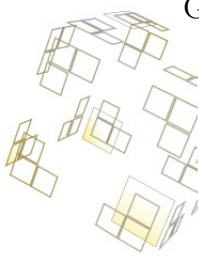




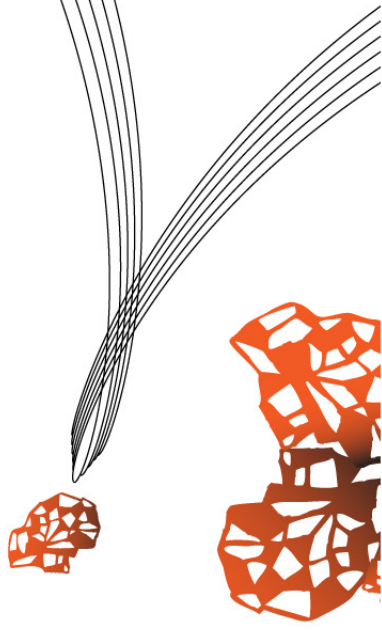
MASTER'S THESIS

Permeance of ICT in Crime in India

Author:
Gaurav MISRA



Supervisors:
Dr. Marianne JUNGER
Dr. Pieter HARTEL



August 19, 2013

UNIVERSITEIT TWENTE.

Summary

This research is aimed at investigating the extent to which Information and Communication Technologies (ICT) have influenced crime in India. The study has been conducted in the city of Kolkata with the help of the Kolkata Police. Three types of offences, namely, residential burglaries, commercial burglaries and frauds, were chosen for the study and data about the suspects, victims and the offences was obtained from the police records corresponding to these cases. We have chosen burglary cases from 2001 and 2012 and fraud cases from 2010, 2011 and 2012. All cases were selected from the Kolkata Police Headquarters. On analyzing our data, we have found that frauds have the highest amount of digital involvement out of the three crimes. We have found that the reliance of suspects on digital technologies for committing the crime is minimal. We have also found some interesting statistics about digital investigation resources employed by the police. It has been observed that camera image confiscation and phone data confiscation have been employed in an unexpectedly high number of cases by the police. Overall, we have found a higher than expected level of digital involvement in crime in India. We have also compared our findings with those from the MO-IT project conducted in the Eastern Region of the Netherlands by the University of Twente. Compared to the Netherlands, crime in India has been found to have a lower degree of digital involvement. The difference between the two countries, however, is less than expected.

Acknowledgements

This research has been completed due to the effort and cooperation of a lot of people. It was a complex project due to the sensitivity of the data which was required to be collected. Moreover, it was a sequel to the research performed here in the Netherlands and the methodology had to be extended to an Indian environment.

First and foremost, I would like to thank both my supervisors, Prof. Dr. Marianne Junger and Prof. Dr. Pieter Hartel. Their unrelenting guidance and support have made this research possible. They have transcended beyond the expected duties of supervisors and helped me make this research possible. It was their vision to extend the research to an Indian environment in order to compare the findings. They assisted me in obtaining relevant letters of support from the Dutch police which helped me convince the Indian police about the legitimacy of the project and obtain the requisite permissions. I would also like to thank Dr. A.L Montoya for her help during the analysis of the data I obtained. We had very limited time to perform the analyses and her expertise was extremely helpful for me.

A special thanks to Elmer Lastdrager who guided me during my literature review. I also want to thank Margo Karemaker who assisted me in adapting the checklist for the Indian project and also gave me useful tips about the practical details of collecting data from the police.

This research would not have even taken off without the support of the Kolkata Police. After some initial reservations, they agreed to assist me and their help throughout the data collection process was invaluable. I would like to thank Additional Commissioner of Police-I, Kolkata, Dr. Sudhir Mishra. He took time out from his incredibly busy schedule and met me multiple times and eventually granted me permission to perform my research at the Kolkata Police Headquarters. I would like to thank all staff of the Anti Bank Fraud and Anti Burglary Squads of the Kolkata Police Headquarters in Lal Bazar for their continued assistance throughout the data collection process. A special thanks to Assistant Commissioner of Kolkata Police Mr. Verghese Kunjachan for his continued assistance and guidance.

Gaurav Misra, August 2013

Contents

1	Introduction	9
1.1	Motivation and Conception	9
1.2	A Description of the MO-IT project	11
2	Research Questions and Related Work	17
3	Research Methodology	27
3.1	Sample	27
3.2	Description of Offences	28
3.3	Representativeness of Data	29
3.4	Data Collection Process	31
3.5	Description of Checklist	32
3.6	Data Entry and Analyses	33
4	Findings	35
4.1	Description of Cases	35
4.2	Characteristics of Suspects	37
4.3	Characteristics of Victims	42
4.4	Distance between Suspect and Victim	44
4.5	Relationship between Suspect and Victim	45
4.6	Digital Aspect of Crime	46
4.7	Digital Characteristics of Suspects	54
4.8	Digital Characteristics of Victims	55
4.9	Arrest and Investigation	56
5	Discussion	63
5.1	Digital Aspect of Crime in India	63
5.2	Comparison between India and the Netherlands	65
6	Conclusions	69
7	Limitations	73
	Bibliography	77
	Appendices	
A	Internet users per 100 people (Netherlands vs India)	81
B	Mobile connection per 100 people (Netherlands vs India)	83

C Relevant Sections of the Indian Penal Code (IPC)	85
D Checklist for Data Collection	115
E Total Incidents of Cognizable Crimes in 2012	139
F Total Incidents of Burglary and Fraud in 2012	141
G Percentage Increase in Burglaries and Frauds from 2011 to 2012	143
H Tables for the Results	147

List of Tables

4.1	Number of cases listed by crime for both countries	36
4.2	Percentage of suspects who have paid/legal work (N=735, in%) .	42
4.3	Number of victims listed by crime (N=843, in%)	43
4.4	Distance between Suspects and Victims listed by offence (N=903, in%)	45
4.5	Digital Modus Operandi listed by type of offence (in%)	47
4.6	Suspect and Victim characteristics for digital and traditional fraud (in%)	49
4.7	Relationship between Suspect and Victim for traditional and digital fraud (N=479, in%)	53
4.8	Localization of traditional and digital frauds (N=299, in%) . . .	54
4.9	Internet activities of Suspects (in%)	55
4.10	Internet activities of Victims (in%)	56
4.11	Physical and Digital Traces and Investigation Resources (N=1124, in%)	57
4.12	Comparing digital and traditional fraud in terms of physical and digital investigation resources (N=481, in%)	60
5.1	Digital Modus Operandi for Crimes in India (N=291, in%) . . .	64

List of Figures

4.1	Age Distribution of suspects for all types of offences	40
5.1	Comparing Age (mean) of Suspects and Victims	67

List of Abbreviations

ATM Automated Teller Machine.

CBI Central Bureau of Investigation.

CCTV Close-circuit Television.

CFSL Central Forensic Science Laboratory.

CIA Central Intelligence Agency.

CID Criminal Investigation Department.

DSP Deputy Superintendent of Police.

FBI Federal Bureau of Investigation.

FIR First Information Report.

GIS Geographical Information Systems.

ICT Information and Communication Technologies.

IPC Indian Penal code.

MO-IT Modus Operandi onderzoek naar door Informatie en Communicatie Technologie (ICT) gefaciliteerde criminaliteit.

NCRB National Crime Records Bureau.

OCTA Organized Crime Threat Assessment.

PwC PricewaterhouseCoopers.

SPSS Statistical Product and Service Solutions.

TFP Total Factor Productivity.

Chapter 1

Introduction

This research project aims to understand the relationship between technology and crime. More specifically, it aims to find out how advancements in technology have impacted crime and how often criminals are relying on Information and Communication Technologies (ICT) to commit the criminal offences.

Technological advancements have greatly impacted our society in many different ways. It has, for example, completely revolutionized the way we communicate with each other. We don't even need a computer to send an email anymore as our smart-phones, which we carry in our pockets, have an Internet connection. We are surrounded by ICT everywhere we go, be it at work, at home or even while we travel. ICT has become ubiquitous in our environment and we think it is interesting to investigate its impact on crime.

The current research has been performed in India and aims to understand the extent to which ICT has penetrated crimes in this country. The data for this research has been collected with the help of the Kolkata Police, in the city of Kolkata.

1.1 Motivation and Conception

Cyber Crime is an increasingly real threat in today's world. Modern society is equipped with new technologies which bring people closer and make communication faster and easier than ever before. The advent of the Internet midway through the 1990s has completely revolutionized communication paradigms in our society. In addition to this, advancements in technology have also changed the criminal world [4]. Clarke suggests in his paper that criminologists and crime scientists need to develop new theories or at least adapt existing theories of crime science in order to accommodate information about technological involvement to keep pace with the criminals. He warns that if we fail to do so, we might be horribly outpaced by the rapid evolution of the criminal world brought about by the extensive use of Information and Communication Technologies (ICT) [4].

The article by Albanese explains how organized crime is dependant on opportunities [1]. The report uses case studies from the US and explains a model of

organized criminal opportunities, the environment for these crimes and the skills required to carry out these organized crimes. One of the findings of this report is that organized crime groups often exploit new developments. Changes in the criminal environment and advancement in technology is one such substantial change which has been regularly exploited by criminals. Albanese agrees with Clarke that crime scientists need to work towards adapting theories in order to help the law enforcement authorities understand the trends of crime and begin to win this arms race.

An important problem faced during analysis of Cyber Crime is its definition itself. There is no agreement in the academic world about the most appropriate definition of Cyber Crime. Moreover, there seems to be a lack of understanding about its definition in legal circles as well. An abundance of confusion is prevalent when dealing with Cyber Crime cases and fixing jurisdiction of Cyber Laws. Leukfeldt, et al., have enumerated various definitions of Cyber Crime within the Dutch establishment [22]. Their paper identifies two extreme definitions from the inventory compiled by the Cyber Crime Programme of the Dutch police force (*Programma Aanpak Cybercrime* in Dutch). The first one defines Cyber Crime as being ‘*any kind of crime that is related to computer systems*’. This definition is narrow and only includes crimes that are committed on computer systems such as hacking and spreading malware while crimes like fraud and stalking using the Internet are ignored [22]. The other extreme definition is ‘*all crime carried out using a digital component*’. This definition is rather broad and may result in crimes where the offender merely makes a phone call, for instance, to be considered as Cyber Crime [22]. There are also various definitions of Cyber Crime within these two extremes which can be found in literature. However, there is ample disagreement regarding this topic and the debate about accurately defining Cyber Crime is still ongoing.

Under these circumstances, it is difficult for the police to correctly categorize Cyber Crimes and treat them accordingly during investigation and even case preparation (including framing charges against the offender). It is quite possible that the police ignore the digital aspect of traditional non-cyber crimes such as burglary, frauds, etc., as they are not traditionally considered to be cyber crimes. For example, fraud committed using an Internet auction such as eBay could be classified as ordinary fraud, without detailing the role ICT has played there [11]. This is unfortunate, because a particular aspect of the offence disappears from view and from the statistics, making the search for effective preventive measures more difficult.

The aforementioned studies make it clear that there is an absence of a clear understanding of digital aspect of crime throughout the world. Our current research positions itself exactly in the middle of this grey area between what is Cyber Crime and what is not. Our study aims to find digital component of traditional offences such as burglary and fraud. As discussed before, the definition of Cyber Crime is not a clear one and we aim to steer clear of even trying to propose a definition for Cyber Crime. We are only concerned with defining the offence at hand using our analysis of the *modus operandi* that is followed by the offenders. Our aim is to try and break each offence down to form a script, similar to a film script, to understand the *modus operandi* followed by the offenders.

From this script, it becomes easier to analyze the offence and various aspects associated with it [35]. Cornish, et al., also explain that crime analysis should focus more on the act of crime itself [6]. They explain the *Rational Choice perspective* which concerns itself with “how crimes actually happen”. They suggest that criminologists and crime analysts should focus more on criminal opportunity in conjunction with desires, preferences and motives of offenders. Our work takes notice of this theory and focuses on the act of crime itself by breaking it down in order to reconstruct the *modus operandi*. The procedure for collection of data is described in some detail later in this report.

This current project is an extension of the MO-IT - *Modus Operandi onderzoek naar door Informatie en Communicatie Technologie (ICT) gefaciliteerde criminaliteit* project done by the University of Twente in 2012 [24, 15]. One of our aims is to be able to analyze the differences, both quantitative as well as qualitative, between the involvement of ICT in crime in India and the Netherlands. The MO-IT project is described in the following section of this report.

1.2 A Description of the MO-IT project

The MO-IT project [24, 15] was done by the University of Twente with the cooperation of the Dutch police in the Eastern part of the Netherlands. The primary objective of this project was to investigate the extent to which crime and criminals depend on ICT. The methodology of this research and the findings are summarized in this section of the report. Our project follows a similar methodology to the MO-IT project and it is important for us to understand it at this point.

1.2.1 Background

Previous studies have been conducted to investigate the amount of Cyber Crime existing in our society. However, these studies attempt to define Cyber Crime and look for traces of their definition in the police files. However, as mentioned earlier, it is evident that there is an absence of a clear understanding of how to define Cyber Crime [22]. In such a situation, the MO-IT approaches the problem differently. The project performs a study which looks at police files for traditional crimes and looks for the ICT component in them using a checklist and coding methods. They also question about the stage of the offence at which ICT was used. Each offence is divided into three stages, ‘before’, ‘during’ and ‘after’. This classification helps to recreate the *Modus Operandi* of the offence and help the researchers understand the commission of the offence more effectively. Moreover, they also evaluate the extent of digital evidence collected during the investigation of the crime and the amount of ICT required to apprehend the offender. Apart from looking at the digital characteristics of the offences itself, the research also looks at offender characteristics for threats and frauds. These two crimes are chosen as they have a comparatively significant amount of ICT involvement as compared to burglaries.

1.2.2 Research Questions

The MO-IT project aims to answer the following research questions [24, 15] :-

1. How much ICT is associated with the modus operandi ‘before’, ‘during’ and ‘after’ the incident?
2. Do digital crimes differ from traditional crimes in terms of the relationships between the victim and the offender or in terms of the physical distance between them?
3. How much ICT is used during the investigation of the offence by the police?
4. How much ICT led to the apprehension of suspect(s)?
5. Which tools used in the criminal investigation are significant predictors of apprehension? Is a model based on physical tools better at predicting apprehension than one based on digital tools?
6. Does the growing presence of ICT influence the type of offenders of threats and frauds?

