transfer the money to his account, and upon making sure of the transaction, he withdrew the money using his card and gave it to the stranger. In response to Captain A's question, Lieutenant K says that the DDI has not provided any information. 'They said we can't give such intelligence out, because there is sensitive information about people that we just can't disclose', adds Lieutenant K. 'I swear the reason is something else and not just sensitive information that they want to protect, the reason is they keep their information for themselves because they want all the credit for any success to go to them only', comments Captain A.

Since knowledge in police work is a source of power (Ericson and Haggerty, 1997), the potential value of the information retained by the DDI officers may explain why they were unwilling in the above example to share it with their colleagues in the station, as to do so could challenge their power. In other words, as Ratcliffe (2008: 206) argues, 'while operational security has often been cited as the reason for keeping information secret, the simple reality is that personal advancement is usually the reason, as information can often be translated into arrests – and a good arrest record can be translated into personal success'. This point is also recognised by Cope (2004: 193), who notes that 'the power associated with withholding or accessing information is a crucial barrier that is manifested throughout "the need to know culture" that engulfs intelligence work'.

Crime data analysis is crucial for intelligence-led policing because it endeavours to deliver 'the right information...to the right people at the right time' (Fletcher, 2000: 114). However, the way Internet fraud data are recorded in Riyadh (as we have seen in the previous chapter) and the constraints placed on the sharing of those data amongst police units (as the above example tells us) do not assist the development of a strategic intelligence about crime trends, which is a key element of intelligence-led model of policing. Nor do they assist a crime analysis attempting to identify links between incidents for investigation, because incident data are not recorded or not shared. As the data presented in Chapter Four and in this chapter reveal, the police do not have a mechanism yet for recording for information's sake.

Officers' poor understanding of Internet crime also appeared to be a significant inhibitor to a model of policing of Internet fraud that is directed by information and intelligence. Generally, both investigators and intelligence officers possessed insufficient knowledge about computer technology and Internet protocols, which restricted their ability to fully comprehend the nature of fraudulent activity in cyberspace. Consequently, not only were there limitations to the usefulness of the intelligence officers' products for the operational policing of Internet fraud, but they also extended to the investigators' ability to ask the right questions and request the relevant information, which would potentially support their investigations. Numerous comments were made on this issue, some of which, such as the one below, expressed a rather pessimistic feeling:

> I'll tell you what. Look, I bet there is no single officer in the entire Saudi police force who knows how to deal with a case relating to the Internet. An officer can excel in a homicide or a theft case, but when faced with an Internet crime he's out of his depth. We are not ready to work on them. We don't have the necessary lens through which to look at this type of crime (PS15).

The difficulties associated with conducting intelligence-led policing of Internet fraud as a result of officers' low level of understanding about the nature of Internet crime highlight fundamental training needs for police officers in the handling of this type of criminal behaviour. However, as will become clear from the discussion provided in the following section, the findings of this research revealed a series of flaws in the DPS training function in relation to Internet fraud, both at strategic and implementation levels.

5.5 Training and the 'Digital Divide'

As policing grows progressively more complex, police training and recruitment needs to deliver pertinent information and attract those with skills commensurate with tackling a multifaceted and complex environment (Flynn, 2000). The importance of training police officers in relation to policing Internet fraud and other types of cybercrime has been emphasised by a number of researchers (see Borrowman et al., 2001; Burns et al., 2004; Cheurprakobkit and Pena, 2003, Hinduja, 2004)). For instance, Hinduja (2004) maintained that educating police officers about cybercrime would promote an appreciation of the complexities that have arisen in this area of enforcement. However, there was a clear convergence among respondents in the current research on identifying the absence of effective training as a key factor behind their departments' unpreparedness to deal with Internet fraud. The data obtained during the research in the police stations and the DDI show that officers in these departments did not have any pre-service or in-service computer-related qualifications.

The existence of a ‘digital divide’ between the police and Internet criminals – with the police being on the disadvantaged side of this divide – that is driven by the combined lack of both equipment for and training on e-policing is troubling from the perspective of the participating officers. One officer underlined exactly this point by saying:

> We are entering an age that isn’t an age of stealing gas bottles. A gas bottle, when sold, can fetch only SR70, but in Internet fraud a key stroke can bring SR100,000. Most children now are proficient with computers and the Internet, even those who are 6 or 7-years old, I’ve seen that myself. Tomorrow, when they become adolescents and easy to influence, they could become deviants and use their proficiency in technology to steal. The police must, must prepare themselves for this reality. They must bridge the gap between officers and Internet criminals, by training on how to deal with these criminals, but that isn’t going to happen unless computer and the Internet become parts of the job tools (PS9).

Officers were clearly unhappy with what they viewed as ignorance on the part of the senior management of the importance of training officers to deal with novel crimes, such as Internet fraud, and absence of this issue on their agenda, as the following comment reveals:

> Investigating Internet crime, be it fraud, hacking, online extortion or any other kind, is now part of police work, nobody can deny that. And we really should have received at least some lectures on that basis (PS15).

Additionally, respondents were conscious of the impact of a lack of training on their ability to handle Internet fraud cases. Particularly within the police stations, a number of officers appeared concerned about their inability to meet the public expectation that police will investigate whatever crime is reported to them, as the following quotation indicates:

> As you know, people always expect the police to investigate any crime. They don’t know that we haven’t been given the training. We don’t have the skills to do it. But there’s an expectation that we will do it, which causes a lot of frustration (PS3).

Besides their criticism of the absence of in-service training programmes, officers also blamed the inadequacy of skills in relation to policing Internet fraud on what was regularly described as ‘improper pre-service training’ which those officers received at King Fahad Security College. In this regard, some officers noted a qualitative mismatch between the content of the teaching of criminal investigation in KFSC and the reality on the ground in police work. For instance, one officer commented:

> Abdullah, you remember when you and I studied at the College. They used to teach us from a criminal investigation textbook that was very theoretical and did not take account of what is actually going on inside police stations. How could what [the author of the textbook] wrote thirty or forty years ago, that was not even based on practical experience, be suitable for these days? So it's a combination, if you will, of poor preparation at the College and shortage of training on the job that's led to where we are now… unable to deal with Internet fraud (PS8).

Generally, it seems that failure to provide police officers with effective training in tackling Internet crime is an international phenomenon that transcends the Saudi context. Numerous studies which have been carried out on the policing of computer-related crime in different contexts highlighted the impact of the lack of training on police capability of handling e-crime cases (Bahr, 1999; Burns et al., 2004; Cheurparkobkit and Pena, 2003; Hinduja, 2004; McKenzie, 2006). However, the problem appeared to be experienced more severely by officers in the departments examined in this research. This only further reinforces concerns raised by various researchers about the failure of the current Saudi police training programmes to take into account the novel types of crime that are emerging as a result of the sudden economic, social and cultural change (Al-Thaqafi, 2006) and to develop the imagination and innovativeness of police officers (Al-Rabaiah, 2001).

Moreover, it is important to point out that although the training of officers was verbally recognised by participants from all levels of management (i.e. top, middle and lower management) as a key to effective policing of Internet fraud, the data show that in reality lower level managers, namely those directing frontline departments (i.e. police stations and the DDI), tend to be an obstacle to educating their officers to obtain the high levels of skill and expertise that can enable them to deal with Internet fraud more effectively. This issue emerged as a major source of concern for operational officers. During interviews, numerous comments were made that not only are there only a few training opportunities, but it is hard to obtain the approval of the department's manager to attend training. The majority of the operational officers spoken to at the case departments pointed out that managers often refused applications to attend training courses. In some locations, the researcher encountered officers who claimed to have been in service for a period of more than ten years without receiving any training, despite their continuous attempts to nominate themselves for training courses, which had always been blocked by their managers. As a result, the majority of the operational officers asserted a pessimistic view that the effectiveness of any strategy to train and qualify police officers to be able to respond to Internet fraud would be reduced by frontline managers' preoccupation with retaining their staff at all times. The following quotation, provided by an investigator who at the time of the research had not received any training for more than ten years, gives an indication of this dominant view:

> What needs to be addressed first is managers' unwillingness to let us go for training. Because even if the DPS was to arrange training programmes in Internet fraud, the officers who really should go on these programmes – I mean us, the investigating officers – won't be able to do so, simply because our managers won't allow us. The seats in those training courses would then go to other officers whose jobs have nothing to do with investigation and never deal with Internet fraud. Undoubtedly, this would be just a waste of resources, wouldn't it? (PS6).

In addition, these respondents made it clear that without the intervention of the DPS higher management to address this situation, officers would continue to lack skills and rely predominately on 'trial-and-error' in the performance of their job. An opinion that was expressed persistently and explicitly in this regard indicated that in order to ensure that officers of police stations and the DDI are among the beneficiaries of any training arrangement, the present requirement that their nomination for training courses be subject to their immediate manager's approval should be abolished. Instead, approval should be granted directly by the Training Division of the Riyadh Police. This, it was mentioned to the researcher, would be a temporary measure that need last only for as long as necessary to enable a sufficient knowledge base and expertise in relation to handling Internet fraud to be established in those departments. One respondent, who advocated such a proposition enthusiastically, described how in his view it would be viably realised in practice:

> In Government, we have the so-called Five-Year Development Plan. Here in the police, a strategic decision should be also made to draw a five-year plan for training officers in Internet crime. During these five years, training should be delivered to 20% of the workforce annually. Each police station across the country should be given a defined number of seats according to its size and location and all these seats must be used, regardless of whether the manager approves or not, by sending one officer at a time. Nomination should be for investigating officers and based on service years and rank (PS14).

In their interviews, five of the six participating frontline managers showed themselves to be less than willing to support and approve the training of their staff as much as they prioritised the fulfilment of performance requirements. They claimed that shortage of officers and accumulation of work left no room for investment in human resource development. Furthermore, they stated that there were increasing pressures from performance supervising bodies, such as the Follow-up and Inspection Department and the provincial branch of the Commission of Investigation and Public Prosecution, and therefore they were concerned that any underperformance would not be tolerated by these bodies even if it resulted from an officer's absence for training. As one manager put it:

> We are under strict and sometimes aggressive scrutiny of performance, and the ultimate responsibility for any underperformance lies on my shoulders. If they [the supervising bodies] detected any delay in our work and I said 'I've got officers absent for training', they would reply: 'You let them go and therefore you have to sort it out'. Nobody will appreciate that I have sent them to improve their skills (PS1).

In such responses, we notice that police frontline managers exhibited themselves to be task-focused, not approving, or at least not encouraging, their staff nomination for training. In their perception, training took officers away from task. Thus, short-term productivity goals were prioritised at the expense of long-term effectiveness.

However, when refusal of applications for training occurred, the impact of that on the unsuccessful applicants appeared to be more profound whenever they felt that it was directed selectively and not applied equally to all staff members. This was clear on a number of occasions during the research, when officers expressed considerable dissatisfaction with what they viewed as the influence of *Wastah* (patronage) and favouritism on managers' decision to approve or refuse applications for training. Regardless of whether real discrimination occurred in relation to nomination for training, the existence of a perception or feeling of unfairness in training nomination criteria appeared to be one of the major sources of organisational conflict and caused tense relationships between officers and their managers, as we have seen in the example provided earlier in this chapter. This should not be surprising when we know that officers on the receiving end of training attached great significance to it not only in terms of improving their professional skills, but also as a way of gaining personal interests. Indeed, extensive conversations with officers revealed that training was not always sought with a view to attaining skills essential to the crime prevention mission. In fact, it was observed that a considerable number of officers looked forward to training courses (of any kind) not necessarily for the knowledge a course may bring, but rather to achieve personal benefits. For example, some officers viewed the training as providing an escape from the daily pressures of their work, as one officer explained:

> The thing isn't just we haven't had training in Internet fraud, the thing is we've had hardly any training at all. I need to go on any training course, I need to walk away from the stress of the work here. Yes, you would need to attend from morning to afternoon, but compared to the situation here where you stay every day two or three hours after home-time and have to come to the Department at night to finish your cases, it's much, much better (DDI2).

Similarly, officers' search for financial gains appeared to be a significant motivation for their enthusiasm to attend training courses. To encourage Saudi officers to nominate themselves and join training courses, the Saudi Officer Service Law (issued in 1974) has set a standard Qualification Reward whereby a bonus of four percent is added to the Basic Salary when a total of 12 months training is achieved. This is not a one-off increase and the addition to an officer's salary can be repeated to a maximum of 30 %. While this link between training and increase in officers' monthly pay seems to be beneficial in terms of increasing the importance of training among officers and, thus, improving their skills and potential, the data suggest that it can negatively influence in-service training. Becoming eligible for the Qualification Reward was found to be a major concern for officers, driving them to seek to attend as many training courses as possible, no matter how relevant these courses were to their task. One officer talked explicitly about this when he described how the shortage of training opportunities had resulted in police stations' officers earning less than the rest of the DPS's officers:

> You've got to know that one of the disadvantages of working in a police station is that training is abundantly available everywhere but police stations. Colleagues outside police stations can enrol on two, three or perhaps more courses in one year. We here may spend 10 to 15 years and not have even 4%. I personally have been in service for about 13 years, but I could only have 9 months training, because all my service has been in police stations. I need any training course, even if they send me to learn to cook beans, I don't mind, honestly I don't mind, as long as it completes the 4% for me (PS15).

5.6 Summary

This chapter has presented the key issues to emerge from the analysis of the data collected from the empirical research regarding the organisational context of the police response to Internet fraud. It began by focusing on the ICU as a cybercrime-specialised arm of the DPS. From the evidence shown in this chapter, it appeared that the creation of the ICU has thus far had little, if any, impact on the policing of Internet fraud in Saudi Arabia. This can be said to be the result of a combination of different factors. For a start, the absence both of formal definition of the crimes relevant to its specialist role and of written policies and procedures concerning its operations has major implications for determining the types of Internet fraud which the ICU is supposed to handle as well as for understanding when and how the unit should be involved when an incident relating to this criminal activity occurs. The ambiguity surrounding the jurisdiction and work mechanism of the ICU opened the door for its staff to apply their own understanding of the responsibility and tasks of their unit. Thus, the ICU's role is narrowly focused on performing reactive undertakings at the request of other DPS investigative units. However, a noticeable and prevalent ignorance of the ICU's existence and role existed across those units, which reflects a serious organisational failure of the centralised management of the DPS to achieve synergy between its divisions. On top of that, building the capacity of the ICU both in terms of human resources and technology has yet to be put into action, rendering it currently incapable of operating as effectively as might be desired.

Given the merely superficial contribution of the ICU, the policing of online fraudulent activity remains primarily dependent on the police stations and the Departments of Detection and Intelligence (DDI), which are the traditional arms of the Saudi policing system. However, in the context of our sample police stations and DDI, the high level of organisational conflict which existed within and between these departments had a significant influence on the way Internet fraud is responded to, particularly in terms of limiting the scope for within- and inter-agency cooperation. Moreover, the research on these sites found no evidence of an intelligence-led approach to policing Internet fraud. The ability to apply such an approach to policing is undermined both by shortage of resources (human and technological) and by deficiencies in the formal structure of information sharing between police units, recording procedures, and officers' lack of knowledge in relation to cybercrime. Finally, the flaws and gaps identified in the area of training raise concerns about their impact on officers' ability to handle Internet fraud.

These findings and assumptions demand looking into how the policing of Internet fraud is carried out in practice, which is the subject of the next chapter.

Chapter Six

Police Response to Internet Fraud: the Operational Context

Chapter Six: Police Response to Internet Fraud: the Operational Context

6.1 Introduction

The last chapter has analysed the data relating to the organisational context of police response to Internet fraud. The analysis in the present chapter is focused on how the policing of Internet fraud is undertaken in practice by Riyadh police. The operational policing of Internet fraud depends upon the cultural conceptualisation in which this aspect of police work is carried out. The social norms and dominant cultural values affect the police response to Internet fraud incidents by shaping officers' attitudes and operational paradigms. In Western societies, the entrepreneurial attitude surrounds everyday life activities and to some extent social relations are controlled in accordance with a capitalist attitude. Reflecting this economic ideology and its concern with economic considerations, the policing of Internet fraud in a Western context is undertaken with the aim of establishing a secure environment for exchange and commerce in cyberspace. As the capitalist thought has become deeply embedded in industrial society, it affects how police perceive and respond to Internet fraud activities. This argument is supported, for example, by the findings of Murff's (2007) study of digital crime investigation trends in the United States, which showed a tendency amongst law enforcement agencies to place priority on computer crimes involving financial losses above the dollar limits set by the United States Attorney General's office. Similarly, McKenzie (2006: 225) reported not only that Internet fraud cases were given priority over other types of e-crime, but also that 'cost of an investigation was seen as the primary factor influencing the decision to launch e-crime investigations'.

In Saudi society, cultural identity is still based on moral and ethical norms because people are born into and bound to the social values of their society and are socialised in accordance with its moral values. In the Saudi context, therefore, it is argued that the police operational response to Internet fraud is likely to be shaped by moral principles and cultural values. This argument is supported by the findings of the research conducted in the Department of Detection and Intelligence (DDI) and five police stations in the Saudi Arabian capital city of Riyadh.

To outline this argument, the chapter is organised into five sections. The first section aims to analyse officers' orientation towards policing Internet fraud. This is achieved through providing a typology of officers in terms of their acceptance of both the organisational goals and the technological means of achieving those goals in the fight against Internet fraud activity. The second section discusses police prioritisation of Internet fraud incidents. In this section, particular emphasis is placed on examining the influential impacts of 'old' cultural values and moral standards on shaping a hierarchy of response to different types of Internet fraud. The chapter moves on, in the third section, to examine how Internet fraud incidents come to police attention. This includes an analysis of how the reporting of Internet fraud is affected by the local Saudi norms. The fourth section looks at how technological systems are utilised in the policing of Internet fraud. Here, not only is the extent to which a proactive response to Internet fraud can be limited by the human mediation of technology demonstrated, but also how cultural traditions and social norms shape officers' perceptions and operation of technological systems. Finally, the chapter concludes by examining the issue of 'policing the police' and highlights the role of religious beliefs in creating a type of self-surveillance of officers' actions.

6.2 Officers' Orientation towards Policing Internet Fraud

A number of Western police researchers have characterised the police as pragmatic conservatives suspicious of technological experimentation (Crank, 1998; Manning, 1992, 2008a; Reiner, 2000a). Other writers have indicated that police response to computer crime is shaped by an occupational subculture in which machismo and heroism coexist with an aversion to innovation. For instance, in an article entitled *Why The Police Do Not Care About Computer Crime,* Goodman (1997: 479), referring to American law enforcement agents, pointed out that 'the internal culture of police departments places a lower value on catching non-violent offenders', which explains, in his view, why 'officers are not clamouring to investigate computer crime'.

However, Goodman's perception of police officers' attitude towards investigating cybercrime seems to have been formed solely on the basis of his personal experience in the Los Angeles Police Department. Nevertheless, his claim of an omnipresent undercurrent of loathing of cybercrime investigations and social stigma against those who perform such work in police culture has hardly been supported by empirical evidence. McKenzie (2006) is perhaps the only researcher to date to have addressed this issue empirically. In his study of the Victoria Police response to e-crime, McKenzie (2006: 219) reported that Australian police officers were united in perceiving e-crime investigations as being 'not as exciting as other stuff'. In stating the police preference for investigating traditional crimes, one police officer was quoted by McKenzie as saying 'we have been brought up on a diet of news which relates to or revolves around violent criminal offences: where we hold the Homicide squad in a high esteem in this state, I think, and in the police force generally' (2006: 219). McKenzie suggested that these preferences influenced decisions about reported incidents, in that 'there was a general reluctance to conduct e-crime investigations...people don't turn their minds to this crime type' (2006: 220).

The previous writers' presentation of police officers' perceptions of and orientation towards handling cybercrime seems, however, like most of the existing literature on police culture, to fail to acknowledge that 'cop culture' is not 'monolithic, universal nor unchanging' (Reiner, 2000a: 109) and to take account, as Chan (1996: 111) emphasises, of the existence of 'internal differentiation' within a police force and 'variation in cultures among police'. Indeed, as Westmarland (2009) suggests, there would be differences in attitudes towards a number of key elements of police work in different departments, forces and countries, and individual officers would also have quite differing takes on important elements of their work.

This section draws on the data obtained in the police stations and the DDI (which were found to be the units with which the responsibility of dealing with online fraud activity primarily lies, as the ICU remained virtually non-existent in operational terms (see section 5.2)) to show that not all officers responded in the same way to Internet fraud investigations. In this respect, it will be illustrated how officers' attitude towards handling this type of cybercrime was shaped not only by the organisational culture, but also by the individual concerns of these officers.

In their study of CCTV in London, Norris and McCahill (2006) adapted Merton's (1938) famous categorisation of modes of adjustment to provide a typology of CCTV operators in terms of their acceptance of both the organisational goals and the technological means of achieving those goals within their work setting. Whilst it is acknowledged that the context of this study differs somewhat from that described by Norris and McCahill (a CCTV control room in which almost all activity was technology mediated), it nevertheless is a context in which officers were faced with computer crime and needed computer technology to address it. Thus, the technology dimension is essential to understand the actions and attitudes of the officers in question. Whilst a number of previous police researchers have offered categorisations of officer types (for example Broderick, 1973; Brown, 1981; Muir, 1977; Reiner, 2000; Shearing, 1981; Walsh, 1977), their typologies are more applicable to patrol officers and lack the technological dimension. For this reason, Norris and McCahill's (2006) adapted typology (see Table 6.1) is better able to capture the behaviours and attitudes observed among Saudi officers addressing cybercrime, and therefore it will be used in this section to describe the orientation of the operational officers of both the police stations and the DDI towards tasks relating to Internet fraud.

Table 6.1 A Typology of Officers According to their Orientation toward Internet Fraud Investigations

	Organisational goals	Techno means
Technophile-work embracer (conformist)	+	+
Technophobe-work avoider (drop-out)	–	–
Technophobe-work embracer (innovator)	+	–
Technophile-work avoider (ritualist)	–	+

Source: adapted from Norris and McCahill (2006: 109).

The first type of officer is the 'technophile-work embracer', who is oriented toward Internet fraud investigations and has a level of technological sophistication that enables him to carry out such investigations effectively. The second is the 'technophobe-work avoider', who not only perceives investigating Internet fraud incidents as a 'risk' to be 'averted', but also lacks the technological sophistication required to undertake this policing activity. Third is the 'technophobe-work embracer', who is committed to the organisational goals pertaining to the policing of Internet fraud but rejects the technological means of achieving them. Finally, we have the 'technophile-work avoider', who rejects the organisational goals concerning the policing of Internet fraud but has a level of technological sophistication required to achieve those goals if he wished to pursue them.

Among the forty operational level officers observed in the police stations and the DDI, the majority (25/62.5%) fell into the technophobe-work embracer category, while a further four (10%) were technophobe-work avoiders. Of the eleven officers who could be described as technophiles, four (10% of the whole sample) were work embracers, while seven (17.5%) were work avoiders.

Certainly, providing various examples of each category of officers would offer deep insight into the typology and help describe officers' orientation towards the policing of Internet fraud more fully. However, to avoid unnecessary repetition, in what follows only one typical example will be used to illustrate each of the categories of the typology.

The technophile-work embracer

Major A is a 37-year-old officer who has worked at the Southern Police Station for around three years. Prior to that, Major A had worked in a Riyadh western police station for over four years, before he was transferred to the northern district of the city, where he spent another eight years. A total of fifteen years of service in Riyadh police stations gave Major A vast practical experience in criminal investigation, especially as he had worked in some of the busiest stations in the city, dealing with a number of very complicated criminal cases. Despite applying for a number of in-service training programmes he was only sent on two courses, one on basic criminal investigation, lasting for four months, and a three-week aimed shooting programme.

Major A was committed to his job and highly conscientious. During the 15-day observational period in his station, not only was he always punctual and observant of the official working hours[14], but he also returned to the office (on seven different days) in the evening to work on his cases. In terms of organisational goals, Major A was basically a 'crime fighter'. He was described by his manager as 'the most efficient investigator in the station'. He had managed to solve almost every case he had dealt with. In particular, according to the manager's record statistics, his investigations had led to the arrest of the perpetrators of many complex cases, including six homicides, nine car thefts, and fifteen burglaries.

However, in his department, Major A was also recognised as 'an electronic crime expert' and thus had been relied upon to solve cases of Internet fraud. During the three years prior to the research, he had led eight Internet fraud investigations. In one case, which involved a 32-year-old male victim who had lost a total of SR307,000 as a

[14] Official working hours in police stations usually started at 07:30 am and lasted for seven hours. On-duty shifts out of working hours began at 02:30 and continued until 07:30 the following day.

result of responding to an online investment scam by a group of three men of two different Arab nationalities, Major A had to pursue the case beyond his jurisdiction. As he explained:

> In 2003 I went to the Eastern region and was able through personal efforts to identify the IPs [Internet Protocol Address] and telephone numbers involved in the case. I was able then to seize seven personal computers. I then wanted to examine those PCs. I contacted the Department of Criminal Evidence Examination, but they said, 'No, we don't have a computer lab'. I saw such a lab once in Malaysia. You bring the PC to them. They consider it as criminal evidence which shouldn't be tampered with or destroyed. So what they do is they basically do imaging of the entire device before they start examining it and they work on the copy rather than the actual PC in order to preserve it. Guess where I found such a lab in SA? I found it in ARAMCO [the Arab-American Oil Company]. Thanks to my personal relations with Dr…. they examined the PCs for me and identified the suspect computer and provided me with an excellent report. They showed me the spy programmes they found in the PC, such as Sub7, and they provided a detailed list of the websites accessed using the PC.

In the above case, Major A was willing to rely on his own means to travel to the Eastern region to seek further evidence which led to the identification of the perpetrators. In addition, his personal relationships provided access to a private institution's investigative resources.

Moreover, his response to Internet fraudulent activity was not entirely reactive, but it involved also some preemptive policing tactics. As we have seen in Chapter Four, one of the obstacles to implementing a proactive approach to policing Internet fraud is that partnership and cooperation between the police and private agencies is limited by a high degree of mistrust and inflexible bureaucratic procedures. However, Major A was able to go beyond the limitations of the formal public/private divide by employing personal forms of partnership to access information generated by private surveillance systems and exploit them for proactive policing of certain online fraud situations. This was evident in his use of the images produced by a bank's ATM point CCTV cameras to proactively monitor and track perpetrators of a specific type of 'online bank account thefts':

> *Extract from field-notes*: At 12:37 Major A went to the station's Chief Investigator to discuss the Case Final Report of an Electricity Company warehouse which had been broken into by a group of 'copper thieves' to steal cable reels. While I was waiting in his office, Corporal K came in with an envelope in his hand. He left the envelope on the desk after writing a note on a small yellow sticky note and attaching it. After ten minutes, Major A returned and when he found the envelope he looked at me and said, 'This is one of the

> things I am doing, Abdullah, to track *Sarraf*[15] fraudsters'. Major A then opened the envelope and showed me a CD which he said had been sent to him by the manager of the neighbourhood branch of [a local bank]. 'I talked to him and he agreed to let his security team analyse the recording of the CCTV cameras at all the *Sarrafs* in our area and provide me with parts of the recording which show people handing in money to someone else after they have withdrawn it from the machine, because he might be a *Sarraf* fraudster, you know'. Major A went on to say, 'When I get a case of this kind and find the *Sarraf* that was used, I can go back to the recordings I have got for that *Sarraf* for the same date and time and they might help me identify the fraudster'.

Major A began targeting '*Sarraf* fraudsters' using this preemptive technique following his investigations of two incidents which revealed that one *Sarraf* had been used in both cases to withdraw the money stolen online from the victims' accounts, after being transferred to other accounts which were used only to avoid any tracking of the perpetrators' identities. These accounts belonged to individuals who were deceived by a fraudster who had approached them at the cash machine and claimed he was in urgent need of cash but had no card to withdraw from his account. He therefore asked for their account numbers so that he could phone-transfer the amount of money he wanted to their accounts and then they would withdraw it for him. Convinced about the man's circumstances, these individuals willingly gave their account numbers to him and the money was transferred, withdrawn from the ATM machine, and then handed over to the man. The fraudster took advantage of the fact that in Saudi banks, Internet and phone banking logons are the same.

In terms of technological sophistication, Major A was the officer with most experience in ICT. He used computers and the Internet very efficiently and showed extensive knowledge about matters such as protection software, anti-virus programmes, programming, file transfer methods, encryption and telecommunication protocols. More importantly, however, he possessed what Hinduja (2004: 352) views as 'applied investigative knowledge as to how computer crime differs from traditional crime', rather than just technical knowledge associated with hardware, software and digital communications, as the following example illustrates:

> *Extract from field-notes*: At 09:20 I was sitting in Lieutenant S's office when the phone rang. Lieutenant S, on answering, handed me the phone. The caller was Major A, who said there was something I might be interested in and invited me to his office. I excused myself from Lieutenant S's office and went

[15] *Sarraf* is the name used in S.A. for an automated teller machine (ATM), while a *Sarraf* card is a type of debit card issued by Saudi banks to their customers. They can only be used presently at ATMs and Points of Sale (POSs). However, the details of this card are a compulsory requirement for registering for Internet and phone banking services.

> straight to Major A. He told me that Dr. [a Friday prayer leader in a large Riyadh mosque] had complained about a loss of SR230,000 from his account. The case had been referred to them by the Riyadh Governor three days previously for investigation, and the complainant had been invited for interview. When the man entered the office, Major A poured him a cup of Arabic coffee from a flask which he kept on a table next to him. He then introduced me to him and reassured him about my presence in the interview. Meanwhile, M, an assistant officer, came in to transcribe the interview in an Investigation Book. In response to Major A's questions, the complainant mentioned that on checking his account the previous Saturday he found that SR230,000 was missing and contacted his bank immediately. The bank told him that the money had been transferred over the last three days to another account through the Internet, although he had not set up an online banking account. He was then given the details of the recipient account and advised to lodge a complaint to the authorities, and he opted to go to the Governor because he thought the police would not help him. With further questioning by Major A the man explained that on the day of the first transfer he received a call from someone purporting to be from his bank, who said that his account had been subject to attempted intrusions by strangers who had got the PIN number, and to protect it from further attempts, his bank account details needed to be updated very urgently, including changing his PIN number, within 30 minutes, otherwise the account would be closed permanently. The complainant had been instructed to proceed to the bank's nearest *Sarraf* and use his card to change the PIN number, but only after he had received another call to advise him what to do when he got to the *Sarraf,* the caller asked him to change the number. He did so but was told that the attempt had failed and that he needed to give the caller the new PIN number and card number so that he could do it. He gave him the numbers and after a moment was told that the details had been updated successfully, but to activate the account, he must make a transaction. He was given a bank account number and asked to transfer SR5 to that account. After he had done so he was thanked and told that everything was now ok.
>
> Major A interrupted the man, saying, 'Of course, the caller was not doing any updating. It was only a ploy to acquire your *Sarraf* card and its PIN numbers'. He explained that AL…..bank requires the first transfer transaction to be made using a *Sarraf* or personally at the branch before they can be made subsequently on the Internet. 'The fraudster must have used the account details to create online access to the account, which allowed him to move the money'.

As can be seen from the above incident, Major A showed 'applied investigative knowledge' in distinguishing the role of the Internet in gaining access to the victim's bank account. Indeed, as the investigation into the case progressed, his surmise as to how the bank account theft might have been completed online was proven to be well founded.

What should be noted, however, is that Major A's expertise in Internet fraud investigation was not founded on formal training and organisation-initiated skill development, since he was not recruited based on pre-service technological knowledge, nor had he received any relevant training while on the job. Rather, it stemmed from his personal interest in the field, enhanced by self-education. In this regard, out-of-work private lessons and informal courses in computer and Internet technologies, as well as tapping into Internet resources, played an important role in shaping his technical experience. Moreover, Major A perceived his personal relationships with several ICT experts both in private and public institutions as constituting a significant resource for his investigations of Internet fraud cases:

> The most important thing is that you deal with these people respectfully. You shouldn’t think that because you are police and in a position of authority everyone is going to take your request as an order that must be obeyed. I approach people in a polite manner and ask them respectfully and they cooperate with me. I succeed only because I have good relationships with people in the banks’ Information Security Departments, and consult colleagues who have expertise. For example, Colonel [....] in the *Arar* [the Northern region of S.A.] police and Lieutenant Con. [....] in *Asharqiyah* [the Eastern region] police have done excellent jobs in investigating this kind of crime, so I contact these officers and ask them about different things. I might even ring an ICT person in a computer shop and ask him about certain things.

Although Major A did not display physical manifestations of piety, such as growing a long beard, his religiosity was evident in his behaviour:

> *Extract from field-notes*: At 11:00 Major A shut the door of his office and grabbed a prayer mat from the lower drawer of the cabinet in the corner. He asked me if I could excuse him while he performed the *Duha* (morning) prayer. I said, ‘Ok’, and then he went on to pray for six minutes. According to Islamic teachings, praying during *Duha* (which is the time between sunrise and noon) is a voluntary but preferable act that Prophet Mohammed used to undertake and recommend to his followers during his lifetime.