1.2.3 Sample

The project examined a random selection of 150 residential burglaries, 150 commercial burglaries, 300 threats and 300 fraud cases that took place in 2011 in five police forces in the eastern part of the Netherlands [24]. Out of these 900 cases, information was coded for 809 cases using the checklist. The region under the jurisdiction of these particular police forces comprises about 19% of the total population of the Netherlands [24]. The data was extracted from the police files between March and June 2012.

1.2.4 Method

The information from the police case files was extracted using a checklist. This checklist has been adapted by our current research in India by making some adjustments to account for the differences between the Netherlands and India. The modified version of the checklist, which was used in our research, is listed in Appendix C at the end of this report and is explained in detail in chapter 3. Seven coders were used during the MO-IT project for the encoding process while only one was used in the Indian study.

Four types of crimes were studied in this research. They are :-

1. *Residential Burglary* - Incidents involving theft inside or outside a house. These offences do not involve violence.
2. *Commercial Burglary* - Incidents involving theft inside or outside a company or an office and not involving violence.
3. *Threats* - Incidents involving various types of intimidating actions including stalking performed either in person or by using some communication medium.
4. *Frauds* - Incidents including all types of deceptive activities such as scams, counterfeiting of money or sensitive documents, insurance fraud, identity theft, etc.

The primary aim of the research is to understand the extent of involvement of digital modus operandi in crimes. The distinction between digital and traditional crime was made by identifying whether the crime was performed on the Internet, whether offenders threatened to disclose digital information, whether email was sent or whether other means of digital communication were used, such as text messages, chat messages, Skype calls, etc. Coders had to carefully read the entire police file as this is not something that is registered in a standardized way by the Dutch police. If at least one digital aspect was found in the file, the crime was considered to be ‘digital’; other crimes were therefore coded as ‘traditional’.

Another important feature of the MO-IT research is that it attempts to create a script corresponding to the modus operandi followed by the criminals. Therefore, as mentioned before, it is important to ascertain whether any act is performed ‘before’, ‘during’ or ‘after’ the execution of the offence. To achieve this, a rule was applied which took into account whether in principle, a time interval between these acts was possible. For instance, in the case of burglary, collecting information on the Internet about houses that may be targeted can be done a long time in advance, therefore it is deemed to be ‘before’ the commission of the burglary. Similarly, if information about the planning or preparation of the offence is recorded in the police files, those details are considered to be ‘before’ the commission of the offence. Conversely, if a stolen item like an ATM card is used to purchase other goods, for example, this action is deemed to be ‘after’ the commission of the burglary.

Seventy cases of the MO-IT study were double coded to perform an inter-rater reliability (i.e. kappa) analysis. 24% of the variables had ‘almost perfect agreement’, 30% had ‘excellent agreement’, 22% had ‘sufficient to good agreement’, 4% had ‘moderate’ agreement whilst 20% had ‘poor’ agreement. In general, though, a clear majority (approximately 76%) had good to excellent agreement which makes the data sufficiently reliable [24].

The data was analyzed initially using cross-tabulations. To compare digital and traditional crimes, a selection was made of threat and fraud cases, since only for these cases there were sufficient numbers of digital crimes available. A logistic regression was used to model the apprehension of offenders on the basis of the type of tools used in the criminal investigation. Three models were generated: digital tools, physical tools and a combined one. The models allow to identify which individual tools are significant predictors of apprehension. It also establishes how much of the phenomenon (i.e. apprehension) can be attributed to digital or to physical tools. Furthermore, a likelihood-ratio test was used to assess whether there were any significant differences between the digital and the physical models and between the individual models and the combined or full model.

1.2.5 Results

In total, 136 residential burglaries, 140 commercial burglaries, 259 threats and 274 fraud cases were coded. A total of 16% of threats and 40% of frauds had a digital aspect in the Modus Operandi [24]. 2.9% of residential burglaries involved digital frauds. These are generally the cases where ATM cards or other sensitive information was stolen and later used in the commission of the fraud. This shows that often different crimes can be combined during one offence and this sort of analysis, without having a prior definition of Cyber Crime, can help us analyze the Modus Operandi more effectively.

Another question is whether digital crimes differ from traditional crimes in terms of the relationships between the victim and the offender or in terms of the physical distance between them. As mentioned before, a selection was made of threats and cases of fraud. Digital offenders and traditional offenders differ with respect to the relationship with their victims. Digital threat offenders threaten their ex-partner more often (28.9%) than in the case of traditional threats (15.5%). Digital fraud occurs more often between business partners (47.3% vs. 24% for digital and traditional fraud, respectively) and occurs less often among acquaintances (1.8% vs. 7% for digital and traditional fraud, respectively) [24].

Another trend that is observed is the increasing geographical distance between victims and offenders for digital crimes as compared to the traditional ones. 19.4% of digital threats involved either the offender or the victim not being in the eastern region of the Netherlands at the time of offence. This figure is lower for traditional threats (7.9%). This difference, however, is not found to be statistically significant. In case of frauds, 64% of digital frauds involved one of either offender or victim to be outside the eastern region. This figure is 19.4% for traditional frauds. However, this does not translate into a growing number of international cases. For digital frauds, only 13.9% involved an international character while for traditional frauds, this number is 12.3%. Thus, there is only a marginal difference between digital and traditional frauds when it comes to international character.

Analyzing the nature of tools used by the police for investigation, the researchers find that, in general, physical tools are used more often than digital ones. As expected, physical tools are used more often to investigate burglaries as compared to threats and frauds. Digital tools, on the other hand, are used to investigate a higher number of commercial burglary and frauds as compared to residential burglary and threats. More than twice the amount of commercial burglaries (29%) use digital tools as compared to investigation of residential burglaries (13%). The authors attribute this difference largely to the amount of cases where confiscation of camera images is used by the police for investigation [24].

In general, physical factors have been found to be linked to apprehension of suspects more often than digital ones. There is an interesting observation regarding digital factors as they are seen to be involved much more in commercial burglary cases (14.5%) than other crimes. Again, this sharp spike is attributed to the general practice of obtaining surveillance footage for investigation which contributes heavily to this number.

As far as the difference in offenders is concerned, the research has some interesting findings in this regard [15]. The number of offenders of digital threats who are employed (40.7%) is higher than the number of employed offenders of traditional threats (17.4%). Offenders of digital threats are more often female, older, less often have a criminal record and more often acted alone as compared to traditional threats. Offenders of digital fraud are more often born in the Netherlands (96%) than traditional offenders (71.6%). Offenders of digital frauds are younger, have a legal occupation and they have a criminal record as compared to traditional frauds. Offenders of digital threats threaten their ex-partner more often (28.9%) than the offenders of traditional threats (15.5% ; significant, $p < 0.05$). Digital fraud occurs relatively frequently between business partners (47.3% vs. 24% for digital and traditional fraud, respectively; significant, $p < 0.05$) and occurs less often among acquaintances (1.8% vs. 7.0% for digital and traditional fraud, respectively; significant, $p < 0.05$) [15].

1.2.6 Conclusions from MO-IT Project

The research shows that frauds have the highest amount of ICT involvement (41%) out of all the crimes which were analyzed [24]. It also finds that digital crimes differ from traditional crimes in terms of the relationship between the victim and the offender and in terms of the geographical distance between them. The distance between offenders and victims increases for digital crimes as compared to traditional crimes. It is observed that ICT allows a greater distance between offenders and victims. This is an important effect of ICT on crime.

The study found that physical tools are more often linked to apprehension than digital ones. However, the regression models show digital and physical tools to be equally strong at predicting apprehension. In other words, physical tools are widely used. Digital ones, on the other hand, are used less often but have as strong an effect on apprehension [24].

A substantial number of differences are found in offender characteristics between traditional crime and digital crimes [15]. There are differences between digital and traditional offenders in terms of gender, age, employment, criminal record among other factors. The results of the research also seem to suggest the digitalization ‘normalizes’ offenders of threats, meaning that they differ less from the overall population than traditional offenders in the police registration do.

1.2.7 Limitations

The sample of cases which were used for this study came from only the eastern region of the Netherlands and the findings may not be extrapolated to the rest of the country owing to differences in Internet usage in different parts of the country. For example, the western or southern part of the country may have different demographic factors as well as a different level of Internet penetration which may impact statistics related to ICT involvement in crime in those areas. Another limitation is that only four types of offences were examined for this research (for offender characteristics, only frauds and threats were examined). The data is gathered from police case files and no other resources are used. Therefore, unreported offences cannot be accounted for in this research. The inferences of digital Modus Operandi depend on the information police have recorded about the case which may or may not be an accurate and sufficient reflection of the offence.

Although our research methodology is very similar to the one followed in the MO-IT project, there are some differences owing to circumstances related to legal or other issues. We explain our research methodology in detail in chapter 3 of this report.

Chapter 2

Research Questions and Related Work

We continue this report by enumerating our research questions and also mentioning our hypotheses related to these questions. We aim to test these hypotheses by the data collected during our study of Indian case files provided by the police in India.

Q. 1) What is the extent of ICT in burglary and frauds in India?

This is the central research question of our study. From existing literature, it is clear that there is a growing trend of involvement of ICT in crime worldwide and that includes India as well.

Recent research shows that the digital component in crimes like burglary is increasing steadily. Europol's Organized Crime Threat Assessment report (OCTA), published in 2011, mentions that dependence on Internet for non-cyber crimes has increased in all territories of the European Union [16]. This report also states that there is a considerable rise in crimes like credit card theft and theft of mobile devices which are part of a burglary case. Even the US Department of Justice Special Report on household burglaries reports that the theft of electronic devices has increased by 6% from 2001 to 2011 [39]. However, a fact that is often ignored is that these stolen items can later be used to commit further offences such as identity theft or other kinds of frauds due to their digital capabilities. Thus, if these cases are only looked at as burglary cases and the digital component (stolen items in this example) is ignored, it will be an incomplete analysis of the offence.

There has been a lot of research about the issues related to crime in India. Our research only focuses on burglaries and frauds. We have chosen these crimes as burglary is considered to be a more 'traditional' crime with respect to ICT and minimal digital involvement is expected. Other studies have confirmed

this expectation in other parts of the world [24]. On the other hand, frauds are considered to be much more dependent on advancements in technology and we expect a higher share of these crimes to contain a digital aspect. The choice of these two crimes with seemingly opposite characteristics with respect to digital involvement was intentional as we wanted to compare crimes with varying degrees of ICT involvement.

Edwardes explains in his book that crimes like burglary and fraud existed in India even during the British rule [7]. Cheque frauds, impersonation of public servants or influential people, forging documents to submit in banks, etc., existed even a century ago and these crimes still exist. The method and means of the crimes have changed with time. Burglaries were very prevalent during the British rule in the early 20th century in India. An ever lasting feature of burglaries has been the low conviction rates. For example, in Bengal in 1917, only 3% of the suspects in burglary cases were convicted [7]. Edwardes attributes this low number to a variety of factors. One of the main reasons mentioned is the reluctance of the people to report these crimes as they were often scared of the prolonged legal battle which would ensue after their complaint. He also cites reasons and justification for the commission of these crimes. One of the more widely accepted reasons for committing a crime is greed. This is especially the motivation behind most economic crimes. Another reason cited in the book is said to be scarcity. This explains the sudden spike in property crimes such as burglary and thefts during wars, droughts and famines. A very important aspect mentioned in the text is the adaptation by both the offenders as well as victims to changing circumstances and new developments. The book cites an example where stronger fences and more manpower were employed in one of the high security army establishments in the frontier province due to repeated burglaries [7]. In a way, offenders and defenders have kept challenging each other by raising the bar higher and this “contest” is still continuing.

Much like in the other parts of the World, there is a growing concern about Cyber Crime in India as well. Wadkar, et al., mention the PricewaterhouseCoopers (PwC) Global Economic Crime Survey which states that Cyber Crime is the 3rd most popular economic crime in India and the 4th most popular in the World [38]. It became more visible with the explosion and commercialization of the Internet. Although this already seems a big problem in the present day, our earlier discussion shows that cases referred to as “Cyber Crime” and statistics associated with it may only tell half the story. In order to understand the actual situation, we need to investigate the nature of the commission of these offences in detail.

Our research methodology is as similar as possible to the MO-IT project [24], which was explained in the previous chapter, in order to enable us to compare our results with their findings. We have used a checklist to extract information from the police case files. This checklist was also used in the MO-IT project. We have added some extra values to some variables which are specific to India such as police district (we have added a value for Kolkata Police), languages spoken (we have added Indian languages), nationality of suspect, etc. The checklist is attached as Appendix D at the end of this report. We describe the structure and purpose of the checklist in some detail in chapter 3.

The use of the checklist enables us to understand each offence from three distinct viewpoints - the offence, the offender and the victim. We are able to record information about all three characteristics of each offence which will help us in our analysis. This will also help us to eventually understand the *modus operandi* (followed by everyone including the victim) of the offence by forming a script which can describe the offence [6].

With the changing landscape of technology and crime, the police have to adapt themselves. It is often a political view of questioning the credibility and the usefulness of police modernization and training programs. However, as Kumar, et al., point out in their paper, police modernization programs have shown results in the recent past in India [20]. They conclude that the introduction of communication gadgets and increased training expenses helps in improving the efficiency of the police departments in India implying that the modernization scheme is working in the desired direction and it needs to be strengthened [20]. They mention that the total factor productivity (TFP) of police force in India increased by about 4 percent in a span of 7 years. Kumar, et al., say that “this improvement in police can be attributed to innovations which were strong enough to offset the losses caused by changes in technical efficiency. This technological progress reveals that over the period of time the frontier is moving outward implying that fewer resources are required to solve the same percentage of crime cases”. Our checklist will help us understand the extent to which digital evidence is being collected by the police in burglary and fraud cases. We will also learn if these confiscations are helping in solving cases. We have a section in the checklist which has questions about factors leading to the arrest of the offender. We have variables corresponding to digital evidence such as confiscation of digital data, confiscation of phone data, etc. We will find out if these are indeed helpful tools for the police to solve cases.