The influence of religiosity on Major A’s undertaking of his job, particularly with regard to his response to Internet fraud, was clear in a number of instances. For example, in a Saudi-style online blackmail case (details of this type of Internet fraud will be given in the following section), he endeavoured to protect the identity of the female victim from negative publicity, as he perceived doing so as a religious duty which he must observe. He explained:

> When we got the man, he agreed to pay the woman back the money he had taken from her, but on the condition that she appeared in court. But that would be very damaging to the woman because she would lose her chastity in the eyes of people forever, although she was innocent throughout the fraud and contacted the criminal and paid him only because she trusted his promise to marry her. So, I included my personal opinion in the report that was submitted to the Riyadh Governor and I asked that the Public Prosecutor undertake private litigation on the victim’s behalf. Fortunately, the Governor endorsed my opinion and her name was preserved. You know, we are required by Allah and his Messenger to protect people’s honour and reputation. After all, she is my sister in Islam and I have an obligation to protect her and help her lead a clean life.

Major A's action in the incident above demonstrates the influential impact of social and religious values on officers' response to Internet fraud. As Saudi society has been built on the basis of these values, one could argue that the policing of Internet fraud would be shaped and performed in accordance with these moral standards, which are deeply ingrained in the culture of society and represent a major aspect of its social and theocratic identity. Indeed, Saudi people seem to hold a solid belief in cultural values and religious norms and their vital roles in their everyday philosophy of life.

It should be mentioned that, in his station, Major A maintained a high profile and enjoyed a great degree of respect and admiration from both management and colleagues because of his expertise in solving Internet fraud cases. In fact, this attitude is demonstrated by the medal and numerous certificates of appreciation that he had been awarded upon successful investigations. It is also reflected in this remark by the station's manager:

> We are lucky to have Major A in our station. Because of him we are seen as at least doing something about Internet fraud, not just standing helpless in the face of cases reported to us (PS10).

Similarly, although with a sense of envy, a colleague commented:

> I really wish I could learn to investigate Internet crime. Look at Major A, he is known even at the PDS level (PS14).

This positive attitude towards an officer with specialist skill in Internet crime investigation clearly contradicts the suggestion in Western literature that such individuals and the functions they perform are not accorded in the internal culture of police departments the same level of respect and admiration given to 'real cops' (Goodman, 1997; McKenzie, 2006). That said, there is an important issue which may help to explain the apparent difference between Western and Saudi perceptions of specialist Internet crime investigators. This issue relates to the fact that the duties of Police Stations are mainly investigative and do not involve responding to emergency calls or patrolling, which are the responsibility of the independent General Department of Patrols. This obviously minimises the opportunities for action and adventure in station officers' work. It should not be surprising, then, that investigative competency, including solving Internet fraud cases, gains paramount importance over machismo and physical bravery. This might explain why Major A volunteered to take on some of the Internet fraud cases which were allocated to his colleagues.

The technophobe-work avoider

Captain S is 28-years-old and holds a Bachelor degree in security sciences. He came from a tribal community in the northern part of the country. Despite having worked in the capital city for almost eleven years, Captain S was still committed to tribal values and traditions. In Saudi tribal communities, social values, such as family allegiance, are moral obligations and should not be ignored. Members of these communities believe that the collective interest of family and relatives should take precedence over individual interests. This mindset led Captain S to put the collective interests of his family and relatives over work duties. For instance, he was in a hurry to leave his interview and asked to postpone it, saying:

> I've just received a call to say that some of my relatives are coming today [from another city]. I have to pick them up from the airport and prepare an *Azoomah* (a collective dinner) in their honour...They are coming to have a medical check-up at the hospital. As I have to accompany them, I don't think I will be in tomorrow either, I am sorry.

Throughout the observational period in his unit, Captain S's frequent absence and avoidance of work were mainly associated with fulfilling the social needs of family, relatives and friends. In tribal culture, fulfilling such social needs is very important in maintaining individual, family and tribal reputation. Captain S emphasised that as long as a person meets his relatives' social needs, he will be referred to with phrases like '*Wnaam*' (he is a helpful person) and '*May Allah brighten his face*' as an indication of his good reputation. He added that not meeting social needs, for whatever reason, would be interpreted as an indication of helplessness and lack of loyalty to the family, tribe or friendship. As Bjerke (1999: 118) has observed, in Arab culture, including Saudi culture, 'loyalty (to family, tribe or friendship) is seen as a virtue and considered more important than efficiency'. This was clear when Captain S left work frequently to take his wife and children to and from work and school, or to accompany a family member to the doctor. He belonged to a conservative and collectivistic society that imposes on its male members social demands and obligations that they have to fulfil, even during work time. While having a family driver is socially acceptable and may confer prestige in non-tribal communities, using the driver for such purposes is socially unacceptable in tribal communities, except under special circumstances, such as disability or illness. Thus, Captain S was reluctant to relinquish social obligations to the driver in an effort to maintain punctuality at work:

> I take my wife to her work every day. I cannot let her go with a stranger such as a family driver. It is not religiously nor even socially acceptable to send a woman out without a *'Mahram'* [e.g. her father, brother, husband and son].

Besides his frequent absence and avoidance of work, Captain S lacked the technological sophistication required to respond to Internet fraud effectively. In particular, he had obtained no qualifications to handle computer crime, either pre-service or on the job. Moreover, his experience of dealing with ICT was very limited, and he expressed a lack of interest in following developments in technology as he had 'more important things in life to care about than computers and the Internet'. This negative attitude towards technology influenced his response to Internet fraud incidents, as the following incident illustrates:

> *Extract from field-note:* It was 17:23 on Monday. Captain S was the full-day duty officer in the Eastern station. In the middle of a conversation in which Captain S was describing to me how he had managed to get transferred from another station in Riyadh to the current one, while we were eating some of the cake Corporal D had brought to us as he was celebrating his promotion to corporal, a man in his forties interrupted, '*Salamu-alaikum*' [peace be upon you, the Muslim greeting]. 'I have been defrauded and I want to report it', said the man, facing Captain S as he appeared to have distinguished him by his uniform. 'How did you get defrauded', replied Captain S. The complainant began to explain that he was doing a doctoral research and often searched the Internet for materials relating to his subject. While doing so, he had come across a website that claimed to provide access to unpublished theses and offer digital versions of books. Having found some publications that he thought would be useful for his work, he decided to buy five items for a total of SR2,350. After he placed his order using his Visa card, he received confirmation of the transaction, which indicated that the purchased items would be sent onto his e-mail within 30 minutes, so that he could download them immediately. Although he never received the items, he was surprised when he found that he was charged double on the online orders. The man mentioned that the website had contact details which indicated that it was based in Jordan, but when he tried to use them, he got no answer.
>
> 'We cannot do anything about it', said Captain S then to the man, 'The police cannot help. You should go to the CITC….They are the people who can locate this website', added Captain S. The man looked disappointed and commented, 'Why should I go to the CITC? You should communicate with them. If the police can't help me in this matter, who else can?'.......He then left after being provided with a description of where the CITC is based by Captain S. Anticipating any questions by me, Captain S smiled and said, 'Look, if I was naïve and took unfinishable cases such as this seriously and opened a case file for it, I could end up having loads of cases at the end of my shift, which would take ages to clear up. How could I find criminals in the Internet when all I know about it is only how to send and receive emails?'.

In the incident above, Captain S could have acknowledged the victim's report and provided only a 'tokenistic' response to the incident, for example, by documenting the information provided by the complainant and then referring the whole case to the

Commission of Investigation and Public Prosecution (CIPP) (as we will see in the following section), since he did not have the technical capacity to investigate it. However, Captain S was a ‘technophobe-work avoider’ and thus he chose to dismiss the incident completely and divert the complainant to another agency as a way of minimising his workload. In fact, this was not the only occasion when Captain S acted in a dismissive manner towards a complaint of Internet fraud being lodged to his station while he was the full-day duty officer. In another incident a man approached the station to report that he had lost SR1,400 in a scam in which he had been deceived into purchasing a herbal prescription advertised on an online medical forum, which he had never received. Captain S managed to avoid being burdened by the investigation of the case, this time not by diverting the complainant to another authority, but rather by convincing him that he was responsible for his victimisation, and that ‘it’s not the police’s responsibility to recoup money handed over too foolishly to thieves lurking in the Net’.

The technophobe-work embracer

This category of officers is epitomised by Major N who, at the time of the study, was in his mid-forties and had five children. He joined the police as an assistant officer after completing secondary school. As the oldest brother of his family, he had to leave school to work to support his parents, brothers and sisters. However, by taking evening classes, he obtained a high school certificate, which contributed to his rapid promotion. In Saudi Arabia, assistant officers can qualify, based on the recommendation of their superiors and subject to the approval of the King, for promotion to be commissioned officers if they completed their prescribed period of service at the rank of Staff Sergeant before they were due for retirement. Therefore, after eighteen years of service as an assistant officer, Major N was first promoted to the rank of Second Lieutenant before his further promotion continued and he had reached his current rank three months prior to the commencement of the fieldwork of this study.

Unlike most of the officers, he did not join the regular off-work meetings in *el-Istraha*, perhaps due to the difference in age and educational qualifications between him and his fellow officers. The other officers were from a younger generation and had commenced service as commissioned officers immediately after graduating from King Fahad Security College. Moreover, he did not share their interests and had a different lifestyle and responsibilities, such as raising his adolescent children and following up their education. Nevertheless, he maintained good relations with colleagues and was respected in his department.

Apart from his basic police mentoring when he was first recruited, Major N had received no further specialised training. He had applied to attend two training courses, a specialist programme in Intelligence and Personal Identification held in a neighbouring Arab country, and a locally-provided year-long English course, but both of his applications were declined by the management on the grounds of a staff shortage. Despite this, Major N appeared to take his job seriously and was an honest and diligent officer. Although his appointment in the Financial Crime Unit was not based on previous investigative experience, he was praised by his manager for achieving several successes. During the observational period, it was noticed that Major N's presence in the department extended beyond the official working hours and he frequently visited his office at different times of the day to work on his cases. For example, he was interviewed in his office at 23:00 on Thursday[16], at his request, because he was already in his office to interview two suspects caught at a cattle auction while trying to sell sheep which they had stolen from their owner's stockyard on the city's periphery.

While Major N was very dedicated to his job, he hated dealing with Internet fraud. As a member of a tribal society that is centred on Islamic cultural traditions and moral values, he appeared to be a conservative person with total adherence to social norms and religious beliefs. This characteristic affected his attitude towards the Internet. As he explained:

> I refused to allow the Internet to enter my house to avoid its negative impact on my children's behaviour. There might be some benefits from the Internet, but they are outweighed by the big evil that it entails. It's a danger and source of temptation through websites that support and spread activities which are decreed illegal by Islam, like pornography. It's also a time waster. If I allowed it in my house, my family and I would waste hours and hours in front of the screen. We wouldn't perform prayers on time; we wouldn't sleep early and wake up in the morning to go to work and school on time; the children wouldn't give attention to their school homework and revision. So I don't like the Internet and don't deal with it.

As one can imagine, it would be very difficult for someone who rejected the Internet on principle and had no experience of using it, as a result of the influence of moral and religious scruples, to understand and be willing to respond to crimes associated with this technology. Indeed, Major N's dislike of dealing with this type of

[16] Thursday is an official weekend holiday in Saudi Arabia.

criminal activity was so intense that on one occasion, when assigned to undertake an Internet fraud-related operation, he ‘unusually’ resisted and negotiated the assignment with the head of the department:

> *Extract from field-notes*: At 11:15 as I was discussing with the head of the department a schedule for his interview, he called Major N to his office. When Major N arrived he was told by the manager that instructions from the Governor had been sent down to the department regarding an online forum used to post offers for assistance, in return for money, in obtaining teaching jobs for those female university graduates who were not employed in the Ministry of Education’s public recruitment competition. The manager asked Major N to monitor the online forum and begin collecting information to track those who were behind the employment facilitation offers. ‘I am not the right person for this job, I hate the Internet and I don’t use it’, replied Major N, who tried to convince the manager that as they needed to respond to the Governor’s instructions speedily and report the actions taken in good time, the assignment should be allocated to an officer who had previous experience in using the Internet and an understanding of the mechanisms of Internet forums. First Lieutenant R was later instructed to undertake the case on the grounds that he held a degree in computer science.

However, the replacement of Major N by First Lieutenant R did not result in a speedy and effective intelligence gathering operation to identify the Internet fraudsters in the incident above. This is because the latter was a ‘technophile-work avoider’, who although possessing the level of technological sophistication required to achieve the organisational goals if he wished to pursue them, rejected those goals, as will be explained below.

The technophile-work avoider

At the time of the study, First Lieutenant R was aged twenty-five, married with a nine-months-old daughter, and had worked at the department for around four years. Unlike the rest of the officers in the department, he started his service with combined qualifications. He had first obtained a university Bachelor degree in Computer Science before joining KFSC to train as a police officer for one year. He used computers and the Internet very proficiently and was up to date with regard to mobile Internet technology. His proficiency in ICT enabled him also to assist two members of his *el-Istraha* group on issues concerning technical problems on their personal computers; he helped one of them to install software, while the other needed his computer to be cleaned of viruses and reformatted. In addition to the desktop computer in his office, he always brought his own laptop, which enabled him to access the Internet at work.

However, although First Lieutenant R had a high level of technological sophistication, he very rarely used the technology in his response to Internet fraud, relying instead on the 'non-technological' means that other 'traditionalist' officers in his department used. For example, as was indicated above, due to his technological background, he was chosen instead of Major N to carry out a surveillance operation to trace those behind online 'employment facilitation' advertisements. However, despite the 'urgency' of the message received from the head of the department, First Lieutenant R made no attempt to place the targeted online activities under his 'electronic gaze', utilising the technology available at his disposal. Nevertheless, as he could not ignore the assignment completely, he resorted to paperwork as a device for 'work avoidance' by writing a request for assistance to the CCIT. The request contained the details that were already available, which included only the name of the website and its URL, and did not specify the type of information needed from the CCIT, which suggests that it might have been intended mainly for the purpose of 'throwing the case away' while staying safeguarded against administrative accountability for delay.

To understand the 'work avoidance' strategy applied by First Lieutenant R in the above example, it is important to know that the DPS, as a Saudi governmental organisation, tends to mirror the hierarchical culture of the Saudi government, in which executive power and decision making are centralised at the top and filtered through many layers of hierarchy. In this environment of power concentration, the administrative policy on communication, whether between departments and units within the DPS or beyond, allows only vertical contact. Accordingly, the request that First Lieutenant R made to the CCIT had to go through the entire hierarchical command structure and be subject to all the standard bureaucratic procedures. In practice, this provided a long period of 'relief' for First Lieutenant R from the 'trouble' of working on the case without being 'blamed' for the delay, as it was 'somebody else's responsibility'. In a sense, this demonstrates Ericson and Haggerty's (1997: 423) observation that in police work, 'investigative efforts are judged not only in terms of case outcomes but also by the process of knowledge production'. In the words of one of Ericson and Haggerty's respondents, 'a thick file shows that the job is done even if the case remains unsolved' (1997: 423).

It seemed that one of the main factors behind First Lieutenant R's avoidance of utilising his technological sophistication in responding to Internet fraud was the tense relationship that had developed between him and his management. Several times during the period of observation, he expressed a desire to leave the department as he felt neglected and unsupported by his superiors. One instance followed an argument with the head of the department over an application for three weeks leave towards the end of Ramadan (the fasting month), which had been refused by the head of department, spoiling First Lieutenant R's plan to join his parents and siblings in their stay in the Holy City of Makkah[17]. His conflict with the management was further fuelled by what he viewed as their depriving him of his 'deserved right' to receive the 'Computer Reward', a salary-added bonus, equal to fifteen percent of the basic monthly wage, prescribed by a Cabinet Resolution for those public sector employees who use computing in the performance of their jobs. The introduction of the Computer Reward was intended to facilitate the integration of computerised work into governmental organisations' systems. First Lieutenant R sought to justify his non-use of the computer in carrying out his job tasks, including the targeting and tracking of an online fraudulent activity, on the basis of not receiving the Computer Reward, as the following quotation reveals:

> Why should I be bothered to use the computer or the Internet, which I pay for from my own pocket, to enhance the position of some people in the management who want to show off to their bosses that they are able to catch Internet criminals when I don't get the Computer Reward which so many officers in the DPS are getting even though they may make little or no use of computers in their work? I am only obliged to do what I get paid for.

It can be argued that this demonstrates the extent to which the implementation of any policy for controlling Internet fraud can be shaped by officers' individual concerns.

As our typology shows, there was a wide variation in the extent to which individual officers accepted or rejected organisational goals related to policing Internet fraud and the technological means of achieving those goals. One of the most important determinants of this variation was the influence of the dominant cultural norms and moral values in Saudi society on officers' behaviours and attitudes. Recall, for instance, that Captain S, who was a technophobe-work avoider, appeared to be less committed to his work punctuality than to his society's cultural norms and social values, and that he completely ignored the Internet incidents brought to his attention, lest responding to them distracted him from fulfilling his tribal and social obligations. Similarly, Major

[17] According to the Islamic doctrine, performing *Umrah* (which is an Islamic ritual that is performed at Makkah at any time of the year and includes circumambulating the *Ka`bah* seven times and walking seven times between the hills of *Safa* and *Marwah*) during the month of Ramadan is considered to be equivalent to performing pilgrimage with the Prophet Mohammed. Therefore, most Muslims, especially Saudis, like to go to Makkah during Ramadan to perform *Umrah* and be close to the Holy Mosque.

N’s lack of technological sophistication seemed to be linked to the influence of his moral scruples and religious beliefs on his attitude towards the Internet. In addition to the impact of the ‘old’ cultural and social norms, the typology also showed that officers’ orientation towards ‘fighting’ Internet fraud is also dependent on the organisational context and individual concerns of officers. As we have seen, First Lieutenant R’s disillusionment with his job as a result of his continuous conflict with the management was reflected in his non-use of his technological expertise to respond to Internet fraud. Conversely, concerns with maintaining a good reputation at work led Major A to become a self-prepared ‘cybercrime fighter’. In general, the differences detected in officers’ orientation towards policing Internet fraud provide clear evidence against assumptions of a universal police culture, under which the concerns of individual officers are readily subsumed. On this evidence, the argument that in police organisations, the entire work force inevitably falls into line behind the dominant organisational and occupational ethos of ‘crime fighting’ or ‘work avoidance’ needs to be treated cautiously, at least with regard to the Saudi context.

6.3 A Hierarchy of Response Shaped by ‘Old’ Cultural Norms and Religious Beliefs

One of the most striking results to emerge from the current research is the influential impact of cultural values on officers’ prioritisation of Internet fraud incidents. As has been argued throughout this thesis, Saudi society remains a fundamentally traditional society, whose cultural norms and social patterns shape the police response to Internet fraud. This cultural ‘identity’ has its consequences on both officers’ attitudes and operational paradigms. Accordingly, the high level of importance that Saudi society accords morality was found to have a considerable influence on officers’ decision to respond to Internet fraud incidents brought to their attention. This was evident in the high priority given to cases that were related to morality, regardless of the size of loss involved, over other types of Internet fraud. These cases, which officers placed at the top of their hierarchy of response, were categorised as ‘Saudi-style blackmails’.

‘Saudi-style blackmails’ are those incidents where the perpetrator succeeds in obtaining ‘compromising materials’ on the victim electronically and then uses them to extort money from that victim. From a legal perspective, such crimes would be classed as extortion, which is conceptually and legally distinct from fraud. However, Saudi police officers, whilst acknowledging that these were blackmail incidents, clearly conceptualised them as fraud, and frequently mentioned them when asked about Internet fraud. This was attributable to their focus on the element of deception involved in such crimes and to a linguistic feature of Arabic, in which the words fraud and deception are synonymous; the term ‘fraud’ is not confined to the connotations of financial gain associated with the word in English. A further explanation, or a compounding factor, may be the absence, as was discussed in Chapter Four, of a clear classification in the police recording system – and, indeed, in the Anti-Cybercrime Law itself – to distinguish between different kinds of cybercrime. This is a source of potential confusion, as the conceptualisation of offences, and hence the response to them, becomes subject to the interpretation of the officers. In this case, their interpretation was dominated by the underhand means employed to obtain the material which becomes the lever in the subsequent blackmail.

The compromising material may be obtained from the victim voluntarily when a perpetrator meets a vulnerable woman on the Internet, whether through e-mails, chatting rooms, or instant messaging services, and exerts pressure on her in various ways, including winning her confidence with promises of love and marriage, until she lets down her guard and sends him photos, and in some cases videos, of herself. Hacking into the victim’s computer is another way of acquiring her pictures, which can also be downloaded from a computer or cell phone left at a repair shop.

An important point worth highlighting is that in many cases the photos are usually quite innocent and if seen anywhere else in the world, would be considered unremarkable. However, in a conservative society such as the Saudi one, the possession of a photo of a woman wearing only her regular clothes and without an *abaya* (a long black robe that covers the body) or *hijab* (a veil which covers the woman’s head and face) is ‘scandalous’ and could damage the woman’s reputation and that of her whole family. Mindful of such serious consequences, police officers sought to provide a prompt response that would avert the publication of the victim’s ‘scandalous’ pictures, as can be seen in the following incident:

> *Extract from field-notes:* At 12:05 Captain B was called to the Chief Investigator office. After 15 minutes he returned to his office holding a green folder. After he sat down he told me that it was a Case File that the Chief Investigator had given him to work on and that it contained a written complaint that a girl accompanied by her sister had submitted to the head of the station before he sent it down to the Chief Investigator. ‘Some pictures which were taken

> of the girl and other women at a wedding party were obtained by an evil-doer, and you know what these evil-doers use such pictures for', said Captain B. 'He began to send her emails, threatening her that if she didn't pay him what he wanted, the pictures would be uploaded on the Internet. He said also that he knew her father's mobile phone number and threatened that the pictures would be sent to him. So the girl paid him, but he just didn't stop blackmailing her until she'd paid him a total of SR30,000 and she came to us only when she could not pay any more money'.
>
> Captain B then did not complete the interview that he had started with a foreigner worker who was arrested selling homemade alcohol. Instead he began immediately preparing a Summoning Letter, using the details of the repair shop provided by the complainant, summoning the shop owner and all the shop workers to attend the station no later than 08:00 tomorrow. He then took the letter to be first endorsed by both the Chief Investigator and then signed by the station's manager. When he returned after 5 minutes, he picked the phone and called Captain R, who is the head of the Administrative Affairs Unit, to ask him to assign one of his staff to collect the Summoning Letter from him and take it to the computer repair shop, where it must be handed to the owner personally. 15 minutes later, Soldier[18] H entered the office and said that he had been instructed by Captain R to take the letter. 'Make sure you hand it in to the shop owner personally and tell him that he and his workers must be with us tomorrow morning', said Captain B to Soldier H as he was passing the letter to him. 'We must find the blackmailer before he begins spreading the pictures, because if that happens the girl's reputation will be destroyed forever', added Captain R.

The concern with the publication of compromising materials and its potential to cause public humiliation and damage the reputation of the victims and their families was not, however, the sole driving force behind the high priority given by the police to Saudi-style blackmails. More importantly, the main impetus was linked with the preservation and sustaining of morality and ethical values. In other words, officers endeavoured to act quickly to protect the female victim from 'slipping' into immoral behaviour as a result of the pressure exerted on her by the 'blackmailer', as can be detected in remarks such as the one below:

> In the majority of the Saudi-style online blackmail cases we have got, the financial gain was the only motive for the perpetrator. But there were also cases where the offenders were more merciless, and their blackmailing went beyond extorting money from the victims to demanding intimate favours from the girl. In these circumstances, our duty is first and foremost to protect the Muslim sister and not sit and watch her being dragged into vice by the evil-doer. Because after all, women are weak and not every girl can remain resistant to the blackmailer's demands to have sex with her, especially if she felt that might be the only solution to make him stop the scandal of the pictures (PS2).

This situation indicates that moral and normative values constituted an important aspect of policing Internet fraud in Riyadh. The aim was to maintain morality and virtue

[18] 'Soldier' is the title of the lowest rank in the hierarchy of assistant officers in the Saudi military and police.

in society. This interpretation is supported by the fact that religious righteousness and moral integrity represent an essential criterion for the recruitment and promotion of Saudi police officers.

In addition to moral and social considerations, the involvement of the Commission for the Propagation of Virtue and the Prevention of Vice, better known locally as the *Alhai'a*, in the handling of Saudi-style online blackmails appeared to play an influential role in the urgency with which this type of Internet fraud incident was treated by the police. In Saudi Arabia, the *Alhai'a* is a governmental institution which undertakes the role of preventing behaviours that are believed to be forbidden by Islamic principles, particularly those related to morality. To fulfil their mission, the *Alhai'a* members have powers that entitle them to observe, search and detain any individual who violates the religious and moral code. Because of their reputation for supporting women victimised by sexual extortion and for dealing with their cases with the utmost sensitivity, victims in some Saudi-style online blackmail incidents bypassed the police and sought support from the *Alhai'a*. Although according to the Saudi Criminal Procedure Code the responsibility for investigating these cases lies with the police, the *Alhai'a* always followed up the cases they had brought to police stations and played a part in the investigative process. This, on the one hand, provided an extra investigative resource for the police but also, on the other hand, placed their response to Saudi-style online blackmails under the close scrutiny of the *Alhai'a*, a circumstance that seemed to heighten officers' attention to these cases, as the following example illustrates:

> *Extract from field-notes*: First Lieutenant D, the officer on full-day duty, returned from inspecting the scene of a burglary to find a member of the *Alhai'a* waiting by a prior arrangement. First Lieutenant D took the *Alhai'a* member to his office on the second floor. 20 minutes later, after the *Alhai'a* member had left, First Lieutenant D told me that the visit was regarding an incident in which a girl had approached the *Alhai'a* and claimed that a man, whom she came to know through chatting in PalTalk before proceeding to talk and exchange emails with him through the Messenger, had been extorting money and intimate favours from her by threatening to send shameful pictures of her and recordings of her conversations with him to her father. 'He submitted the case to me six days ago but he has kept inquiring what has happened to it ever since. Today he came to ask me to give him the information that my investigation has revealed so far', said First Lieutenant D, who explained that the *Alhai'a* member wanted this information because the cybercrime unit in his branch aimed to utilise it in their efforts to trace the blackmailer electronically. First Lieutenant D then commented, 'Their [the *Alhai'a*] continuous inquiries about the case put me under tremendous pressure, because if he [the *Alhai'a* member] had not found any information

> today, they would say, “You’re not giving attention to our cases” and they might report that to the Governor’.

What can be read from this extract is that the fundamental ethos of ‘protecting morality’ and enforcing moral values that underpins the mission of the *Alhai’a* is in effect extended to the realm of police work through their persistent participation in the investigation of Saudi-style online blackmails they bring to the attention of the police. This persistence of follow-up monitoring contributes, as we have seen in the example above, to the prioritisation of this type of incident by police officers. This phenomenon demonstrates the influential role of the *Alhai’a* as the ‘guardians’ of virtue and moral values, which are the source of legitimacy to both the Saudi people and government.

While Saudi-style online blackmail incidents occupy a high position in the police’s hierarchy of response to Internet fraud because of their association with morality, officers expressed worries about the complexity of the social tasks required from them when dealing with such incidents. The most challenging of those tasks was to ensure the safety of female victims from any potential harm by members of their family. This challenge can best be appreciated by highlighting the nature of the Saudi conservative culture, in which honour is an intangible asset that is dependent on the community’s perceptions. In such an honour-based society, the reputation and social standing of an individual, a family or a community is based on the behaviour and morality of its members. Therefore, the consequences of damaging one’s honour or the honour of one’s family can be so serious that the family of a girl who becomes subject to a moral scandal might literally kill her or at least inflict serious physical harm. Officers drew the researcher’s attention to two high profile cases that happened a decade ago; in one case a girl was taken to a remote part of the desert and burned to death by her own brothers, while in the other the victim was shot dead by her father.

In theory, the woman’s protection can be achieved by ensuring extreme confidentiality so that the incident is dealt with without the knowledge of those relatives who are likely to be dangerous to the victim. However, in practice, confidentiality is undermined by the Criminal Procedures Code’s requirement that police interview with a woman be attended by her *Mahram* (guardian) – e.g. her father, husband or brother – to prevent any *Khulwa* (illegal seclusion) of an officer with a woman. This rule is based on the important norm in Saudi society of segregation of the sexes. The Qur’an (the holy book of Islam) and Hadith (sayings of the Prophet Mohammed) emphasise gender separation and the privacy of Muslim women. They also stress that in public, Muslim women must wear their veil (*hijab*) and avoid talking with men directly. The following Qur'anic verse is indicative:

> And when you ask [the wives of the Prophet and believing women generally] for anything you want, ask them from behind a screen. This is purer for your hearts and their hearts (*Surah Al Ahzab* (The Confederates): verse 53).

Segregation is strictly applied in all public spheres, including hospitals, schools, universities, banks, shops, restaurants and even public parks. As can be inferred from the above Qur'anic verse, it is a precautionary mechanism designed to protect women's chastity by preventing any attempt at immoral contact between men and women.

In line with this cultural practice, and because of the absence of female officers in the Saudi police, the *Mahram* of female victims of online blackmail incidents had to be informed and present throughout the investigative process. This required officers to be prepared to develop social counselling skills and apply precautionary measures to address the issue of honour-related violence to which female victims might be exposed in online blackmail incidents, as a result of the matter becoming known to male relatives. In highlighting some of these skills and protective measures, one officer stated:

> When a woman comes to us on her own to report that she has been subject to online blackmailing, we call her guardian to attend the station and then inform him about the matter. We sit with him and try our best to explain to him the girl's innocence. In incidents where the woman contributed to her victimisation by engaging in immoral communication with the perpetrator, we exert extra efforts to convince her guardian to forgive her sins and explain that every human being is vulnerable to such things. We even involve a *Shiekh* (religious clerk) or a member of the *Alhai'a* to provide religious counselling to the male relative or relatives if there is more than one. In addition to that, we don't let them walk out with the victim until they sign a written pledge not to harm the girl (PS17).

Exposing the victimised woman to potential honour-related violence was not, however, the only disadvantage that appeared to be associated with the strictly applied culture-based procedure of conducting police investigation only with the knowledge and during the presence of a *Mahram*. Another challenge cited by officers was that the victim would more likely be deterred by the presence of her male guardian from providing important details of her encounter with the blackmailer, especially if they implied immoral behaviour. Officers indicated that the lack of such details often complicated their mission of tracing the perpetrator.

Besides Saudi-style online blackmails, a high priority in police response to Internet fraud was also given to incidents which involved targeting elderly people at

ATM machines to prey specifically on those unable to use their *Sarraf* cards on their own. The incident described below, for example, triggered a prompt response from Major A, who quickly initiated an operation to trace the fraudster utilising his informal liaison with the bank's Security Department manager:

> *Extract from field-notes*: At 08:00 on Tuesday, while Major A was waiting for Captain M to relieve him, one of the shift's assistant officers brought in an elderly man in his mid-seventies. Major A helped the elderly man to sit down on the sofa in the corner, poured him a cup of Arabic coffee and invited him to take some dates from the bowl close by. The man reported that SR45,000 had been stolen from his bank account. He then went on to explain that he had gone to withdraw cash from the *Sarraf* attached to a bank close to his residence, and that because he was illiterate, he had asked a young man standing nearby to perform the transaction on his behalf, as he usually did. The young man took the card and using the password the elderly man had given him, he withdrew SR2000 and handed it in to the elderly man, but gave him a counterfeit card instead of returning his own card. This was brought to his attention by his bank two days later when he went to complain that he had visited a *Sarraf* but the card did not work for him. The elderly man was also informed that in addition to ATM transactions, e.g. cash withdrawals, remittances and bill payments, the stolen card had apparently also been used to register for online banking services on the complainant's account, which enabled online transfers to third-party accounts. The incident was recorded in an Investigation Book by Major A, who asked for further details, including a description of the suspect, then reassured the man and recorded his contact number. Before the man left, he was asked by Major A if anyone was there to take him home now and he said he was in his car.
>
> When Captain M arrived to take over as the officer on full-day duty, Major A briefed him, then asked me to accompany him to his office. There, he called the local bank branch's Security Department manager, whom Major A said he had known for around three years now. Major A checked whether there were CCTV cameras that covered the *Sarraf* area, informed the bank official about the incident of the elderly man and asked to be provided with recorded images from the CCTV for the time of the encounter with the fraudster. After he ended the call, Major A told me that the recorded CCTV images along with the details of the recipient of the transfers from the victim's account, which the bank's Security Department agreed to send to him shortly, would be enough to trace the fraudster who 'did not have mercy or respect for the old and vulnerable'. Delayed for three hours after the end of his shift by the handling of the elderly man's complaint, Major A left the station at 12:05, extremely exhausted.

In the above incident the officer showed a great deal of respect toward the elderly man and took his complaint very seriously. Not only did he extend his presence in the station after the end of his shift to address the incident, which he could have left to the relieving officer to handle, but he also employed personal relationships to obtain the bank's cooperation in reaching a quick resolution to the case. The high level of priority given to Internet frauds targeting elderly victims observed in this incident was also confirmed in the interviews, which showed that this variant of Internet frauds was perceived by officers, at both managerial and operational levels, as representing not only offenders' greediness and opportunism, but also their immorality and lack of 'manly' characteristics:

> We focus on fraudulent activity that targets elderly people at *Sarrafs*. The perpetrators of such activity need to be pursued more vigorously because they combine the act of stealing with the heinous and unmanly behaviour of taking advantage of the trusting nature of the elderly victims and the decline in their abilities, which is totally against our Islamic and Arabic values (DDI4).

It seems, as the above comment implies, that by prioritising Internet fraud incidents which involved targeting elderly users of ATMs, officers were trying to adhere to a religious and cultural principle that the elderly should be shown respect and consideration. In Saudi society, older people are regarded with deep respect and reverence and given priority in all walks of life. The root of this cultural tradition is found in the *Hadith* (sayings of the Prophet Mohammad), which is the second most important source of Islamic law and normative behaviour after the Qur'an:

> Amr bin Shu'aib (May Allah be pleased with him) on the authority of his father who heard it from his father reported: the Messenger of Allah (peace be upon him) said: 'He is not one of us who shows no mercy to younger ones and does not acknowledge the reverence due to our elders' (At-Tirmidhi and Abu Dawud, cited in Darussalam, 2003: 53).

While officers appeared to have a 'moral' imperative to provide a swifter response to Internet fraud incidents which they perceived as violating moral and cultural values, the data obtained in this research show that other types of Internet fraud were less likely to be given the same level of priority. Indeed, the extent to which incidents of what might be characterised as 'pure' Internet fraud were acted upon by the police was dependent on the type of officer responding to the incident. As the example discussed previously in this chapter shows, the absence of the moral dimension did not lessen the efforts made by officers who can be described as 'technophile-work embracers' to pursue resolution of an Internet fraud case. Moreover, these officers' response to 'pure' Internet frauds was not entirely reactive, but it involved also some preemptive policing tactics. For instance, personal forms of partnership were employed to access information generated by private surveillance systems and exploit them for proactive targeting of '*Sarraf* fraudsters'.

Conversely, a typical response to incidents of 'pure' Internet fraud by officers from the 'technophobe-work embracer' and 'technophile-work avoider' categories is illustrated in the following quotation:

> We record the complaint and take all the details that the victim can provide. Then we pass the case to the Commission of Investigation and Public Prosecution because it is they who should conduct the investigation. We can't afford to waste time and efforts on cases where the loss is only minor (PS2).

Here, the police response to an incident is basically 'tokenistic', involving only recording the complaint and referring it immediately to an external agency. No real investigative work is undertaken and no attempts are made to collect information that could lead to the identification and consequently apprehension of the offender(s). However, some police officers might choose to ignore the incident completely. In such a situation, as we have seen, complainants might be diverted to another agency that is very often irrelevant, or alternatively they might just be told that they were responsible for their victimisation and that there was no action that the police could take.

It is important to note that these 'morality non-violating' cases are responded to in the context of myriad other calls on police resources defined within the police natural agenda of 'serious matters' (of which morality-related events are defined as more urgent) and 'minor incidents'. They are thereby stripped of their meaning from the victim's point of view, and are reified in the form of an incident record.

Based on the discussion provided in this section, it can be argued that whereas previous research (e.g. McKenzie, 2006; Murff, 2007) shows that policing of Internet fraud in Western contexts is carried out with a 'capitalist' mentality that is preoccupied with economic and commercial considerations, such as the sustaining of profitability and loss prevention (Garland, 2001), the main concern in the Saudi police response to online fraudulent activity is focused on upholding religious and cultural principles. When such principles are perceived by officers to have been violated, an Internet fraud incident becomes a high priority for the police, regardless of how large or small was the loss. This is attributed to the powerful influence of cultural values and moral standards in shaping Saudi police officers' attitude towards Internet fraud and their response to it. Therefore, it appears plausible to state that the dominant influential function of cultural values is an important factor and plays a major role both in the policing of Internet fraud and in understanding the process of performing this aspect of police work in the context of Saudi society.

6.4 Saudi Norms and Detection of Internet Fraud

The findings of the current research revealed that Internet fraud incidents are reported by victims, rather than detected by the police in the process of policing. It is worth noting that no incidents came to police attention in the departments examined during the fieldwork of this study through, for example, online police patrolling or undercover operations. This reflects what is known about the involvement of the police in the detection of crime in general, which is highlighted by Norris (1987: 26) as follows:

> Contrary to the popular mythology surrounding police investigations which portrays them as involving painstaking detective work; piecing together disparate clues to put a name to an unsolved crime, the police are highly dependent on victims and witnesses for the identification of offenders.

To support his argument, Norris cites several UK researchers' findings which show that the police were responsible for discovering, either directly or indirectly, only about fifteen percent of crime.

In the context of the Saudi policing system, the reporting of Internet fraud has to follow a specific procedure. According to respondents, when Internet fraud occurs, the victim has to go to the police department to make an official report in person. The police cannot accept reports submitted through other means, such as the telephone or Internet. The DPS's senior management representative explained this direct reporting policy, saying:

> Even if a person phoned the police to report an Internet fraud he would be asked to visit the police station in his neighbourhood and put his complaint in writing. The reason for accepting the reporting of crime only in this way is that the Criminal Procedures Code establishes that in order for any person to be arrested in any crime of those crimes of *al-hagg al-khass* (private right) there must be a claimant and a written claim (SO1).

As the above quotation indicates, this reporting procedure is created in accordance with a standard rule in the Saudi Criminal Procedures Code for initiation of prosecution. This rule is based on a *Shari'ah* Law criterion for accepting a claim for trial, which distinguishes between two categories of crimes in terms of who may be the initiator of the allegation of a criminal action. These are crimes of public right and crimes of private right. According to Muslim jurists, in crimes of public right the allegation does not need to be initiated in any specific manner and the criminal action is to be dealt with irrespective of who brought it to the attention of the authority. By contrast, crimes of private right are prosecuted only on a demand by a private claimant. In line with this procedural rule and as Internet fraud is considered a type of theft, which is classified under the category of crimes of private right, the process of handling an Internet fraud incident is not initiated by the police without a written complaint from a known claimant.

Although compliance with the principles of the Criminal Procedures Code was stated by officers as the basis for allowing Internet fraud reports to be received only in writing and from known complainants, it appeared that the application of this reporting procedure was also intended to perform an undeclared function. As the data show, this restricted way of receiving reports served to eliminate the negative effects of false reports of some types of Internet fraud. In this respect, officers highlighted cases involving telephone complaints from anonymous women about attempted online blackmail, which were not always found to be entirely true. The implications of this situation are underlined in the following quotation:

> Sometimes we receive a call from a woman alleging that someone is trying to blackmail her on the Internet, but she wants to remain anonymous. We can't just accept that and go after the person she accused of blackmailing her. This is because we have seen cases where the allegation turned out to be untrue and made only to take revenge on the accused by distorting his reputation, or where the woman was implicated in an immoral relationship with the man and wanted to get rid of him this way. So the claimant here must be specified for one important reason, which is that the accused has the right, if found not guilty, to seek what is called 'restoration of dignity' (PS10).

As has already been explained, in a conservative and fundamentally traditional society such as the Saudi one, whose cultural identity and social life is built around the concepts of honour and moral integrity, the effects of engaging in any immoral behaviour on the reputation and social position of individuals and their family can be devastating. The direct reporting policy can be understood, therefore, as a mechanism employed by police to verify that there is a 'credible victim' who was 'genuinely' victimised by Internet fraud, and to deter 'malicious' reports which might jeopardise the reputation and social life of innocent people.

Officers were candid, however, about the likelihood of the deterrent effect of the direct reporting procedure extending to discourage genuine victims from requesting police assistance. For instance, an opinion frequently expressed during the research was that Internet fraud incidents related to morality would be a far more visible problem if anonymous reporting was allowed, because embarrassment, negative social stigmatisation and fear of family members' oppression often prevent real victims from reporting their victimisation to the police, as it involves revealing their identity. This assumption is emphasised in the following quotation with regard to Saudi-style online blackmails:

> When a girl gets defrauded as a result of getting involved in an indecent relationship on the Internet, I mean when she is tricked into sending obscene photos of herself to the fraudster and he uses these photos to blackmail her, you wouldn't expect every girl who becomes embroiled in this situation to come to the police and tell them about the obscenity. Some of them will continue to pay the fraudster to buy their reputation as long as she has the money, because she realises that she can't remain anonymous (PS17).

Difficulty in reporting Internet fraud incidents can also hinge on the attitudes of police towards victims. The data revealed a tendency amongst officers to belittle certain victims of Internet fraud, blaming them for their own victimisation. An example of this attitude was shown earlier in this chapter in the case of 'the technophobe-work avoider' in relation to victims of misleading online advertisements. We can recall that the officer managed to dismiss the victim who approached the station to report having lost SR1,400 in a online herbal prescription purchasing scam by convincing him that he was responsible for his victimisation, and that recovery of money lost through such carelessness was not the police's responsibility. However, the type of victims who appeared to be afforded the least respect are the male victims of Saudi-style online blackmails. These are men who become subjected to extortion as a result of revealing scandalous images of themselves in online encounters with fraudsters posing as women ready to engage in both online and real-world illicit relationships. Such victims, as the following comments illustrate, are perceived by officers not only as precipitating their victimisation, but also as morally culpable, an attitude which arguably is expected to impact on the manner in which these victims' reports are received in police departments:

> I have no sympathy for those decadent men who agree to appear naked on webcams and then come to us to say, 'I have been deceived'. This is not about deception; this is about total immorality and degradation (PS5).

> It is difficult to understand how a man can get tricked by a woman who he knows only on the Internet – and this woman could turn out to be a man using a voice-modifying device to sound like a woman – into exposing himself in shameful postures. So when they get blackmailed over the shameful photos they provided willingly, they deserve it (DDI3).

Since police subculture is guided by the dominant culture in their particular society (Waddington, 1999), which means that members of police are also members of a society and share its values, it can be argued that officers' perceptions of male victims of this particular type of Internet fraud were affected by the influence of morality and its principles, which represent a dominant aspect of the Saudi social identity. In other words, the behaviour of these victims was intolerable to officers because it was contrary to the dominant principles of morality.

The issue that might be raised here is to what extent ‘old’ cultural norms and social values can provide a basis for giving a high or low priority to Internet fraud incidents. On the one hand, we have seen how officers’ prompt response to Saudi-style online blackmails that are directed against female victims was influenced by the moral values and cultural traditions of the Saudi society. On the other hand, however, the same moral values and cultural norms appear to contribute to an indifferent attitude towards online blackmails if a man was at the receiving end of the scam. This issue demonstrates the importance of considering the distinctive characteristics of Saudi society in any attempt to understand the extent to which the policing of Internet fraud in this non-Western context can follow the principles of ‘new penology’ as applied in Western societies.

6.5 Human Mediation of Technology: the Limits to a Proactive Response to Internet Fraud

For the policing of Internet fraud in Saudi Arabia to mirror the central features of the ‘new’ penology, it would be expected to be carried out in a manner that incorporates proactive targeting of online deceptive actions. However, one of the main themes to emerge from the current research of police response to Internet fraud in Riyadh was the extremely low level of proactive policing of Internet fraud. This was mainly due, as was indicated in Chapter Four, to the insufficient technological infrastructure in police departments. For instance, technological systems to conduct surveillance and intelligence gathering operations in cyberspace were provided only at a minimal level. Computers were supplied to four of the seven police units visited during the fieldwork, but only in one of these units was the number of computers supplied sufficient for the investigative staff. In a number of departments, some officers used personal computers which they had managed to obtain from outside the organisation through their own means.

However, even when technological equipment was available to officers in some departments, its use for proactive policing purposes was dependent on organisational context. It also relied, to a great extent, on how officers read and employed these technological apparatus.

In terms of the impact of the organisational context on human mediation of technology, it is fair to state that organisational conflict appeared to be one of the most important determinants of officers' use or non-use of technology to respond proactively to Internet fraud. This assumption can be supported by the evidence found of the close link between some officers' avoidance of employing the technological means at their disposal in the policing of Internet fraud and the intense work relationships that existed in their departments and their disillusionment with their jobs. As we remember, First Lieutenant R, who represented the 'technophile-work avoiding' type of officer, was very proficient in dealing with information and computer technology. However, when he was assigned to undertake surveillance of an online fraudulent activity (see p. 177), he resorted to the 'traditional' police device of paperwork to fulfil the assignment. The reason was, essentially, that he felt discriminated against by his manager and unsupported in his attempts to obtain the monthly bonus usually granted to government employees using computers in their work. In another site, it was observed that one officer had left a computer set unpacked in the corner of his office for more than three months as he was anticipating transfer from his department following a series of tense arguments with its manager. This officer was a member of the station's Intelligence Unit which, according to the DPS Organisation and Functions Guide (DPS/DPD, 2009), is responsible for conducting surveillance and covert observation operations, mainly to detect the perpetrators of incidents reported to the station, but also to uncover ongoing criminal activities.

To use the technological systems provided in some police departments to respond to Internet fraud in a proactive way, the operational officers must first have sufficient knowledge of these systems and understand how they can be utilised to fulfil this aspect of police response. However, as was already highlighted in Chapter Five, this was not found to be the case with most of the officers who participated in the current research, due to a variety of different factors, including the noticeable shortage of formal training. The effect of the lack of technological know-how on police officers' ability to operate the existing technology in a way that would allow the interception and prevention of Internet fraud activity was highlighted by the Chief Investigator of one station, who said:

> You've got people here that, let's face it, they are just not qualified, not only for Internet fraud, but any technology-related crime. They have computers in their offices, but they only use them for typing letters and things like that, not more. Even those who have personal computers and use the Internet, they use it for things like browsing websites, sending and receiving e-mails, and maybe chatting. You can't rely on them to intercept fraudsters' communications on social networking sites, for example, to track those who exchange indecent images of women or children which are eventually used for extortion. The majority of our officers don't even know what IP address means, or that it can lead to information about a suspect through his account with the Internet service provider. I read the other day that some police forces in advanced countries have begun to use such surveillance techniques as remote hacking on computers to obtain information from a suspect's computer without that person's knowledge. This is impossible to see here, where officers aren't able to protect their computer from hacking let alone to use it to track criminals on the Internet. I guess the only way our police could use this surveillance technique is by employing former hackers (PS17).

With the nature and cultural values of the Saudi society and their influential impacts on individuals' mind-set, cultural norms and traditional values can shape practical attitudes and the pre-emptive response to Internet fraud. This issue can be illustrated by the rejection of pre-emptive policing of Internet fraud by some officers on the grounds that this system of policing and its surveillance activities are in conflict with Islamic principles and considerations. For these officers, the notion of pre-empting fraudulent activities online based on dataveillance, wired surveillance, and the spread of distrust among Internet users involves *tajassus* (spying), which is forbidden by the clear text of the Qur'an. For example, one respondent stated:

> When you say monitoring what people do on the Internet to know if someone is misbehaving, that basically means spying on people. We are warned by the Qur'an against indulgence in spying and surreptitious activities. I wouldn't be encouraged to go this way (PS21)

Making technologies of online surveillance available to the police would entail undesirable social implications according to one officer, who hypothesised what would ensue:

> Rogue officers, who don't fear Allah, would exploit these technologies to get hold of pictures of ladies and use these photos dishonourably. The lives of those innocent ladies would be ruined (PS15).

The officer indicated that for this reason, specific criteria should be applied for selecting officers to deal with cases involving female victims:

> The officers who deal with Saudi-style online blackmails should be mature officers, those who are married and have children. Young officers shouldn't be involved in this type of cases because they might be tempted to approach the woman in an immoral way (PS15).

This point of view reflects the officer's perception that the involvement of young officers, although they may be more technically proficient, could be avoided due to cultural norms and moral values that are related to the social and cultural characteristics of Saudi society. This reflects police commitment to the cultural values held in Saudi society.

Moreover, cultural norms and traditional values can place limits on the utility of technological systems for a proactive response to Internet fraud. For instance, the DDI and the police stations each had a computer which was connected to the Ministry of Interior's National Information Centre (NIC) and had access to the database that was available in the NIC system. The database, which is built on data reported from various governmental departments, contains records of personal information, for instance, the name, age, job, blood type, number of cars owned, vehicle registrations and ownership, traffic fines, criminal records, number of wives and children, their names, age, and residence information, including address and telephone number. The operators of the NIC terminals had a code number, which allowed them to go into the system and search the database through the national identity serial number. For foreign people, the NIC system can be searched by using the residency number of a foreign person for information, including name, sex, nationality, date of birth, date of entering the country, the serial number of the visa, the job, the number of passport or renewal, issue or renewal of residence, and the name of the Saudi sponsor (their national identity number). Using this surveillance facility, police were able to obtain phone numbers and other information necessary for identifying Internet fraud suspects and tracking their movements. However, the utility of this surveillance facility for policing purposes, including those related to Internet fraud, appears to be limited by the fact that a considerable part of a NIC terminal operator's time can be devoted to attending the demands of relatives and friends to run a variety of queries on the system, the most frequent of which concerns traffic fines. On numerous occasions during the research, concerns were voiced about the dilemma in which officers are placed as a result of this situation; the following is a typical example:

> I constantly receive requests from relatives or friends to check their records on the system, especially to see if they have traffic violations. I am under enormous pressure from these requests, but I can't refuse them. If I ignored a colleague or relative's request, it would be a serious discourtesy that could affect my relationship with them. You know the stigma in our society for not being helpful to your friends and relatives (DDI4).

This shows that with the employment of advanced surveillance systems, the power of the Saudi 'old' cultural traditions and social norms still has its effect on the process of utilising these technological systems and shaping their mechanisms, which can place limits on their potential role in the prevention and investigation of Internet fraud. The salience of this issue in the Saudi context raises serious questions about the validity of assumptions reiterated in the Western-dominated literature on policing which place more emphasis on the influence of organisational factors on police decisions in relation to the adoption of new technologies for proactive policing. This is an important point as writers such as Chan (2003), Ericson and Haggerty (1997) and Manning (1992, 2008a), in their analysis of the incorporation of information and communication technologies in police intelligence gathering systems, tended to view these technologies and their associated practices as being primarily mediated by the organisational and occupational concerns of frontline officers, paying less attention to the impact of the wider cultural and social circumstances on officers' perceptions and operation of technologies. Amongst the rare exceptions to this trend in the Western literature is McCahill's (2002) study of the rise of visual surveillance technologies in an English city, which concluded that the operation of CCTV systems has to be understood as the outcome of the complex interplay between technological, organisational and cultural factors.

A crucial issue is when technology falls into the wrong hands. This concern requires examination of how officers might 'abuse' technologies by employing them for unwarranted functions, as the following example illustrates:

> *Extract from field-notes*: At 10:30 on Sunday morning, Major S picked up the phone and called Corporal F to his office, while he was still involved in an ongoing discussion with an army officer friend who had come to seek advice on what to do about what he viewed as the police siding with the security guards who had beaten his brother at one of the gates of the National Guard housing area. As soon as Corporal F entered, he was asked by Major S to move the computer sitting on his main desk to a smaller desk to his left. 'We need to finish entering the data in these questionnaires to the SPSS by the beginning of next week, because the guy who is going to do the analysis has said he will be busy for the rest of the summer and therefore he wants to start my work no later than Saturday next week', said Major S after he pulled out the box containing the questionnaires from beneath his front desk and put it in front of Corporal F, who was still moving the computer. By the time Corporal F had finished setting up the computer on the side desk, the visitor had left the office after Major S's attention began to be distracted by the continuous interruptions of phone calls and as he had to attend to other incidents. However Major S's instructions to Corporal F continued until he had completed the installation of the SPSS software on the computer and began entering the data from the questionnaires. 'From tomorrow I

> will come early in the morning. I need to work while the office is less busy, because if we continue like this I think I won't be able to finish on time', said Corporal F.

As can be read from this extract, the officer employed his work computer and a member of his assistant staff to fulfil a task he had to perform in the research he was undertaking to obtain a Master's degree from a local university. As a result of this 'abuse' of technology, the officer's work computer could not be used to carry out policing functions, including those related to responding to Internet fraud, for an average of four hours a day over the four-day period that followed the incident described above.

While this incident was the only one of its kind that was observed during the fieldwork, the invisibility of such a practice to the management draws our attention to the extent to which the 'policing of the police' might exist to watch the actions of those who are responsible for watching others. This issue is discussed further below.

6.6 Policing the Police

The idea that police are subject to growing surveillance, and that most of this surveillance comes from their own devices, has become a recurring theme in recent works of Western police researchers. For instance, Peter Manning (1988: 155) has suggested that the police 'are servants of the public in name only, for although the public pays them, they work for the machines that lurk behind them, glow in front of them, click and buzz in their ears and fill the air with dull electronic sounds'. Similarly, Ericson and Haggerty (1997) point out that the very surveillance technologies police officers use to monitor the actions of others are also used to watch the behaviour of police officers themselves. As a demonstration of this situation, Ericson and Haggerty highlight the fact that police cars are equipped with video cameras and computer terminals, while police buildings are equipped with access cards, surveillance cameras and computers to monitor police officer activity.

In the current research, there was no evidence of a 'panopticisation' of police departments to allow the actions of the 'watchers' to be under constant external gaze. Unlike the 'wired police department' described in the accounts of Western researchers, the physical setting of the police branches examined in Riyadh did not seem to be designed to incorporate electronic communication and surveillance technologies in the supervision of officer conduct, relying instead on the traditional human supervisory functions. For instance, CCTV systems were installed only in the Central and Southern police stations. However, in both sites, the systems were solely intended for security functions, as cameras were fitted only externally to monitor the entrances and surrounding areas of the station. Moreover, the absence of computerised reporting systems in all the departments studied meant that whether an incident was acknowledged in the first place was left entirely to the officer's discretion, which also seemed to determine the type of data to be obtained in the reporting process. It also prevented an automatic tracking of the progress of investigations and allowed officers to continue to avoid systematic assessment of the completeness, reliability and validity of the knowledge they produced. In addition, control of personnel attendance was not automated, but rather depended on the practices of individual managers. In four of the seven case departments, officers were required to sign an attendance book in the office of the department's manager, while the punctuality of the *afrad* (assistant officers) was overseen by their immediate supervisors. Such arrangements were not observed in the remaining three organisations, where managers seemed to be more concerned about officers' effectiveness and efficiency in clearing up allocated work than their punctuality.

This environment of low visibility appeared to have had an impact on the way some officers responded to Internet fraud. This can be exemplified by incidents highlighted earlier in this chapter that involved 'deviant' practices, such as the failure to acknowledge a report of an Internet fraud incident and the misuse of technological systems that could be used for responding to Internet fraud, which can be linked to the absence or weakness of close managerial supervision. Evidence handling is a crucial aspect of the police response to Internet fraud, which can be affected by the inexistence of surveillance arrangement and follow-up approach in observing officers. In the interview with a member of the Department of Forensic Evidence's Computer Crime Unit (DFE/CCU), he sounded an alarm of concern about this issue by recounting an instance in which evidence was lost, in his opinion, as a result of not having a 'chain of custody' system in place:

> Two months ago, we had a computer sent to us for examination as part of the investigation of an online blackmail incident. When the computer reached us it was obvious that the machine had been left unprotected from sun and dust for a long while. So when we began examining the computer, it was already damaged and all the data on it were completely lost. But you can't say how that happened

> or who was responsible, because there is no system to establish what we call the chain of custody for the evidence (DFE/CCU 3).

The fact remains, however, that the practices highlighted above were isolated cases and, therefore, they cannot be taken as a sign of a widespread culture amongst police. In fact, during the fieldwork, a general atmosphere of commitment and conscientiousness was observed amongst officers in terms of the quality of their performance and punctuality. The application of specific criteria in selecting police officers might have contributed to this discipline. Some of the criteria according to which officers are selected were indicated in the interview with the DPS's senior management representative, who also stated:

> You are a member of King Fahad Security College and you know that not everyone can be accepted to enter the College and become a police officer. It is only those with high achievement in their pre-college education and who pass the personal interview and all other tests of fitness for military and security service who would be accepted to enrol in the College. The mechanism of selecting officers which begins first at KFSC and continues here in the DPS when we appoint the officers who work in the investigative branches results in creating discipline and appreciation of job values such as attendance, productivity and above all commitment to preserving the security of their people and country (SO1).

Besides the influence of the selection standards, work commitment can also be attributed to an internal surveillance that is linked with a religious belief that a person is in the presence and under the continuous observation of Allah (God). Officers' sense of being permanently visible and watched by Allah can be noticed in phrases such as '*if you can avoid your boss's gaze, you can't escape that of Allah*' and '*Allah shahed'* (God is witness), which were echoed by officers throughout the research. Bearing in mind that there will be rewards and punishment both in this world and in the hereafter, Muslims strive to comply with all Allah's commands, since they know that He monitors them all the time. As one of Allah's commands, a Muslim is urged to perfect the job he/she is employed to do and be devoted to fulfilling its duties and responsibilities. According to the Islamic doctrine, optimal performance of one's job is a condition for the lawfulness of the payment received for that job. In other words, those employees who breach their job's obligations are faced with the prospect of being subject to God's punishment for illegitimate earning. Awareness of this consequence was particularly evident in the expression '*I don't want to feed my children Haram* (ill-gotten provisions)', which is a metaphor used by many of the officers who participated in the present study to assert that they practised self-surveillance of their job performance to avoid any doubts of illegitimate earning of livelihood.

This element of the Muslim faith is presumed to generate a type of consistent self-discipline, enabling officers to control themselves irrespective of the existence or absence of surveillance, except for the fear of God. Indeed, as Maudoodi (1979) affirms, within the Muslim nation, fear of penalty and desire for rewards from Allah are the most effective controllers of human behaviour. The deterrence force of punishment and rewards in Islam is primarily designed as an instrument for disciplining the soul through internalising a 'spiritual' surveillance that warns a person against committing unacceptable behaviour.

Having said this, it is acknowledged that officers differed in their level of religiosity and consequently not all had the same degree of commitment to religious values; this is why some officers were described as work-avoiders. The awareness of such variations in commitment, moreover, may explain why some managers were not content to rely on individuals' self-monitoring, but perceived a need for surveillance technologies. For instance, one police station manager sought to install a computer-based surveillance system for tracking the development of a case from the moment the criminal action is reported to the police station until it becomes stored in the archive:

> I have talked to the management of Riyadh Police and said to them, 'Why not, instead of receiving daily reports of criminal occurrences from stations, have that done through a centralised computer system?' I succeeded to persuade them of the importance of such a system, and my station has been chosen to be the prototype of this project before it can be applied on a wider level. So we are now in the process of installing a system whereby the development of a case is monitored electronically from A to Z. This would begin when a person comes to the station to report a crime. The report will be recorded on the computer and the reporter will then be given a reference number which he will use to follow up his case. From there on, all the actions taken on the case will be recorded on the system, which means that we will be able to know how many cases we have got and what has been done to each of them, and the monitoring of the case will continue until it is finally stored in the archive (PS12).

6.7 Summary

This chapter has analysed the policing of Internet fraud as applied in practice by Riyadh police officers. The most striking result to emerge from this analysis is that the police response to Internet fraud is shaped by the cultural and social characteristics of Saudi society. This view is supported by the findings presented in this chapter, which demonstrate the influential impacts of Saudi social norms and cultural traditions on officers' attitudes towards policing Internet fraud and their perceptions of this part of their 'crime-fighting' mission. Moreover, the significant difference between the policing of Internet fraud in Western and Saudi contexts in terms of police decision to respond to incidents brought to their attention is in relation to the preoccupation with morality and cultural values shown by Saudi police officers. Although responding to a new type of crime, Saudi police officers still stick to the cultural values and religious principles of their conservative society in their prioritisation of Internet fraud incidents. As the findings have shown, Internet fraud cases which are associated with morality and cultural values are positioned at the top of police hierarchy of response, irrespective of the size of the financial loss involved. This stands in stark contrast to the type of factors determining police decisions to respond to Internet fraud in a Western context (McKenzie, 2006; Murff, 2007). As social relations in Western societies are built around the principles of a capitalist ideology, financial and commercial concerns are given more attention by police when responding to Internet fraud activity. This is also influenced by the powerful intervention of the private sector in public life and the impact of the consumerist culture and its values of loss prevention and profit maximisation, according to which Western societies have become regulated (Garland, 2001).

Local Saudi norms and cultural values have also affected how Internet fraud occurrences come to police attention. This is particularly evident in terms of the influence of the concepts of honour and moral integrity, which represent a major aspect of the cultural identity of Saudi society, on shaping both the reporting procedure and officers' attitudes towards certain types of Internet fraud victims, something which has its consequences for the extent to which Internet fraud victimisations might be reported to the police. Similarly, police commitment to the cultural and religious values held in Saudi society has limited the use of technological systems to respond proactively to Internet fraud. In this respect, while new computer software is increasingly used by Western police forces to monitor cybercriminals and target online fraudulent activity, such 'dataveillance' systems have restricted use in a traditional society where the notion of pre-empting fraudulent activities online would be rejected as it might violate religious beliefs. In addition, enhancing 'morality' and eliminating any chance for potential temptation to approach a woman in an 'immoral' way can be a crucial reason for preventing young officers, who might be more technically proficient, from dealing with incidents involving female victims. Finally, in the context of watching police actions, this chapter has revealed that the creation of self-discipline would be shaped and generated internally by the potential consequences of values and norms that people believe in.

Having built a solid empirical background through in-depth interviews and observation as well as analysis of available documents, the next chapter will take us back to theory to discuss the significance of the present research’s findings for broader theoretical debates on policing and crime control in late modernity.

Chapter Seven

Back to Theory

Chapter Seven: Back to Theory

7.1 Introduction

This thesis has sought to provide a detailed micro-sociological account of how Internet fraud is policed in Saudi Arabia by conducting a case study in Riyadh, the capital city. It was important, however, to assess the extent to which the findings of the current study fit in with contemporary global trends in crime control and policing, particularly those related to cybercrimes. To this end, the research was bound to draw on Western debates and theoretical perspectives, since they continue to dominate the existing literature in this area. The evidence produced by this research demonstrates clearly the implications of the specific political, cultural and social characteristics of the Saudi context for the police response to Internet fraud. This points to the need to take into account differences between countries in the political, social and cultural domains in any attempt to examine the applicability of Western-developed crime control perspectives in a non-Western context.

The preceding three chapters concentrated on presenting the main findings of the study. In this chapter, the aim is to discuss the theoretical implications of those findings in the light of the current debates on crime control in late modernity. This theoretical analysis seeks to generate new insights about the study's data, and by so doing, contribute to the existing literature on policing and crime control strategies in contemporary societies. To achieve this aim, the chapter begins by discussing the current trend of pluralising the policing of Internet crimes, indicating the limitations to the applicability of this policing approach in the Saudi context. This is followed by an attempt to enrich and add ideas to current debates on police mediation of risk by highlighting how this issue is shaped not only by organisational, occupational and individual concerns, but also by the religious norms and social mores of those working in a non-Western setting. Finally, possible directions for future research that could build on the contribution of this work are suggested, before the thesis closes by offering succinct concluding remarks on the value and interest of the research and its outcome.

7.2 Crime Control in Late Modernity and the Policing of Internet Fraud in a Non-Western Context

Existing literature on the policing of Internet fraud in late-modern industrial societies suggests that developments in this arena should not be seen as isolated from the wider transformations in 'penality' which have been taking place for a number of years in those societies. As Garland (1996, 2001) has argued, from the 1970s, there has been an increasing recognition on the part of governments in Western societies that the central state has reached the limits of its capability to exercise sovereignty over the problem of crime, particularly as it takes on characteristics associated with globalisation. Governments' response to this predicament has been characterised by a highly contradictory pattern of policy development. Garland points out that on the one hand the political implications of an admission of this deficiency would be such that governments are loath to acknowledge it openly, and continue both to express on society's behalf an outraged response to crime and to engage in 'symbolic' demonstrations of power and control. On the other hand, contrary to this 'expressive' mode of 'acting out' through a continued trend of punitiveness in both rhetoric and practice, there has been an attempt to face up to the predicament and develop new pragmatic 'adaptive' strategies, including a 'responsibilisation' strategy of delegating crime control duties to the private sector and the wider civilian population. Thus, some writers have argued that in late-modern societies, crime control is addressed not only by central-state agencies such as the police, but beyond the state apparatus, by the organisations, institutions and individuals of civil society (Garland, 1996, 2001; O'Malley, 1992). State authorities, according to Garland (1997: 188), are seeking to:

> enlist other agencies and individuals to form a chain of coordinated action that reaches into criminogenic situations, prompting crime-control conduct on the part of the 'responsibilised' actors...Central to this strategy is the attempt to ensure that all the agencies and individuals who are in a position to contribute to these crime-reducing ends come to see it as being in their interests to do so. 'Government' is thus extended and enhanced by the creation of 'governors' and 'guardians' in the space between the individual and the state.

Government-initiated responsibilisation strategies are leading to the development of 'hybrid policing' (Johnston, 1992) networks, which blur the boundaries between public and private policing. These developments have prompted Johnston and Shearing (2003) to advance a much broader conception of 'security governance', which they prefer to the narrow concept of 'policing', in part to escape what they see as its analytical, state-centred straitjacket and its conventional association with the public police. Johnston and Shearing argue that governance of security is increasingly so complex that it is no longer solely or even primarily the preserve of the state, but rather exercised under ‘plural’ auspices. This ‘pluralistic’ model of policing refuses to give conceptual priority to the state agents and encourages the analysis of security governance beyond the state.