Digital forensics is increasingly being used by the police to trace digital footprints of the offenders [34]. Tamilarasi explains that the police are increasingly dependent on digital evidence such as mobile phone records, email conversations, hard disk drives, etc., for clues during an investigation. With the increase in digital communication between people, important clues can be found about the cases by tapping into the digital data related to any offender and vital clues are often found. Obviously, there is a valid privacy concern when it comes to digital forensics but law enforcement agencies usually get what they need by obtaining permissions from the courts. It is also common for the police to hire external digital forensic experts for help in some cases where the in-house expertise of the police falls short [34]. This development is extremely relevant for our research as the presence of ICT in crime can be investigated by collecting digital evidence about the offence. As mentioned earlier, our checklist ensures we look for digital evidence collected by the police in all the cases we studied.

Even though it seems that digital forensics is being increasingly used in investigation of crimes in India and that the police are equipping themselves for the same, there is research available which argues that the digital forensic capabilities of India are way behind their European or American counterparts [21]. Lallie states that the aftermath of the Mumbai terror attacks in 2008 have

brought the digital forensic capabilities of India into sharp focus. All major terrorist attacks leave a trail of digital evidence such as call records, emails, etc., behind them. The police and other investigating authorities have to collect all the digital evidence and piece together the clues in order to solve the cases. Of course, similar things happen for lesser offences like threats or frauds as well and the scale of evidence is much less. Lallie's paper is about comparing the digital forensics environment in India to the western world. The paper notes that India has a two-tier police system where there is the Central Bureau of Investigation (CBI) which is the national investigating agency under the central government as well as the state police forces for each state in the country. The CBI is specifically responsible for investigating terrorism, inter-state crime and corruption within the Government and public sector¹. It also acts as a point of guidance and support for state police forces if required. The CBI incorporates the Central Forensic Science Laboratory (CFSL), itself incorporating the Computer Forensic Division which provides forensic services, assistance with on-site seizure of evidence, expert testimony, research services and training. As India is a member of Interpol², the CBI may involve expertise from other members of the Interpol in very serious and international border-less crimes. The Mumbai terror attacks were a prime example of this situation when the Federal Bureau of Investigation (FBI) of the United States were invited to the investigation and given unprecedented access to evidence and intelligence³. In our project, we have worked with the cooperation of the Kolkata Police department which is the police force responsible for law enforcement in the metropolitan city of Kolkata. It is autonomous of the West Bengal state police force but relies on central agencies such as the CBI for forensic intelligence when required.

Another positive outcome of technological advancements is innovation in crime detection and analysis technologies. Kumar, et al., present a Geographical Information Systems (GIS) based model to perform spatial and temporal analysis of burglaries in Chennai, a metropolitan city in southern India [18]. This helps the law enforcement authorities to identify crime hot spots and to take adequate and appropriate measures in order to curb the threat of criminals by preparing well. The research reports that a high percentage (57%) of burglaries in Chennai are repeat burglaries which means that the same house is robbed at least twice in more than half of the total burglaries in the city. In such a scenario, this spatial and temporal analysis will definitely help the police to lay honey traps for the burglars in case they fall into the hot spots already identified by the police. The data about the crimes for this research has been provided by the Chennai Police.

Wadhwa, et al., explain another new method of dealing with fraud investigation [37]. They explain the concept of Forensic accounting which can be used to investigate and eventually curb white collar crimes such as financial frauds. Their paper states that this is becoming an increasingly important area for financial institutions such as banks as well as the police and that they are increasingly employing a higher number of forensic accounting experts to crack fraud cases. Although forensic accounting, as a concept, has been widely known

¹<http://cbi.nic.in/aboutus/aboutus.php>

²<http://www.interpol.int/>

³<http://www.fbi.gov/news/testimony/fbi-role-in-mumbai-investigation>

for many decades, its use in fraud investigation is comparatively new. However, according to the authors, there is a lot of unused potential in this mechanism which can be used by the police and investigative authorities to try and curb financial frauds and other corporate crimes. Our research will tell us the extent of use of digital forensics by the police in investigating frauds and burglaries. With our data, we can analyze how much it is being used in the present day by the police.

Evidence from existing literature suggests that digital crime is an omnipresent threat across the world. The law enforcement in India are also adapting themselves to the latest technological developments but seem to be lagging behind the Western world in this regard [21]. Our research will shed light on the extent of ICT in burglary and frauds in the city of Kolkata and we will be in a position to comment on the growing trend of digitalization of crime in India.

Hypothesis: We expect some considerable amount of ICT involvement to be present in fraud cases. We expect the proportion of involvement of ICT to be almost negligible for burglaries as they are generally much less dependent on technology.

Q. 2) How does India compare with the Netherlands in terms of influence of ICT on crime?

As we mentioned earlier in this report, one of our aims is to compare our findings from the Indian data with the findings from the MO-IT study performed by Montoya, et al., in the Eastern part of the Netherlands [24, 15] which was explained in detail in the previous chapter.

There are many aspects to consider when performing such a cross national research. The first thing to consider is the difference between the technological development of the Netherlands and that of India. As we know, these are two very differently developed countries having numerous differences in culture, economy, government and law. Our project aims to investigate the extent to which ICT is used in burglary and fraud and hence knowing the difference in the level of Internet connectivity in these two countries is a good starting point for us. We find that there is a humongous gap in the level of Internet connectivity between the two countries. Appendix A shows the latest World Bank data regarding number of Internet connections per 100 people in these two countries. According to latest data compiled in 2011, 92.3% people in the Netherlands have Internet connectivity while this figure is only 10.1% in India. It should be mentioned here that there is a considerable increasing trend in Internet connectivity in India between 2009 and 2011 (the percentage has risen from 5.1% in 2009 to 10.1% in 2011) and it is reasonable to expect that this trend will continue in the future due to rapid development of ICT. However, there is no denying the fact that these two countries are extremely different technological environments and the comparison in the findings of our research will have to be taken in context with this information. This is a really interesting and significant statistic for our research as there is, clearly, a large difference in Internet penetration in both

countries. It would be interesting to see whether this translates to a similar difference in penetration of ICT in crime in these countries.

Similarly, if we look at the statistics for number of mobile cellular subscriptions per 100 people (including both pre-paid and post-paid connections) listed in Appendix B, we find that there were about 115 connections for every 100 people in the Netherlands in 2010, whereas the figure was around 61 for India at the same time. It should be mentioned that the trends in both countries are opposite. The mobile connections per 100 people are decreasing in the Netherlands since 2008 (125 in 2008 to 115.4 in 2010) while there is a sharp increase in the same statistic in India since 2005 (7.9 in 2005 to 61.4 in 2010). However, as mentioned earlier, it is still a large enough difference for India to catch up. When dealing with statistics regarding mobile penetration, we need to consider the fact that many people possess multiple mobile devices. The figures mentioned in the World Bank data are number of subscriptions per 100 people. However, it should be taken into account that this does not mean that the number of unique mobile subscribers (or users) is same as this number. For instance, the global telecom body GSM Association (GSMA) says that only about 26% of the total Indian population were unique subscribers of mobile connections in 2012⁴. This is much lower than the number provided in the World Bank dataset. The GSMA believes that, in India, the average number of sim cards each mobile subscriber has is 2.2. This also explains the fact there is a higher number of mobile connections in the Netherlands than the total number of people.

Hypothesis: Our expectation, based on information found during the literature survey, is that the extent of ICT in crime will be lower in India as compared to that in the Netherlands as we have observed that Internet connectivity is much higher in the Netherlands as compared to India. We expect this disparity to be manifested in the influence of ICT on crime as well.

Q. 3) What are some other contrasting features of frauds and burglaries between these two countries?

We have the opportunity to analyze information about offences committed in two very different environments. As we know, crime depends on a lot of social and situational factors. Hence, we would like to utilize our data to try and identify other interesting differences apart from involvement of ICT. We have the opportunity to examine factors like age of offenders, sex of offenders, localization of offenders, relationship between offenders and victims and a lot of other aspects of the offences and compare the two countries.

Cross-national research about crime trends and statistics is somewhat of a rare occurrence in the academic world. It is even rarer if we start searching for comparisons between the western countries such as US, UK or other European

⁴http://articles.timesofindia.indiatimes.com/2012-12-13/telecom/35795693_1_bouverot-mobile-connections-gsma

countries with Asian counterparts [27]. There are a variety of reasons for this void. The United Nations Forum on Crime and Society mentions some of these reasons [32]. The first problem mentioned in this report is regarding the difference in the way a particular crime is defined in different countries. The penal code of the country in question contains the definition of the crimes as well as prescribes the punishment for an offender. We faced this problem in our research as the Dutch study had considered threat cases (*bedreiging* in Dutch) but we found that threats are non-cognizable offences in India. Hence, the police had not recorded information about cases where only threats were an offence and we could not use case files corresponding to this offence in our study in India. Our study was thus restricted to residential burglaries, commercial burglaries and frauds.

Another potential hurdle in such a research is the disparity in the rate of reported crimes in different countries. This is a significant problem for us as we have relied entirely on data collected by the police for our analysis and we have no way of accounting for or analyzing unreported crimes in this present study. Various studies have been conducted to estimate the amount of crime reporting in different countries. Most of these researches are crime victim surveys which interview victims of crimes and compare these findings with the official police data. There is evidence to show that violent crimes are more likely to be reported by the victims and also be taken more seriously by the police as compared to other crimes like property theft, etc. [32]. The UN Forum report says that the ratio of reported crime to total committed crime is higher in the European Union as compared to the rest of the World. On the other hand, the figures in Asian countries are much lower. Some researchers estimate crime reporting in India to be as low as 30 to 40% [3]. This figure means that out of every 100 offences that are committed in India, only about 30-40 are reported to the police.

We were able to find some cross-national research in the area of crime. Kumar, et al, provide a comparison between Ireland and India with respect to IT laws and Cyber Crime [19]. Their paper cites a PricewaterhouseCoopers (PwC) Irish crime report published in 2011 which states that Cyber Crime is the second largest crime in Ireland. They compare different types of frauds occurring in India and Ireland and find that India has higher proportion of Cyber Crime fraud and Accounting fraud than Ireland among all types of frauds. On the other hand, frauds like asset misappropriation and money laundering form a larger proportion of frauds in Ireland as compared to India.

There is an additional aspect regarding the perception of crime in different countries. Crimes and perceptions toward crime depends on a lot of factors such as society, culture, education, etc. Therefore, it is interesting to observe the differences in opinion of the general population of different countries regarding criminals, laws and crime in general. Pasupuleti, et al., provide an interesting comparison of opinions of Indian and US university students about crime, offenders and punishment [27]. Their research methodology involved surveying undergraduate students from an Indian university (in the southern state of Andhra Pradesh) and some undergraduate students from an American university. The number of participants was similar in both cases and participants came from varied educational backgrounds to try and maintain the neutrality

of the survey. They also mention that crime reporting in India is much lower than that of US but rate of committing of offences, like burglary for example, is much higher in India. They mention that they found quite substantial differences in opinions between Indian and American students. For example, a higher proportion of Indian students feel that crime is a threat to society while more American students agree with death penalty as compared to their Indian counterparts. Their research underscores the hypothesis that people in different countries perceive crime differently due to various social, cultural and political reasons. Our research focuses on the use of digital technology in crime which is also influenced by other factors such as technological advancement in the country, average level of education and training, etc. Differences in such aspects result in contrasting findings for our comparison.

When we are studying crime, we also have to account for the differences in legal systems in both countries. The Dutch legal system is based on Napoleonic law or *Code Law* [23]. On the other hand, the Indian Penal Code, which prescribes the guidelines for punishing offenders, is based on British Common Law or *Case law* owing to India's colonial past [5]. There are many procedural differences between these two legal systems. Napoleonic law is strictly coded and the adjudicators only refer to written laws which are static unless they are amended. Conversely, common law is very dynamic in nature and can depend on precedents set in past trials. This type of law evolves even independently of amendments depending on the precedents set by previous adjudicators [36]. We are unable to predict whether this difference of legal systems in these countries will affect the comparison of our findings in any way.

Since we are dealing with crimes related to ICT, it is important to focus our research in this area and the developments in the legal system in this regard. To deal with Cyber Crime, the government of India drafted the Information Technology Act in 2000 which contained laws to guide the citizens and the police to deal with Cyber conduct. Many researchers feel that the IT Act has been unsuccessful in dealing with Cyber Crime. It has been amended in 2008 with some new additions but it is still thought to be struggling to catch up with the advancements in technology [25, 19, 30, 9].

The cyber laws in India can also be ambiguous while determining accountability of participants in a Cyber Crime offence [30]. Rangaswamy details his study regarding Cyber Cafe owners in the paper. Cyber cafes are public Internet cafes where people can go and pay to surf the Internet on a workstation provided by the cafe owner. The paper highlights an important aspect of accountability when it talks about crimes committed using these public Internet cafes. The owners of these cafes are not really vigilant about the activity of their customers. It also raises the important question of surveillance versus privacy. For the cafe owners, maintaining business is paramount and they cannot afford to drive away customers by being seen to snoop around their monitors to check for malicious activity. This is a pretty large grey area and is also extremely significant as a large portion of rural and semi-urban India is online only because of such Internet cafes and their activity provides more questions than answers at the moment.

Another important development in this area has been the 2008 amendment to the IT Act which was originally drafted in 2000. The original IT Act has stated that investigation and by implication recording a statement committed under the IT Act must be carried out by ‘*a police officer not below the rank of Deputy Superintendent of Police*’. This meant that a lot of cases went unreported as a Deputy Superintendent of Police (DSP) is not available at all police stations in the country. However, the new amendment enables Inspectors to be in charge of investigations of such cases which makes it more accessible for the normal public. Earlier, only DSPs had to undergo training to investigate cases related to Cyber Crime but now all inspectors have to be trained. This requires more police personnel to be trained to deal with such cases as the number of inspectors easily outweighs the number of DSPs. The 2008 amendment also provides each state with the freedom to develop their own procedures with respect to investigation of Cyber Crime. The paper also reports that an increasing number of training programs are held for police personnel to help them cope with the demands of digital forensic investigation. Most state police forces, including the Kolkata Police, are developing Cyber Police capabilities in collaboration with private sector partners⁵.

Overall, we find evidences supporting the claim that both crime and law enforcement are evolving in India due to the advent of new technologies. However, as mentioned earlier in this report, this evolution seems to lag behind the western world. This assertion provides validity to our project which aims to compare and contrast the findings of research done in the Netherlands and India regarding the use of ICT in crime.

Hypothesis: Statistics suggest that offenders in India are likely to be younger as simply India is a much younger country (in terms of median age of the population) as compared to the Netherlands. The median age of the Netherlands is 41.8 years (combined population of males and females) whereas that of India is 26.7 years (data compiled in 2013)⁶. We also expect less digital evidence to be used in investigation of crimes in India as compared to Dutch cases as it has been mentioned that the Indian law enforcement agencies are lagging behind their western counterparts when it comes to digital forensic capabilities [34].

⁵<http://www.kolkatapolice.gov.in/DetectiveDepartment1.html>

⁶<https://www.cia.gov/library/publications/the-world-factbook/fields/2177.html>

Chapter 3

Research Methodology

This chapter explains our research methodology in detail. We begin by mentioning the sample of data used in our project and its representativeness. We explain the processes involved in collection of the data from the police case files. We also explain the contents of the checklist which was used to extract this data. After this, we elaborate on the type of analyses we have performed on the collected data using SPSS.

As mentioned before, our research methodology closely resembles the one followed by the MO-IT project [24, 15] which was explained in some detail in chapter 1. However, there are some differences in how the project was performed in India. These differences are mainly due to circumstances related to permissions and local laws. We highlight these differences as well as other aspects of our methodology in the following paragraphs.

3.1 Sample

We have selected three crimes for our analysis. These are - residential burglaries, commercial burglaries and frauds. The burglaries were from the 2011 and 2012 crime indexes and the frauds were from 2010, 2011 and 2012 crime indexes. In total, we had 174 residential burglaries, 57 commercial burglaries and 62 fraud cases that we examined. It should be mentioned here that these cases were listed in the corresponding crime index of the years mentioned above. This does not necessarily mean that all of these crimes were committed in these years. In some cases, the date of offence was much earlier than 2010 but the case has only been handed over to the Kolkata Police Headquarters during these years.

One major difference between this study and the MO-IT study in the Netherlands is that we have not looked at threat cases. As mentioned earlier, threats (*bedreiging* in Dutch) is a non-cognizable offence in India. A non-cognizable offence is one in which the police cannot file a First Information Report (FIR) or make any arrests [17]. Thus, no police data could be found for these cases and they had to be ignored for the Indian study.

3.2 Description of Offences

We have looked at primarily two offences for our research, namely, Burglary and Fraud. In India, criminal offences and their punishments are defined by the Indian Penal Code [5]. We looked at the Indian Penal Code (IPC) and found that the crimes that we are looking at, can be looked at as a combination of several offences of the IPC. The relevant sections of the IPC are attached in Appendix C at the end of this report ¹.

We look at the definitions related to both our crimes in the following paragraphs :-

1. *Burglary* : This is not defined as an offence itself in the IPC. There is a combination of definitions related to this offence which we will refer here.
 - (a) *Trespassing* : Section 441 of the IPC defines trespassing as a criminal offence. A criminal trespass is defined as “whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence”. Sections 442 to 445 define different types of trespassing. A specific instance of criminal trespassing is defined in section 442 as “house-trespass”. This is specific to house or living areas. Another important definition can be found in section 445 related to “House-breaking”. Section 445 lists six possible ways in which a person may be guilty of house breaking. All these definitions of trespassing are relevant as burglary cases often involve these charges.
 - (b) *Theft* : Section 378 of the IPC defines the act of theft. The definition states “whoever, intending to take dishonestly any movable property out of the possession of any person without that person’s consent, moves that property in order to such taking, is said to commit theft”. Therefore, a burglary case generally involves charges of trespassing combined with theft. Hence, it is important for us to understand how the law defines these offences.
2. *Fraud* : Section 25 defines what “fraudulently” means. It states that “a person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise”. There are multiple sections of the IPC which define different types of fraudulent offences. We list them below :-
 - (a) *Counterfeit* : Section 28 defines counterfeiting as causing one thing to resemble another thing, “intending by means of that resemblance

¹The entire text can be found from the website of the Ministry of Home Affairs, <http://mha.nic.in/pdfs/IPC1860.pdf>

to practice deception, or knowing it to be likely that deception will thereby be practiced”. There are a lot of different types of counterfeiting ranging from counterfeit currency, documents, identification, etc. Depending on the article which has been duplicated, the offence assumes varying levels of seriousness and severity of punishment is different. Sections 231 to 254 describe different types of counterfeiting and their punishment.

- (b) *Forgery* : A more relevant definition of preparing fake or forged documents is defined in section 463. It defines forgery as the act of preparing a false document, or a part of a document “with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed”. This is a very relevant definition for our research and our data includes many cases under this section.
- (c) *Cheating* : Section 415 defines cheating as the act of “deceiving any person, fraudulently or dishonestly inducing the person to deliver any property to any person, or to consent that any person shall retain any property, or intentionally inducing the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property”. This type of offence was also encountered in our research and hence this definition is significant for us.
- (d) *Criminal Breach of Trust* : Section 405 defines criminal breach of trust as dishonest misappropriation of property when the offender has been entrusted with the said property before the offence. This also includes breach of contractual obligations.

All the above offences are considered under the larger label of “frauds” in our research and we shall present our own categorization of frauds when we discuss our results.

This section has described how the IPC has defined the crimes relevant to our research. It is evident that there is no direct mapping between the definitions of these crimes in the Netherlands (described in chapter 1) and in India. Nevertheless, it is important for us to understand what exactly we mean when we refer to a particular offence in our research in the context of Indian law.

3.3 Representativeness of Data

It is important to understand the context in which we can begin to analyze the data we have collected. The first important thing to be noted is that all

cases were received from the Kolkata Police Headquarters. It is important to understand that this is not a police station in itself but it is at the top level of the police administration in the city of Kolkata. It has the jurisdiction of the entire city and can receive cases from any police station of the city at any given time.

We look at the statistics published by the National Crime Records Bureau (NCRB) ² to understand the meaning of our findings which are described later on in this report. Kolkata is a large metropolitan city in the eastern part of India. Appendix E contains the NCRB statistics for total number of cognizable crimes in the year 2012 in 53 major Indian cities. From Table 1.6 in Appendix E, it can be seen that Kolkata has a population of 14.1 million people. This is less than only two of the cities in the list, Delhi (16.3 million) and Mumbai (18.4 million). It can be observed that a total of 25370 cognizable crimes were reported in Kolkata in the year 2012. This constitutes 5.4% of all reported cognizable offences in the 53 major cities mentioned in the Appendix E. This figure of 5.4% is lower than only three of the cities mentioned in the list, namely, Delhi (10.1%), Mumbai (6.4%) and Bengaluru (6.2%).

Our research only focuses on burglaries and frauds. Appendix F lists the total number of burglaries, thefts and frauds reported in 2012. The Indian Penal Code differentiates between three types of fraud, namely, “Criminal Breach of Trust”, “Cheating” and “Counterfeiting” as discussed in the previous section. We consider all these to be frauds and have included all of these offences in our study. From Table 1.15, it is seen that there were a total of 96 burglaries and 4960 thefts reported in Kolkata in the calendar year of 2012. However, 659 thefts were auto thefts (car thefts) and hence we exclude them. Without these, there were 4301 other thefts in Kolkata in 2012. It is impossible to predict the exact number of thefts which are relevant for our research as some thefts do not involve “house-break” or “trespassing” and hence cannot be considered valid for our research. Moreover, there were 428 cases of criminal breach of trust, 2100 cases of cheating and 26 cases of counterfeiting reported. Thus, a total of 2554 fraud cases were reported in the year 2012.

Perhaps, it is even more interesting to note the rate of increase of burglary and frauds from 2011 to 2012 in all the major cities. If we look at Table 1.13 in Appendix G, we find that burglary has increased by 52.4% in Kolkata between 2011 and 2012. This is the third highest rate of increase after Asansol (133.3%) and Varanasi (58.7%). A few interesting facts emerge from this information. It is to be noted that Asansol is in the same state as Kolkata, i.e, West Bengal. It is also important to point out that both Varanasi and Asansol have lower number of burglaries than Kolkata (73 and 21 compared to 96). We also find that a large number of cities display a decrease in the number of burglaries from 2011 to 2012. However, Kolkata is showing an opposite trend as the number of burglaries is growing there. It is clear from this data that burglary in Kolkata is an increasing problem as compared to other cities and we will get a useful sample of cases for our study.

²<http://ncrb.nic.in/>

Similarly, if we look at the figures for fraud, criminal breach of trust has gone up by 28.5%, cheating has increased by 29.2% but counterfeiting has gone down by 58.7% which is seemingly a quite sharp decrease. It is important for us to remember these statistics before analyzing our findings about frauds in the city. These numbers may explain some of the trends we observe about the number of each type of frauds we study in our research.

3.4 Data Collection Process

All the data for our research has been collected from the Kolkata Police. The data was coded at the Kolkata Police Headquarters. Prior permission was sought to perform this research and after waiting for requisite clearances, the data collection process began on 18th March 2013. All the data was collected from crime indexes maintained by the police. It was not possible to obtain access to the actual case files as all the cases we analyzed are currently under trial in court. Therefore, the police did not allow us access to case files. Nevertheless, the crime indexes were studied. A crime index is used by the police to record information about the cases they are currently investigating or have investigated in the past. It is like a database of case details containing some information about the suspects, a brief description of the offence itself as well as some information about the complainant. Each section of the police maintains its own crime index on an annual basis. Thus, a crime index stores information of all cases which came to that particular section of the police force during a calendar year. The entries are updated as and when progress is made in the investigation and subsequently the trial of the case.

As discussed in the previous section, we looked at three specific crimes, namely, residential burglaries, commercial burglaries and frauds. For the fraud cases, we worked with the cooperation of the Anti Bank Fraud Squad of the Detective Department at the Kolkata Police Headquarters ³ and for the burglary cases (both residential and commercial) we worked with the Anti Burglary Squad of the Detective Department of the headquarters. For frauds, crime indexes of 2010, 2011 and 2012 were checked whereas only crime indexes of 2011 and 2012 were checked for burglary cases. The reason for this disparity is that the Anti Bank Fraud Squad receives a much lower number of cases annually as compared to the Anti Burglary Squad.

The data collection was done with the help of a checklist. The checklist was used by the coder to extract information about each case from the crime index provided by the police. The contents of the checklist and their significance is described later in the following section of this report.

In this project, only a single coder was involved. All the coding was done at the respective sections (Anti Bank Fraud and Anti Burglary) of the Detective Department at the Kolkata Police Headquarters to safeguard confidentiality of police data. The time for coding each case file was noted in the checklist. The

³<http://www.kolkatapolice.gov.in/DetectiveDepartment1.html>

coding was finished within 10 minutes for 57.3% of all cases which were analyzed. A further 35.2% of the cases required between 10 and 20 minutes of coding time. The rest 7.5% cases took more than 20 minutes of coding time. The minimum amount of time required to code a file was 4 minutes and the maximum was 40 minutes.

3.5 Description of Checklist

The data collection process has been described in the previous portion of this report. As explained before, all the data was collected from crime indexes provided by the Kolkata Police. The information regarding digital *modus operandi* has to be mined from these crime indexes. In order to do this, we employed a checklist. This checklist was used to extract relevant information from the crime indexes and store them in a suitable way from which they can be easily used for analysis. In this part of the report, we explain the utility as well as the structure of this checklist. The checklist is attached as Appendix D at the end of this document.

This checklist was used by the coder to enter the information. The coder would read the information about a particular case in the crime index provided by the police and fill up the checklist. The checklist aims to collect as much data about the digital aspect of the crime as well as suspects and victims as possible. We discuss some of the features of the checklist below.

- *Preliminary information about the offence* - Basic details such as location, date of offence, date of cognizance, police district, etc., are noted in the beginning of the checklist. Information such as the number of offenders involved, whether the offenders have been arrested or not, whether the case has been submitted to the public prosecutor or not are also recorded. There is also a section where the time taken to code each file is duly noted.
- *Digital modus operandi* - There are questions in the initial part of the checklist which are aimed at understanding whether the offence was committed digitally or not. In case of burglaries, online theft of data is categorized as digital burglary. For frauds, this scope is much larger as computer systems and other digital technologies can be used to commit various frauds like identity theft, phishing, etc.
- *Other characteristics of the offence* - Apart from the information related to the digital *modus operandi*, other information such value of plunder (in Euros), items gained during offence, whether personal information of the victim is stolen or not, etc., is recorded. At the end of the checklist, a summary of the offence is written by the coder in order to retain some qualitative information about the offence.
- *Basic information about offender* - Personal details like name, address or any contact details are not recorded in our research. However, some basic

details such as year of birth, nationality, country of birth, city of residence, occupation, highest level of education, marital status, etc., are recorded with the help of the checklist.

- *ICT related activity of offender* - There are questions which inquire about the online behavior of the offender. This information has to be explicitly present in the crime index. For this to happen, the police has to investigate about this and record this information. There are questions which check whether the offender was active on social media, home-sales sites, online shopping websites, his/her own website, Youtube, Skype, etc. Another thing which is to be looked for is whether the offender was using utilities like email, chat, sms, etc., to communicate either before, during or after the offence. The status of the offender's computer is also investigated. Whether the offender had updated operating systems and anti-virus programs installed on his/her computer is also noted.
- *Basic information about victim* - Information similar to that recorded for the offender is also noted for the victim.
- *ICT related activity of victim* - Similar questions about the ICT related behavior of the victim is also noted.
- *Relationship between offender and victim* - There are questions which aim to investigate the relationship between the offender and victim. We check whether the offender and victim were business partners, buyer/seller, acquaintances, family members, employee/employer, criminal contacts, etc.

All the functions of the checklist which have been mentioned in the text above have a very important role in our research and will help us to answer our research questions.