Moreover, the ‘governance of security’ is underpinned by a new risk mentality that adds a new layer to the more established punitive mentality (Ericson and Haggerty, 1997; Garland, 1996, 2001; Feely and Simon, 1994). This future-oriented rationality is focused on the prevention and reduction of risk through the intensive use of statistical techniques. Dupont (2004: 78) points out that ‘the prevalence and multidimensional implications of risk prevent any single player, no matter how large and resourceful, to shoulder it alone. Thus, the creation of partnerships and networks ensure a pooling of resources and dilution of liability, making risk easier and more acceptable to handle’.

This late-modern framework of crime control has informed the way the policing of Internet fraud is conducted in Western contexts. As we have seen in Chapter Two, in Western societies, approaches to the policing of Internet fraud reflect broader crime control strategies and dilemmas, and the dual shift between the ‘new’ and ‘old’ penology. The establishment of Specialist Cybercrime Units (SCUs) or similar, for example, can be interpreted in terms of the new penology as conscious attempts by the state to demonstrate its determination and competence to address the cybercrime problem. The findings of this thesis suggest that the Saudi state’s response to Internet fraud has followed this trend. However, while the ‘expressive gestures’ in Western states’ response to cybercrime appear to be intended domestically to reassure the public, the evidence presented in Chapter Four, which contained an analysis of Saudi Arabia’s recently enacted Anti-Cybercrime Law and of the creation of the Informational Crime Unit (ICU), highlights the importance given to the concern for global image in the introduction of these legal and organisational innovations. For instance, although the Anti-Cybercrime Law constitutes the main legal reference for controlling Internet fraud in Saudi Arabia, it falls short in addressing many aspects of Internet fraud, including significant gaps with regard to issues like jurisdiction and enforcement mechanism. Such serious limitations, along with the seemingly rushed and uninformed legislation process by which the Law was introduced, raise legitimate doubts as to whether tackling cybercrime was in fact the primary reason for the introduction of this law.

In much the same way as the Anti-Cybercrime Law, the influence of non-domestic concerns on the Saudi state's decision to create the ICU is evident. This assumption is based on an interpretation of both a published government policy (the NCITP) and the views of those interviewed at the ICU, which point to a direct link between the formation of the new unit and the state's desire to construct and display an image of a security that would attract international investors to the Kingdom, as well as to demonstrate its commitment as a signatory to regional and international cybercrime treaties. The findings discussed in Chapter Five also provide support to the above view of the purpose of the ICU, as they show that this unit existed only in name in the DPS's organisational structure, but remained virtually non-existent in operational terms, due to a combination of factors, including ambiguity of jurisdiction and work mechanism and lack of resources.

Meanwhile, existing Western literature informs us that a system of 'plural' policing of Internet fraud has been developed, in which a variety of quasi-public, private and corporate organisations have increasingly become involved, alongside the professional 'public' police, in regulation, investigation and security provision. These developments fit well with the wider trend of 'responsibilisation' and encouragement of private sector and ordinary citizens' involvement in various services, including crime control.

Some writers have assumed, on the basis of a first cut of influential works of theorists of 'governmentality', that the 'security network' approach offers a common conceptual platform to interpret the complexity of security provision across a whole spectrum of configurations and can bridge the gap between state-centred and pluralist views of security. Such an assumption is reflected in Wall's (2008) 'Internet's order-maintenance assemblage' thesis, in which he argues that the Internet is actually the site of multi-level governance involving divergent actors with different regulatory purchase of the Internet environment. Wall points out that understanding the position of the public police within the broader network of security that constitutes the policing of cyberspace facilitates more realistic expectations and appreciation of the police role, and also assists the identification of the variety of cross-sector networked issues that the police ought to address in order to participate in the policing of the Internet.

7.2.1 Applying Plural Policing of Internet Fraud in an Autocratic State

Despite the apparent empirical support for the importance of the ‘Internet’s order-maintenance assemblage’ in theorising the policing of Internet fraud in Western societies, in Saudi Arabia, the implementation of this pluralistic model of policing seems to be modest. Private policing in Saudi Arabia is still restricted to guarding and patrolling privately owned spaces, such as retail areas and shopping malls, which relies on personnel employed by private security companies (Alhadar and McCahill, 2011; De Jong, 2002). Apart from these limited security functions, the Saudi law still does not permit the private sector to undertake other aspects of police work, such as crime investigation, apprehension or forensic examination. As these policing activities are owned exclusively by the sovereign state, partnership policing of Internet fraud in the manner described in the existing Western literature does not formally exist in Saudi Arabia. Unlike Western nations, Saudi society appears to be far from ready to implement the licensing of private investigators and detectives, whether online or offline.

In Riyadh, the only observed example of public-private cooperation in policing Internet fraud was in police liaison with banks and Internet Service Providers (ISPs). The former were requested to provide account details for individuals involved in cases under investigation, and the latter assisted in identification of suspects’ IP addresses or other telecommunications details. However, the effectiveness of this liaison, usually initiated by the police, appeared to be reliant on the use of informal channels and personal relationships, which proved to be crucial to overcome the obstacles created by rigid communication procedures and conflicting organisational goals.

The lack of a public-private partnership culture which promotes collaboration and information sharing between the police and the private sector for the prevention of cybercrime has apparently limited the scope for risk-based and pre-emptive policing of Internet fraud. Thus, instead of a policing approach that is shaped by ‘a shift towards instrumental forms of governance that focus attention less on the past and more on the future’ (Johnston and Shearing, 2003: 98), the Saudi police response to Internet fraud remains a reactive one that is concerned with past crimes and focuses less on prevention. Ericson and Haggerty (1997) have argued that in order to address risk properly, information needs to be gathered and exchanged intensively between those that experience it and those who can prevent it and ensure against it. However, in Riyadh, ‘local security networks’ (Dupont, 2004) involving the police and banks, for instance, were not in place to prevent breaches that resulted in acquisition of customers’ banking information and eventually theft from their accounts. When, on rare occasions, such a form of partnership existed informally, proactive policing of certain online fraud situations was possible. This was evident in the case of Major A (the technophile-work embracer), who employed personal relationships to gain access to the images produced by a bank’s ATM point CCTV cameras and used them to proactively target ‘*Sarraf* fraudsters’ (see Chapter Six).

Surveillance is a fundamental element of any preventive policing strategy (Johnston and Shearing, 2003). In cyberspace, Wall (2008) argues that monitoring Internet traffic for the purpose of cybercrime prevention requires the assistance of the ISPs, whose fear of civil sanctions encourages them to be compliant with the demands of the public police. Although the Anti-cybercrime Law provided a legal obligation for the CCIT to assist in the policing of informational crimes, the current study failed to identify evidence of police cooperation with the ISPs, as part of the CCIT framework, for preventative policing and real-time interventions in relation to Internet fraud. Such cooperation only took place, according to interviewed officers, with the General Detective Directorate (GDD), which represents the internal intelligence services, apparently in the context of counter-terrorism.

All of the above gives substance to Dupont’s (2004: 87) observation that while ‘the diffusion of responsibilities’ seems to be the theme ‘that unites views of modern policing in late modern societies’, ‘national contexts differ greatly and [this] warns us against a tendency to assign a global significance to developments occurring in the United States, Canada or the United Kingdom’. Other countries, Dupont goes on to note, ‘might follow different paths that need to be understood as well as the trends’ found in Western countries (2004: 87).

Having discussed the limited implementation of plural policing of Internet fraud in Saudi Arabia, it is evident that Garland’s account of crime control in late modernity is not entirely up to the job of theorising penal transformation in an ‘autocratic state’. While his notion of ‘expressive gestures’ may provide a persuasive interpretation of the Saudi state response to cybercrimes by introducing the Anti-Cybercrime Law and establishing the ICU, the evidence discussed above shows no emphasis on ‘prevention’ and ‘partnership’ in the policing of Internet fraud as an illustration of the ‘adaptation’ identified by Garland in strategies of crime control in Western contexts. At this point, it seems that the limitations of Garland's late-modern penal framework in explaining the current situation in an autocratic state like Saudi Arabia are primarily associated with the great extent to which the shaping of this theoretical model was influenced by Foucauldian ideas, particularly those pertaining to the analysis of 'power'. Further discussion of this issue and how Garland's theory might be modified to expand its capacity to account for crime control trends in non-Western contexts is provided below.

7.2.1.1 State Power and Domination.

Garland (2001:120) suggests that the punishment of criminals is the business of the state, regarding it as symbolic of state power, while the control of crime 'is increasingly deemed to be "beyond the state" in significant respects'. In this argument, Garland, inspired by the work of Michel Foucault, as acknowledged early in *The Culture of Control* (2001: 3), draws upon the concept of 'government'. 'Government' in Foucault's theoretical scheme refers to the activities of the state, but also, more broadly, to processes of 'action at distance' which operate through mechanisms of self-regulation and self-control (Foucault, 1991). Foucault's idea of 'government', on which Garland built his work, is contained within a much wider analysis of 'power' in general. This analysis is marked by a tendency to regard as misleading the assumption in modern public discourse that power is to be understood as mainly vested in or attributable to a central sovereign authority or authorities. Power, in Foucault's interpretation, is a diffused social function in which individuals and groups are engaged. Its operation is not confined to any one group, position in the social structure, or specific site. For Foucault (1980: 98), power 'is never localised here or there, never in anybody's hands, never appropriated as a commodity or piece of wealth'. Rather, Foucault believed, power 'is employed and exercised through a net-like organisation' and individuals 'are always in the position of simultaneously undergoing and exercising this power' (1980: 98). In other words, instead of perceiving power as something located in and symbolised by the sovereign, Foucault suggested that power permeates society in such a way that 'nothing will be changed if the mechanisms of power that function outside, below and alongside the State apparatuses, on a much more minute and everyday level, are not also changed' (1980:60). Thus, it is this Foucauldian notion of the 'omnipresence' and 'specificity' of power relations that underlies Garland's view of the dispersion of crime control functions and responsibilities beyond the state, to local organisations and communities in civil society.

There are, however, distinct problems inherent in aspects of the Foucauldian analysis of power that Garland draws upon, pertaining to the failure to acknowledge the reality of central state power. As Sibeon (2004) points out, Foucault and other postmodern theorists influenced by his work, including here Garland, have gone too far in their relational conception of power, to the point of neglecting not only that social actors possess power, but also that some actors may become more powerful than others. One can agree with the claim that most of us are both exercisers of power and the target of its exercise, and the related conception of power as 'relational'. However, the argument that the central power of the state is limited and has no relevance in theorising the structure of power in contemporary societies is an argument that needs to be discussed from a practical overview and analysed from a different perspective informed by other political systems and social norms. The idea that power is centralised in the state, or the idea that power is concentrated as a result of the class structure of modern societies, cannot be rejected or downplayed in theorising contemporary application of state power. Kumar (2008) draws our attention to the need to recognise that despite the fact that global or 'macro' forms of power would be nothing without 'micro-powers', some groups continue to be disproportionately powerful. For this reason, Kumar argues that Foucault's notion of power as 'capillary' may be more meaningful viewed through a lens of class analysis than would otherwise be the case.

Despite the persistent concentration of state power and the continuous state monopoly over the provision of security in some non-Western societies, Garland fails to acknowledge this reality and discuss it within his late-modern crime control framework. Garland's *Culture of Control* thesis has been hailed as 'the most sweeping and stimulative account of the nexus of crime and social order put forth since Foucault' (Wacquant, 2009: 298). However, Garland can be criticised for an insufficiency of empirical evidence (Henderson, 2002) and for neglecting 'the larger global issues' beyond the UK and the US (Matthews, 2002: 225). These weaknesses seem to have led him to a sweeping application of Foucauldian conceptions of power in his discussion of criminal justice in late modernity, in consequence of which it fails to explain adequately penal policies and practices in non-Western societies. It may be suggested, therefore, that Garland's adoption of these conceptions should be modified because notwithstanding his claims of the decline of sovereign power, there are grounds to believe that, however pluralist modern societies may be, power is nevertheless concentrated in the sovereign state. Here, it seems that Garland's late-modern crime control framework would be strengthened if combined with certain insights from Weber's theory of 'state power'. Particularly relevant in this regard are Weber's theories regarding 'domination', which seem to be more suited to explain how the degree of pluralism in crime control is dependent on the way in which state power is exercised, which varies from one society to another depending on the type of political system and social norms.

Weber (1968a: 212) defines domination 'as the probability that certain specific commands (or all commands) will be obeyed by a given group of persons'. According to Weber, domination constitutes a special case of power, and thus it does not include every mode of exercising power over other persons. Weber points out the features associated with domination by noting that 'every genuine form of domination implies a minimum of voluntary compliance, that is, an *interest* (based on ulterior motives or genuine acceptance) in obedience' (1968a: 212 emphasis in original). While Weber acknowledges that not every case of domination utilises economic means, he still believes that domination which is founded on a position of monopoly, or what he calls 'domination by virtue of a constellation of interests', remains the bottom-line of other types of domination (Weber, 1968b: 943). The influence in this form of domination is derived from the exclusive 'possession of goods or marketable skills guaranteed in some way and acting upon the conduct of those dominated, who remain, however, formally free and are motivated simply by the pursuit of their own interests' (1968b: 943). However, Weber points out that 'monopolistic domination' in the broader sense is in no way produced only by the exchange relationships of the market, and that 'even mere possession can be a basis of power in forms other than that of the market' (1968b: 945).

Applied in the Saudi context, this Weberian notion of 'monopolistic domination' might help explain the current situation in which the state continues to claim monopoly over the provision of security against both external and internal threats, placing restrictions on non-state agencies' participation in policing activities. As pointed out in Chapter Two, the Saudi state has endeavoured to maintain its power by seeking to be the main supplier of public services, emphasising its importance to the everyday lives of all its citizens. This is stated in the Kingdom's Basic Law of Governance, which establishes that the protection and promotion of the welfare of the public is the duty of the state. In particular, Article 34 of the Basic Law of Governance confines the provision of military and security services to the state, which is obliged, according to Article 36, to provide security for all its citizens and all residents within its territory. In the Saudi context, therefore, the state's reluctance to relinquish its functional monopoly over the practice of policing can be understood in terms of the implications of such a strategy for the state's efforts to assert its domination over its people.

An indication of the state's concern to maintain its monopoly of policing functions can perhaps be inferred from the work of Al-Saud (2000), a member of the royal family, whose modest reform proposals may be seen as reflecting the vision of the country's rulers with regard to the form policing should take. Al-Saud (2000) drew a distinction between what he called 'functional' decentralisation, whereby policing services might be devolved to non-government entities, and 'territorial' decentralisation, whereby certain responsibilities, currently performed at central level, would be transformed to local levels, and he made clear that his proposals for change were confined to the latter. Invoking Islamic values and cultural traditions, he argued that any move towards functional decentralisation might be perceived as 'Western' or 'liberal' and would be unlikely to gain acceptance in Saudi society.

The crucial issue, however, is that 'the continued exercise of every domination...always has the strongest need of self-justification through appealing to the principles of its legitimation' (Weber, 1968b: 954). The reason for the centrality of legitimacy for a domination, as Weber points out, 'lies in the generally observable need of any power, or even of any advantage of life, to justify itself' (1968b: 953). Legitimacy, therefore, is an important social value, different from self-interest, which social authorities can invoke to elicit respect, obedience and cooperation (Tyler, 1990).

Appreciation of how 'legitimate authority', which in the Weberian sense is instrumental to a continuous domination, is maintained in Saudi Arabia and Western countries is essential to understanding the variations in the degree to which plural policing has been adopted in these contexts. In Western societies, the 'social contract', as a figurative basis for state legitimacy, has been replaced by forms of 'community' or 'parochial' contracts, in which conformity is premised upon the idea of negotiated consent and a degree of mutuality (Wood and Kempa, 2005; Crawford, 2003b). As Crawford (2003b: 502) notes, legitimacy rests upon a degree of legitimate consent, since 'people are more likely to abide by the terms of a contract in which they have actively participated'. In these societies, therefore, the development of social control strategies that incorporate non-state players can be seen as a symptom of this new way of legitimating the state and its apparatus, because they ensure submission and conformity through the integration of civil society and citizenship in the process of control.

The above indicated shift in the way in which the legitimacy of the state and its authorities is conceived of is combined with the broader neo-liberal legitimation approach that is currently dominant in Western societies. As Herbert (1999) points out, privatisation, devolution and other attempts to downsize government bureaucracies have come to constitute the basis for state legitimacy in these neo-liberal times. Thus, it is not surprising, given this ideological environment, to see the development of community policing and the growth of private security, because they demonstrate overt efforts at reducing state initiative (O'Malley and Palmer, 1996). This view is emphasised by Herbert (1999: 166), who argues that since the very term 'community' is particularly appealing in terms of state legitimacy, 'state-sponsored efforts at various forms of privately-driven crime reduction register broad legitimacy in a neo-liberal environment even if they mask an equally legitimate growth of the crime-control apparatus'.

In Saudi Arabia, a state which embraces the Islamic *Shari'ah* as the basis for all its systems, the legitimacy of the state authority should be viewed in light of the Islamic theory of governance. According to many Muslim scholars and jurists, Islam is not only a religion, but a comprehensive system governing public, social and political life, and Islamic *Shari'ah* is a complete moral code that prescribes for every eventuality, including governance (Al-Atawneh, 2009). Therefore, the link between religion and government has always been stressed. For example, the Shafi'i scholar, Al-Mawardi, one of the most famous political thinkers of the Middle Ages, stated that God ordained for the community (*al-umma*) a leader through whom He protected the community (*al-milla*); and He entrusted to him authority (*al-siyasa*), so that the management of affairs should proceed on the basis of right religion (*din mashru'*) (cited in Lambton, 1981: 85). In the same vein, Ibn Taymiyya, another ancient Muslim thinker, insisted that social justice requires Islamic government that upholds Islamic law, adhering to the principles of commanding right and forbidding wrong (Ibn Taymiyya, 1985). Ibn Taymiyya's pupil, Ibn Al-Qayyim, viewed politics as inseparable from religion, since only Islamic government would safeguard religious values (Ibn Al-Qayyim, 1986). Even today, the unity of religion and politics is still asserted in Islamic debate on governance. Modern

Muslim scholars maintain the traditional creed of the inseparability of religion and state, and regard the protection of Islam and its values as central to the government's role and a key rationale for its existence (Al-Qaradawi, 1997; Al-Turabi, 1997; Al-Wahidi, 1988; Al-Atawneh, 2009).

According to Islamic political discourse, ancient and contemporary, governance or *siyasa* must embrace *Shari'ah*, and for this reason it is referred to in the classic Islamic literature as *siyasa shar'iyyah*. The term *siyasa shar'iyyah* is defined as 'the administration of the affairs of subjects, carried out by attention to their well-being and needs, their property and honour, and the dispatch of justice between and amongst them' (Ibn Khaldun,1982: 213). While it is not intended to provide a comprehensive account of the Islamic theory of governance or *siyasa shar'iyyah*, the focus here will be particularly on one fundamental principle of governance that offers some insight into the issue of state legitimacy in an Islamic country like Saudi Arabia, namely, the Islamic view of authority-holders or rulers.

In Islam, God (Allah) is the only sovereign and source of legitimate law (Abu El Fadl, 2004). However, from the earliest times it has been recognised that this sovereignty is exercised on earth through human agency in the form of authority-holders who command allegiance and obedience. Islamic political theory views legitimate government as bound by *Shari'ah* law and subject to a social contract (*'aqd*) between the ruler and the populace, who give their *bay'a* (allegiance or consent to the ruler) in exchange for his undertaking to discharge his obligations to protect them and to uphold *Shari'ah*. Provided the ruler fulfils these duties, obedience to him is a religious obligation (Abu El Fadl, 2004; Ibn Taymiyya, 1985; Ibn Al-Qayyim, 1986; Al-Qaradawi, 1997, Lambton, 1981).

A central feature of Islamic political thought is the absence of a systematic mechanism for defining the authority-holders' scope of authority, which results in conferring broad executive and judicial powers on the ruler within the structure of the governance or *siyasa shar'iyyah* doctrine. These powers, as Peters (2005) explains, may be undertaken by the head of state himself, but usually they are delegated to law enforcement agencies, notably the judge (the *qadi*), but also other security personnel, such as governors, military commanders and police officers, with parameters of the jurisdictions of these officials differing from time to time and from one place to another.

The former analysis of the notion of authority and authority-holders as theorised in Islamic political discourse enables us to realise that the authority of the King in Saudi Arabia, given the state's religion-based political system, is defined according to the classical Muslim theory of absolute authority of the Islamic leader. In this case, the principle of the ruler's total authority and the people's religious obligation to obey him, as emphasised in the Islamic theory of governance (*siyasa shar'iyyah*), serves as the basis for legitimising the state and its institutions in Saudi Arabia. It should be noted, however, that in Saudi Arabia authoritarian power can be unwittingly drawn not only from religion/the sacred, but also from tribal or clan social structures and from long-standing cultural norms. In sum, the legitimacy of the Saudi state's ruler is established both religiously and traditionally. In other words, to use Weber's terms, the validity of the King's (the dominant) authority rests on the grounds of 'an established belief in the sanctity of immemorial traditions and the legitimacy of the status of those exercising authority under them' (1968c: 328). This principle also extends to legitimate the actions of the police and prescribe obedience to them, as one of the judicial organs that the ruler establishes to maintain the welfare of the public.

The issue that needs to be considered here is that such an approach to legitimating the state and its apparatus conduces towards an authoritarian state and hierarchical structures rather than to dispersal of functions and creation of participative networks. Such a political culture, as Dupont (2004: 78) argues, does not facilitate 'the emergence of security networks and instead cement[s] the domination of hierarchical structures'.

However, despite the established legitimacy of the state and its police explained above, attempts have been made by the Saudi Ministry of Interior to gain public confidence that the police are acting for citizens. Indicative of this approach is the increasing interest in community policing in recent years. Thus, in the last decade or so, as Al-Harbi (2008) points out, the notion of community policing began to gain increasing prominence in the pronouncements of officials from the Ministry of Interior. However, the findings of Al-Harbi's research revealed that signs of the implementation of community policing were only evident in the fight against terrorism where, following the May 2003 Al-Qaeda attacks on Western and government targets in Riyadh, closer cooperation between citizens and security forces has resulted in the capturing of many wanted terrorists and the foiling of numerous planned attacks. Apart from cooperation in the 'war on terror', Al-Harbi concluded, although only based on the views expressed by the members of public who participated in his study, that comprehensive implementation of community policing remained very much restricted by inherent difficulties related to the organisation and culture of the Saudi police. The same findings were confirmed by another researcher (Sharaf, 2009) who, based on interviews with police officers, suggested that community policing is inapplicable in the Saudi context. Given the existing structural and cultural obstacles within the police organisation to even this limited form of plural policing, therefore, we should not be surprised to find, as the discussion below will show, that the culture and organisation of the police constrained their own willingness and ability to enter into partnership policing of Internet fraud.

7.2.1.2 The Police Organisation and Culture

Aside from the state and its policy, the findings of this study highlighted problems associated with police organisation and culture that seemed to hinder embracing a plural model of policing Internet fraud. As we can recall from Chapter Four, the majority of police officers greeted with reluctance the idea of allowing the policing of Internet fraud to take place beyond the state, although some of them acknowledged the ability of commercial policing entities to attain technological capabilities that would outstrip those owned by the police in this arena. To understand why officers appeared opposed to the involvement of the private sector in the policing of Internet fraud, it is rather important to view their concerns in their organisational context. The Saudi policing system, as was explained earlier in this thesis, has maintained a centralised national police force. Saudi police operations are coordinated from central headquarters, while assignment of personnel for service delivery is accomplished through the bureau. Decisions pertaining to policies and procedures are formulated by those at the top of the pyramid and passed through the chain of command down to the front line officer. As Wall (2008) points out, networked policing of Internet fraud would involve flattening the structure of policing division of labour. However, there appears to be no inclination toward any form of decentralisation of the Saudi police, at least in the foreseeable future. Logically speaking, throughout its long history, the traditional paramilitary system must have led the Saudi police agency to develop a formidable command and control bureaucracy that de-emphasised flattened and networked forms of policing in which private actors are equal partners. In fact, regardless of their rank, officers who have grown up in this system are not in the best position to dismantle it.

Workload is yet another point we need to consider when discussing the obstacles created by the police organisation to the emergence of a plural policing approach towards Internet fraud. Because the organisation is understaffed, officers are overworked and have little time to interact with members of the public. Added to this, the ability of police departments to be true partners with private sector actors is questionable, given that cooperation between and within these departments themselves in the policing of Internet fraud is limited by organisational conflict and tense officer-management relationships. More precisely, if effective cooperation cannot be achieved internally within and between police departments (see § 5.3 and 5.4), it would be unrealistic to expect the construction of partnership and policing networks with external private sector bodies.

It is true that some officers have shown some concern over the lack of police-private sector collaboration and appeared critical of senior management's rejection of their proposals for borrowing experts from the information technology sector to assist in police investigations of Internet fraud cases. However, at the same time, they have not called for any changes in legislation or in the manner in which the police organisation is structured or managed. Rather, on the contrary, those officers might be opposed to any substantial reform because they find it difficult to depart from the routine that shaped their personality and gave them important positions in the hierarchy of power. For all of those officers, any new arrangements would certainly threaten the status quo. Such an interpretation would be consistent with Rondinelli's (1979) argument that any new arrangements involving diffusion of power would not be advocated and supported by those who perceived such change as posing a danger or threat to their positions.

Also, as we have seen from Saudi police senior chiefs, their attitude towards partnership with the private sector for policing Internet fraud is one of scepticism and mistrust, perceiving any form of private actors' involvement as allowing 'outsiders' to have access to 'sensitive' information about citizens and about the system as a whole (see p. 133). For individuals who, as was highlighted in Chapter Two, are given strict and prolonged military training at the highest level, it is natural that they extol the virtues of their paramilitary system and appear sceptical about the participation of citizens in undertaking policing functions. Continuing on this theme of training, an issue raised in Chapter Five was the lack of specialist training in the policing of Internet fraud. Such training would inevitably imply training in the uses of information technology, which might have given officers a better appreciation of its potential for networked policing. In Western societies, information technology is an important element of the plural policing model. Ericson and Haggerty (1997) argue that the availability of such technology in Western police organisations has been a major factor in transforming the role of the police from law enforcers to brokers of information, connecting them with outside agencies for the purpose of information exchange, which is a key element of the plural policing approach. Chan (2003) similarly emphasises the importance of information technology in facilitating collection and use of data from 'a broader variety of government and non-government sources' (2003: 658). It might be suggested, then, that the availability of sufficient and up-to-date technological resources, together with competence in and understanding of their use, would not only facilitate information exchange between police and external agencies at a practical level, but would also promote an appreciation of the potential value of such cooperation. Both the resources and the understanding of how to exploit them were, however, found to be lacking in the police settings investigated. Participants reported an overly theoretical and outdated pre-service training that did not provide an adequate preparation for understanding and addressing cybercrime, but there were few in-service training opportunities available. Not only that, but lower level managers were reluctant to support applications for training due to workload and performance pressures that resulted in the prioritisation of short-term productivity, making officer absence, even for training, undesirable. In such circumstances, officers had little opportunity or encouragement to develop either the requisite practical skills or the mind-set for plural policing. In sum, the Saudi police appear to be an organisation that pays less attention to innovation, and generates only a police personality characterised by conservatism, suspicion, a sense of alienation, cynicism and pessimism (Reiner, 2000a).

7.3 Police Mediation of Risk in a Theocratic Society

The policing of Internet fraud may reflect the increasing significance of the 'risk prediction' techniques emphasised by the new penology. The 'risk mentality' is concerned with 'forestalling future crime by identifying risks on the basis of past patterns of offending' (Ekblom, 1998, cited in Johnston and Shearing, 2003: 122). This involves actuarial methods for classifying 'individuals and groups as particular bearers of risk who, once identified, can become the target of proactive intervention' (Norris and McCahill, 2006: 114). In the case of policing Internet fraud, Wall (2008) argues that a 'risk-based' policing approach is possible by relying, for example, on computer-centred surveillance technologies to 'predict' and 'pre-empt' fraudulent behaviour in cyberspace before it takes place, based on analysis of intelligence data derived from different multimedia sources. According to Wall (2008), the collected information that is produced from this online surveillance process allows profiles to be constructed, making it easier to anticipate potential 'risks' in cyberspace before they occur. Individuals and activities that match the 'simulated' risk (Bogard, 1996) can, then, be the target of pre-emptive intervention.

The question, however, is what are the 'criteria' that shape both the process of identifying signs of 'risk' and the way the police respond to it? This is the issue that needs to be discussed and analysed based on the argument that the mediation of risk is influenced by the dominant cultural ideas, values and interests of the studied society. Although in the context of the policing of Internet fraud this matter has received little attention from Western scholars, the scant empirical evidence available suggests that in capitalist societies, risk is perceived predominantly from a rational economic perspective (Murff, 2007; McKenzie, 2006). This might be attributed to what Crawford (2003a) calls 'the cross-fertilisation' of mentalities and practices that has resulted from the interactive nature of public/private policing developments in capitalist countries.

As the evidence presented earlier in this thesis has shown, however, in non-Western settings, religious values and mores result in risk being conceived of by police rather differently. In a conservative society like Saudi Arabia, people are brought up to appreciate and adhere to religious values and cultural traditions. Accordingly, the influence of these factors on how Saudi police both conceptualise and address risk should not be surprising. As Mawby (2003: 35-6) argues, 'police systems are closely embedded in the wider structure and the culture of their societies'. In what follows, we will discuss the implications of Saudi religious and cultural values for the types of risk singled out for attention by police in Internet fraud activity as well as the impact of these values on officers' mediation of risk-prediction technology.

7.3.1 The Policed Risk: 'Moral' Policing versus Policing Fraud

Existing research shows that policing Internet fraud in Western contexts is carried out with a 'capitalist' mentality that is preoccupied with economic and commercial considerations, such as the sustaining of profitability and loss prevention (Garland, 2001). As Ericson and Haggerty suggest, in risk society, 'efficiency in loss reduction is *the* moral imperative' (1997: 124 emphasis in original). This was not found to be the case in the Saudi context, as the findings reveal that the main concern in the Saudi police response to online fraudulent activity is upholding religious and cultural principles. Therefore, the criteria of financial loss (Murff, 2007) or the cost of investigation (McKenzie, 2006), which influence police perception of risk in capitalist societies, appear to be less important for Saudi police than the degree of violation of religious and social values involved in Internet fraud incidents. This is reflected in the characteristics of those Internet fraud incidents which police officers prioritised over others.

In Riyadh, as was elaborated in Chapter Six, officers placed the category of 'Saudi-style blackmails' at the top of their hierarchy of response to Internet fraud incidents. Since this type of incident usually involves scandalous materials on the victim being obtained electronically and then used by the perpetrator to extort money, risk is associated with the serious social consequences that could result from the publication of these materials. In such a conservative society, where even the appearance of a woman's face is unacceptable, disclosing pictures implying indecency would have lasting damaging effect on the woman's reputation and that of her whole family. In such a situation, officers' priority was to provide an urgent response that would avert the publication of the victim's 'scandalous' pictures. In addition, officers perceived risk in Saudi-style blackmails in terms of the potential for the female victim to 'slip' into immoral behaviour as a result of the pressure exerted on her by the 'blackmailer'. In other words, officers were keen to act quickly to protect the female victim's morality. In this regard, police officers demonstrated commitment to the fundamental ethos of maintaining morality and virtue in society which underpins the mission of the Commission for the Propagation of Virtue and the Prevention of Vice (*Alhai'a*), whose involvement in handling Saudi-style blackmail cases provided an extra investigative resource for the police, but also placed their response under close scrutiny.

Saudi Arabia is a society which sets great store by honour and individual morality and behaviours affect the reputation and social standing not only of the person concerned, but of his/her family and community. For this reason, a girl or woman who becomes embroiled in a moral scandal that tarnishes her family's good name may be vulnerable to severe reprisals, even to the extent of murder, to restore the family's honour. Officers, conscious of this risk, tried to protect female victims of Saudi-style blackmails. It might be thought that the woman's safety could be assured by dealing with the complaint confidentially, away from anyone who might be motivated to harm the victim. However, confidentiality for female victims is virtually impossible to assure in practice, since religion and law demand that women can be interviewed only in the presence of a *Mahram* (guardian). Officers therefore were required to negotiate with and counsel victims' relatives and take steps to avert violence perpetrated in the name of honour.

The second priority in police responses to Internet fraud was incidents involving the victimisation of elderly people who had difficulty using their *Sarraf* cards at ATMs and were defrauded by those purporting to help them. As in the previous example, this type of incident was interpreted in the light of moral values, which outweighed the issue of financial loss in police considerations of the seriousness of such offences. Arab culture and Islam enjoin respect and care for the elderly, so that this class of fraud was seen as a violation of an honoured religious and cultural principle. The police attitude in these cases was manifested in the highly respectful and considerate treatment of elderly complainants in police stations. Many officers viewed care and reverence for the elderly not only as an observance of social norms but even as an act of worship performed in obedience to the teachings of the Prophet. Conversely, the perpetrators in this kind of case were viewed with particular contempt, not only for their greed, but for their immorality and lack of proper 'manly' virtues. Thus, police attitudes towards such incidents reflect their internalisation of and commitment to traditional social and religious values.