3.6 Data Entry and Analyses

In the previous section, we described our checklist in some detail. This checklist is used to code the information present in the crime indexes provided to us by the police. From looking at the checklist in Appendix E, it is clear that different types of data is entered into it. These types are :-

- *Numeric values* - Most entries in the checklist are of this type. Most questions have five possible outcomes and all these outcomes have corresponding numeric codes, namely, "Yes (1)", "No (0)", "Unknown (99)", "Inapplicable(88)" or "Something different (77)". Additionally some other questions such as age, number of suspects, number of victims, number of witnesses, time taken to code, etc., are also numeric in nature. Moreover,

the options for many questions such as nationality of offender/victim, police district, languages spoken, etc., are also assigned numeric values for ease of coding and subsequent analysis.

- *Strings* - Some entries in the checklist are of string type. Answers to questions about location, case number, description of occupation of offender, summary of offence, etc., are coded as string type entries.
- *Date* - The third type of data in the checklist is dates. Beginning date of offence, ending date of offence, date of cognizance are coded as date type entries in the checklist.

We have used the SPSS tool for our data analysis. All the data we recorded in the checklist for each case was translated into a record in our SPSS file which is used to analyze our data. All the questions in the checklist were assigned a variable in the SPSS file. The type of the SPSS variable was dependent on the above mentioned data type of the information it contained.

The data has been analyzed from mainly three different viewpoints - offender characteristics, offence characteristics and the victim characteristics. We have used cross-tabulations for our analysis and our findings are presented in the next chapter in detail.

Chapter 4

Findings

In this chapter, we elaborate on the results we have obtained through our analyses. We begin this chapter by describing the offences in general. We then describe the basic characteristics of the suspects and victims of the cases we studied before moving on to explore the digital characteristics of the offences. We conclude the chapter by mentioning the results related to the investigation resources used by the police to arrest the suspects.

4.1 Description of Cases

As mentioned in earlier sections, we focused our research on three particular crimes in the Indian part of our study. These are - Residential Burglary, Commercial Burglary and Frauds. We used the crime indexes for 2011 and 2012 for the burglaries. The burglary section of the Kolkata Police receives both residential and commercial burglaries and hence the crime index contains both types of crimes. The distinction between residential and commercial burglaries was made by the coder by reading the description of the offence. For frauds, we used the crime indexes for 2010, 2011 and 2012. We tabulate the number of cases listed by crime in both Netherlands and India in table 4.1.

As can be seen from the table, we studied a total of 293 cases in India. We had 174 residential burglary cases, 57 commercial burglary cases and 62 fraud cases. The number of residential burglaries is marginally higher than in the Netherlands (136) but for commercial burglaries and frauds, it is substantially lower.

Sometimes, it is possible that an offence is not completed and the offender is caught or stalled during the commission of the offence (Table 1, Appendix H). As we can see from the table, all cases of residential and commercial burglaries we studied in India were completed while a small fraction (1.6%) of fraud cases were unsuccessful attempts. However, these numbers are substantially higher for the Dutch cases. As many as 30% of the commercial burglaries studied in the Dutch research were unsuccessful attempts. Residential burglaries (18.4%) and frauds (18.6%) also have non-trivial amount of unsuccessful attempts. This

Table 4.1: Number of cases listed by crime for both countries

Type of Crime	India	The Netherlands
Residential Burglary	174	136
Commercial Burglary	57	140
Fraud	62	274
Total	293	550

large disparity between the countries may be explained by the possibility that the crime index maintained by the Kolkata Police contains details of mostly successfully completed offences. However, we have not been able to confirm this assertion during our research.

4.1.1 Kind of Location

Another interesting aspect of the offence is the kind of location where it was committed (Table 11, Appendix H). As can be seen from the table, there is not that much variety in residential burglaries. Most of these offences are committed in homes (98.9% for India and 97.1% for the Netherlands). However, a very interesting observation can be made from the numbers for commercial burglaries. As high as 10.5% of the 57 commercial burglaries studied in India happened in a place of worship. This can be explained by the fact that a lot of temples in India contain a lot of items of jewelery such as crowns, thrones, swords, etc. Thus, these establishments seem to be an attractive target for burglars. Another contrast can be found when looking at the number for crimes on the Internet. In the Netherlands, 33% of the frauds happened on the Internet. However, this number is comparatively quite low (8.1%) in India. This is consistent with our hypothesis made in the chapter 2 based on the disparity in Internet penetration of both the countries (Appendix A).

An interesting observation about frauds in India is that a large number of them happened in banks (48.4%) and ATMs (17.7%). This trend is not observed in the Netherlands. The very high number of Indian frauds occurring in banks and ATMs can be explained by the fact that we obtained our data from the *Anti Bank Fraud* department of the Kolkata Police. This department is a subsection of the Detective Department in the Kolkata Police Headquarters and was established as a specialized section for handling bank frauds. However, it also handles other frauds as can be seen from the variety of cases studied during our research.

Overall, we find that frauds in both countries show a greater variety in terms of kind of location as compared to the other types of offences. The most common location for frauds in India was found to be banks (48.4%) whereas the maximum number of the Dutch fraud cases took place on the Internet (33%).

4.1.2 Plunder

In any offence, the offender gains some materialistic things such as money, electronics, jewellery, etc. This information is important as it also forms the basis of the confiscation as well as the investigation performed by the police as we will observe in a later section of this chapter. We observe that India has a higher percentage of cases where money is gained by the offender as compared to the Netherlands for all three types of offence (Table 12, Appendix H). The same is also true for jewellery. In case of electronics, however, the Netherlands have a higher percentage for residential burglaries (35.3%) as compared to India (21.3%). This means that over a third of the residential burglaries in the Netherlands involve theft of electronic items such as computers, laptops, TV, CD player, etc. However, for commercial burglary and fraud, India has a higher percentage of electronics gained (26.3% and 1.9% respectively) than in the Netherlands (12.9% and 1.1%). This is due to the fact that our research in India contained a few commercial burglaries where electronics shops were targeted by the offender and hence inflating the number of stolen electronic devices for the Indian data. Another important observation is that India has a higher percentage of mobile phones gained for all three offence types as compared to the Netherlands. This may be due to the fact that our data was obtained from Kolkata, which is a metropolitan city and has a larger average of mobile connections as compared to rural parts of the country, hence biasing the data to some extent. It is also possible that lesser number of mobile phones are stolen in the Netherlands as the general public is aware of the pitfalls of stealing them due to the modern mobile tracing capabilities available. They know that it will not be very lucrative for them to steal mobile phones as they can be tracked and eventually caught by the police. On the other hand, such knowledge may not be that commonly available for burglars in India and they seem to think that stealing mobile phones is lucrative and beneficial for them.

When electronic items or mobile phones are gained from any offence, this may have an effect on the ICT aspect of the offence as well as the investigation by the police. We will discuss this in more detail in a later section of this chapter.

4.2 Characteristics of Suspects

The second part of this chapter focuses on the suspects of our cases. The information regarding the suspects is available to varying degrees in different cases. As mentioned before, our only source of information was the crime indexes provided to us by the police and all our findings are based on data obtained from there. We highlight some of the important findings about the suspects in this section.

4.2.1 Number of Suspects

The first thing to observe is the number of suspects involved in any offence (Table 2, Appendix H). By looking at the numbers, we find that residential burglary mostly involves one suspect in both India (87.4%) and the Netherlands

(79.8%). The security systems in residential establishments are not expected to be as sophisticated and hence a lesser number of people can successfully commit such an offence. We find that residential burglaries have the highest percentage of single offender as compared to other types of offence in both countries.

For commercial burglaries, these percentages drop in both countries. 77.2% of commercial burglaries involved a single offender in India while this number is as low as 53.3% in the Netherlands. 5.8% of commercial burglaries involve more than three offenders in the Dutch cases while none of the commercial burglaries in India involve more than three offenders. A higher number of offenders generally means a larger conspiracy and hence this distinction is important for us. Commercial burglaries in India have been found to be performed in shops, religious places, etc., as we will see later in this report. We did not find many commercial burglaries in large commercial organizations and most scenes of these crimes were small shops, temples, schools, etc., which are similar to residential burglaries in terms of security. This may explain the fact that a large group of offenders is not required for these offences. On the other hand, we find that most of the commercial burglaries in the Netherlands were performed in business organizations (93.5%). They are generally equipped with a higher amount of security and hence involve a larger conspiracy. This explains the relative disparity between the two countries in terms of number of offenders for commercial burglaries. It should also be mentioned here, however, that the difference between India and the Netherlands in terms of number of offenders for commercial burglaries is not statistically significant.

For frauds, we observe a large contrast for both countries. For the Netherlands, a large majority of 86.5% cases involve only a single offender. However, this number drops to 31.6% for frauds in India. A substantial number of cases (35%) involve more than three offenders and the highest number of involved offenders is as high as twelve. This may point to the fact that frauds, in general, involve a larger aspect of planning and conspiracy and, as a result, additional help is often required. However, in the Netherlands, this does not seem to be the case as it has the highest percentage (86.5%) of single offenders in all three crimes. Another important factor here is the location. Most frauds in India were committed in banks or ATMs. On the other hand, we find that the most popular location for Dutch frauds was the Internet. It is not hard to imagine that offenders are more likely to work individually when committing crime on the Internet and this explains the high proportion of cases where there was only a single offender for the Dutch fraud cases. It should also be noted that the data for fraud cases is statistically significant.

4.2.2 Gender of Suspects

An important piece of information while studying suspect characteristics is their gender (Table 3, Appendix H). A quick glance tells us that a higher percentage of total offenders in India (97.3%) are male as compared to the Netherlands (85.7%). The low number of women suspects in India as compared to the Netherlands can be explained to the difference in the sex-ratio of both coun-

tries. According to the *World Factbook* ¹ published by the Central Intelligence Agency (CIA) of the USA, the sex-ratio in India in 2013 is 1.08 males per female while it is 0.98 in the Netherlands. If we look at the state of West Bengal in particular, the census figures from 2011 ² reveal that the sex-ratio in this state (1.05) was very similar to the national average (1.06) in 2011. Another important factor is the involvement of women in economic activities. Women who are regularly involved in economic activities are possibly more likely to commit economic crimes such as frauds. According to World Bank data, in 2011, 29% of females above the age of 15 in India were economically active ³. On the other hand, the number in the Netherlands is exactly double that of India. 58% of Dutch women over the age of 15 were found to be economically active in 2011. This is a very significant difference between the two countries and possibly contributes to the explanation of the disparity between the different gender ratios in the suspects from both countries.

If we look at the specific crimes, we find that fraud is the offence with the most female offenders in both India (5.6%) and in the Netherlands (18.9%). However, in all the types of offences, the percentage of female offenders in the Netherlands is higher than that in India.

4.2.3 Age of Suspects

When analyzing crime, it is interesting for us to look at the age of the offenders who commit these crimes (Table 4, Appendix H). We find that most of the offenders in India (60%) and the Netherlands (43%) are between the age of 18 and 30. We only found 1.1% juvenile offenders (below the age of 18) in India whereas in the Netherlands this percentage is higher (9.3%). When we look at each type of offence, 78.5% of offenders in residential burglaries in India are below 30 years of age whereas it is 58.1% in the Netherlands. For commercial burglaries the proportion of offenders below 30 years of age is 60.5% in India and 51.6% in the Netherlands and for frauds it is 41.6% and 45% respectively. Thus, for both countries, residential burglaries have the highest number of offenders below the age of 30 while frauds have the least.

Figure 4.1 shows the age distribution for suspects in both countries for each type of offence. It is clear from the figure that both countries have a peak value in the age group between 18 to 29 years for all offences. It is also interesting to note that the shape of the curves for all three offences are strikingly similar for both the countries. The peaks are higher for Indian suspects for all types of offences while the values are relatively equally distributed in the Netherlands. An interesting observation is that the number of suspects in the range of above 40 years is consistently higher in the Netherlands while the range for below 30 years, India has higher numbers. These trends are consistent across all types of offences. The fact that the suspects for Indian offences are almost consistently younger than the Dutch offenders for each type of offence is consistent with

¹<https://www.cia.gov/library/publications/the-world-factbook/fields/2018.html>

²<http://www.census2011.co.in/sexratio.php>

³[http://data.worldbank.org/indicator/SL.TLF.CACT.FE.ZS/countries/1W-IN-NL?](http://data.worldbank.org/indicator/SL.TLF.CACT.FE.ZS/countries/1W-IN-NL?display=default)
display=default

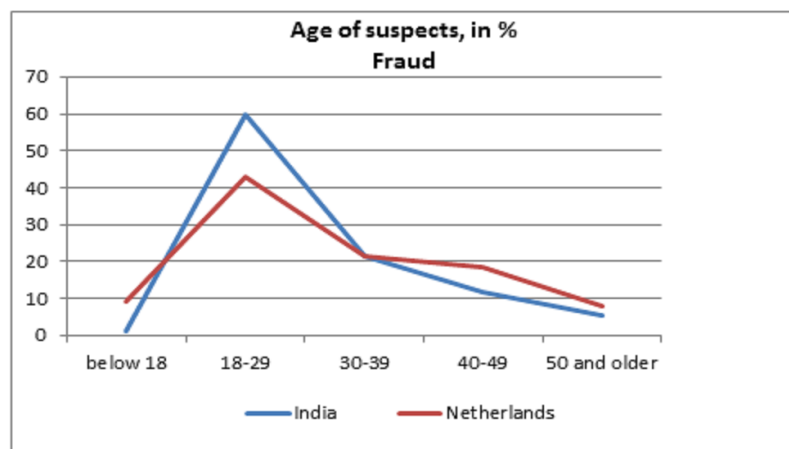
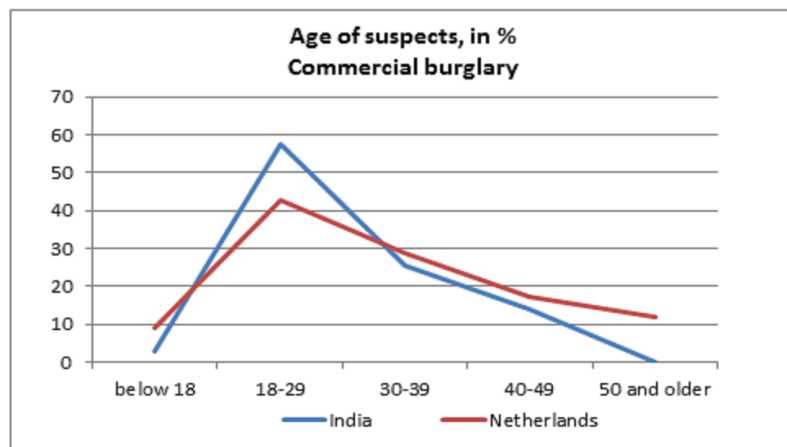
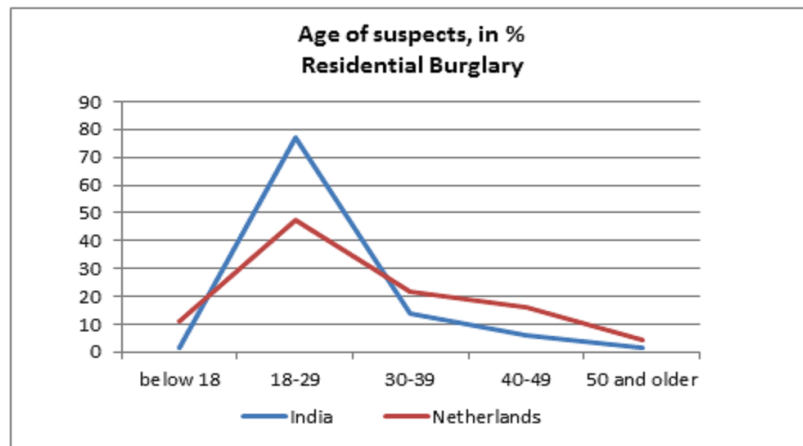


Figure 4.1: Age Distribution of suspects for all types of offences

our third hypothesis mentioned in chapter 2. As we noted earlier, the median age of India (26.7) as compared to the Netherlands (41.8) and this results in our observation that suspects are younger in India for all types of offences as compared to the Netherlands.