Given the way police officers' perception of Internet fraud incidents was filtered through the lens of religious and cultural values, cases of 'pure' Internet fraud, involving only financial loss, did not carry the same 'moral' imperative as the above types of incident. In such cases, the speed and level of response was more variable, depending on the officer concerned. A 'technophile-work embracer', even in the absence of such a moral imperative, might still be inclined to engage in a proactive targeting, or to follow up complaints to the point of resolution. 'Technophobe-work embracers' and 'technophile-work avoiders' appeared often to give a 'tokenistic' response, recording the complaint then forwarding it to be dealt with by an external agency, while a 'technophobe-work avoider' might take no action at all. The key issue to be noted is that officers' responses to these 'pure' Internet frauds occurred in the context of numerous other demands on their time and resources, and 'morality-violating' offences were perceived as more serious and, hence, of greater priority for action. In this situation, the meaning of an incident from the victim's point of view was of secondary concern.

The above discussion seems to suggest that the existence of the moral dimension can be viewed as an indication of a high priority in police response to Internet fraud, whereas its absence would allow incidents to be relegated to the bottom of the police hierarchy of response. However, whether this dichotomy captures the complexity of the influence of moral values and cultural norms on police prioritisation of Internet fraud is another question. As we have seen above, officers' urgent response to Saudi-style online blackmails directed against female victims was influenced by the moral values and cultural traditions of Saudi society. However, the same moral values and cultural norms appeared to contribute to an indifferent attitude towards online blackmails if a man was on the receiving end of the scam. As noted previously in discussion of the detection of Internet fraud (see § 6.4), men who became victims of extortion, having been duped into providing scandalous images of themselves online to correspondents misrepresenting themselves as women willing to enter into illicit virtual and actual relationships, were seen by officers as responsible for their victimisation, and morally blameworthy. Since the police reflect the dominant culture in their particular society (Waddington, 1999), officers condemned the behaviour of these victims because it contravened the principles of morality, which are fundamental to the Saudi social identity. This was an example of how traditional cultural norms and social values would influence the degree of priority accorded to Internet fraud incidents, highlighting the necessity of taking account of such normative cultural influences when seeking to understand the police response to Internet fraud in the Saudi context.

That said, it could be an exaggeration to claim a distinction between 'moral' policing in non-Western societies such as Saudi Arabia and 'amoral' policing in the West. Ericson and Haggerty (1997) point out that despite the dominance of instrumental or risk-based values, moral discourse continues to find its space within social control systems in Western societies. They argue that morality is embedded not only in ‘risk technologies and systems of risk management’ but also in ‘the classification schemes and risk assessment data used for probability calculations’ (1997: 123). Citing Gusfield’s (1981) analysis of the public discourse on drink-driving, for example, Ericson and Haggerty note that drink-related accidents are perceived as caused by people acting ‘immorally’. According to Ericson and Haggerty, Gusfield’s analysis shows ‘how actual law enforcement decisions about impaired driving involve fine-grained moral evaluations of the drinking driver and the circumstances of his or her accidents’ (1997: 124). Another example of the way crime control judgements in Western societies are influenced by prevailing moral standards is the historical tendency of police to ignore instances of domestic violence, unless they impinged on public order, maintaining traditional social norms of male dominance and control (Simon, 2007). The more recent trend to use surveillance to ‘protect’ women from such abuse paradoxically raises another moral issue, since it poses a risk of escalation by male perpetrators, in an attempt to assert their control; moreover, victims who forcefully resist may themselves risk being charged as offenders (Coleman and McCahill, 2011). Moral assumptions about social features as producing criminogenic lifestyles are also argued to be the rationale behind current police practices, such as sweeps, crackdowns and intense patrolling, which are targeted differentially at areas of specific ethnicity and class, with the crimes of the poor and marginalised as the prime focus of such practices (Manning 2008b).

Thus, it can be seen that policing policies and practices in both contexts are subject to moral judgment about how society ought to be organised, and the meanings attached to social behaviours. The difference appears, however, to be in the extent and nature of such influence. What we need to remember, therefore, is that variations exist between societies in their cultures, and these variations would mean that not only would police in diverse contexts conceptualise policing technologies differently, but also the functions these technologies are used to perform by police officers in different nations might be influenced by the extent of their belief in and commitment to the society’s dominant cultural norms and social values. This argument can be further illustrated by discussing the impact of traditional values on police conceptualisation and operation of technology.

7.3.2 Traditional Values and the Mediation of Technology

In the theorisation of a risk-based policing of Internet fraud, computer-assisted data mining techniques have been presented as ‘the key to unlocking the “disciplinary” potential of networked technology’, enabling both the monitoring and ‘pre-emption’ of Internet fraudulent activities (Wall, 2008: 189). These techniques are made possible by the growth of surveillance computer software, which can analyse Internet traffic data flow to anticipate possible future fraudulent schemes (Ballard, 2006). However, as Graham (1998: 388) has pointed out, ‘the reality of technological innovation is a great deal less deterministic and a great deal more “messy”, difficult, contingent and open to contested interpretations and applications’ (quoted in McCahill, 2002: 186). Researchers who adopt the SCOT approach have long stressed the active role of organisational members and the importance of social context and processes in shaping the implementation of information technologies. They argue that the consequences of the introduction of a specific technological system into an organisational context cannot be understood in a ‘deterministic’ or ‘rationalist’ way, but rather they should be viewed ‘interpretively’ as emerging from the interplay among a range of technical, psychological, social, political and cultural factors (Orlikowski and Robey, 1991; Robey and Sahay, 1996).

Although the issue of whether and to what extent new technologies and computerised surveillance databases are incorporated into existing police intelligence systems to effect a ‘risk-based’ crime control of Internet fraud has not been subject to empirical investigation, general research on policing and information technology conducted in some Western countries has drawn attention to how the human mediation of this technology places limits on its disciplinary potential (Chan, 2001, 2003; Chan et al., 2001; Manning, 2008a; Meehan, 1998; Sheptycki, 2003). Consequently, one of the main concerns of the current study has been to investigate the extent and nature of police use of computer-centred technologies to undertake a proactive approach towards policing Internet fraud. Despite the general insufficiency of technological infrastructure in Riyadh police departments, the data collected on officers’ use of the available technology for proactive policing of Internet fraud confirmed the findings of Western researchers in terms of the effect of the organisational context on this issue. In this regard, the current research highlighted the close link between some officers’ non-use of technology and the tense work relationships that existed in their departments and their disillusionment with their jobs.

However, the marked difference between previous research and the present study in terms of police mediation of technology is in relation to the impact of religious and cultural values, an issue on which Western police researchers had nothing to say. As the discussion in Chapter Six shows, the influence of traditional values can restrict officers' use of surveillance technologies for proactive policing of Internet fraud in a number of ways. For instance, those officers who perceived the monitoring of Internet users' activities as constituting a form of *tajassus* (spying), which is forbidden in Islam, were not only less than enthusiastic to use technologies of online surveillance, but also saw making these technologies available in police departments as inappropriate. Such concerns seem to echo McCahill and Norris's (2003) notion of 'misappropriation of personal information', the most common form of which, as evidence in a number of Western contexts has shown, is the use of surveillance technologies by police and security staff to intimately observe women for voyeuristic purposes (Coleman and McCahill, 2011). In the Saudi context, then, it was not the concern with the potential use of technology as a surveillance mechanism by supervisors (Ericson and Haggerty, 1997), but rather the prohibition, in Islam, of spying and covert activities which provoked some officers' aversion to some aspects of information technology. It could be argued that those officers strove to be true Muslims, whose fear of penalty and desire for rewards from Allah compelled them to comply with all Allah's commands, since they knew that He was monitoring them all the time. The deterrent force of punishment and rewards both in this world and in the hereafter is an essential element of the Muslim faith, and it is presumed to shape every aspect of Muslims' behaviour.

Moreover, the ability to operate the existing technology in a way that would allow the interception and prevention of Internet fraud activity was limited by the fact that some officers had insufficient knowledge of technology to use it in a proactive way. While this was largely attributed to organisational factors, mainly, the lack of pre-service or in-service training, the findings reveal that religious beliefs and cultural values can also contribute to self-imposed ignorance of technology. Recall, for example, Major N, who was very dedicated to his job, but hated dealing with Internet fraud due to his technophobic attitude toward the Internet. He expressed adherence to Saudi religious and cultural norms and refused to allow the Internet into his house, perceiving it as a 'liberal' and 'manipulative' communication medium that is very difficult to control and can bring deviance, distraction and confusion to the home and family.

In fact, rejection of new technologies on religious and cultural grounds is nothing new in Saudi Arabia. For instance, Al-Naim (2008) points out that Western innovations have always been met with some degree of resistance from conservative Saudis, who viewed them as a threat to their Islamic identity and cultural values. Al-Naim describes how the TV, cars, telephones and other inventions struggled to find their way into Saudi society. He argues that in every aspect of their life, people in Saudi Arabia 'thought about the impact of the imported values and technology on their morals and social values...[and] as a result, the change was limited to physical issues rather than values' (2008: 129). With regard to the Internet, it could be argued that the late and relatively limited penetration of this technology in Saudi Arabia and the current filtering policy are linked to concerns about its cultural impact.

Another illustration of the influence of the Saudi culture and social norms in terms of limiting the scope for risk-oriented utilisation of technology in the policing of Internet fraud can be seen with regard to officers' operation of computer-based databases. In the US, Manning (2008a: 189) found that the vast increase in capacity to process information that was introduced to the data repository in some departments 'had little consequence on the ground except to increase the number of ad hoc queries to databases' which 'were incident based, not problem based' and 'had little to do with altering the social conditions or access to criminal opportunities or "crime prevention"'. As we have seen in Chapter Six, the same can be said about the terminal points introduced to the DDI and the police stations, which were connected to the Ministry of Interior's National Information Centre (NIC). These NIC terminals, which enabled the police to tap into a wide range of information from different governmental sources, were used heavily by officers. However, the majority of the queries that NIC terminal operators ran on the system were not for the purpose of obtaining information which might be used for identifying and preventing risks of Internet fraud or other crimes. Instead, and unlike their counterparts in Manning's sample, who after all used the databases for policing purposes, a considerable part of NIC terminal operators' time in Riyadh police departments was devoted to attending to the demands of relatives and friends who wanted to check their records for traffic fines and other sorts of queries. Officers were under enormous pressures to respond to such demands because refusal to do so would be a serious discourtesy that could affect their relationships with their friends and relatives. Despite the concerns voiced by some officers about the dilemma in which they were placed as a result of this situation, still they wanted to avoid being stigmatised in their society as unhelpful.

It is important to recognise that in a tribal culture, such as that widely prevailing in Saudi society, fulfilling the social needs of family, relatives and friends has crucial implications for individual, family and tribal reputation. Fulfilment of relatives' social needs is acknowledged in phrases like '*Wnaam*' (he is a helpful person) and '*May Allah brighten his face*', whereas failure to do so, for whatever reason, might lead to an individual being perceived as helpless and disloyal to the family, tribe or friends. As Bjerke (1999: 118) has commented, in Arab culture, including Saudi culture, loyalty (to family, tribe or friendship) is a virtue that exceeds in importance other considerations, such as efficiency. Tribal belonging goes beyond holding the name of the tribe, emphasising commitment to established traditions and norms, and being supportive of other members. Failure to fulfil this moral obligation evokes the displeasure of others and can sometimes lead to ostracism (Al-Saif, 1997). Emphasising the concern for friendship, Al-Faleh (1985) also argues that the concept of friendship in Arab culture is taken beyond boundaries that are familiar in the West, e. g. making it very unusual for an Arab openly to refuse a friend's request.

The issue that needs to be considered, therefore, is that with the employment of advanced surveillance systems, the power of the Saudi 'old' cultural traditions and social norms still has its effect on the process of utilising these technological systems and shaping their mechanisms, which can place limits on their potential role in the prevention and investigation of Internet fraud. The focus on this issue becomes even more pertinent when it is realised that, as Al-Awaji (1971, cited in Al-Naim, 2008: 129) has stated, not only has the social value system continued to dominate social life in Saudi Arabia, but also it has compelled institutions to adapt their behaviour to its demands.

As has been discussed in Chapter Two, the effect of the wider society's dominant cultural values was given no attention by Western researchers in their studies of public police operation of information technologies. This does not mean that this issue is completely lacking in pertinence in Western societies. Research carried out in the UK, for instance, has shown that the use of new surveillance technologies by private police officers is shaped by local cultural traditions (McCahill, 2002). This shows that Saudi Arabia is not a unique case and that it remains logical to argue that cultural traditions and social norms would be important factors in shaping police attitude and utilisation of technology in every context, an issue which requires due attention in any attempt to understand and analyse this aspect of police work.

Aside from raising important questions about the manner of police utilisation of risk-prediction technology, the above discussion suggests the need for a re-assessment of some key assumptions in the theoretical literature of surveillance and social control. Looking at the debate on surveillance and technology in recent years, evidence can be seen of the influence of Foucault's (1977) *Discipline and Punish* and Orwell's (2004[1949]) novel *Nineteen Eighty-Four* on the thinking of many criminologists and social theorists about the implications of ongoing developments in surveillance technology for policing. Thus, Marx (1985), for example, has claimed that policing has been transformed by the introduction of information technology, which he sees as heralding the demise of traditional policing and social control, and marking a significant move towards the creation of a 'maximum surveillance society'. According to Marx, 'with computer technology, one of the final barriers to total social control is crumbling' (1985: 21). The Internet is alleged to have been successfully transformed by state agencies, such as the police, into one of the most effective tools of monitoring and controlling behaviour, which is seen as another manifestation of an Orwellian scenario in which state power is enhanced by technological innovation. For instance, McGuire (2010: 497), classifying online surveillance into surveillance of Internet interactions and surveillance that uses the Internet, has commented on a police surveillance that is no longer 'focused upon targeted, or intelligence-driven data acquisition but a generalised scrutiny of any kind of communications'.

Perhaps influenced by such visions of the spread of information technology into the realm of policing, upholders of civil rights and privacy advocates have also voiced concerns about the impact of online policing on liberty and freedoms in society. As Kozlovski (2007) points out, serious concerns have been raised about the tendency of online policing to expand the mechanisms of social control and remove the limitations that once constrained policing powers. Particularly worrying for opponents of online policing, according to Kozlovski, are tactics such as predictive data mining, which are seen as defying the form of probable cause and particularised suspicion, thereby increasing the possibility for the police to monitor and potentially restrain non-criminal activities.

Such accounts of the implications of the introduction of computer technologies into the police surveillance and information systems for the issues of power and civil liberty take a deterministic view, assuming that the police use these technologies in a ‘calculated, controlled and ruthlessly efficient manner’ (Walker, 1983: 694). This deterministic view of the relationship between surveillance and technology can also, as McCahill (2002: xiv) points out, be observed in the writings of many commentators on CCTV, who tend to suggest that these systems are used in certain, pre-defined ways that either aim ‘to detect and prevent crimes or to extend the disciplinary potential of panoptic systems’, paying no attention to the need for ‘a detailed micro-sociological account of the construction and operation of visual surveillance systems in different institutional settings’.

However, this research has provided evidence that contrary to such assumptions, it is not necessarily the case that the police are becoming more repressive as a result of the introduction of computer-mediated surveillance technologies, or that the spread of these technologies marks the arrival of the Orwellian future. As the evidence presented in Chapter Six and discussed further earlier in this section shows, when computer technology was available to officers in the investigated police departments in Riyadh, its use for online surveillance purposes in the policing of Internet fraud was very limited. This is hardly surprising, as only a few officers had the ability and desire to use the surveillance functions of this technology. This, in part, can be attributed to organisational issues, such as the lack of specialist training and the existence, in some departments, of unfavourable work relationships which affected some officers’ willingness to utilise their computer proficiency. However, the reason for the limited scope for online surveillance in the policing of Internet fraud in the current research appears to be far more fundamental than merely organisational factors. It seems that the influence of the society’s religion and culture has mediated the impact of the available technological equipment, with officers appearing to be more concerned to adhere to the dominant religious principles and social norms rather than to incorporate online surveillance into their policing approach towards Internet fraud. Suffice it here to recall the remark of one officer who justified his objection to the idea of online surveillance in policing by saying:

> When you say monitoring what people do on the Internet to know if someone is misbehaving, that basically means spying on people. We are warned by the Qur’an against indulgence in spying and surreptitious activities. I wouldn’t be encouraged to go this way (PS21)

Thus, while the findings of the present study support Norris and McCahill's (2006) argument that the potential of new surveillance technologies to transform policing must be viewed in the light of the fact that these technologies are shaped by the values and practices of those who use them, they demonstrate the particular salience of this consideration in a theocratic society like Saudi Arabia, where people's life continue to be dominated by religious and cultural values.

Against this background, it seems ironic that despite the warning sounded four decades ago by a pioneering surveillance writer (Rule, 1973: 34) against the danger of speculating on the consequences of the changes in the technology of surveillance before first undertaking the 'close documentation of existing practices and painstaking analysis of their relations to their social contexts', speculative and deterministic predictions continue to be made in today's discourses on police engagement in online policing and surveillance. This raises the concern that these issues – given the growing literature on Panopticonism, risk and insecurity, and the relationship between surveillance and social control – will become over-theorised and divorced from reality unless more of an effort is made to understand them in their real-life contexts, with due attention paid to the political, cultural and social particularities of those contexts.

7.4 Future Directions

In this thesis, the researcher has sought to present an in-depth analysis of the policing of Internet fraud in a Saudi Arabian city. To date, very little research has been conducted in this part of the world on the issue of policing in general, let alone policing Internet crimes. While this research is written in the context of the cybercrime environment, it represents a contribution to the research body on policing in non-Western societies. Not only has the present research described how Internet fraud is policed in Riyadh, but also it has given invaluable insight into why the policing of this crime is performed in a particular way. That said, however, this project remains only one step towards addressing the gaps and discontinuities that continue to exist in this area of knowledge.

At this point, two directions in which to continue this research are recommended. First, for the reasons discussed in Chapter Three, this research focused only on Riyadh city. However, Saudi Arabia is a large country, consisting of a wide variety of regions which vary significantly in many demographic aspects, including urbanism and tribalism. Although it is true that the Saudi culture is homogeneous in the sense that people in this country have the same religion, language, ethnicity and share common values, similarities and commonalities at the macro level do not necessarily mean homogeneity at the micro level. According to Al-Saif (1997), Saudi society can in fact be divided into three categories; nomadic and semi-nomadic Bedouin tribes; settled agriculturists; and urbanized city dwellers. Al-Saif also points out that Saudi society is composed of tribal and non-tribal classifications. These categories and classifications may be reflected in variations among regions in how Saudi people in each region interpret and articulate common cultural values and social norms, the degree to which they adhere to them, and ultimately the extent to which these cultural values and social norms influence the behaviour and attitude of Saudi police. Moreover, the selected city Riyadh is, in some aspects, different from other cities in the Kingdom when one takes into consideration the fact that facilities and resources, although seen as insufficient by the study participants, are presumably more available to police in this city because it is the capital city. Police in other regions may lack such advantages, which could have an impact on their response to Internet fraud. More importantly, the variations between Riyadh and other cities in socio-economic and technological conditions may have some implications in terms of the extent and nature of online fraudulent activity experienced. Thus, while this study has provided unprecedented insights into the policing of Internet fraud in Saudi Arabia, its findings remain limited by the fact that they were generated from a single region. However, homogeneity among regions should not be taken for granted, and therefore, research could be extended geographically to cover, for instance, the major cities of the other four main provinces of the Kingdom, i.e. the Eastern, Western, Sothern and Northern regions. This would allow for some further tests of the present findings and their generalisation to the police forces of other cities.

Moreover, in the broader theoretical context, this case study of Saudi Arabia reemphasised the importance of moral and cultural factors in the study of policing and crime control. The marked difference between the findings of the present research and previous observational studies on policing is that the influence of the spiritual and moral dimensions in shaping police officers’ attitudes and operational paradigms is rarely if ever referred to directly by those who have attempted to provide a detailed micro-sociological account of police work. What is missing in this endeavour is examining deeply the role of cultural traditions and religious values in guiding police response to Internet fraud and other types of crimes in different settings. More empirical research is needed to outline the real impact of moral and cultural values on the performance and outcomes of police response to cybercrime within both Western and non-Western societies. This direction would show how the police's perception and mediation of risk in the online environment is shaped by traditional norms within different social and cultural contexts. Together with the work undertaken in the present thesis, future attempts in this theoretical line might combine to establish a theoretical framework to explain the continued influential role of religion and national and local cultures in the design and implementation of crime control strategies in contemporary societies.

7.5 Concluding Remarks

While the Western literature has been reviewed in this thesis to establish a theoretical background against which the policing of Internet fraud in Saudi Arabia can be analysed, the researcher has been under no illusion that concepts of social control developed in Western liberal democracies are entirely appropriate for understanding policing in authoritarian and/or theocratic political contexts (Wood and Kempa, 2005). Indeed, the present findings demonstrate that the situation in Saudi Arabia is markedly different from what has been theorised and practised in Western countries. This leads us to suggest that due to cultural differences in societies, it is difficult to generate a global theorisation of the functions and operations of policing systems, or to reconcile insights coming from the broad globe with the realties in local worlds.

The point that needs to be highlighted and considered in understanding and theorising policing in late-modern societies is that there is an exercise and practice of policing in another part of the world with its own social identity, cultural character and ideological particularity. The mediation of risk in theocratic societies like Saudi Arabia has its particular characteristics that Western criminological perspectives have little to say about. This study has thrown light on this issue by exploring it in relation to the policing of Internet fraud, but it remains an intriguing case for further criminological research – one that may lead to important empirical and theoretical insights about the nature of contemporary crime control policies and practices, which will no doubt enrich the discipline. It is hoped that this challenge is taken up soon and extended even beyond the boundaries of the Saudi context and the narrow focus on policing Internet fraud.

References

References

Abdraboh, B. (1986) *Saudi Arabia Forces of Modernization*. Jeddah: Al-Nore Press (in Arabic).

Abo-Hasirah, M. (1998) *Education, Political Development and Stability in Saudi Arabia*. Unpublished PhD Thesis, Southern California University, US.

Abu El Fadl, K. (2004) *Islam and the Challenge of Democracy*. Boston: Princeton University Press.

Ackroyd, S., Harper, R., Hughes, J. A., Sharpiro, D. and Soothill, K. (1992) *New Technology and Practical Police Work*. Buckingham: Open University Press.

Alahmari, A. (1997) *The Organization of Police in Saudi Arabia*. Riyadh: Samha Press (in Arabic)

Al-Atawneh, M. (2009) 'Is Saudi Arabia a Theocracy? Religion and Governance in Contemporary Saudi Arabia', *Middle Eastern Studies*, 45(5): 721-737.

Al-Awaji, I. (1971) *Bureaucracy and Society in Saudi Arabia*. Unpublished PhD Thesis, University of Virginia, the USA.

Albanese, J. (2007) 'Fraud: The Characteristic Crime of the Twenty-First Century', in J. Albanese (ed.) *Combating Piracy: Intellectual Property Theft and Fraud*. London and New Brunswick: Transaction Publishers, pp. 1-12.

Al-Bishr, K. (2000) *Crime Prevention in Saudi Arabia*. Riyadh: Nayef Arab Academy (in Arabic).

Al-Faleh, M. (1985) 'Cultural Influences on Arabian Management Development: a Case Study of Jordan', *Journal of Management Development*, 6(3): 19-33.

Al-Farsy, F. (2003) *Modernity and Tradition: The Saudi Equation*. London: Knight Communications Ltd.

Al-Gahtani, S. (2004) ‘Computer Technology Acceptance Success Factors in Saudi Arabia: An Exploratory Study’, *Journal of Global Information Technology Management*, **7**(1): 5.

Algarni, A. (2011) ‘Is a Shari’ah-based Law Compatible with Cybercrime? An Inquiry into the Saudi Regulations on Internet Fraud’, *In-Spire Journal of Law, Politics and Societies*, 5(2): 1-17.

Al-Ghamidi, S. F. (1981) *Structure of the Tribe and Urbanisation in Saudi Arabia*. Jeddah: Al-Shrooq Press (in Arabic).

Al-Gheraibi, A. (1994) *Work Orientations and Achievement of Managers in Government, Semi-Private and Private Organisations in Saudi Arabia*. Unpublished PhD Thesis, University of Glasgow, Glasgow, UK.

Alhadar, I. and McCahill, M. (2011) ‘The Use of Surveillance Cameras in a Riyadh Shopping Mall: Protecting Profits or Protecting Morality?’, *Theoretical Criminology*, 15(3): 315-330.

Al-Hakeem, M. (2007) ‘Cyber Crime Takes Toll in Saudi Arabia’, *Gulf News* [online]. Available at: http://archive.gulfnews.com/articles/07/09/26/10156113.html (Accessed on 17 March 2009).

Al-Harbi, M. (2008) *The Role of Police in Saudi Arabian Society: A Study to Investigate the Attitudes of Civilians toward the Police Patrol Officers*. Unpublished PhD Thesis, University of Manchester, Manchester, UK.

Alharthi, A. (1990) *The Organization and its Jobs*. Riyadh: Safeer Press (in Arabic).

Al-Joware, I. (1983) *Development and Family in Saudi Arabia*. Unpublished PhD Thesis, University of Florida, Florida, US.

Alminshawi, M (2003) *Internet Crimes in Saudi Society*. Unpublished MA Dissertation, Naif Arab Academy for Security Sciences, Riyadh, Saudi Arabia (in Arabic).

Al-Naim, M. (2008) ‘Riyadh: A City of “Institutional Architecture”’, in Y. Elsheshtawy (ed.) *The Evolving Arab city: Tradition, Modernity and Urban Development*. London: Routledge, pp. 118-151.

Al-Nimir S. and Palmer, M. (1982) ‘Bureaucracy and Development in Saudi Arabia: A Behavioural Analysis’, *Public Administration and Development*, 2(2): 93-104.

Al-Omary, A. (1984) *The Saudi Arabian Family in Transition*. Unpublished MA Dissertation, University of Cardiff.

Al-Otaibi, A. (1995) ‘Executive Power in the Kingdom of Saudi Arabia’, in M. Al-Tawail (ed.) *Public Administration in the Kingdom of Saudi Arabia*. Riyadh: Institute of Public Administration, pp. 70-92 (in Arabic).

Al-Qaradawi, Y. (1997) *The Philosophy of State in Islam*. Cairo: Dar al-Shuruq (in Arabic)

Al-Rabiah, I. (2001) *Training Effectiveness*. Unpublished MA Dissertation, Um al Qura University, Makkah, Saudi Aabia (in Arabic).

Al-Riyadh Daily (2007) ‘Saudi Banks Warns Customers against Mobile and Internet Fraudulent Messages’, 10th October, [online]. Available at: http://www.alriyadh.com/2007/10/10/article285877.html (Accessed on 23 November 2007).

Al-Riyadh Daily (2008)’Catching Criminals is Difficult, but the Anti-Cybercrime Law will Put a Curb on Internet and Mobile Phones Misuse’, 14th February, [online]. Available at: http://www.alriyadh.com/2008/02/14/article317580.html (Accessed on 14 December 2008).

Al-Romaih, Y. (1993) *Social Discipline and Delinquency in Saudi Arabia*. Unpublished PhD Thesis, Washington State University.

Alsaggaf, Y. (2004) ‘The Effect of Online Community on Offline Community in Saudi Arabia’, *Electronic Journal on Information Systems in Developing Countries*, 16(2): 1-16 [online]. Available at: http://www.ejisdc.org/ojs2/index.php/ejisdc/article/viewFile/97/97 (Accessed 3 October 2010).

Al-Saif, M. (1997) *An Introduction to the Study of the Saudi Society*. Riyadh: Al-Kheraiji Publisher (in Arabic).

Al-Saud, M. (2000) *Decentralisation in Saudi Arabia: Theory and Practice – With Special Reference to the Police and Security Services: A Proposal for Change*. Unpublished MA Dissertation, Brunel University, UK.

Alshalhoob, M. (2000) *The Organization of Security Agencies in Saudi Arabia*. Riyadh: Samha Press (in Arabic).

Al-Sharidah, K. (1999) *Modernisation and Socio-culture Transformation in Saudi Arabia*. Unpublished PhD Thesis, Kansas State University, US.

Al-Shaygi, H. (1992) *Criminality among Migrant Workers in Saudi Arabia and its Causes*. Unpublished PhD Thesis, University of Bristol, Bristol, UK.

Al-Thaqafi, M. (2006) *Security Training: Present and Future*. Unpublished MA Dissertation, Nayef Arab University for Security Sciences, Riyadh, Saudi Arabia (in Arabic).

Al-Trawnah, T. and Al-Lawzi, S. (1995) 'Administrative Control: an Empirical Study of the Actuality of Administrative Control from the Standpoint of Public Employees', *Mutah Research and Studies*, 10(6): 145-173 (in Arabic).

Al-Turabi, H. (1997) *Insights into the Philosophy of Governance in Islam*. Umm al-Fahm: Centre for Contemporary Studies (in Arabic).

Al-Wahidi, F. (1988) *The Philosophy of Political and Constitutional Governance in Islam*. Gazza: Al-Hay'a al-Khayriyya Print (in Arabic).

Al-Watan Daily (2009) 'Electronic Crimes: The Public Security General Director Discloses Experts and Equipment to Track Offenders', 10th May, Issue no. 3145.

Alzahrani, A. (1999) *The Administration and Organization in Security Departments in Saudi Arabia*. Riyadh: Samha Press (in Arabic).

Asharq Al Awsat (2005) 'Ministry of Trade and Industry Warns against New Criminal Trend', 3rd November, [online]. Available at: http://www.aawsat.com/details.asp?section=43&issueno=9827&article=329814&search=وزارة التجارة تحذر&state=true (Accessed on 3 September 2008).

Atkinson, P. and Coffey, A. (2004) ‘Analysing Documentary Realities’, in D. Silverman (ed.) *Qualitative Research: Theory, Method and Practice*. London: Sage, pp. 56-75.

Babbie, E. (2001) *The Practice of Social Research*. Wadsworth: Thomson Leaning Inc.

Bahr, A. (1999) *Impediments to Internet Crime Investigations*. Unpublished MA Dissertation, Naif Arab Academy for Security Sciences, Riyadh, Saudi Arabia (in Arabic).

Bailey, C. (1996) *A Guide to Field Research*. London: Pine Forge Press.

Ballard, M. (2006) ‘Police Offered Robot Eye: Intelligence Gets “Intelligent”’, *The Register*, 1 June [online]. Available at: http://www.theregister.co.uk/2006/06/01/police_eye/ (Accessed on 21 October 2008).

Barry, A., Osborne, T. and Rose, N. (1996) ‘Introduction’, in A. Barry, T. Osborne and N. Rose (eds.) *Foucault and Political Reason: Liberalism, Neo-liberalism and Rationalities of Government*. London: UCL Press, pp. 1-18.

Bayley, D. H. and Shearing, C. D. (1996) ‘The Future of Policing’, *Law and Society Review*, 30(3): 585-606.

Bayley, D. H. and Shearing, C. D. (2001) *The New Structure of Policing: Description, Conceptualisation, and Research Agenda*. Washington D.C.: National Institute of Justice.

Becker, H. S. and Geer, B., (1967) ‘Participant Observation and Interviewing: a Comparison’, in G. J. McCall and J. L. Simmons (eds.) (1969) *Issues in Participant Observation: a Text and Reader*. London: Addison-Wesley, pp. 78-87.

Beer, E. (2007) ‘KSA Tackles Cybercrime’, ITP.net [online]. Available at: http://www.itp.net/494649-ksa-tackles-cybercrime/?tab=article (Accessed on 2 December 2010).

Bell, D. (2001) *An Introduction to Cybercultures*. London: Routledge.

Berg, B. (2001) *Qualitative Research Methods for the Social Science*. Neeham Heights, MA: Allyn and Bacon

Berg, S (2008) 'Identity Theft Causes, Correlates and Factors: A Content Analysis', in F. Schmalleger and M. Pittaro (eds.) *Crimes of the Internet*. Upper Saddle River, New Jersey: Pearson, Prentice Hall, pp. 225-250.

Biderman, A. and Lynch, J. (1991) *Understanding Crime Incidence Statistics: Why the UCR Diverges from the NCS*. New York: Springer-Verlag.

Bieger, G. & Gerlach, G. (1996) *Educational Research: a Practical Approach*. Albany: Delmar Publishers.

Bittner, E. (1967) 'The Police on Skid-row: a Study of Peace Keeping', *American Sociological Review*, 32(5): 699-715.

Bittner, E. (1970) *The Functions of Police in Modern Society*. Chevy Chase, MD: National Institute of Mental Health.

Bjerke, B. (1999) *Business Leadership and Culture: National Management Styles in the Global Economy*. Cheltenham, UK: Edward Elgar Publishing Limited.

Blaikie, N. (2000) *Designing Social Research*. Oxford: Blackwell Publishers Ltd.

Bogard, W. (1996) *The Simulation of Surveillance: Hyper-control in Telematic Societies*. New York: Cambridge University Press.

Borrowman, S., Young, A., Stammbaugh, H., Copping, T., Williams, W., Beaupre, D., Cassaday, W., Baker, R., and Icove, D. (2001) 'Electronic Crime Needs Assessment for State and Local Law Enforcement', National Institute of Justice, US Department of Justice, [online]. Available at: http://www.ncjrs.gov/pdffiles1/nij/186276.pdf (Accessed on 17 March 2008).