4.2.4 Country of Origin

97.1% of the suspects in Indian cases are born in India and 75.8% of suspects in Dutch cases are born in the Netherlands (Table 5, Appendix H). Thus, there is a higher percentage (24.2%) of foreign offenders for Dutch crimes as compared to India (2.9%). For Indian cases, the highest number of foreign offenders are observed for fraud cases (5.6%) whereas for the Dutch cases, residential burglaries have the highest number of foreign offenders (28.1%) as compared to other offences.

The large disparity in number of foreign born offenders between the two countries can be attributed to the difference in international migrant stock in both countries ⁴. According to World bank data, in 2010, only 0.5% of people living in India were born outside the country. On the other hand, in the same year, 10.5% of people living in the Netherlands were migrants. This is a huge disparity and manifests itself in our research as well.

4.2.5 Education

Since we are trying to identify the digital aspect of crime, it is important for us to know whether the suspects come from an IT related educational background (Table 6, Appendix H). It should be mentioned again that the number of offenders for Indian cases for whom this information was available is very small (44). It can be seen that 12% of fraud offenders in India received digital training. This can be explained by the fact that some of the offenders in fraud cases in India were employees of banks and were highly educated. On the other hand, information about education was not easy to find for burglary suspects and the ones we found did not have high educational qualifications. Due to the really low number of burglary suspects in India for whom this information was available, the comparisons are not statistically significant.

Interestingly, the highest percentage of offenders who received digital training for Dutch cases are found for commercial burglaries (1.5%). This is a higher proportion than fraud (0.4%) and hence it shows a different trend to Indian cases in this respect. The information for fraud cases is statistically significant.

4.2.6 Employment

Table 4.2 lists the percentage of offenders in both countries who had paid/legal work listed by type of offence. The first thing to note from this table is that the number of offenders for Indian cases for whom employment information was

⁴<http://data.worldbank.org/indicator/SM.POP.TOTL.ZS>

Table 4.2: Percentage of suspects who have paid/legal work (N=735, in%)

Type of Crime	India	The Netherlands
Residential Burglary	16.0	16.0
N	25	162
Pearson Chi-Square	0.004	
Commercial Burglary	75.0	20.6
N	12	204
Pearson Chi-Square	18.604***	
Fraud	66.7	9.6
N	51	281
Pearson Chi-Square	93.702***	
Total	53.4	14.7
N	88	647
Pearson Chi-Square	74.531***	

*** p <.001 (significant).

available is pretty low (88). Therefore, the statistics are skewed and may not provide an accurate picture. Nevertheless, we find that commercial burglaries have the highest percentage (75%) of offenders who are employed. For the Dutch cases, it is observed that the employment information is available for a much larger number of cases (647) and that commercial burglaries have the highest percentage (20.6%) of offenders who had paid/legal work as compared to the other two types of offence. It should be noted that the statistics for both commercial burglaries and frauds are significant ($p < .001$) whereas the ones for residential burglaries are not.

4.3 Characteristics of Victims

In the previous section, we focused on some basic information we gathered about the suspects of the offences. In this section, we take a look at some similar kind of information we gathered for the victims of these offences.

4.3.1 Number of Victims

We can see from table 4.3 that all offences in the Indian study involved exactly one victim. It should be mentioned that all the cases we studied contained information about only the complainant who registered the case with the police. There is no information about additional victims present in the case indexes which were studied. However, this is not the case in the Netherlands. We see that 11.8% of the residential burglaries in the Netherlands involved more

Table 4.3: Number of victims listed by crime (N=843, in%)

Number of Victims	Residential Burglary		Commercial Burglary		Fraud	
	India	Netherlands	India	Netherlands	India	Netherlands
0	0.0	3.7	0.0	2.1	0.0	8.0
1	100.0	84.6	100.0	95.0	100.0	87.2
2	0.0	9.6	0.0	2.1	0.0	4.4
3	0.0	2.2	0.0	0.0	0.0	0.0
5	0.0	0.0	0.0	0.0	0.0	0.4
8	0.0	0.0	0.0	0.7	0.0	0.0
Pearson Chi-Square	28.820***		2.955		8.841*	

* $p < .05$ (significant).

*** $p < .001$ (significant).

than one victim. Out of the three types of offences, commercial burglaries have the highest percentage (95%) of single victims in the Netherlands. However, it should also be pointed out that the information for commercial burglaries are not found to be statistically significant.

4.3.2 Gender of Victims

We observe that there is a vast majority (80.4%) of male victims in Indian offences (Table 7, Appendix H). However, the gender ratio is not so skewed in the Netherlands. Only 57.9% of the victims are male while 42.1% are female. Again, this overall disparity can be explained by the reasons mentioned for gender of suspects in previous section.

In India, the highest number of female victims can be found in residential burglaries (23%), which is also the case in the Netherlands (51.1%). This is not really surprising as the likelihood of women being affected by residential burglaries is higher than commercial burglaries or frauds due to the simple fact that women in both countries are much more likely to stay at home than go out to work, as mentioned in the previous section.

The lowest proportion of female victims in India can be found for fraud cases (13.3%) while, in the Netherlands, it can be found in commercial burglaries (19.6%). For Indian frauds, most of them involved banks and ATMs and the complainant was an employee of the bank. As we have stated numerous times, much higher number of males are employed in India as compared to the females. This explains the skewed gender ratio for victims as well as suspects of economic offences such as frauds.

4.3.3 Age of Victims

It can be seen again that a very small number (55) of files contained this information about the victims in the Indian cases (Table 8, Appendix H). The youngest victim in India was 17 years old whereas it was 4 years in the Netherlands. The oldest victim in India was 75 years of age while it was 90 years in the Netherlands. It is clear that a larger number of victims (41%) in the Netherlands were above the age of 50 as compared to India (30.9%). Overall, the victims in India are marginally younger than in the Netherlands. However, the difference between the two countries is not as high as it is for suspects.

Looking at specific types of offences, we find that frauds in India have the highest number (83.3%) of victims above the age of 40. As mentioned before, the complainants of most fraud cases in India were high ranking officers in banks and hence have a higher average age as compared to the other two offences. For residential and commercial burglaries, the percentage of victims above the age of 40 is 57.5% and 44.4% respectively.

However, the scenario is not as skewed in favor of any particular type of offence in the Netherlands. Both commercial burglaries (65.3%) and frauds (63.2%) have similar amount of victims above the age of 40 while Residential burglary (59%) is only marginally behind. Thus, it can be said that the age distribution for victims in the Netherlands is much more equal across different types of crime as compared to India.

4.3.4 Nationality of Victims

We observe that 99% of all victims in Indian cases are born in India whereas 89.4% of the victims in Dutch cases are born in the Netherlands (Table 9, Appendix H). We note that these percentages are higher than the percentage of foreign born suspects in both countries, as mentioned in an earlier section. All victims in both residential and commercial burglaries in India are born in India. Frauds in India have about 4.8% foreign victims. The highest percentage of foreign victims in the Netherlands can be found for commercial burglaries (16.3%).

4.4 Distance between Suspect and Victim

Another significant aspect of every offence is the geographical proximity between the suspect and the victim. It is important for us to try and identify differences between the distance between suspect and victim for different types of offences. This information is presented in table 4.4.

When we look at the numbers in this table, we find that both types of burglaries are much more localized in the geographical relationship between the suspects and victims. In India, we find that both residential burglary (97.9%) and commercial burglary (95%) have a very high percentage of cases where both victims and suspects were resident in West Bengal. In the Netherlands, these numbers are quite high as well, but lower than in India (86.2% for residential

Findings

Table 4.4: Distance between Suspects and Victims listed by offence (N=903, in%)

Distance between Suspect and Victim	Residential Burglary		Commercial Burglary		Fraud	
	India	Netherlands	India	Netherlands	India	Netherlands
Both in Local Province ¹	97.0	86.2	95.9	82.4	83.4	45
Either Suspect or Victim outside Local Province	3.0	10.1	4.1	14.4	15.5	39.4
Both Suspect and Victim outside Local Province	0.0	1.4	0.0	1.1	0.5	2.8
International	0.0	1.4	0.0	1.1	0.5	2.8
N	202	138	74	187	193	109
Pearson Chi-Square	340.000***		261.000***		279.954***	

¹ Local province in India means West Bengal and in the Netherlands it means the Eastern part of the country which was the sample space for the study.

*** p < .001 (significant).

burglary and 82.4% for commercial burglary).

In both countries, frauds have the least number of cases where both the victim and suspect are from the local region (83.4% for India and 45% for the Netherlands). The frauds in the Netherlands show a quite large extent of offences where at least one of the suspect or victim is outside the Eastern region (39.4%). The high number of fraud cases in the Netherlands where the suspect and victim are not located in the same province can possibly be explained by the fact that 33% of fraud offences in the Netherlands were committed on the Internet. The Internet enables a suspect to commit an offence even if he/she is not in the geographical proximity of the victim. The absence of frauds committed on the Internet in India may explain the relatively high number of cases (83.4%) where both the suspect and victim were present in the same province.

When it comes to international suspects or victims, we find that there is a negligible amount of such cases found in both countries. Fraud in the Netherlands has the highest number of internationally located suspects and/or victims (2.8%) but even this number is really low.

4.5 Relationship between Suspect and Victim

It is important for us to know whether the victim and the suspect of a particular offence share any kind of relationship (Table 10, Appendix H).

It is clear from the table that a higher number of offences (33%) in the Netherlands have suspects and victims sharing some kind of relationship as

compared to Indian cases (7.1%). Frauds have the highest number of cases where suspect and victim share a relationship in the Netherlands (43.8%) while the same is true for commercial burglaries in India (16.2%). For commercial burglaries in India, we found quite a few cases where the employees of the victim committed the offence. A few commercial burglaries involved theft in shops which were committed by the people who were hired by the shop owner and worked there. This highly influences the cases where there is an “other relationship” between the suspect and victim for commercial burglaries in India (14.9%).

The most common relationship between suspect and victim in the Netherlands is business partner (17.5%). A large number of frauds (33.2%) in the Netherlands have been committed by suspects who were business partners of the victims. On the other hand, the most popular relationship between the suspect and victim is “other relationship”. As mentioned earlier, this is the most common relationship in commercial burglaries in India.

When we look at the numbers for contact established between suspect and victim before the offence, we find that the Indian cases have a higher percentage (14.4%) than the Dutch cases (9.3%). This is primarily due to the quite high proportion of fraud cases (36.4%) in India which involve contact between suspect and victim before the offence. Fraud cases in India have been found to happen more in banks. For such offences, it is essential for the suspect to have some interaction with the victim’s organization. For example, the suspect may want to open a fraudulent bank account and has to begin the formalities for the same. Other frauds such as cheating, scams, etc., also involve some interaction between the suspect and the victim which enables the suspect to lure the victim.

4.6 Digital Aspect of Crime

The primary objective of our research is to identify the extent of ICT in crime in India. After having observed the basic characteristics of the suspects, victims and the offences in the earlier sections, we move on to focus our attention to the digital aspect of the offences in this part of the report.

4.6.1 Digital Modus Operandi

We begin our analysis of the digital aspect by investigating whether the offences involved a digital modus operandi. We categorize an offence to have a digital modus operandi if some digital technology has been used in commission of the offence by the offender.