Bottomley, K. and Coleman, C. (1981) *Understanding Crime Rates*. Farnborough: Gower.

Bottomley, K. and Pease, K. (1986) *Crime and Punishment: Interpreting the Data*. Milton Keynes: Open University Press.

Bowling, B. and Foster, J. (2002) ‘Policing and the Police’, in M. Maguire , R. Morgan and R. Reiner (eds.) *The Oxford Handbook of Criminology*. Oxford: Oxford University Press, pp. 980-1033.

Braithwaite, J. (2000) ‘The New Regulatory State and the Transformation of Criminology’, *British Journal of Criminology*, 40(2): 222-238.

Branscomb, A. (1995) ‘Anonymity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspace’, *Yale Law Journal*, 104(7): 1639-1679.

Brenner, S. (2002) ‘Organized Cyber-crime? How Cyberspace May Affect the Structure of Criminal Relationships’, *North Carolina Journal of Law and Technology*, 4(1): 1-41.

Brenner, S. (2007) ‘Cybercrime: Re-thinking Crime Control Strategies’, in Y. Jewkes (ed.) *Crime Online*. Cullompton: Willan Publishing, pp. 12-28.

Brewer, J. (1993) ‘Sensitivity as a Problem in Field Research: A Study of Routine Policing in Northern Ireland’, in C. Rezetti and R. Lee (eds.) *Researching Sensitive Topics*. Newbury Park: Sage, pp. 125-145.

Brimson, N. J. and Al-Ghazzawi, B. T. (2010) *Saudi Arabia Investment Guide*. Riyadh: Al-Ghazzawi Professional Association and Herbert Smith LLP.

British Society of Criminology (2006) ‘Code of Ethics for Researchers in the Field of Criminology’, [online]. Available at: http://britsoccrim.org/codeofethics.htm (Accessed on 1 April 2008).

Broder, M. (1999) *Risk Analysis and the Security Survey* (2nd edition). London: Butterworth-Heinemann.

Broderick, J. (1977) *Police in a Time of Change*. Morristown, NJ: General Learning Press.

Brown, J. (1996) ‘Police Research: Some Critical Issues’, in F. Leishman, B. Loveday and S. Savage (eds.) *Core Issues in Policing*. London: Longman, pp. 177-190.

Brown, M. (1981) *Working the Street*. New York: Sage

Brown, S. (2003) *Crime and Law in Media Culture*. Buckingham: Open University Press.

Bryman, A. (2008) *Social Research Methods* (3rd edition). Oxford: Oxford University Press

Bulmer, M. (2002) 'The Ethics of Social Research', in N. Gilbert (ed.) *Researching Social Life* (2nd edition). Thousand Oaks, CA: Sage, pp. 45-57.

Burgess, R. (1982) 'Keeping Field-notes', in R. Burgess (ed.) *Field Research: a Sourcebook and Field Manual*. London: Routledge, pp. 292-297.

Burns, R. G., Whitworth, K. H. and Thompson, C. Y. (2004) 'Assessing Law Enforcement Preparedness to Address Internet Fraud', *Journal of Criminal Justice*, 32(5): 477-493.

Cabinet Office (2002) *Identity Fraud: A Study*. London: Cabinet Office.

Capeller, W. (2001) 'Not Such a Neat Net: Some Comments on Virtual Criminality', *Social and Legal Studies*, 10: 229-242.

Carrabine, E., Cox, P., Lee, M., and South, N. (eds.) (2002) *Crime in Modern Britain*. Oxford: Oxford University Press.

Cassell, C. and Symon, G. (1994) *Qualitative Methods in Organisational Research: a Practical Guide*. London: Sage.

Cassell, J. (1988) 'The Relationship of Observer to Observed When Studying up', in R. G. Burgess (ed.) *Studies in Qualitative Methodology: A Research Annual Vol 1, Conducting Qualitative Research.* London: JAI Press, pp. 89-108.

Castel, R. (1991) 'From Dangerousness to Risk', in G. Burchell, C. Gordon, and P. Miller (eds.) *The Foucault Effect: Studies in Governmentality*. Chicago: University of Chicago Press, 281-298.

Castells, M. (1997) *The Information Age: Economy, Society and Culture, Volume 2: The Power of Identity*. Oxford: Blackwell.

Castells, M. (2000) *The Information Age: Economy, Society and Culture, Volume 3: End of Millennium* (2nd edition). Oxford: Blackwell.

Castells, M. (2002) *The Internet Galaxy: Reflections on the Internet, Business and Society*. Oxford: Oxford University Press.

Central Department of Statistics and Information (2010) *Statistical Yearbook*, [online]. Available at: http://www.cdsi.gov.sa/yb46/Pages/MixFPage.htm (Accessed on 22 April 2012).

Chan, J. (1996) 'Changing police culture', *British Journal of Criminology*, 36(1): 109-134.

Chan, J. (2001) 'The Technological Game: How Information Technology is Transforming Police Practice', *Criminology and Criminal Justice*, 1(2): 139-159.

Chan, J. (2003) 'Police and New Technologies', in T. Newburn (ed.) *Handbook of Policing*. Cullompton: Willan, pp. 655.79.

Chan, J., Brereton, D., Legosz, M. and Doran, S. (2001) *e-Policing: the Impact of Information Technology on Police Practices*. Brisbane: Criminal Justice Commission.

Cheurprakobkit, S. and Pena, G. T. (2003) 'Computer Crime Enforcement in Texas: Funding, Training and Investigating Problems', *Journal of Police and Criminal Psychology*, 18(1): 24-37.

Chung, T. (2008) *Policing Internet Fraud: A Study of the Tensions between Private and Public Models of Policing Fraudulent Activity in Cyberspace with Particular Focus on South Korea and Special Reference to the United Kingdom and the United States*. Unpublished PhD Thesis, Leeds University, Leeds, UK.

Clarke, R. (1988) 'Information Technology and Dataveillance', *Communications of the ACM*, 31(5): 498-512.

Coffey, A. and Atkinson, P. (1996) *Making Sense of Qualitative Data: Complementary Strategies*. Thousand Oaks CA: Sage.

Cohen, F. (2002), 'Computer Fraud Scenarios-Robbing the Rich to Feed the Poor', *Computerfraud and Security*, 1: pp. 5 -6.

Cohen, S. (1985) *Visions of Social Control*. Cambridge: Polity Press.

Cohen, S. (1994) ‘Social Control and the Politics of Reconstruction’, in D. Nelken (ed.) *The Futures of Criminology*. London: Sage, pp. 63-88.

Coleman, R. and McCahill, M. (2011) *Surveillance and Crime*. London: Sage.

Collins, B. and Mansell, R. (2005) ‘Cyber Trust and Crime Prevention’, in R. Mansell and B. Collins (eds.*) Trust and Crime in Information Societies*. Cheltenham, UK: Edward Elgar, pp. 11-55.

Communications and Information Technology Commission (CITC) (2007a) *Anti-Cybercrime Law*, [online]. Avialablae at: http://www.citc.gov.sa/English/RulesandSystems/CITCSyste/Documents/LA_004_%20E_%20Anti-Cyber%20Crime%20Law.pdf (Accessed on 14 March 2012).

Communications and Information Technology Commission (CITC) (2007b) ‘Review of Current Legislations and Selected Legal Cases’, [online]. Available at: http://wikileaks.org/leak/saudi-gov-tech-spam/Review-of-Current-Legislations-in-Saudi-Arabia-V1.0-Final.pdf (Accessed on 8 April 2009).

Communications and Information Technology Commission (CITC) (2010) *Annual Report*, [online]. Available at: http://www.citc.gov.sa/arabic/MediaCenter/Annualreport/Documents/PR_REP_006A.pdf (Accessed on 23 March 2011).

Cope, N. (2004) ‘Intelligence Led Policing or Policing Led Intelligence? Integrating Volume Crime Analysis into Policing’, *British Journal of Criminology*, 44(2): 188-203.

Cope, S., Leishman, F. and Starie, P. (1995) ‘Hollowing-out and Hiving-off: Re-inventing Policing in Braitain’, in J. Lovenduski and J. Stanyer (eds.) *Contemporary Political Studies, Vol. 2*. Belfast: Political Studies Association of the United Kingdom, pp. 552-565.

Cordesman, A. and Obaid, N. (2005) *National Security in Saudi Arabia: Threats, Responses and Challenges*. London: Praeger Security International.

Crank, J. P. (1998) *Understanding Police Culture*. Cincinnati, OH: Anderson.

Crawford, A. (2003a) ‘The Pattern of Policing in the UK: Policing Beyond the Police’, in T. Newburn (Ed.) *Handbook of Policing*. Willan: Cullompton, pp. 136-168.

Crawford, A. (2003b) ‘Contractual Governance of Deviant Behaviour’, *Journal of Law and Society*, 30(4): 479-505.

Crawford, A. (2006) ‘Networked Governance and the Post-regulatory State? Steering, Rowing and Anchoring the Provision of Policing and Security’, *Theoretical Criminology*, 10(4): 449-479.

Crawford, A. (2008) ‘Plural Policing in the UK: Policing Beyond the Police’, in T. Newburn (Ed.) *Handbook of Policing* (2nd edition). Willan: Cullompton, pp. 147-181.

Crawford, A. and Lister, S. (2004) ‘The Patchwork Future of Reassurance Policing in England and Wales: Integrated Local Security Quits or Frayed, Fragmented and Fragile Tangled Webs?’, *Policing: An International Journal of Police Strategies and Management*, 27(3): 413-430.

Cukier, W. and Levin, A. (2008) ‘Internet Fraud and Cybercrime’, in F. Schmalleger and M. Pittaro (eds.) *Crimes of the Internet*. Upper Saddle River, New Jersey: Pearson, Prentice Hall, pp. 251-279.

Dantzker, M. L. and Hunter, R. D. (2006) *Research Methods for Criminology and Criminal justice: a Primer* (2nd edition). Sudbury, Mass: Jones and Bartlett Publishers.

Darussalam (Research Division) (2003) 100 *Ahadith about Islamic Manners*. Birmingham: Darussalam

De Jong, M. (2002) ‘Peace of Mind? Perceptions of Contractual Security Guarding at Commercial Banks in Saudi Arabia’, *Security Journal*, 15(1): 33-47.

De Vaus, D. (2001) *Research Designing in Social Research*. London: Sage Publications.

Denscombe, M. (2007) *The Good Research Guide for Small-scale Projects* (3rd edition). England: Open University Press Buckingham.

Denzin, N. and Lincoln, Y. (2000) *Handbook of Qualitative Research*. London: Sage Publications.

Directorate of Public Security/Department of Planning and Development (DPS/DPD) (2009) *The DPS Organisation and Functions Guide*, Unpublished Document. Riyadh: DPS (in Arabic).

Doherty, N. and Perry, I. (2001) 'The Cultural Impact of Workflow Management Systems in the Financial Services Sector', *The Service Industries Journal*, 21 (4): 147-166.

Dupont, B. (2004) 'Security in the Age of Networks', *Policing and Society*, 14(1): 76-91.

Dyer, W. G. and Wilkins, A. L. (1991) 'Better Stories, not Better Constructs, to Generate Better Theory: a Rejoinder to Eisenhardt', *Academy of Management Review*, 16(3): 613-619.

Edelson, E. (2003) 'The 419 Scam: Information Warfare on the Spam Front and a Proposal for Local Filtering', *Computers and Security*, 22(5): 392-401.

Eisenhardt, K. M. (1989) 'Building Theory from Case Study Research', *Academy of Management Review*, 14(4): 532-550.

Ekblom, P. (1998) *The Crime and Disorder Act. Community Safety and the Reduction and Prevention of Crime. A Conceptual Framework for Training and the Development of a Professional Discipline*. London: Home Office.

El-Guindy, M. (2008) 'Cybercrime in the Middle East', *International Systems Security Association (ISSA) Journal*, June: 16-19, [online]. Available at: http://www.ask-pc.com/lessons/CYBERCRIME-MIDDLE-EAST.pdf (Accessed on 19 March 2009).

Ericson, R. (1982) *Reproducing Order: a Study of Police Patrol Work*. Toronto: University of Toronto Press.

Ericson, R. and Haggerty, K. (1997) *Policing the Risk Society*. Oxford: Claredon Press.

Ericson, R. V., Baranek, P. M. and Chan, J. B. L. (1987) *Visualising Deviance: A Study of News Organisation*. Milton Keynes: Open University Press.

Facey, W. (1990) *The Kingdom of Saudi Arabia*. London: Stagy International.

Fairchild, E. and Dammer, H. (2001) *Comparative Criminal Justice Systems* (2nd edition). Belmont, CA: Wadsworth.

Federal Bureau of Investigation (FBI) (2003) 'About Internet Fraud Complaint Centre' [online]. Available at: http://www.fbi.gov/hq/cid/fc/ifcc/about/about_ifcc.htm (Accessed on 13 October 2008).

Feeley, M. and Simon, J. (1994) 'Actuarial Justice: The Emerging New Criminal Law', in D. Nelken (ed.) *The Futures of Criminology*. London: Sage, 173-201.

Fielding, N. (2002) 'Ethnography', in N. Gilbert (ed.) *Researching Social Life* (2nd edition). Thousand Oaks, CA: Sage, pp. 145-163.

Finch, E. (2007) 'The Problem of Stolen Identity and the Internet', in Y. Jewkes (ed.) *Crime Online*. Cullompton: Willan Publishing, pp. 44-59.

Fletcher, M. and Plakoyiannaki, E. (2008) 'Case Study Selection: An Overview of Key Issues for International Business Researchers', EIBA, 24th EIBA Annual conference, Tallinn, Estonia, 11-13 December, [online]. Available at: http://eiba2008.ttu.ee/public/Papers/85.pdf (Accessed on 13 March 2011).

Fletcher, R. (2000) 'An Intelligent Use of Intelligence: Developing Locally Responsive Information Systems in the Post-Macpherson Era', in A. Marlow and B. Loveday (eds.) *After Macpherson: Policing After the Stephen Lawrence Inquiry*. Lyme Regis: Russell House, pp. 113-125.

Flynn, P. (2000) *Education in Policing and for the Millennium and Beyond*. Cambridge: Institute of Criminology, University of Cambridge.

Fontana, A. and Frey, J. H. (2000) 'Interviewing: the Art of Science', in N. Denzin and Y. Lincoln (eds.) *Handbook of Qualitative Research*. Thousand Oaks, CA: Sage, pp. 645-72.

Foucault, M. (1977) *Discipline and Punish: the Birth of Prison.* London: Allen Lane.

Foucault, M. (1980) *Power/Knowledge: Selected Interviews and Other Writings 1972-1977* (edited by Colin Gordon). New York: Pantheon Press.

Foucault, M. (1991) 'Governmentality', in G. Burchell (ed.) *The Foucault Effect: Studies in Governmentality*. Hemel Hempstead: Harvester Wheatsheaf, pp. 87-104.

Fox, J. C. and Lundman, R. J. (1974) 'Problems and Strategies in Gaining Research Access in Police Organisations', *Criminology*, 12(1): 52-69.

Fried, F. (2001) 'Cyber Scam Artists: A New Kind of .con', *Crime Scene Investigator Network*, [online]. Available at: http://www.crime-scene-investigator.net/CyberScam.pdf (Accessed on 11 January 2008).

Gandy, O. (2003) 'Data Mining and Surveillance in the Post-9.11 Environment', in F. Webster and K. Ball (eds.) *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*. London: Pluto Press, pp. 26-41.

Garland, D. (1996) 'The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society ', *British Journal of Criminology*, 36/4: 445–71.

Garland, D. (1997) '"Governmentality" and the Problem of Crime', *Theoretical Criminology*, 1 (2): 173-214.

Garland, D. (2001) *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford: Oxford University Press.

Gazzaz, O. (2006) *Transnational Communications: Internet Influence and Regulation: The Case Study of Saudi Arabia*. Unpublished PhD Thesis, University of Leicester, Leicester, UK.

Ghauri, P. and Gronhaug, K. (2005) *Research Methods in Business Studies: a Practical Guide* (3rd edition). Edinburgh: Pearson Education Limited.

Giddens, A. (1990) *The Consequences of Modernity*. Cambridge: Polity.

Gold, R. L. (1958) 'Role in Sociological Field Observations', in G. J. McCall and J. L. Simmons (eds.) (1969) *Issues in Participant Observation: a Text and Reader*. London: Addison-Wesley, pp. 30-39.

Goodman, M. (1997) ‘Why the Police Don’t Care about Computer Crime’, *Harvard Journal of Law and Technology*, 10(3): 245-294.

Goold, B. (2004) *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*. Oxford: Oxford University Press.

Gordon, G., Willox, N., Rebovich, D., Regan, T. and Gordon, J. (2004) ‘Identity Fraud: A Critical National and Global Threat’, *Journal of Economic Crime Management*, 2(1): 3-47.

Grabosky, P. (2000) Computer Crime: A Criminological Overview. Conference Paper, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 15 April, Vienna, [online]. Available at: http://www.aic.gov.au/conferences/other/compcrime/index.html (Accessed on 20 April 2009).

Grabosky, P. (2001) ‘Virtual Criminality: Old Wine in New Bottles?’, *Social and Legal Studies*, 10: 243-249.

Grabosky, P. and Smith, R. (1998) *Crime in the Digital Age: Controlling Communications and Cyberspace Illegalities*. New Jersey: Transaction.

Grabosky, P., Smith, R. and Dempsey, G. (2001) *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge: Cambridge University Press.

Graham, S. (1998) ‘Spaces of Surveillant Simulation: New Technologies, Digital Representations and Material Geographies’, *Environment and Planning D: Society and Space*, 16(4): 483-504.

Graham, S. and Marvin, S. (1996) *Telecommunications and the City: Electronic Spaces, Urban Places*. London: Routledge.

Granovsky, Y. (2002) ‘Yevrost Tainted by Gray Imports’, *The Moscow Times*, July 9th, 8, [online]. Available at: http://www.themoscowtimes.com/stories/2002/07/09/045.html (Accessed on 24 April 2008).

Grazioli, S. and Jarvenpaa, S. (2003) 'Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence', *International Journal of Electronic Commerce*, 7 (4): pp. 93-118.

Greer, C. (2005) 'Crime and Media', in C. Hale, K. Hayward, A. Wahidin, and E. Wincup (eds.) *Criminology*. Oxford: Oxford University Press, pp.157-182.

Guba, E. G., and Lincoln, Y. S. (1989) *Fourth Generation Evaluation*. Newbury Park, CA: Sage Publications.

Gummesson, E. (2000) *Qualitative Methods in Management Research*. London: Sage Publications.

Gusfield, J. (1981) *The Culture of Public Problems: Drinking-Driving and the Symbolic Order*. Chicago: University of Chicago Press.

Haggerty, K. and Ericson, R. (2000) 'The Surveillant Assemblage', *British Journal of Sociology*, 51(4): 605-622.

Hajela, S. (2005) *Role of Information and Communication Technologies in Managing Globalization at the National and Regional Levels.* Working Paper, the International Conference on Strengthening Regional Cooperation for Managing Globalization, Moscow, 28-30 September, [online]. Available at: http://www.unescap.org/tid/projects/globalize_hajela.pdf (Accessed on 10 December 2011).

Hakim, C. (2000) *Research Design: Successful Designs for Social and Economic Research*. London: Routledge

Hall, C. (2005) 'Internet Fuels Boom in Counterfeit Drugs', *Sunday Telegraph*, 16 August, [online]. Available at: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/08/16/ndrugs16.xml (Accessed on 13 March 2008).

Hallsworth, S. (2002) 'The Case for a Postmodern Penality', *Theoretical Criminology*, 6(2): 145-63.

Hammersley, M. and Atkinson, P. (2007) *Ethnography: Principles in Practice* (3rd edition). London: Routledge.

Hamza, F. (1963) *The Saudi Arabian Country* (2^{ed} edition). Riyadh: Al-Nasar Modern Publishers (Originally published in 1937) (in Arabic).

Harvey, D. (1989) *The Conditions of Post-modernity*. Oxford: Blackwell.

Harvey, D. (2005) *A Brief History of Neoliberalism*. New York: Oxford University Press.

Helms, C. (1981) *The Cohesion of Saudi Arabia*. London: Croom Helm.

Henderson, B. (2002) 'The Poverty Trap or the Political Trap', *The Oxonian Review*, 1(1), [online]. Available at: http://www.oxonianreview.org/wp/the-poverty-trap-or-the-political-trap-ideology-and-methodology-in-garland%e2%80%99s-culture-of-control/ (Accessed on 23 February 2012).

Herbert, S. (1997) *Policing Space: Territoriality and the Los Angeles Police Department*. Minneapolis: University of Minnesota Press

Herbert, S. (1999) 'The End of the Territorially-Sovereign State? The Case of Crime Control in the United States', *Political Geography,* 18(2): 149-172.

Hinduja, S. (2004) 'Perceptions of Local and State Law Enforcement Concerning the Role of Computer Crime Investigative Teams', *Policing: An International Journal of Police Strategies Management,* 27(3): 341-357.

Hobbs, D. (2000) 'Researching Serious Crime', in R. King and E. Whincup (eds.) *Doing Research in Crime and Justice*. Oxford: Oxford University Press, pp. 153-182.

Hobbs, D. (2006) 'Ethnography', in V. Jupp (ed.) *The Sage Dictionary of Research Method*. London: Sage, pp. 101-103.

Holdaway, S. (1982) 'An Inside Job: a Case Study of Covert Research on the Police', in M. Bulmer (ed.) *Social Research Ethics*. London: Macmillan, pp. 59-79.

Holdaway, S. (1983) *Inside the British Police: a Force at Work*. Oxford: Blackwell.

Holt, T. and Graves, D. (2007) 'A Qualitative Analysis of Advance Fee Fraud E-mail Schemes', *International Journal of Cyber Criminology*, 1(1): 137-154.

Hope, T. (2005) 'What Do Crime Statistics Tell Us', in C. Hale, K. Hayward, A. Wahidin and E. Wincup (eds.) *Criminology*. Oxford: Oxford University Press, pp. 39-59.

House of Lords (2008) *Europol: Coordinating the Fight against Serious and Organised Crime*. European Union Committee, 29th Report of Session 2007-08, HL, Paper 183. London: The Stationery Office Limited.

Huey, L. (2002) 'Policing the Abstract: Some Observations on Policing Cyberspace', *Canadian Journal of Criminology,* 44(3): 243-254.

Ibn Al-Qayyim, M. (1986) *Ways of Judgement in Islamic Legal policy*. Riyadh: Dar Al-Watan (in Arabic)

Ibn Khaldun, A. (1982) *The Introduction*. Alexandria: Dar Ibn Khaldun (in Arabic).

Ibn Taymiyya, A. (1985) *Islamic Legal policy on the Betterment of the Ruler and the Ruled*. Damascus: Dar al-Bayan Publishing (in Arabic)

Jewkes, Y. (2004) *Media and Crime*. London: Sage.

Jewkes, Y. (2010) 'Public Policing and Internet Crime', in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime*. Cullompton: Willan Publishing, pp. 525- 545.

Jewkes, Y. and Yar, M. (2008) 'Policing Cybercrime: Emerging Trends and Future Challenges', in T. Newburn (ed.) *Handbook of Policing* (2nd edition). Cullompton: Willan Publishing, pp. 580-605.

Johnson, D. and Post, D. (1996) 'Law and Borders – the Rise of Law in Cyberspace', *Stanford Law Review,* 48(5): 1367-1402.

Johnston, L. (1992) *The Rebirth of Private Policing*. London: Routledge.

Johnston, L. (2000a) 'Transnational Private Policing: The Impact of Global Commercial Security', in J. W. E. Sheptycki (ed.) *Issues in Trnasnational Policing*. London: Routledge, pp. 21-42.

Johnston, L. (2000b) 'Private Policing: Problems and Prospects', in F. Leishman, B. Loveday and S. Savage (eds.) *Core Issues in Policing* (2nd edition). London: Longman, pp. 67-82.

Johnston, L. (2006) ‘Transnational Security Governance’, in J. Wood and B. Dupont (eds.) *Democracy, Society and the Governance of Security*. Cambridge: Cambridge University Press, pp. 33-51.

Johnston, L. and Shearing, C. (2003) *Governing Security: Explorations in Policing and Justice*. London: Routledge.

Johnston, W. J., Leach, M. P., and Liu, A. H. (2001) ‘Using Case Studies for Theory Testing in Business-to-business Research: the Development of a More Rigorous Case Study Methodology’, *Advances in Business Marketing and Purchasing,* 9: 215-241.

Jordan, T. (1998) *Cyberpower: A Sociology and Politics of Cyberspace and the Internet*. London: Routledge.

Jordan, T. (1999) *Cyberpower: the Culture and Politics of Cyberspace and the Internet*. London: Routledge.

Joseph, J. (2003) ‘Cyberstalking: an International Perspective’, in Y. Jewkes (ed.) *Dot.cons: Crime, Deviance and Identity on the Internet*. Cullompton: Willan Publishing, pp. 105-125.

Jupp, V. (1998) *Methods of Criminological Research*. London: Routledge.

Kapiszewski, A. (2006) ‘Saudi Arabia: Steps toward Democracy’, *Journal of Asian and African Studies,* 41: 459-482.

Katyal, N. (2003) ‘Digital Architecture as Crime Control’, *Yale Law Journal,* 112(8): 2261-2289.

King, A. and Thomas, J. (2008) ‘You Can’t Cheat an Honest Man: Making ($$$s and) Sense of the Nigerian E-mail Scams’, in F. Schmalleger and M. Pittaro (eds.) *Crimes of the Internet*. Upper Saddle River, New Jersey: Pearson, Prentice Hall, pp. 206-224.

King, N. (1994) ‘The Qualitative Research Interview’, in C. Cassell and G. Symon (eds.) *Qualitative Methods in Organisational Research: A Practical Guide*. London, Sage, pp. 14-36.

Klopfenstein, B. (2002) 'The Internet and Web as Communication Media', in C. A. Lin and D. J. Atkin (eds.) *Communication Technology and Society: Audience Adoption and Users*. Cresskill, NJ: Hampton Press, Inc, pp. 353-378.

Kostiner, J. (1997) 'State, Islam and Opposition in Saudi Arabia: the Post Desert-Storm Phase', *Middle East Review of International Affairs*, 1(2), [online]. Available at: http://meria.idc.ac.il/journal/1997/issue2/jv1n2a8.html (Accessed on 22 February 2009).

Kozlovski, N. (2007) 'Designing Accountable Online Policing', in J. M. Balkin, K. Eddan, J. Grimmelmann, N. Kozlovski, S. Wagman and T. Zarsky (eds.) *Cybercrime: Digital Cops in a Networked Environment*. New York: New York University Press, pp. 107-134.

Kumar, C. (2008) 'Analytical Marxism and Foucault's Theory of "Disciplinary Power"', *Imprints: Egalitarian Theory and Practice*, 10(2): 113-143.

Kurian, T. (1989) *World Encyclopaedia of Police Forces and Penal Systems*. New York: Facts on File.

Lambton, A. K. S. (1981) *State and Government in Medieval Islam.* Oxford: Oxford University Press.

Lee, R. M. (1993) *Doing Research on Sensitive Topics*. London: Sage Publications

Lessig, L. (1999) *Code and Other Laws of Cyberspace*. New York: Basic Books.

Levi, M. (2001) 'Between the Risk and the Reality Falls the Shadow: Evidence and Urban Legends in Computer Fraud', in D. Wall (ed.) *Crime and the Internet*. London: Routledge, pp. 44-58.

Levi, M. and Maguire, M. (2004) 'Reducing and Preventing Organized Crime: an Evidence-based Critique', *Crime, Law and Social Change*, 41(5): 397-469.

Levi, M. and Wall, D. (2004) 'Technologies, Security and Privacy in the Post-9/11 European Information Society', *Journal of Law and Society*, 31(2): 194-220.

Lin, C. A. (1998) 'Exploring Personal Computer Adoption Dynamics', *Journal of Broadcasting and Electronic Media*, 42(1): 95-112.

Lincoln, Y., and Guba, E. (1985) *Naturalistic Inquiry*. Newbury Park, CA: Sage Publications.

Loader, I. (1999) 'Consumer Culture and the Commodification of Policing and Security', *Sociology*, 33(2): 373-392.

Long, D. (2003) 'The Role of the Extended Family in Saudi Arabia', *Saudi-American Forum Essay Series*, [online]. Available at: http://www.saudi-american-forum.org/Newsletters/SAF_Essay_09.htm (Accessed on 4 March 2009).

Lyon, D. (1994) *The Electronic Eye: The Rise of Surveillance Society*. Cambridge: Polity Press.

Macaulay, S. (1986) 'Private Government', in L. Lipson and S. Wheeler (eds.) *Law and the Social Sciences*. New York: Russell Sage Foundation, pp. 445-518.

Mackey, S. (1987) *The Saudis: Inside the Desert Kingdom*. New York: Meridian Book.

Maguire, E., Shin, Y., Zhao, J. and Hassell, K. (2003) 'Structural Change in Large Police Agencies During the 1990s', *Policing: An International Journal of Police Strategies Management*, 26(2): 251-275.

Maguire, M. (2008) 'Researching Street Criminals in the Field: a Neglected Art?', in R. King and E. Wincup (eds.) *Doing Criminological Research*. London: Sage, pp. 263-290.

Mann, D. and Sutton, M. (1998) 'Netcrime: More Change in the Organization of Thieving', *British Journal of Criminology*, 38(2): 210-229.

Manning, P. (1988) *Symbolic Communication: Signifying Calls and the Police Response*. Cambridge Massachusetts: MIT Press

Manning, P. (1992) 'Information Technologies and the Police', in M. Tonry and M. Norris (eds.) *Modern Policing*. Chicago: University of Chicago Press, pp. 349-398.

Manning, P. (2008a) *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*. New York: New York University Press.

Manning, P. (2008b) ‘A View of Surveillance’, in S. Leman-Langlois (ed.) *Techno-crime: Technology, Crime and Social Control*. Portland: Willan Press, pp. 209-242.

Marenin, O. (2005) ‘Building a Global Police Studies Community’, *Police Quarterly*, 8(1): 99-136.

Marron, D. (2008) ‘Alter Reality: Governing the Risk of Identity Theft’, *British Journal of Criminology*, 48(1): pp. 20-38.

Martin, E. (ed.) (2003) *Oxford Dictionary of Law* (5th edition). Oxford: Oxford University Press.

Marx, G. (1985) ‘The Surveillance Society: the Threat of 1984-style Techniques’, *The Futurist,* June: 21-26.

Marx, G. (1988) *Undercover: Police Surveillance in America*. Berkeley, California: California University Press.

Marx, G. (2005) ‘The New Surveillance’, in T. Newburn (ed.) *Policing: Key Readings*. Cullompton: Willan, pp. 761-785.

Matthews, R. (2002) ‘Book Review: Crime and Control in Late Modernity’, *Theoretical Criminology*, 6(2): 217-226.

Maudoodi, S. (1979) *Ethical Viewpoint of Islam*. Lahore: Islamic Publications.

Mawby, R. I. (2003) ‘Models of Policing’, in T. Newburn (ed.) *Handbook of Policing*. Cullompton, Devon: Willan Publishing, pp. 15-40.

May, C. (2002) *The Information Society: A Sceptical View*. Cambridge: Polity.

May, T. (2001) *Social Research: Issues, Methods and Process* (3rd edition). Buckingham: Open University Press.

McCahill, M. (2002) *The Surveillance Web: the Rise of Visual Surveillance in an English City*. Devon: Willan Publishing.

McCahill, M. (2008) ‘Plural Policing and CCTV Surveillance’, in M. Deflem (ed.) *Surveillance and Governance: Crime Control and Beyond*. Bingley: Emerald Group Publishing, pp. 199-222.

McCahill, M. and Norris, C. (2002) ‘Literature Review’, Working Paper no. 2, On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts, March, [online]. Available at: http://www.urbaneye.net/results/ue_wp2.pdf (Accessed on 21 November 2011).

McCahill, M. and Norris, C. (2003) ‘Victims of Surveillance’, in P. Davis, V. Jupp and P. Francis (eds.) *Victimization: Theory, Research and Policy*. Basingstoke: Palgrave Macmillan, pp. 121-47.

McCall, G. J. and Simmons, J. L. (1969) *Issues in Participant Observation: a Text and Reader*. London: Addison-Wesley.

McCormick, K. and Visano, L. (1992) ‘Regulating an Urban Order: Policing Pathologies in the Carceral City’, in K. McCormick and L. Visano (eds.) *Understanding Policing*. Toronto: Canadian Scholars’ Press, pp. 229-246.

McGuire, M. (2010) ‘Online Surveillance and Personal Liberty’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime*. Cullompton: Willan Publishing, pp. 492-519.

Mckenna, R. (2008) ‘Fighting Cybercrime – A Perspective from the Washington State Attorney General’, [online]. Available at: http://www.atg.wa.gov/uploadedFiles/Home/News/Press_Releases/2008/Cybercrime%20-%20Fench%publication%20final.pdf (Accessed on 15 September 2008).

McKenzie, S. (2006) *Partnership Policing of Electronic Crime: An Evaluation of Public and Private Police Investigative Relationships*. Unpublished PhD Thesis, University of Melbourne, Melbourne, Australia.

McLaughlin, E. and Murji, K. (1999) ‘The Postmodern Condition of the Police’, *Liverpool Law Review*, 21(2/3): 217-240.