We have listed the presence of a digital modus operandi for different types of offences in table 4.5. We list the percentage of cases which involve an unwanted email being sent, a digital threat being issued, digital forgery or digital burglary. We can also observe the stage of the offence at which the digital technology was used. This helps us to try and recreate the script of the offence as mentioned earlier in this report. In both countries, commercial burglaries do not manifest a

Table 4.5: Digital Modus Operandi listed by type of offence (in%)

Digital Modus Operandi	Residential Burglary		Commercial Burglary		Fraud	
Unwanted email sent	India	Netherlands	India	Netherlands	India	Netherlands
Before the offence	0.0	0.0	0.0	0.0	1.6	1.1
During the offence	0.0	0.0	0.0	0.0	1.6	2.6
After the offence	0.0	0.0	0.0	0.0	0.0	0.0
Total	0.0	0.0	0.0	0.0	1.6	3.6
Pearson Chi-Square	-		-		0.662	
Digital Threat	India	Netherlands	India	Netherlands	India	Netherlands
Before the offence	0.0	0.0	0.0	0.0	0.0	0.0
During the offence	0.0	0.0	0.0	0.0	0.0	1.1
After the offence	0.0	0.0	0.0	0.0	0.0	0.7
Total	0.0	0.0	0.0	0.0	0.0	1.5
Pearson Chi-Square	-		-		0.916	
Digital Forgery	India	Netherlands	India	Netherlands	India	Netherlands
Before the offence	0.0	0.7	0.0	0.0	16.7	9.5
During the offence	0.0	0.7	0.0	0.0	23.3	38.7
After the offence	0.0	1.5	0.0	0.0	5.0	2.9
Total	0.0	2.9	0.0	0.0	23.3	40.1
Pearson Chi-Square	5.185*		5.960*		37.362***	
Burglary in Digital Form	India	Netherlands	India	Netherlands	India	Netherlands
Before the offence	0.0	0.0	0.0	0.0	3.2	0.0
During the offence	0.0	0.0	0.0	0.0	1.6	5.1
After the offence	0.0	0.0	0.0	0.0	0.0	0.0
Total	0.0	0.0	0.0	0.0	3.2	5.1
Pearson Chi-Square	-		-		0.396	

* p < .05 (significant).

*** p < .001 (significant).

digital component. In the Netherlands, a small percentage (2.9%) of residential burglaries involve digital forgery. However, in India, both commercial as well as residential burglaries have shown no digital aspect in our study. This is along expected lines as burglaries are generally less dependent on ICT as compared to frauds.

We find that a total of 1.6% of frauds in India involve “unwanted emails” being sent to the victim. This percentage is marginally higher for frauds in the Netherlands (3.6%). Digital threats are absent in the Indian cases whereas we see a small number of frauds in the Netherlands (1.5%) which have this component. It is important to note that digital threats are not used before the offence while unwanted emails are not sent after the offence. This clearly tells us about the utility of each type of digital modus operandi for different stages of the offence. Unwanted mails are often sent for phishing and cheating offences to lure the victim or feed them with wrong information and hence are used before or during the offence itself. On the other hand, threats are generally not useful before the commission of the offence and are generally employed to force the victim to act in a certain way during or after the commission of the offence.

The most common digital modus operandi we found is the digital forgery. 23.3% of frauds in India were digital whereas this number is higher in the Netherlands (40.1%) We also find that 2.9% of residential burglaries in the Netherlands involve digital frauds. Fraud in both India and the Netherlands contain small number of digital burglaries (3.2% for frauds in India while 5.1% for frauds in the Netherlands). These digital burglaries are often used to steal user credentials or credit card information of the victims and used by the suspect for monetary gains. It should be mentioned here that the findings regarding the digital forgery are significant as mentioned in the table.

4.6.2 Comparison of Suspect and Victim Characteristics for Digital and Traditional Fraud

It is interesting for us to compare the basic characteristics of suspects and victims for traditional and digital frauds. Digital frauds in this context are defined as those fraud cases which involved a digital aspect in them, as listed in table 4.5. We only chose frauds for this comparison as the other two offences, residential burglaries and commercial burglaries, involve negligible digital modus operandi according to our study, as shown in table 4.5.

Table 4.6 lists the differences in suspect and victim characteristics for traditional frauds as compared to digital ones for both India and the Netherlands. We look at gender, age, country of origin, employment, previous criminal records and number of suspects and victims involved for both traditional and digital frauds in both countries.

Table 4.6: Suspect and Victim characteristics for digital and traditional fraud (in%)

	Frauds in India			Frauds in the Netherlands		
Percentage of Females	Traditional	Digital	p-value	Traditional	Digital	p-value
Suspects	6.9	2.0		18.9	19.1	
Victims	15.9	7.1		40.7	42.7	
Age (below 40 years)						
Suspects	62.3	89.8	***	62.2	73.0	
Victims	25.0	0.0		28.2	45.7	**
Native local¹						
Suspects	97.9	84.0	***	71.6	96.0	
Victims	88.7	100.0	*	86.1	92.4	
Employment						
Suspects	80.0	18.2	***	11.8	6.3	
Victims	96.6	90.0		16.9	13.4	
Suspects (above 18 years)	79.4	18.2	***	17.4	25.0	
Victims (above 18 years)	66.7	50.0		22.2	13.5	
Antecedents						
Suspects	0.0	6.0	**	8.8	11.7	
Victims	0.0	0.0		0.6	0.0	
Number of Suspects/Victims						
Single Suspect	29.3	35.7		82.4	94.4	*
Single Victim	100.0	100.0		95.7	94.6	*

¹ Local refers to birthplace as India for Indian offences and Netherlands for Dutch cases.

* p < .05 (significant).

** p < .01 (significant).

*** p < .001 (significant).

Gender

When we look at the gender of suspects, we find that, for Indian cases, traditional fraud has a higher number of female suspects (6.9%) as compared to digital frauds (2%). However, an opposite trend is observed in the Dutch cases. The amount of female offenders for traditional frauds in the Netherlands (18.9%) is marginally less than in digital frauds (19.1%). Overall, we see that there is a higher number of female offenders in both types of frauds in the Netherlands as compared to India.

When we look at the gender for victims, we again find that traditional frauds in India (15.9%) have a higher number of female victims as compared to digital frauds (7.1%). Again, this trend is slightly reversed for the Dutch cases. We find that the number of female victims in traditional frauds (40.7%) is slightly lower than digital frauds (42.7%). Similar to what we observed for suspects, Netherlands has more female victims as compared to India for both traditional and digital frauds.

From the table, we find that the figures for gender of suspects and victims in both countries is not found to be statistically significant.

Age

There is a higher number of suspects for digital frauds (89.8%) below the age of 40 years as compared to traditional fraud (62.3%) in Indian cases. This is also the situation in the Netherlands where number of suspects below the age of 40 is higher in digital frauds (73%) as compared to traditional frauds (62.2%). So, in both countries, we find that digital frauds have younger offenders as compared to traditional frauds. We find that the age information for suspects in India is found to be statistically significant while that in the Netherlands is not.

The information about age for victims in Indian frauds is not found to be significant. The number of cases where age information about victims was found was extremely low and hence the statistics are insignificant. This information, however, is significant for Dutch cases. We find that a higher number of victims of digital fraud (45.7%) are below the age of 40 as compared to traditional frauds (28.2%).

Country of Origin

Digital frauds (84.0%) in India had a lower number of suspects who were born in India as compared to traditional frauds (97.9%). However, this trend is reversed in the Netherlands where digital frauds (96%) have a higher number of locally born offenders as compared to traditional frauds (71.6%). Thus, digital frauds in India involve a higher percentage of international offenders as compared to traditional frauds while an opposite trend is observed in the Netherlands.

For victims in India, traditional frauds have a lower number of Indians (93.5%) as compared to digital frauds (100%). A similar trend is observed in the Netherlands as well with traditional frauds having 86.1% of the victims

born in the Netherlands as compared to 92.4% for digital frauds.

Employment

When we look at employment, we find that a very high number of suspects of traditional frauds (80%) were employed according to our data. This can be explained by the fact that a large number of traditional fraud cases we studied were involving bank frauds. To perform bank frauds, an offender is generally an account holder and is employed. For digital frauds, we find that the number of employed suspects is pretty low (18.2%). Even in the Netherlands, traditional frauds (11.8%) have a higher number of employed suspects as compared to digital frauds (6.3%). However, if we focus only on offenders above the age of 18, the trend in the Netherlands becomes the opposite. Traditional frauds have 17.4% of the suspects who are employed while digital frauds have 25%.

For victims in Indian frauds, traditional frauds (96.6%) have a higher number of victims who have paid or legal work as compared to digital frauds (90%). We find that in both traditional as well as digital frauds in India, the percentage of victims who have employment is very high. As explained before, a large number of frauds we studied were involving banks or other commercial organizations and generally the victim was an employee of a bank or any other organization. In the Netherlands, traditional frauds (16.9%) have more victims who are employed as compared to digital frauds (13.4%). If we look at victims above the age of 18, we find that the findings are not significant due to the absence of information about age of victims in a lot of cases. The number of victims who are employed in India comes down substantially for both traditional (66.7%) as well as digital fraud (50%). This inconsistency in the data can be explained by the absence of information about the age of the victims in a large majority of Indian fraud cases.

Antecedents

We find that 6% of suspects of digital frauds in India had a prior criminal record. None of the suspects of traditional frauds in India were found to have a past criminal record with the police. In the Netherlands, 11.7% of the suspects in digital frauds had a criminal record as compared 8.8% for the traditional frauds. Thus, for both countries, a higher number of suspects of digital frauds were found to have prior criminal record as compared to traditional frauds.

None of the victims of Indian frauds were found to have a past criminal record while only 0.6% of frauds in the Netherlands had a victim who has a prior criminal history with the police.

Number of Suspects and Victims

We find that a higher number of digital frauds (35.7%) had a single suspect as compared traditional frauds (29.3%) in India. The same observation is made for Dutch frauds where 82.4% of the traditional frauds had only a single suspect

as compared to 94.4% of digital frauds. This finding is along expected lines as digital frauds are considered to be more easily accomplished individually as compared to traditional frauds which may involve a larger conspiracy which requires a larger group of people. If we compare the two countries, we find that a much larger majority of frauds, both digital as well as traditional, involve a single suspect in the Netherlands. This may be explained by the fact that frauds are generally sophisticated offences and require a higher number of people in an Indian environment. This can be due to the lower amount of Internet penetration in India as compared to the Netherlands. Another related reason is that a significant number of digital frauds in the Netherlands were committed on the Internet which generally require lesser number of suspects. We found no frauds in India which were committed on the Internet.

All frauds in India involved a single victim. As explained before, the crime indexes of the Kolkata Police only contained details about a single complainant. Hence, all cases we studied have information about a single victim. Traditional frauds in the Netherlands (95.7%) had a marginally higher number of cases with a single victim who was affected as compared to digital frauds (93.6%).

4.6.3 Relationship between Suspects and Victims for Digital and Traditional Frauds

We have already discussed the various types of relationships between the suspects and victims in an earlier section of this chapter (Table 10, Appendix H). However, it is important for us to decipher this information for traditional and digital frauds in order to identify any possible difference. This information is presented in table 4.7.

When we look at the statistics, we find that there are very few fraud cases in India in which there was a relationship between the suspect and the victim. It is also evident that the suspect and the victim have a relationship for a higher number of traditional frauds as compared to digital frauds in India. The suspect and the victim were business partners in 2.7% of traditional frauds in India while it was 2% for digital frauds. The most common relationship between the suspect and the victim for traditional frauds was “other relationship” which includes the cases where the suspect was an employee of the victim. We did not find any fraud cases where the suspect and victim were family members, partners, ex-partners, criminal contacts, friends on social network, fellow gamers or chat friends. It should again be noted that our information was obtained from the crime indexes maintained by the police and hence any relationship between the suspect and victim has to be discovered by the police and mentioned in the file for us to record it in our analysis. The information about relationship between the suspect and victim is not found to be statistically significant.

In Netherlands, however, the situation is different. The suspect and the victim were business partners in a higher number of digital frauds (47.3%) as compared to traditional frauds (24%). We should also note that the statistics for only business partner, acquaintances and ex-partners relationship types are

Table 4.7: Relationship between Suspect and Victim for traditional and digital fraud (N=479, in%)

Type of Relationship	Frauds in India			Frauds in the Netherlands		
	Traditional	Digital	p-value	Traditional	Digital	p-value
Business Partners	2.7	2.0		24.0	47.3	***
Related/Family	0.0	0.0		1.2	0.9	
Acquaintances	2.7	0.0		7.0	1.8	*
Residents	0.7	0.0		0.6	1.8	
Ex-Partners	0.0	0.0		3.5	0.0	*
Partners	0.0	0.0		0.0	0.0	
Criminal Contacts	0.0	0.0		0.0	0.0	
Friends on social network	0.0	0.0		1.2	0.0	
Fellow Gamers	0.0	0.0		0.0	0.0	
Chat friends	0.0	0.0		0.6	0.9	
Other Relationship	4.1	0.0		5.3	0.9	
N	146	50	-	171	112	-

* p < .05 (significant).

*** p < .001 (significant).

significant.

4.6.4 Localization of the Offence

We look at the comparison of the distance between the suspect and victim for traditional and digital frauds in table 4.8.

We find that traditional frauds in both countries are much more localized as compared to digital frauds. As many as 93.6% of the traditional frauds in India have both the suspect and the victim in West Bengal. On the other hand, only 54% of the digital frauds have both the suspect and the victim in the province. This means that digitization provides a larger radius for offenders to operate in and they can commit an offence and affect a victim who is not geographically very close at the time of offence. The same situation is observed for the Dutch frauds as well. 57.5% of the traditional frauds in the Netherlands involved both the suspect and the victim from the Eastern region of the country whereas, for digital frauds, this number is comparatively much lower (19.4%).

When it comes to international offences, we find that the number is very low in India. Only 2% of the digital frauds had an international component while none of the traditional frauds had this. In comparison, the Dutch frauds exhibit a little more international component for both traditional (12.3%) and digital (13.9%) frauds. However, the distinction between traditional and digital frauds

Table 4.8: Localization of traditional and digital frauds (N=299, in%)

Distance between Suspect and Victim	Frauds in India			Frauds in the Netherlands		
	Traditional	Digital	p-value	Traditional	Digital	p-value
Both in the local ¹ province	93.6	54.0	***	57.5	19.4	**
Either suspect or victim outside local province	6.4	42.0	***	27.4	63.9	**
Both suspect or victim outside local province	0.0	2.0	***	2.7	2.8	**
International	0.0	2.0	***	12.3	13.9	**
N	140	50	-	73	36	-

¹ Local province for Dutch cases is the Eastern part of the Netherlands which was the sample space for this study and for Indian cases is West Bengal.

** p <.01 (significant).

*** p <.001 (significant).

in terms of international involvement in the Netherlands is minimal.

4.7 Digital Characteristics of Suspects

We have discussed the basic characteristics of the suspects for all types of offences earlier in this report. In this part, we look at the digital characteristics of the suspects and their dependence on Information and Communication Technology (ICT). The Internet related activities of the suspects are summarized in table 4.9.