McNeill, P. (1990) *Research Methods*. London: Routledge.

McQuade, S. (2006) *Understanding and Mapping Cybercrime*. Boston: Allyn and Bacon.

Meehan, A. (1998) ‘The Impact of Mobile Data Terminal (MDT) Information Technology on Communication and Recordkeeping in Patrol Work’, *Qualitative Sociology*, 21(3): 225-254, [online]. Available at: http://www.springerlink.com/content/v16443633614568x/ (Accessed on 12 June 2011).

Merriam, S. (2009) *Qualitative Research: a Guide to Design and Implementation*. San Francisco: John Wiley and Sons.

Merton, R. (1938) ‘Social Structure and Anomie’, *American Sociological Review*, 3(5): 672-682.

Meyerson, M. (1994) ‘Virtual Constitutions: the Creation of Rules for Governing Private Networks’, *Harvard Journal of Law and Technology*, 8(1): 129-153.

Miles, M. B. and Hubennan, A. M. (1994) *Qualitative Data Analysis*. Thousand Oaks, CA: Sage.

Miller, S. M. (1952) ‘The Participant Observer and Over-Rapport’, in G. J. McCall and J. L. Simmons (eds.) (1969) *Issues in Participant Observation: a Text and Reader*. London: Addison-Wesley, pp. 87-89.

Ministry of Communications and Information Technology (MCIT) (2003) *Information and Telecommunication Technology in Saudi Arabia*. Document submitted by the MCIT to the World Summit on the Information Society (WSIS), Geneva 2003-Tunis 2005.

Ministry of Communications and Information Technology (MCIT) (2005) *The National Communications and Information Technology Plan: the Vision towards the Information Society*, [online]. Available at: http://www.slideshare.net/AlHaqqNetwork/saudi-arabia-the-national-communications-and-information-technology-plan (Accessed on 24 April 2009).

Ministry of Economy and Planning (2005) *Eighth Development Plan, 2005-2009*. Riyadh: Ministry of Economy and Planning Press (in Arabic).

Ministry of Economy and Planning (2006) *Statistical Yearbook*. Riyadh: Government Press (in Arabic).

Ministry of Economy and Planning (2007) *Statistical Yearbook*. Riyadh: The Government Press (in Arabic).

Ministry of Economy and Planning (2010) *Ninth Development Plan, 2010-2014,* [online]. Available at: http://www.mep.gov.sa/index.jsp;jsessionid=358969EF5712EF91149EF25A405A796E.alfa?event=ArticleView&Article.ObjectID=79 (Accessed on 15 May 2011).

Ministry of Planning (1999) *Statistical Yearbook*. Riyadh: Government Press (in Arabic).

Muir, Jr.,W.K. (1977) *Police: Streetcorner Politicians*. Chicago, IL: University of Chicago Press.

Murff, K. (2007) *Digital Crime Investigation Trends in State and Local Enforcement*. Unpublished PhD Thesis, Sam Houston State University, US.

Nachmias, C. and Nachmias, D. (1996) *Research Methods in the Social Sciences* (5th edition). London: ARNOLD.

Neuman, W. L. (2000) *Social Research Methods: Qualitative and Quantitative Approaches* (4th edition). Boston: Allyn and Bacon.

Newman, G. R. and Clarke, R. V. (2003) *Superhighway Robbery: Preventing E-Commerce Crime*. Cullompton, Devon: Willan Publishing.

Nhan, J. (2008) *Policing Cyberspace: the Compatibility of the Internet with Traditional Forms of Law Enforcemnet, Law and Policy*. Unpublished PhD Thesis, University of California Irvine, California, US.

Nhan, J. and Huey, L. (2008) 'Policing through Nodes, Clusters and Bandwidth: the Role of Network Relations in the Prevention of and Response to cybercrime', in S. Leman-Langlois (ed.) *Techno-crime: Technology, Crime and Social Control*. Portland: Willan Press, pp. 66-111.

Niblock, T. (1982) *State, Society and Economy in Saudi Arabia*. London: Croom Helm.

Noaks, L. and Wincup. E. (2004) *Criminological Research: Understanding Qualitative Methods*. London: Sage

Norris, C. (1987) *Policing Trouble: an Observation Study of Police Patrol Work in Two Police Forces*. Unpublished PhD Thesis, University of Surry, Surry, UK.

Norris, C. and McCahill, M. (2006) 'CCTV: Beyond Penal Modernism?', *British Journal of Criminology*, 46(1): 97-118.

Nyambegera, S., Sparrow, P. and Daniels, K. (2000) 'The Impact of Cultural Value Orientations on Individual HRM Preferences in Developing Countries: Lessons from Kenyan Organisations', *International Journal of Human Resource Management*, 11(4): 639-663.

O'Brien, R. (1985) *Crime and Victimization Data*. Beverly Hills, CA: Sage.

O'Malley, P. (1992) 'Risk, Power and Crime Prevention', *Economy and Society,* 21(3): 252-75.

O'Malley, P. (1997) 'Policing, Politics and Postmodernity', *Social and Legal Studies*, 6(3): 363-381.

O'Malley, P. (1999) 'Volatile and Contradictory Punishment', *Theoretical Criminology*, 3(2): 175-96.

O'Malley, P. and Palmer, D. (1996) 'Post-Keynesian Policing', *Economy and Society,* 25(2): 137-155.

Ogura, T. (2006) 'Electronic Government and Surveillance-oriented Society', in D. Lyon (ed.) *Theorizing Surveillance: the Panopticon and Beyond*. Cullompton: Willan Publishing, pp. 270-295.

Oliver, P. and Jupp, V. (2006) 'Snowball Sampling', in V. Jupp (ed.) *The Sage Dictionary of Research Method*. London: Sage, pp. 281-282.

Oppenheim, A. (2005) *Questionnaire Design, Interviewing and Attitude Measurement*. London: Pinter.

Orlikowski, W. and Robey, D. (1991) ‘Information Technology and the Structuring of Organisations’, *Information Systems Research*, 2(2): 143-169.

Orwell, G. (2004[1949]) *Nineteen Eighty Four*. Fairfield: 1st World Library.

Osborne, D. and Gaebler, T. (1993) *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector*. Reading, MA: Addison-Wesley.

Owen, T. (2007) ‘Culture of Crime Control: Through a Post-Foucauldian Lens’, *The Internet Journal of Criminology* [online]. Available at: http://www.internetjournalofcriminology.com/Owen%20-%20Culture%20of%20Crime%20Control.pdf (Accessed on 12 March 2009).

Padgett, D. K. (1998) *Qualitative Methods in Social Research: Challenges and Rewards*. London: Sage Publications

Pakes, F. (2004) *Comparative Criminal Justice*. Cullompton: Willan Publishing.

Partington, D. (2002) *Essential Skills for Management Research.* London: Sage.

Peters, R. (2005) *Crime and Punishment in Islamic law: Theory and Practice from the Sixteenth to the Twenty-first Century*. Cambridge: Cambridge University Press.

Poster, M. (1990) *The Model of Information: Post-structuralism and Social Contexts*. Cambridge: Polity.

Pratt, J. (2000) ‘Emotive and Ostentatious Punishment’, *Punishment and Society*, 2(4): 417-439.

Punch, K. F. (1998) *Introduction to Social Research: Quantitative and Qualitative Approaches*. London: Sage.

Punch, K. F. (2005) *Introduction to Social Research: Quantitative and Qualitative Approaches* (2nd edition). London: Sage Publications.

Punch, M. (1989) ‘Researching Police Deviance: a Personal Encounter with the Limitations and Liabilities of Fieldwork’, *British Journal of Sociology*, 40(2): 177-204.

Rajehi, M. (1981) *The Impact of Social Change on Police Development in Saudi Arabia: a Case Study of Riyadh Police Department*. Unpublished PhD Thesis, Michigan State University, East Lansing, Michigan, US.

Rashid, N. and Shaheen, E. (1987) *King Fahad and Saudi Arabia's Great Evolution*. Washington: Library of Congress.

Ratcliffe, J. H. (2008) 'Knowledge Management Challenges in the Development of Intelligence-Led Policing', in T. Williamson (ed.) *The Handbook Of Knowledge-Based Policing: Current Conceptions and Future Directions*. Chichester: John Wiley and Sons, pp. 205-220.

Reiner, R. (1992) 'Policing a Postmodern Society', *Modern Law Review,* 55(6): 761-781.

Reiner, R. (2000a) *The Politics of the Police* (3rd edition). Oxford: Oxford University Press.

Reiner, R. (2000b) 'Police Research', in R. King and E. Wincup (eds.) *Doing Research on Crime and Justice*. Oxford: Oxford University Press, pp. 205-235.

Reiner, R. (2002) 'Media Made Criminality: the Representation of Crime in the Mass Media', in R. Reiner, M. Maguire and R. Morgan (eds.) *The Oxford Handbook of Criminology*. Oxford University Press, Oxford, UK, pp. 302-340.

Reitinger, P. (2000) 'Encryption, Anonymity and Markets: Law Enforcement and Technology in a Free Market Virtual World', in D. Thomas and B. D. Loader (eds.) *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge, pp. 132-152.

Rheingold, H. (1994) *The Virtual Community: Homesteading the Electronic Frontier*. New York: Harper Perennial.

Rhodes, R. (1994) 'The Hollowing out of the State: The Changing Nature of the Public Service in Britain', *Political Quarterly,* 65(2): 138-151.

Robey, D. and Sahay, S. (1996) 'Transforming Work through Information Technology: A Comparative Case Study of Geographic Information Systems in County Government', *Information Systems Research,* 7(1): 93-110.

Robson, C. (2002) *Real World Research: a Resource for Social Scientists and Practioner-Researchers*. Oxford: Blackwell Publishers.

Rogers, E. M. (1986) *Communication Technology: the New Media in Society*. New York: The Free Press.

Rogers, E. M. (2002) 'The Information Society in the New Millennium: Captain's Log, 2001', in C. A. Lin and D. J. Atkin (eds.) *Communication Technology and Society: Audience Adoption and Users*. Cresskill, NJ: Hampton Press, Inc, pp. 43-64.

Rondinelli, D. A. (1979) 'Administration of Integrated Rural Development Policy', *World Politics,* 31(3): 389-416.

Rose, N. (1993) 'Government, Authority and Expertise in Advanced Liberalism', *Economy and Society,* 22(3): 283-99.

Rose, N. (1996) 'Governing "Advanced" Liberal Democracies", in A. Barry, T. Osborne and N. Rose (eds.) *Foucault and Political Reason: Liberalism, Neo-liberalism and Rationalities of Government*. London: UCL Press, pp. 37-64.

Rose, N. and Miller, P. (1992) 'Political Power beyond the State: Problematics of Government', *British Journal of Sociology,* 43(2): 173-205.

Rule, J. (1973) *Private Lives, Public Surveillance.* London: Allen-Lane.

Ruona, W. (2005) 'Analysing Qualitative Data', in R. Swanson and E. Holton III (eds.) *Research in Organizations: Foundations and Methods of Inquiry*. San Francisco: Berrett-Koehler Publishers, pp.233-264.

Sait, S., Al-Tawil, K., Sanadullah, S. and Faheemuddin, M. (2007) 'Impact of Internet Usage in Saudi Arabia: a Social Perspective', *International Journal of Information Technology and Web Engineering,* 2(2): 81-107.

Sandelowski, M. (2011) '"Casing" the Research Case Study', *Research in Nursing and Health,* 34(2): 153-159.

Sandywell, B. (2006) 'Monsters in Cyberspace: Cyberphobia and Cultural Panic in the Information Age', *Information, Communication and Society,* 9(1): 39-61.

Sandywell, B. (2010) ‘On the Globalisation of Crime: the Internet and New Criminality’, in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime*. Cullompton, Devon: Willan Publishing, pp. 38-66.

Sarantakos, S. (1998) *Social Research*. London: Macmillan Press Ltd.

Saunders, M., Lewis, P. and Thornhill, A. (2003) *Research Methods for Business Student*. Edinburgh: Pearson Education Limited.

Savirmuthu, A. and Savirmuthu, J. (2007) ‘Identity Theft and Systems Theory: the Fraud Act 2006 in Perspective’, *Scripted*, 4(4): 436-61.

Seale, C. (1999) *The Quality of Qualitative Research*. London: Sage Publications.

Sellin, J. and Wolfgang, M. (1964) *The Measurement of Delinquency*. New York: Wiley.

Sharaf, Z. (2009) *Community Policing: Prospects of Implementation in the Kingdom of Saudi Arabia*. Unpublished PhD Thesis, University of Aberdeen, UK.

Shearing, C. and Stenning, P. (1983) ‘Private Security: Implications for Social Control’, *Social Problems*, 30(5): 493-506.

Shearing, C. D. (1981) ‘Subterranean Processes in the Maintenance of Power: an Examination of the Mechanisms Coordinating Police Action’, *Canadian Review of Sociology and Anthropology*, 18(3): 283-298.

Shearing, C. D. (1992) ‘The Relationship between Public and Private Policing’, in M. Tonry and N. Morris (eds.) *Modern Policing*. Chicago: University of Chicago Press, pp. 399-433.

Shearing, C. D. (1996) ‘Public and Private Policing’, in W. Saulsbury, J. Mott and T. Newburn (eds.) *Themes in Contemporary Policing*. Plymouth: Latimer Trend and Co., pp. 83-95.

Shearing, C. D. (2001) ‘A Nodal Conception of Governance: Thoughts on a Policing Commission’, *Policing and Society*, 11(3/4): 259-272.

Shearing, C. D. (2005) ‘Nodal Security’, *Police Quarterly*, 8(1): 57-63.

Shearing, C. D. (2006) ‘Reflections on the Refusal to Acknowledge Private Governments’, in J. Wood and B. Dupont (eds.) *Democracy, Society and the Governance of Security*. Cambridge: Cambridge University Press, pp. 11-32.

Shearing, C. D. and Wood, J. (2003) ‘Nodal Governance, Democracy and the New “Denizen”’, *Journal of Law and Society,* 30(3): 400-419.

Sheptycki, J. (2003) *Review of the Influence of Strategic Intelligence on Organised Crime Policy and Practice,* Final Report. London: The Home Office.

Sheptycki, J. W. E. (2002) *In Search of Transnational Policing: Towards a Sociology of Global Policing*. Aldershot: Ashgate.

Shields, R. (1996) ‘Introduction: Virtual Spaces, Real Histories and Living Bodies’, in R. Shields (ed.) *Cultures of the Internet: Virtual Spaces, Real Histories, Living Bodies*. London: Sage, pp. 1-10.

Sibeon, R. (2004) *Rethinking Social Theory*. London: Sage.

Simon, J. (2007) *Governing through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear*. Oxford: Oxford University Press.

Siraj, K. and Addas, M. (1969) *The General Obligations of Internal Security Forces in Saudi Arabia*. Beirut, Lebanon: Dar-Al-Arabiyah (in Arabic).

Siraj-Addin, K. (1969) *General Duties of the Internal Security Forces in Saudi Arabia*. Riyadh: Samha Press (in Arabic).

Smith, R. (2003) ‘Travelling in Cyberspace on a False Passport: Controlling Transnational Identity-Related Crime’, paper presented at the British Criminology Conference Selected Proceedings, July 2002, [online]. Available at: http://www.britsoccrim.org/bccsp/vol05/smith.htm (Accessed on 28 February 2008).

Smith, R. (2007) ‘Consumer Scams in Australia: an Overview’, *Trends and Issues in Crime and Criminal Justice,* No. 331, [online]. Available at: http://www.aic.gov.au/publications/tandi2/tandi331.pdf (Accessed on 15 September 2008).

Snyder, F. (2001) ‘Sites of Criminality and Sites of Governance’, *Social and Legal Studies*, 10: 251-256.

Souryal, S. (1987) ‘The Religionisation of a Society: the Continuing Application of Shari’a Law in Saudi Arabia’, *Journal for the Scientific Study of Religion*, 26(4): 429-449.

Souryal, S. (1988) ‘The Role of Shari’ah Law in Deterring Criminality in Saudi Arabia’, *International Journal of Comparative and Applied Criminal Justice*, 12(1): 1-25.

Spradley, J. P. (1980) *Participant Observation*. New York, Holt: Rinehart and Winston.

Stake, R. E. (1995) *The Art of Case Study Research*. Thousand Oaks, CA: Sage

Standage, T. (1998) *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century’s Online Pioneers*. London: Phoenix.

Stenning, P. C. (1989) ‘Private Police and Public Police: Towards a Redefinition of the Police Role’, in D. J. Loree (ed.) *Future Issues in Policing: Symposium Proceedings*. Ontario: Canadian Police College, pp. 169-192.

Stenson, K. (2005) ‘Sovereignty, Biopolitics and the Local Government of Crime in Britain’, *Theoretical Criminology*, 9(3): 265-287.

Sumner, M. (2006) ‘Ethics’, in V. Jupp (ed.) *The Sage Dictionary of Social Research Methods*. London: Sage, pp. 96-98.

Terranova, T. (2004) *Network Culture: Politics for the Information Age*. London: Pluto Press.

The Cyber Security Forum (2011) *Conference Report and Recommendations – Positioning the UK as a Global Leader in Cyber Security*. London: The Cambridge Cyber Defence Project, [online]. Available at: http://www.cybersecurityforum2011.com/media/CyberSecurityForum2011Report.pdf (Accessed on 12 December 2011).

The High Commission for the Development of Al-Riyadh (2006) *Factual Points in the Development of Riyadh*. Riyadh: Aljazera Press (in Arabic).

The Home Office (2010) *Cybercrime Strategy*. Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, March. Surry: The Stationery Office Limited

The Independent (2001) 'World Report Saudi Arabia', 17 June.

Thomas, D. and Loader, B. (2000) 'Introduction – Cybercrime: Law Enforcement, Security and Surveillance in the Information Age', in D. Thomas and B. Loader (eds.) *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge, pp. 1-13.

Travers, M. (2001) *Qualitative Research through Case Studies*. London: Sage Publication.

Turkle, S. (1995) *Life on the Screen: Identity in the Age of Internet*. New York: Simon and Schuster.

Tyler, T. R. (1990) *Why People Obey the Law*. New Haven: Yale University Press.

United Nations (2000) Crimes Related to Computer Networks. Background Paper for the Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April, [online]. Available at: http://www.uncjin.org/Documents/congr10/10e.pdf (Accessed on 7 December 2008).

Van Maanen, J. (1978) 'On Watching the Watchers', in P. K. Manning and J. Van Maanen (eds.) *Policing: a View from the Street*. Santa Monica, California: Goodyear Publishing Company, pp. 309-349.

Vasilliev, A. (2000) *The History of Saudi Arabia*. London: Saqi Books.

Vidich, A. J. (1955) 'Participant Observation and the Collection and Interpretation of Data', in G. J. McCall and J. L. Simmons (eds.) (1969) *Issues in Participant Observation: a Text and Reader*. London: Addison-Wesley, pp. 78-87.

Wacquant, L. (2009) *Punishing the Poor: The Neoliberal Government of Social Insecurity*. Durham, N.C.: Duke University Press.

Waddington, H. (1986) ‘Participant Observation’, in C. Cassell and G. Symon (eds.) (1994) *Qualitative Methods in Organisational Research: a Practical Guide*, London: Sage Publications, pp. 107-122.

Waddington, P. A. J. (1999) *Policing Citizens: Authority and Rights*. London: UCL Press.

Wakefield, A. (2005) ‘The Public Surveillance Functions of Private Security’, *Surveillance and Society,* 2(4): 529-545.

Walker, C. (1983) ‘Book Review: *The Policing Revolution: Police Technology, Democracy, and Liberty in Britain,* by S. Manwaring-White’, *Public Law*: 694-695.

Walker, C. and Akdeniz, Y. (2003) ‘Anti-terrorism Laws and Data Retention: War is over?’, *Northern Ireland Legal Quarterly,* 50(2): 159-182.

Walker, N. (2003) ‘The Pattern of Transnational Policing’, in T. Newburn (ed.) *Handbook of Policing*, Cullompton: Willan, pp. 111-135.

Wall, D. (2000) ‘Policing the Internet: Maintaining Order and Law on the Cyberbeat’, in Y. Akdeniz, C. Walker and D. Wall (eds.) *The Internet, Law and Society*. Harlow: Longman, Pearson Education, pp. 154-174.

Wall, D. (2001) ‘Cybercrimes and the Internet’, in D. Wall (ed.), *Crime and the Internet*. London: Routledge, pp. 1-17.

Wall, D. (2002) DOT.CONS: *Internet Related Frauds and Deceptions upon Individuals within the UK*. Final Report to the Home Office, March (unpublished).

Wall, D. (2003) ‘Mapping out Cybercrimes in a Cyberspatial Surveillant Assemblage’, in F. Webster and K. Ball (eds.) *The Intensification of Surveillance: Crime Terrorism and Warfare in the Information Age*. London: Pluto Press, pp. 112-136.

Wall, D. (2008) *Cybercrime: the Transformation of Crime in the Information Age*. Cambridge: Polity.

Walsh, J. (1977) ‘Career Styles and Police Behaviour’, in D. Bayley (ed.) *Police and Society*. Beverly Hills, CA: Sage, pp. 149-175.

Walsh, M. (2001) *Research Made Real: A Guide for Students*. London: Nelson Thornes.

Wardak, A. (2005) ‘Crime and Social Control in Saudi Arabia’, in J. Sheptyki and A. Wardak (eds.) *Transnational and Comparative Criminology*. London: GlassHouse Press, pp.91-116.

Weber, L. (2007) ‘Policing the Virtual Border: Punitive Preemption in Australian Offshore Migration Controls’, *Social Justice: Special Issue on Transnational Criminology* 34(2), [online]. Available at: http://findarticles.com/p/articles/mi_hb3427/is_2_34/ai_n29429013/?tag=content;col1 (Accessed on 29 November 2011).

Weber, M. (1968a) *Economic and Society: an Outline of Interpretive Sociology*, Vol. 1 (edited by Roth, G. and Wittich, C.). New York: Bedminster Press.

Weber, M. (1968b) *Economic and Society: an Outline of Interpretive Sociology*, Vol. 3 (edited by Roth, G. and Wittich, C.). New York: Bedminster Press.

Weber, M. (1968c) *The Theory of Social and Economic Organization*. New York: The Free Press.

Webster, F. (2002) *Theories of the Information Society* (2nd edition). London: Routledge.

Westmarland, L. (2001) ‘Blowing the Whistle on Police Violence: Gender, Ethnography and Ethics’, *British Journal of Criminology*, 41(3): 523-535.

Westmarland, L. (2009) ‘Police Cultures’, in T. Newburn (ed.) *Handbook of Policing* (2nd edition). Cullompton, Devon: Willan Publishing, pp. 253-280.

Williams, P. (2001) ‘Organised Crime and Cybercrime: Synergies, Trends and Responses’, *Arresting Transnational Crime*, an Electronic Journal of the U.S. Department of State – August 2001, 6 (2), [online]. Available at: http://www.crime-research.org/library/Cybercrime.htm (Accessed on 21 June 2009).

Willig C. (2001) *Qualitative Research in Psychology: Adventures in Theory and Method*. Buckingham: Open University Press

Wincup, E. (1997) *Waiting for Trial: Living and Work in a Bail Hostel*. Unpublished PhD Thesis, Cardiff University, Cardiff, UK.

Wood, J. and Kempa, M. (2005) 'Understanding Global Trends in Policing: Explanatory and Normative Dimensions', in J. Sheptycki and A. Wardak (eds.) *Transnational and Comparative Criminology*. London: GlassHouse Press, pp. 287-316.

Yar, M. (2005) 'The Novelty of Cybercrime: an Assessment in Light of Routine Activity Theory', *European Journal of Criminology*, 2(4): 407-427.

Yar, M. (2006) *Cybercrime and Society*. London: Sage.

Yar, M. (2008) 'The Computer Crime Control as Industry, Virtual Insecurity and the Market for Private Policing', in K. Franko-Aas, H. Gundhus and H. Lomell (eds.) *Technologies of Insecurity: the Surveillance of Everyday Life*. London: Routledge-Cavendish, pp. 189-204.

Yar, M. (2010) 'The Private Policing of Internet Crime', in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime*. Cullompton: Willan Publishing, pp.546-561.

Yin, R. K. (2009) *Case Study Research: Design and Methods* (4th edition). London: Sage Publications.

Young, M. (1991) *An Inside Job: Policing and Police Culture in Britain*. Oxford: Oxford University Press.

Zedner, L. (2006) 'Policing Before and After the Police: the Historical Antecedents of Contemporary Crime Control', *British Journal of Criminology*, 46(1): 78-96.

Zinn, R. (2010) 'Inside information – Sourcing Crime Intelligence from Incarcerated House Robbers', *South Africa Crime Quarterly,* 32: 27-35, [online]. Available at: http://www.iss.co.za/uploads/CQ32Zinn.pdf (Accessed on 13 February 2011).

Appendices

Appendences

Appendix A: Interview Schedules

Appendix A.1: Interview Schedule (Police Stations and the DDI)

THE UNIVERSITY OF HULL

Policing Internet Fraud in Saudi Arabia

Schedule for Semi-structured Interviews

Police Stations and the DDI

Day	Date	Location	Interviewee Code	Time
	/ /2009			from am/pm to am/pm

Introduction

Thank you very much for your participation in this research. My research focuses on the policing of Internet fraud in Saudi Arabia/Riyadh and I am interested in obtaining a professional opinion based on your experience in dealing with crime. To assist me in making an accurate record of what you say, do you agree to me taping this conversation? All recorded interviews will be destroyed once transcribed. I can assure you that I will discretely handle your responses and you will remain anonymous. The information will be used for academic purposes only.

You may request a copy of the interview transcript if you want to check what has been written. Throughout the interview, if you wish to add comments or ask any questions, please do so. You may stop the interview at any time.

Section One: General / Introductory:

Q1. Is Internet fraud a problem in Riyadh / Saudi Arabia?

Q2. What is the extent of the problem?

Q3. Are there different kinds of Internet fraud? What are they?

Q4. Please could you describe a typical case?

Q5. Who are the fraudsters? How do you know? Where do they operate from? Does this pose a problem?

Q6. Who is most targeted by this crime? What victim categories are most affected?

Section Two: Organisational Context:

Q1. How have the police as an organisation responded to this problem? Any changes being made?

Prompts: standard operating procedures, training strategy, recruitment strategy.

Q2. Are there any specialist computer crime units? Where? Who works in them? How many? What do they do?

Q3. What level of priority is Internet fraud assigned in your department? Why?

Q4. Is there any specialist equipment / software that is used to deal with this problem? What is it? How does it work? Who operates it?

Q5. Is there a training programme in place? What does it entail? Who is on the programme? How long? Where is it held? How effective is it? E.g. in improving legal knowledge, investigative skills, evidence collection etc.

Section Three: Operational Context:

Q1. How do you / your organisation go about policing this problem?

Q2. Could you tell me your own experiences with Internet fraud cases?

Prompts: Type of cases, number of cases, decision making, detection, investigation.

Q3. Does the organisation respond reactively (to past events that come to your attention) or proactively (real time interception)?

Probe: Can you give examples?

Q4. How does Internet fraud come to your attention? Is it reported? Who? When? Why? How?

Q5. Have there been any measures taken to encourage victims of Internet fraud to report their victimisation to the police (e.g. setting up campaigns to raise awareness about Internet fraud, setting up a reporting centre, making available different ways of reporting) what are they?

Q6. Presumably these forms of crime are committed by people you cannot actually see and who could be anywhere in the world. How does one go about monitoring or policing a digital persona?

Q7. Presumably these crimes could also be committed by people living in national jurisdictions outside of Saudi Arabia. Does this pose any problems? What are they?

Probe: Can you give examples / stories?

Q8. Does the policing of this problem involve any cross-agency cooperation? Who with? How? When? Where? Why?

Prompts:
- Police departments in Riyadh
- Police departments in Saudi Arabia
- International / global Police agencies
- Private sector

Q8.1 What is the relationship like with these bodies?

Prompts: Problems, conflicts.

Q9. Do you think your department / the police have been successful in solving Internet fraud cases in Riyadh?

Probe: How? Why? Can you give examples of successful investigations?

Section Four: The Future:

Q1. How do you see the future in terms of how to police / respond to this problem?

Q2. What changes would you like to see?

Prompts: Resources – Organisational – Cooperation – Legal - Training

Section Five: Personal Details:

Before we end this interview, I would like to obtain some demographic information about you which will assist analysis of the interview.

1- What is the highest level of education you have completed?

- High school □
- Bachelor's degree in Security Sciences □
- Other Bachelor's degree □
- Master's degree □
- Diploma □
- Doctorate □
- Other: specify ………… □

2- Do you have any computer-related qualifications? Yes □ No □

If yes, what is it?

Bachelor's degree in Computer Science □ Training Course □ (How many) □
Master's degree or above in Computer Science □ Other: specify……………. □

3- Do you speak English? Yes □ No □

4- What is your present job title?

5- How many years have you been in the police?

6- How many years have you been in your present position?

Closing

Thank you very much for spending your valuable time to answer my questions. If there is anything you would like to add or you feel I have missed, please feel free to express yourself.

Appendix A.2: Interview Schedule (the ICU)

THE UNIVERSITY OF HULL

Policing Internet Fraud in Saudi Arabia

Schedule for Semi-structured Interviews

The Informational Crime Unit (ICU)

Day	Date	Location	Interviewee Code	Time
	/ /2009			from am/pm to am/pm

Introduction

Thank you very much for your participation in this research. My research focuses on the policing of Internet fraud in Saudi Arabia/Riyadh and I am interested in obtaining a professional opinion based on your experience in dealing with crime. To assist me in making an accurate record of what you say, do you agree to me taping this conversation? All recorded interviews will be destroyed once transcribed. I can assure you that I will discretely handle your responses and you will remain anonymous. The information will be used for academic purposes only.

You may request a copy of the interview transcript if you want to check what has been written. Throughout the interview, if you wish to add comments or ask any questions, please do so. You may stop the interview at any time.

Section One: General / Introductory:

Q1. Is Internet fraud a problem in Riyadh / Saudi Arabia?

Q2. What is the extent of the problem?

Q3. Are there different kinds of Internet fraud? What are they?

Q4. Please could you describe a typical case?

Q5. Who are the fraudsters? How do you know? Where do they operate from? Does this pose a problem?

Q6. Who is most targeted by this crime? What victim categories are most affected?

Section Two: Organisational Context:

Q1. How have the police as an organisation responded to this problem? Any changes being made?

Prompts: standard operating procedures, training strategy, recruitment strategy.

Q2. Since we are in the ICU, I would like to discuss how and why this unit came into existence. So could you please tell me who decided to set up this unit?

Q3. Who are the 'key players' involved in the construction of this unit?

Q4. Why did they decide to set it up? Why now?

Q5. Do all the 'key players' agree on what the unit should look like?

Probe: Was there any disagreement or conflict?

Q6. Who funded the unit?

Q7. What does the unit consist of in terms of technology and personnel?

Q8. Who works / is going to work in the unit?

Q9. How are they selected?

Q10. Do they / will they receive training?

Q11. How does the unit work in practice?

Q12. Now let us move on to talk more specifically about Internet fraud. What level of priority is Internet fraud assigned in your department? Why?

Q13. Is there any specialist equipment / software that is used to deal with this problem? What is it? How does it work? Who operates it?

Q14. Is there a training programme in place? What does it entail? Who is on the programme? How long? Where is it held? How effective is it? E.g. in improving legal knowledge, investigative skills, evidence collection etc.

Section Three: Operational Context:

Q1. How do you / your unit go about policing this problem?

Q2. Could you tell me your own experiences with Internet fraud cases?

Prompts: Type of cases, number of cases, decision making, detection, investigation.

Q3. Does the unit respond reactively (to past events that come to your attention) or proactively (real time interception)?

Probe: Can you give examples?

Q4. How does Internet fraud come to your attention? Is it reported? Who? When? Why? How?

Q5. Have there been any measures taken to encourage victims of Internet fraud to report their victimisation to the police (e.g. setting up campaigns to raise awareness about Internet fraud, setting up a reporting centre, making available different ways of reporting) what are they?

Q6. Presumably these forms of crime are committed by people you cannot actually see and who could be anywhere in the world. How does one go about monitoring or policing a digital persona?

Q7. Presumably these crimes could also be committed by people living in national jurisdictions outside of Saudi Arabia. Does this pose any problems? What are they?

Probe: Can you give examples / stories?

Q8. Does the policing of this problem involve any cross-agency cooperation? Who with? How? When? Where? Why?

Prompts:

- Police departments in Riyadh
- Police departments in Saudi Arabia
- International / global Police agencies
- Private sector

Q8.1 What is the relationship like with these bodies?

Prompts: Problems, conflicts.

Q9. Do you think your unit / the police have been successful in solving Internet fraud cases?

Probe: How? Why? Can you give examples of successful investigations?

Section Four: The Future:

Q1. How do you see the future in terms of how to police / respond to this problem?

Q2. What changes would you like to see?

Prompts: Resources – Organisational – Cooperation – Legal - Training

Section Five: Personal Details:

Before we end this interview, I would like to obtain some demographic information about you which will assist analysis of the interview.

1- What is the highest level of education you have completed?

- High school □
- Bachelor's degree in Security Sciences □
- Other Bachelor's degree □

- Master's degree □
- Diploma □
- Doctorate □
- Other: specify ………… □

2- Do you have any computer-related qualifications? Yes □ No □

If yes, what is it?

Bachelor's degree in Computer Science □ Training Course □ (How many) □

Master’s degree or above in Computer Science □ Other: specify……………. □

3- Do you speak English? Yes □ No □

4- What is your present job title?

5- How many years have you been in the police?

6- How many years have you been in your present position?

Closing

Thank you very much for spending your valuable time to answer my questions. If there is anything you would like to add or you feel I have missed, please feel free to express yourself.

Appendix A.3: Interview Schedule (Senior Officers at the DPS / Riyadh Police)

THE UNIVERSITY OF HULL

Policing Internet Fraud in Saudi Arabia

Schedule for Semi-structured Interviews

Senior Officers at the DPS / Riyadh Police

Day	Date	Location	Interviewee Code	Time
	/ /2009			from am/pm to am/pm

Introduction

Thank you very much for your participation in this research. My research focuses on the policing of Internet fraud in Saudi Arabia/Riyadh and I am interested in obtaining a professional opinion based on your experience in dealing with crime. To assist me in making an accurate record of what you say, do you agree to me taping this conversation? All recorded interviews will be destroyed once transcribed. I can assure you that I will discretely handle your responses and you will remain anonymous. The information will be used for academic purposes only.

You may request a copy of the interview transcript if you want to check what has been written. Throughout the interview, if you wish to add comments or ask any questions, please do so. You may stop the interview at any time.

Section One: General / Introductory:

Q1. Is Internet fraud a problem in Riyadh / Saudi Arabia?

Q2. What is the extent of the problem?

Q3. Are there different kinds of Internet fraud? What are they?

Q4. Please could you describe a typical case?

Q5. Who are the fraudsters? How do you know? Where do they operate from? Does this pose a problem?

Q6. Who is most targeted by this crime? What victim categories are most affected?

Section Two: Organisational Context:

Q1. How have the police as an organisation responded to this problem? Any changes being made?

Prompts: standard operating procedures, training strategy, recruitment strategy.

Q2. As a senior officer in the management of the DPS / Riyadh police, could you please some information about the ICU and how it came into existence? Could you please begin by telling me who decided to set up this unit?

Q3. Who are the ‘key players’ involved in the construction of this unit?

Q4. Why did they decide to set it up? Why now?

Q5. Do all the ‘key players’ agree on what the unit should look like?

Probe: Was there any disagreement or conflict?

Q6. Who funded the unit?

Q7. What does the unit consist of in terms of technology and personnel?

Q8. Who works / is going to work in the unit?

Q9. How are they selected?

Q10. Do they / will they receive training?

Q11. How does the unit work in practice?

Q12. Now let us move on to talk more specifically about Internet fraud. What level of priority is Internet fraud assigned in police departments? Why?

Q13. Is there any specialist equipment / software that is used to deal with this problem? What is it? How does it work? Who operates it?

Q14. Is there a training programme in place? What does it entail? Who is on the programme? How long? Where is it held? How effective is it? E.g. in improving legal knowledge, investigative skills, evidence collection etc.

Section Three: Operational Context:

Q1. How do your officers / departments go about policing this problem?

Q2. Do they respond reactively (to past events that come to your attention) or proactively (real time interception)?

Probe: Can you give examples?

Q3. How does Internet fraud come to their attention? Is it reported? Who? When? Why? How?

Q4. Have there been any measures taken to encourage victims of Internet fraud to report their victimisation to the police (e.g. setting up campaigns to raise awareness about Internet fraud, setting up a reporting centre, making available different ways of reporting) what are they?

Q5. Presumably these forms of crime are committed by people you cannot actually see and who could be anywhere in the world. How does one go about monitoring or policing a digital persona?

Q8. Presumably these crimes could also be committed by people living in national jurisdictions outside of Saudi Arabia. Does this pose any problems? What are they?

Probe: Can you give examples / stories?

Q9. Does the policing of this problem involve any cross-agency cooperation? How? When? Where? Why?

Prompts:

- Between police departments
- With International / global Police agencies
- With private sector

Q8.1 What is the relationship like with these bodies?

Prompts: Problems, conflicts.

Q9. Do you think your officers / departments have been successful in solving Internet fraud cases?

Probe: How? Why? Can give examples of successful investigations?

Section Four: The Future:

Q1. How do you see the future in terms of how to police / respond to this problem?

Q2. What changes would you like to see?

Prompts: Resources – Organisational – Cooperation – Legal - Training

Section Five: Personal Details:

Before we end this interview, I would like to obtain some demographic information about you which will assist analysis of the interview.

1- What is the highest level of education you have completed?

- High school □
- Bachelor's degree in Security Sciences □
- Other Bachelor's degree □
- Master's degree □
- Diploma □
- Doctorate □
- Other: specify ………… □

2- Do you have any computer-related qualifications? Yes □ No □

If yes, what is it?

Bachelor’s degree in Computer Science □ Training Course □ (How many) □
Master’s degree or above in Computer Science □ Other: specify……………. □

3- Do you speak English? Yes □ No □

4- What is your present job title?

5- How many years have you been in the police?

6- How many years have you been in your present position?

Closing

Thank you very much for spending your valuable time to answer my questions. If there is anything you would like to add or you feel I have missed, please feel free to express yourself.

Appendix A.1: Interview Schedule (DFE/CCU)

THE UNIVERSITY OF HULL

Policing Internet Fraud in Saudi Arabia

Schedule for Semi-structured Interviews

Department Forensic Evidence/Computer Crime Unit (DFE/CCU)

Day	Date	Location	Interviewee Code	Time
	/ /2009			from am/pm to am/pm

Introduction

Thank you very much for your participation in this research. My research focuses on the policing of Internet fraud in Saudi Arabia/Riyadh and I am interested in obtaining a professional opinion based on your experience in dealing with crime. To assist me in making an accurate record of what you say, do you agree to me taping this conversation? All recorded interviews will be destroyed once transcribed. I can assure you that I will discretely handle your responses and you will remain anonymous. The information will be used for academic purposes only.

You may request a copy of the interview transcript if you want to check what has been written. Throughout the interview, if you wish to add comments or ask any questions, please do so. You may stop the interview at any time.

Section One: General / Introductory:

Q1. Is Internet fraud a problem in Riyadh / Saudi Arabia?

Q2. What is the extent of the problem?

Q3. Are there different kinds of Internet fraud? What are they?

Q4. Please could you describe a typical case?

Q5. Who are the fraudsters? How do you know? Where do they operate from? Does this pose a problem?

Q6. Who is most targeted by this crime? What victim categories are most affected?

Section Two: Organisational Context:

Q1. How have the police as an organisation responded to this problem? Any changes being made?

Prompts: standard operating procedures, training strategy, recruitment strategy.

Q2. Is there a specialist section for Internet crime? Where? Who works in it? How many? What do they do?

Q3. Is there any specialist equipment / software that is used to deal with Internet fraud cases? What is it? How does it work? Who operates it?

Q5. Is there a training programme in place? What does it entail? Who is on the programme? How long? Where is it held? How effective is it?

Section Three: Operational Context:

Q1. How do you / your unit go about handling Internet fraud cases?

Q2. Could you tell me your own experiences with Internet fraud cases?

Prompts: Type of cases, number of cases, evidence collection, evidence examination.

Q3. How does evidence in Internet fraud cases come to your unit? How is collected? Who collects it? When? Why?

Q4. Presumably these forms of crime are committed by people you cannot actually see and who could be anywhere in the world. How does one go about tracking a digital persona?

Q7. Presumably these crimes could also be committed by people living in national jurisdictions outside of Saudi Arabia. Does this pose any problems? What are they?

Probe: Can you give examples / stories?

Q8. Does the policing of this problem involve any cross-agency cooperation? Who with? How? When? Where? Why?

Prompts:

- Police departments in Riyadh
- Police departments in Saudi Arabia
- International / global Police agencies
- Private sector

Q8.1 What is the relationship like with these bodies?

Prompts: Problems, conflicts.

Q9. Do you think your department / the police have been successful in solving Internet fraud cases?

Probe: How? Why? Can you give examples of successful investigations?

Section Four: The Future:

Q1. How do you see the future in terms of how to police / respond to this problem?

Q2. What changes would you like to see?

Prompts: Resources – Organisational – Cooperation – Legal - Training

Section Five: Personal Details:

Before we end this interview, I would like to obtain some demographic information about you which will assist analysis of the interview.

1- What is the highest level of education you have completed?

- High school □
- Bachelor's degree in Security Sciences □
- Other Bachelor's degree □
- Master's degree □
- Diploma □
- Doctorate □
- Other: specify ………… □

2- Do you have any computer-related qualifications? Yes □ No □

If yes, what is it?

Bachelor's degree in Computer Science □ Training Course □ (How many) □

Master's degree or above in Computer Science □ Other: specify……………. □

3- Do you speak English? Yes □ No □

4- What is your present job title?

5- How many years have you been in the police?

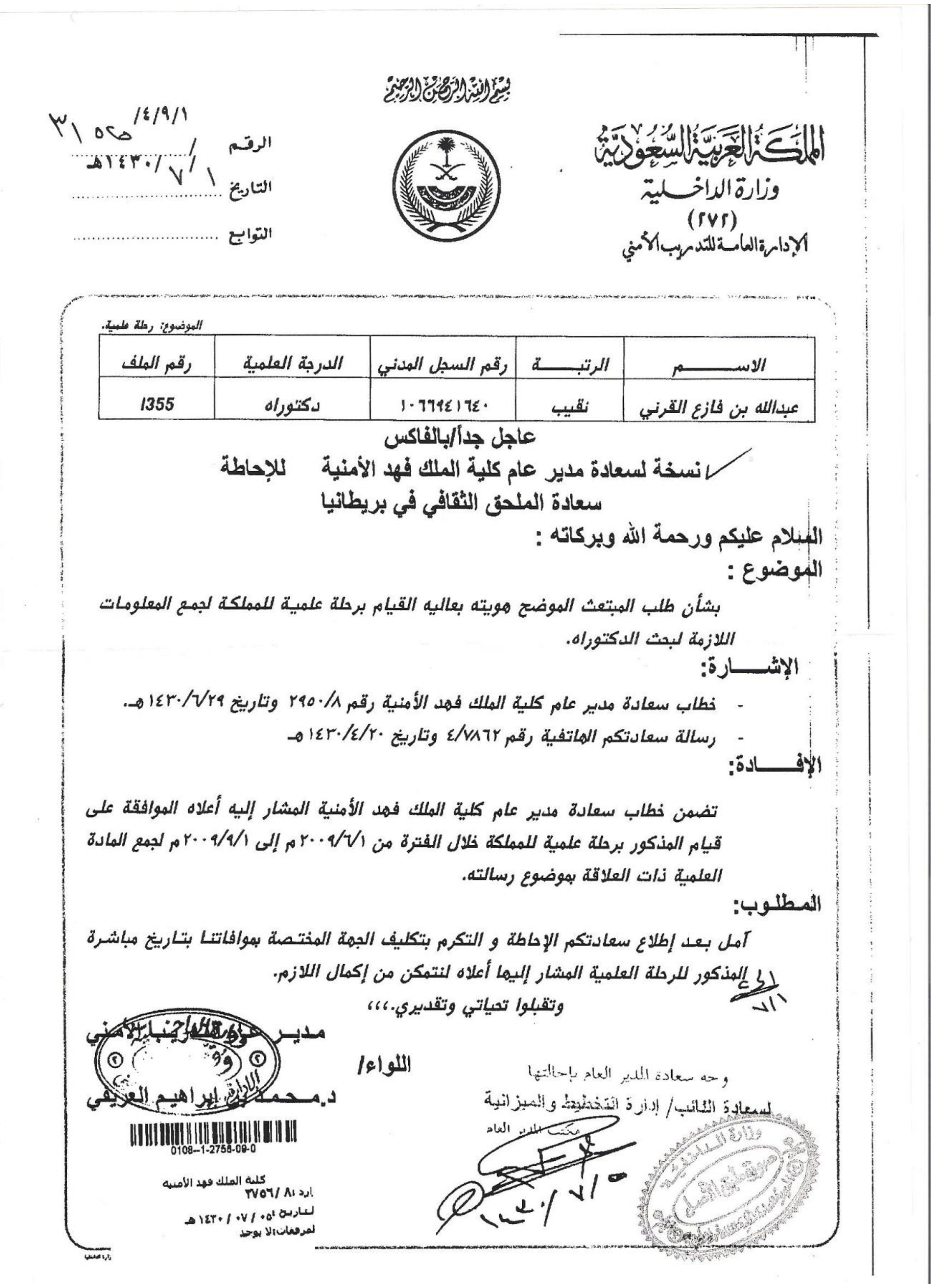
6- How many years have you been in your present position?

Closing

Thank you very much for spending your valuable time to answer my questions. If there is anything you would like to add or you feel I have missed, please feel free to express yourself.

Appendix B: Important Letters

Appendix B.1: Sponsor’s Approval of Fieldwork Plan



بسم الله الرحمن الرحيم

المملكة العربية السعودية
وزارة الداخلية
(٢٧٢)
الإدارة العامة للتدريب الأمني

الرقم ..../ ٣١ ٥٢ه /١٤/٩/١
التاريخ ١ /٧/ ١٤٣٠هـ
التوابع ....

الموضوع: رحلة علمية.

الاسم	الرتبة	رقم السجل المدني	الدرجة العلمية	رقم الملف
عبدالله بن فازع القرني	نقيب	١٠٦٦٩٤١٦٤٠	دكتوراه	1355

عاجل جداً/بالفاكس

✓ نسخة لسعادة مدير عام كلية الملك فهد الأمنية للإحاطة

سعادة الملحق الثقافي في بريطانيا

السلام عليكم ورحمة الله وبركاته :

الموضوع :

بشأن طلب المبتعث الموضح هويته بعاليه القيام برحلة علمية للمملكة لجمع المعلومات اللازمة لبحث الدكتوراه.

الإشـــارة:

- خطاب سعادة مدير عام كلية الملك فهد الأمنية رقم ٢٩٥٠/٨ وتاريخ ١٤٣٠/٦/٢٩هـ.
- رسالة سعادتكم الهاتفية رقم ٤/٧٨٦٢ وتاريخ ١٤٣٠/٤/٢٠هـ

الإفـــادة:

تضمن خطاب سعادة مدير عام كلية الملك فهد الأمنية المشار إليه أعلاه الموافقة على قيام المذكور برحلة علمية للمملكة خلال الفترة من ٢٠٠٩/٦/١م إلى ٢٠٠٩/٩/١م لجمع المادة العلمية ذات العلاقة بموضوع رسالته.

المطلوب:

آمل بعد إطلاع سعادتكم الإحاطة و التكرم بتكليف الجهة المختصة بموافاتنا بتاريخ مباشرة المذكور للرحلة العلمية المشار إليها أعلاه لنتمكن من إكمال اللازم.

الى
١/٧

وتقبلوا تحياتي وتقديري.،،،

مديـر عـام التدريب الأمني

اللواء/

د.محمد بن إبراهيم العريفي

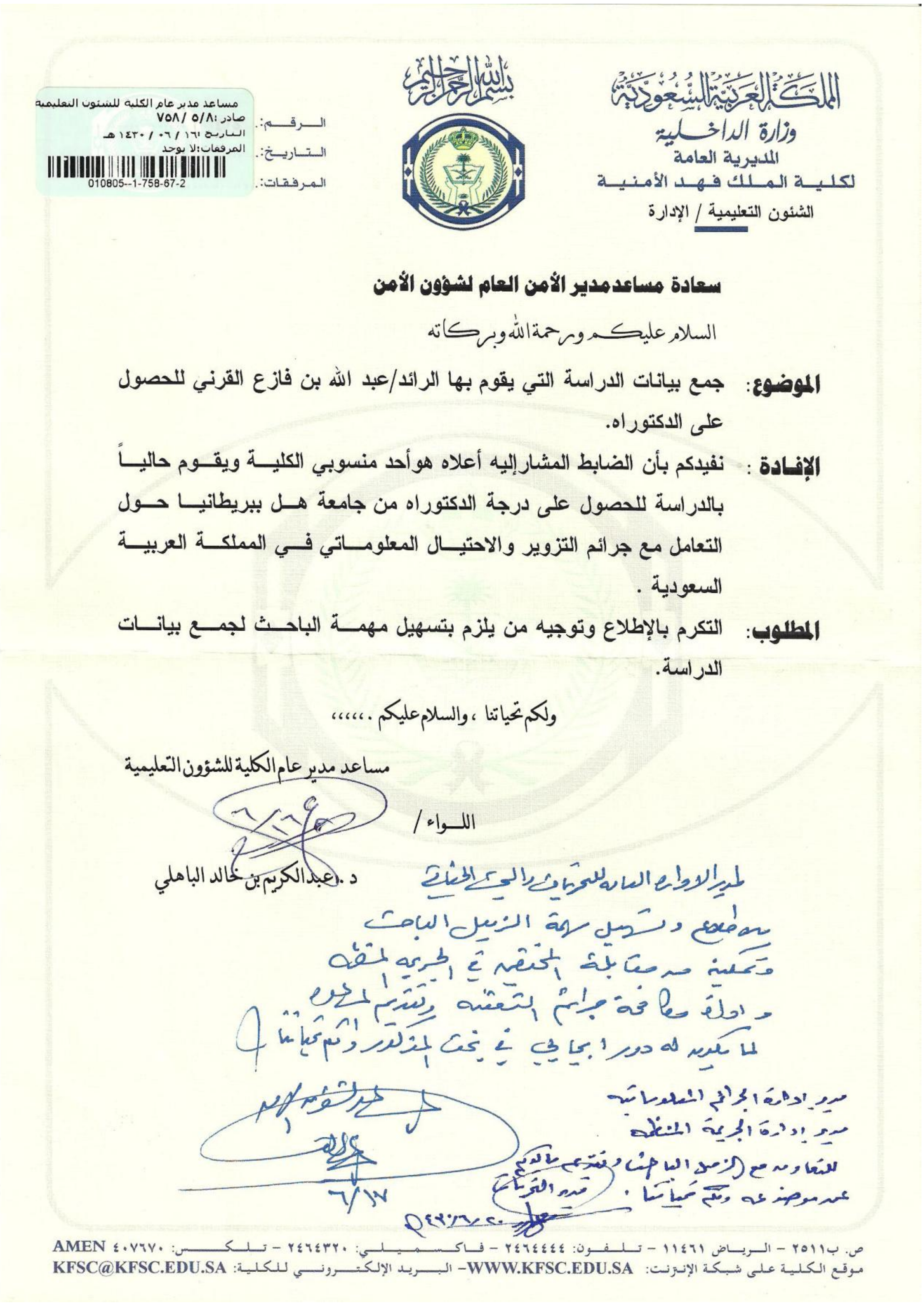
0108-1-2758-09-0

كلية الملك فهد الأمنية
وارد ٨١/ ٣٧٥٦
التاريخ ٠٥/ ٠٧/ ١٤٣٠هـ
المرفقات:لا يوجد

وجه سعادة المدير العام بإحالتها
لسعادة النائب/ إدارة التخطيط والميزانية
مكتب المدير العام
١٤٣٠/٧/٥

وزارة الداخلية
صورة طبق الأصل

Appendix B.2: The DPS's Permission to Conduct the Fieldwork



المملكة العربية السعودية
وزارة الداخلية
المديرية العامة
لكلية الملك فهد الأمنية
الشئون التعليمية / الإدارة

بسم الله الرحمن الرحيم

الرقم:
التاريخ:
المرفقات:

مساعد مدير عام الكلية للشئون التعليمية
صادر :٥/٨/ ٧٥٨
التاريخ :١٦/ ٠٦ / ١٤٣٠ هـ
المرفقات :لا يوجد
010805--1-758-67-2

سعادة مساعدمدير الأمن العام لشؤون الأمن

السلام عليكم ورحمة الله وبركاته

الموضوع: جمع بيانات الدراسة التي يقوم بها الرائد/عبد الله بن فازع القرني للحصول على الدكتوراه.

الإفادة : نفيدكم بأن الضابط المشارإليه أعلاه هوأحد منسوبي الكلية ويقوم حالياً بالدراسة للحصول على درجة الدكتوراه من جامعة هل ببريطانيا حول التعامل مع جرائم التزوير والاحتيال المعلوماتي في المملكة العربية السعودية .

المطلوب: التكرم بالإطلاع وتوجيه من يلزم بتسهيل مهمة الباحث لجمع بيانات الدراسة.

ولكم تحياتنا ، والسلام عليكم .،،،،

مساعد مدير عام الكلية للشؤون التعليمية

اللـواء /

٦/١٦

د .عبدالكريم بن خالد الباهلي

لمدير الإدارة العامة للتحريات والبحث الجنائي
للإطلاع وتسهيل مهمة الزميل الباحث
وتمكينه من مقابلة المختصين في الجريمة المنظمة
وإدارة مكافحة جرائم التقنية وتقديم ما يحتاج
لما سيكون له دور إيجابي في بحث المذكور وتقبلوا تحياتنا

٦/١٧

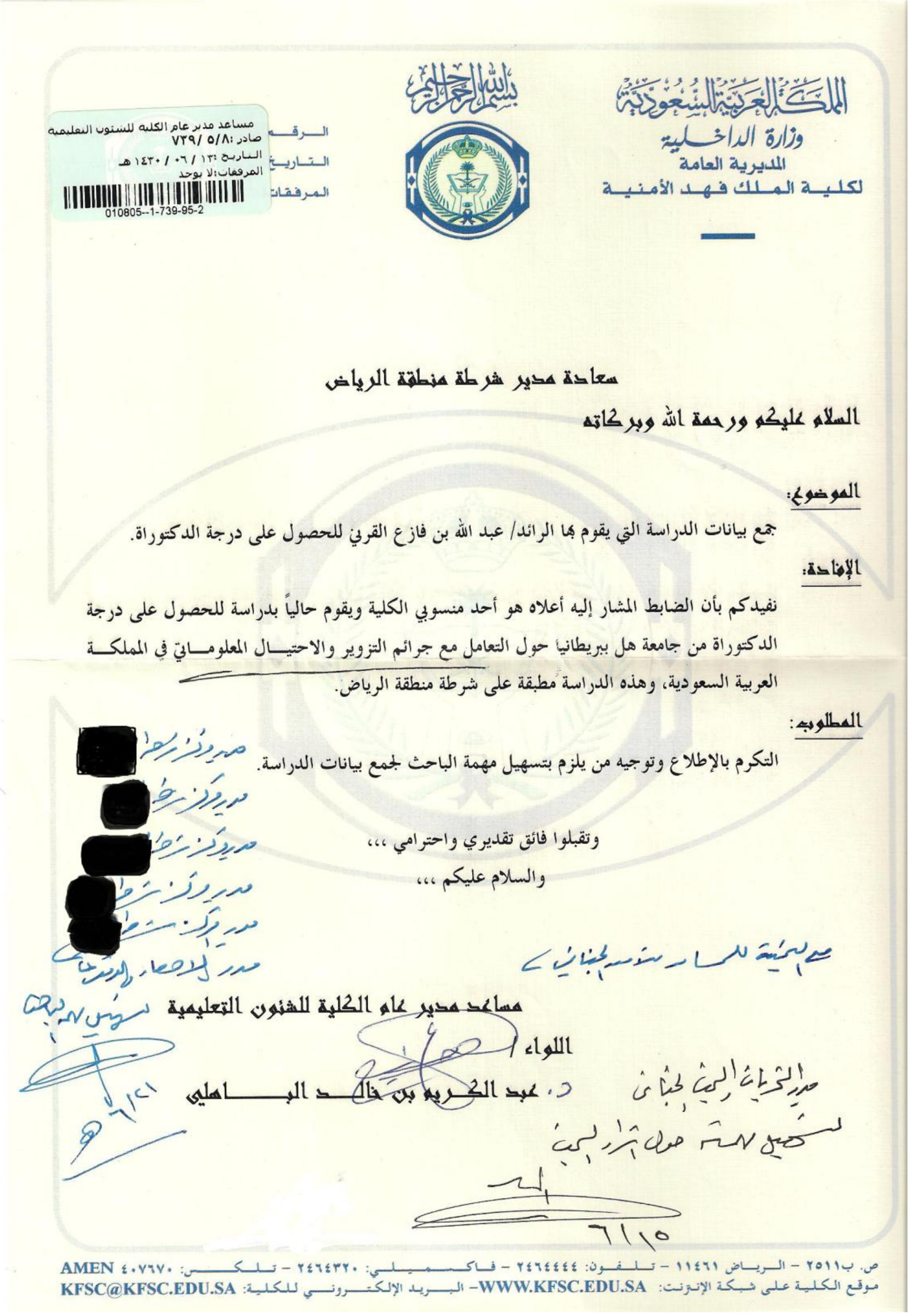
مدير إدارة الجرائم المعلوماتية
مدير إدارة الجريمة المنظمة
للتعاون مع الزميل الباحث وتقديم ما يلزم
عن موضوعه وتقبل تحياتنا

مدير التحريات

٢٠/٦/١٤٣٠هـ

ص. ب٢٥١١ – الرياض ١١٤٦١ – تلفون: ٢٤٦٤٤٤٤ – فاكسميلي: ٢٤٦٤٣٢٠ – تلكس: ٤٠٧٦٧٠ AMEN
موقع الكلية على شبكة الإنترنت: WWW.KFSC.EDU.SA- البريد الإلكتروني للكلية: KFSC@KFSC.EDU.SA

Appendix B.3: Riyadh Police's Permission to Conduct the Fieldwork



بسم الله الرحمن الرحيم

المملكة العربية السعودية
وزارة الداخلية
المديرية العامة
لكلية الملك فهد الأمنية

الرقم
التاريخ
المرفقات

مساعد مدير عام الكليه للشئون التعليميه
صادر :٥/٨/ ٧٢٩
التاريخ :١٣/ ٠٦ / ١٤٣٠هـ
المرفقات:لا يوجد
010805--1-739-95-2

سعادة مدير شرطة منطقة الرياض

السلام عليكم ورحمة الله وبركاته

الموضوع:

جمع بيانات الدراسة التي يقوم بها الرائد/ عبد الله بن فازع القرني للحصول على درجة الدكتوراة.

الإفادة:

نفيدكم بأن الضابط المشار إليه أعلاه هو أحد منسوبي الكلية ويقوم حالياً بدراسة للحصول على درجة الدكتوراة من جامعة هل ببريطانيا حول التعامل مع جرائم التزوير والاحتيال المعلوماتي في المملكة العربية السعودية، وهذه الدراسة مطبقة على شرطة منطقة الرياض.

المطلوب:

التكرم بالإطلاع وتوجيه من يلزم بتسهيل مهمة الباحث لجمع بيانات الدراسة.

مدير مركز شرطة [redacted]
مدير مركز شرطة [redacted]
مدير مركز شرطة [redacted]
مدير مركز شرطة [redacted]
مدير مركز شرطة [redacted]
مدير إدارة الإحصاء والمعلومات

وتقبلوا فائق تقديري واحترامي ،،،

والسلام عليكم ،،،

مع التحية للمساعد للشؤون الجنائية

مساعد مدير عام الكلية للشئون التعليمية

اللواء /

د. عبد الكريم بن خالد الباهلي

لتسهيل مهمته

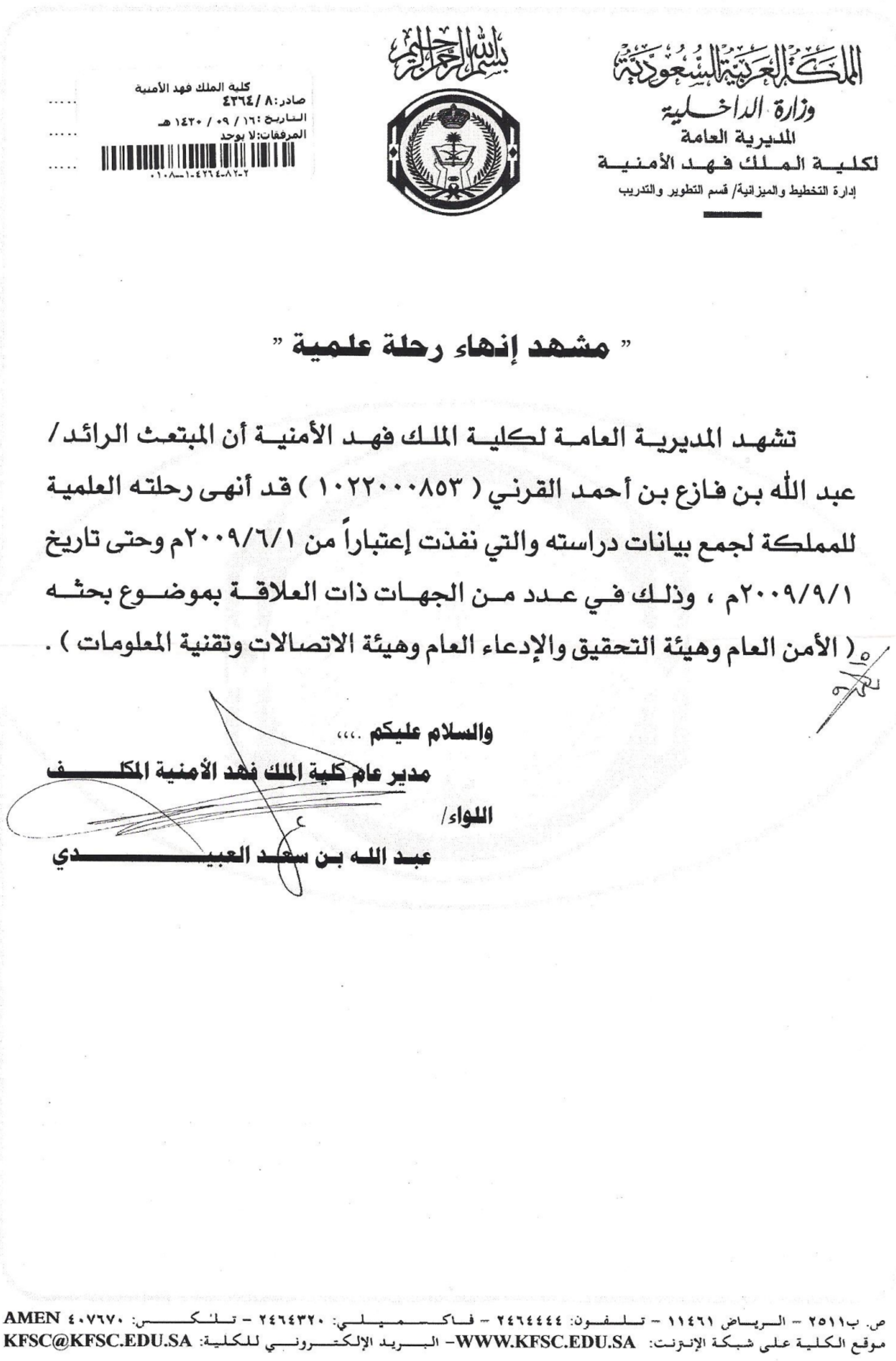
٦/٢١

مدير إدارة البحث الجنائي
لتسهيل مهمته حول إجراء البحث

٦/١٥

ص. ب٢٥١١ – الرياض ١١٤٦١ – تلفون: ٢٤٦٤٤٤٤ – فاكسميلي: ٢٤٦٤٣٢٠ – تلكس: ٤٠٧٦٧٠ AMEN
موقع الكلية على شبكة الإنترنت: WWW.KFSC.EDU.SA– البريد الإلكتروني للكلية: KFSC@KFSC.EDU.SA

Appendix B.4: Sponsor’s Confirmation of Completion of Fieldwork



المملكة العربية السعودية
وزارة الداخلية
المديرية العامة
لكلية الملك فهد الأمنية
إدارة التخطيط والميزانية/ قسم التطوير والتدريب

بسم الله الرحمن الرحيم

كلية الملك فهد الأمنية
صادر: ٨ / ٤٣٦٤
التاريخ: ١٦/ ٠٩ / ١٤٢٠ هـ
المرفقات: لا يوجد
٠١٠٨--١-٤٢٦٤-٨٢-٢

" مشهد إنهاء رحلة علمية "

تشهد المديرية العامة لكلية الملك فهد الأمنية أن المبتعث الرائد/ عبد الله بن فازع بن أحمد القرني (١٠٢٢٠٠٠٨٥٣) قد أنهى رحلته العلمية للمملكة لجمع بيانات دراسته والتي نفذت إعتباراً من ٢٠٠٩/٦/١م وحتى تاريخ ٢٠٠٩/٩/١م ، وذلك في عدد من الجهات ذات العلاقة بموضوع بحثه (الأمن العام وهيئة التحقيق والإدعاء العام وهيئة الاتصالات وتقنية المعلومات) .

والسلام عليكم ،،،

مدير عام كلية الملك فهد الأمنية المكلف

اللواء/

عبد الله بن سعد العبيدي

ص. ب٢٥١١ - الرياض ١١٤٦١ - تلفون: ٢٤٦٤٤٤٤ - فاكسميلي: ٢٤٦٤٣٢٠ - تلكس: ٤٠٧٦٧٠ AMEN
موقع الكلية على شبكة الإنترنت: WWW.KFSC.EDU.SA - البريد الإلكتروني للكلية: KFSC@KFSC.EDU.SA