For both countries, the Internet does not seem to be an effective source for information regarding plunder for residential and commercial burglaries. For frauds, the number of suspects who became aware of the plunder because of the Internet is higher in the Netherlands (2.5%) as compared to India (0.5%).

We find that the number of suspects active on the Internet and social media is lower in India for all types of offences as compared to the Netherlands. Frauds have the highest number of suspects who are active on the Internet and social media for both India (6.8%) and the Netherlands (36.7%).

Quite a lot of suspects of frauds in India (25%) are found to have a profile on social media or other online communication platforms. As mentioned earlier, a lot of the suspects in fraud cases in India were working in banks or other financial organizations. Thus, they have been found to have profiles on social media. The suspects of residential burglaries and commercial burglaries in India

Table 4.9: Internet activities of Suspects (in%)

Type of Internet activity	Residential Burglary		Commercial Burglary		Fraud	
	India	Netherlands	India	Netherlands	India	Netherlands
Aware of plunder via social media, Internet, etc.	0.0	0.0	0.0	0.0	0.5	2.5
N	203	162	74	204	196	281
Pearson Chi-Square	-		-		2.748	
Active on Internet or social media	0.5	8.6	0.0	5.9	6.8	36.7
N	203	162	74	204	196	281
Pearson Chi-Square	15.184***		4.549*		40452***	
Have profile on social media, etc.	0.0	10.5	0.0	10.3	25.3	2.8
N	203	162	74	204	196	281
Pearson Chi-Square	22.343***		8.240**		53.697***	

* p < .05 (significant).

** p < .01 (significant).

*** p < .001 (significant).

have not been found to have these profiles. It should be mentioned again that this data has been taken from the crime index maintained by the police and the absence of information about the Internet activities of the suspect may also mean that the police did not investigate about such activities.

For Dutch cases, it is found that both residential burglaries (10.5%) and commercial burglaries (10.3%) have a higher number of offenders who have a profile on social media as compared to frauds which have a very low percentage (2.8%). This is a completely opposite trend to the one found for Indian cases. It should also be noted that the information about the awareness of plunder via the Internet is not found to be statistically significant.

For frauds in India, we find that the dependence on social media is higher before (10.3%) and during (7.4%) the offence as compared to after its commission (2.3%) (Table 16, Appendix H). However, as mentioned in the table, these numbers for frauds are found to be statistically insignificant.

4.8 Digital Characteristics of Victims

Table 4.10 lists the Internet related activities of the victims of all the types of offences.

Table 4.10: Internet activities of Victims (in%)

Type of Internet activity	Residential Burglary		Commercial Burglary		Fraud	
	India	Netherlands	India	Netherlands	India	Netherlands
Active on social media	0.0	1.4	0.0	0.7	5.5	14.0
N	174	146	57	141	55	278
Pearson Chi-Square	2.399		0.406		3.063	
Active on Internet	0.0	4.1	0.0	2.8	19.7	42.8
N	174	146	57	141	61	278
Pearson Chi-Square	7.287**		1.650		11.291***	
Communicated via Internet	0.0	5.5	0.0	2.8	19.7	1.1
N	174	146	57	141	61	278
Pearson Chi-Square	9.799**		1.650		40.892***	

* p < .05 (significant).

** p < .01 (significant).

*** p < .001 (significant).

Overall, we find that a higher number of victims in the Netherlands are active on social media as compared to those in India. In both the countries, frauds have the highest number of victims who are active on social media (5.5% for India as compared to 14% in the Netherlands).

In India, we find that the victims of residential and commercial burglaries are not active on the Internet. For frauds, however, we see that there are 19.7% of the victims who are active on the Internet. This is still a much lower percentage as compared to victims of frauds in the Netherlands (42.8%). In the Netherlands, both residential (4.1%) and commercial burglary (2.8%) have a small percentage of victims who are active on the Internet.

We find that victims of frauds in India often communicate via the Internet (19.7%). This percentage is higher than fraud victims in the Netherlands. This can be explained by the fact that most fraud victims we found were high ranking officers in banks who are generally well versed with new communication technologies.

4.9 Arrest and Investigation

Our data is dependent on the data collected by the police during their investigation of the offence. In this section, we highlight some of the statistics related to investigation of the offences and apprehension of the offenders.

Table 4.11: Physical and Digital Traces and Investigation Resources (N=1124, in%)

Physical	Residential Burglary		Commercial Burglary		Fraud	
	India	Netherlands	India	Netherlands	India	Netherlands
Forensic Investigation of Crime Scene	0.0	37.7	0.0	31.4	24.0 ¹	0.4
Physical Traces of Suspect Found	0.0	43.2	0.0	41.7	0.0	8.5
Pearson Chi-Square	132.526***		53.192***		23.116***	
Digital						
	India	Netherlands	India	Netherlands	India	Netherlands
Digital Data (YouTube videos, etc.) Confiscated	0.0	2.5	0.0	0.5	0.0	5.0
Camera Images Confiscated	0.0	3.7	0.0	21.1	41.5	2.1
Phone Data Confiscated	31.5	6.2	14.9	7.8	13.4	2.8
Digital Traces of Suspect Found	0.0	3.7	0.0	1.5	16.0	24.2
Digital Investigation and Confiscation - Total	31.5	13.6	14.9	25.5	62.0	29.2
Pearson Chi-Square	16.113***		3.498		51.395***	

¹ Forensic investigation of documents was performed.

*** p < .001 (significant).

In India, we find that 95.9% of all offenders have been arrested according to the data we collected (Table 13, Appendix H). On the other hand, only 41.8% of the suspects in the Netherlands have been shown as arrested by the police. The number of arrested suspects is lowest for frauds in both India (77.4%) and the Netherlands (14.2%). It should also be noted here that all the results of table 13 of Appendix H have been found to be statistically significant.

4.9.1 Confiscation and Investigation Resources

It is important for us to try and find out the nature of the confiscations made by the police while investigating a particular offence. We are particularly interested to find out whether the police rely on digital confiscations and investigative resources. Table 4.11 lists the physical and digital traces found by the police and also the investigative resources used by them in solving the crimes.

Physical Resources

We have found an absence of forensic investigation for burglaries in India. On the other hand, the Dutch police carries out forensic examination of the scene of crime for both residential (37.7%) as well as commercial (31.4%) burglaries. For frauds in India, we found that 24% of the cases involved forensic examination of documents. This directly depends on the type of fraud that was committed. In all these cases, documents were forged and hence they had to be examined forensically by the police to ascertain their authenticity.

During our study, we have found no information about physical traces of the suspect being found by the police for the crimes in India. In the Netherlands, however, we find that quite a few cases of residential burglary (43.2%) and commercial burglary (41.7%) involve physical traces of the suspect being found by the police.

It should again be mentioned that all information was collected from crime indexes for the Indian study and information about any investigative resource has to be mentioned in the crime index for us to include it in our statistics. This information was not found to be consistent for all cases. Some cases had more information about the nature of the investigation process and resources than others.

Digital Resources

Looking at table 4.11, we find that confiscation of digital data such as YouTube videos or Internet messages is absent in Indian cases. We did not find any information about such confiscations by the Indian police. In the Netherlands, frauds (5%) have the highest number of cases where the police have confiscated digital data.

An interesting resource for investigation is confiscation of camera images and the data related to this provide some varying results for both countries. Commercial burglary in the Netherlands have the highest number of confiscation of camera images (21.1%) out of all the three crimes. This is primarily due to the camera surveillance available at most business. In the event of a burglary, the police asks for the footage from the surveillance cameras from the victim organization and uses it for the investigation. In India, however, the situation is different. We do not find any evidence of camera image confiscation being used in investigation of burglaries. The fraud cases in India have a large number of instances where camera images were confiscated (41.5%) and used by the police. This can be explained by the fact that 17.7% of frauds took place in ATMs (Table 11, Appendix H). For these offences, the camera images from the ATM have been used by the police.

A large number of both residential (31.5%) and commercial burglaries (14.9%) in India involve confiscation of phone data as compared to the Netherlands. This can be explained by the comparatively larger number of mobile phones gained in burglaries in India as compared to the Netherlands (Table 12, appendix H). When a mobile phone theft is reported, the police tries to confiscate phone data

of the stolen phone to trace the offender.

We find that frauds in both India (16%) and the Netherlands (24.2%) have the highest amount of cases where the digital traces of the suspect have been found by the police. There was no information found about digital traces in any of the burglaries studies in India.

When we look at the total amount of digital investigation resources used by the police in both countries, we find that frauds have the highest proportion in both India and the Netherlands. For Indian cases, the majority of this value is due to the large amount of confiscation of camera images in case of frauds and phone data in case of burglaries.

Comparison of Digital and Traditional Fraud

Table 4.12 shows a comparison of digital and traditional frauds in terms of physical and digital confiscations and investigative resources for both countries.

We find that 26.1% of the traditional frauds in India involved forensic examination of documents. There is no forensic investigation found for digital frauds either in India or the Netherlands.

Traditional frauds in the Netherlands (11.7%) have a higher number of cases where the physical traces of the suspect have been found by the police as compared to digital frauds (1.8%). As explained in the previous section, we did not find any information about physical traces being found in the Indian files during our study.

When it comes to digital data being confiscated, we find that only digital frauds in the Netherlands (12.6%) contain this aspect of investigation. No digital data has been confiscated for the Indian cases.

We have already mentioned that confiscation of camera images is observed to be substantially higher in Indian cases as compared to the ones in the Netherlands. Here, we see that confiscation of camera images is more common for digital frauds (57.1%) as compared to traditional frauds (34.8%) in India.

We observe that phone data confiscation is more common in digital frauds in both India and the Netherlands. Overall, Indian frauds involve a higher number of phone data confiscations as compared to the Dutch counterparts.

Digital traces of the suspect are found for digital frauds more often as compared to traditional frauds in both the countries. 35.7% of the digital frauds in India involve digital traces of the suspect being found as compared to only 8.7% for traditional frauds. Similarly, 56.8% of the Dutch fraud cases involve finding the digital traces which is much higher than traditional frauds (6.1%). Overall, the Dutch frauds have a higher number of cases where the digital traces of the suspect have been confiscated as compared to the Indian frauds.

Table 4.12: Comparing digital and traditional fraud in terms of physical and digital investigation resources (N=481, in%)

Physical	Frauds in India			Frauds in the Netherlands		
	Traditional	Digital	p-value	Traditional	Digital	p-value
Forensic Investigation of Crime Scene	26.1 ¹	0.0	*	0.6	0.0	
Physical Traces of Suspect Found	0.0	0.0		11.7	1.8	**
Digital						
Digital Data (YouTube videos, etc.) Confiscated	0.0	0.0		0.0	12.6	***
Camera Images Confiscated	34.8	57.1		3.1	0.0	
Phone Data Confiscated	10.9	14.3		1.8	3.6	
Digital Traces of Suspect Found	8.7	35.7	*	6.1	56.8	***
Digital Investigation and Confiscation - Total	47.8	92.9	**	9.8	57.7	***

¹ Forensic analysis of documents was performed.

* p < .05 (significant).

** p < .01 (significant).

*** p < .001 (significant).

If we look at the overall picture of digital investigation, we find that 92.9% of digital frauds involve a digital aspect in the investigation process. The number of traditional frauds which have a digital aspect of investigation is almost half of this number (47.8%). The gap between digital and traditional frauds is even larger in the Netherlands. 57.7% of the digital frauds involve a digital aspect of investigation whereas the corresponding number of traditional frauds is only 9.8%. We also note that frauds in India seem to have a higher number of cases where digital investigation is used as compared to the Netherlands. However, it should be mentioned that most of the total count is due to the large number of camera image confiscations and phone data confiscations in India. These two aspects heavily affect the numbers for digital investigation in India and make it much larger for frauds as compared to the Netherlands.

4.9.2 Factors Leading to Arrest of Suspects

We looked at the various investigative resources employed by the police in order to solve the cases. The motive of any investigation is to eventually arrest the suspect and put him under trial in court. For this, the police needs to gather evidence using different techniques (both digital and otherwise) as explained previously (Table 14, Appendix H).

We find that all burglary cases in India depend heavily on the statements of the victim. This is found to be an essential resource for the investigation. It should be mentioned here that the victim's statement is just one of the resources the police uses. For burglary cases, the victim provides a list (with varying degrees of accuracy) of stolen items to the police. This helps the police to look for plundered goods and also aids in the investigation, as can be seen from the table. We also find that phone data is often useful for the police to solve both residential (30%) and commercial burglary (13.9%) cases in India. This can be attributed to the number of cases where mobile phones were stolen. For burglaries in the Netherlands, it is found that a lot of suspects are caught during the act itself. We have found no information of the same happening in the Indian cases. Witness statements are also found to be a useful resource, especially for commercial burglaries, in both India (91.7%) and the Netherlands (34.9%).

Digital evidence used in solving residential burglaries is higher in India (30%) as compared to the Netherlands (6.1%). This owes exclusively to the number of phone data confiscations we have discussed earlier. For commercial burglaries, the difference in digital evidence used between the two countries is minimal. It should be noted here that the findings for commercial burglary are not found to be statistically significant.

For fraud cases as well, there are ample differences between the investigation by the police in the two countries. Indian frauds have a higher number of cases involving witness statements as well as statements of victims as compared to the Netherlands. Another observation is that the number of camera image confiscations in Indian fraud cases (47.3%) is much higher than that of the Netherlands 4.7%. Also, a large number of frauds in India involve the plunder of the offence being found by the police. This signifies that material goods are gained in quite a few frauds in India which can be later found by the police during investigation. In general, a higher number of fraud cases in India involve digital evidence as compared to the Netherlands. This gap is largely inflated due to the vast difference in the number of cases involving camera image confiscation for frauds in India.

Chapter 5

Discussion

In the previous chapter, we have discussed the results of our study in considerable detail. Now, in this chapter, we look at how our findings answer our research questions and whether the findings are consistent with the hypotheses we described in chapter two.

5.1 Digital Aspect of Crime in India

Our primary research question was to find the extent of ICT involvement in crime in India. We defined digital modus operandi by including various variables about the offence. We categorized an offence to have a digital modus operandi if unwanted information had been published online by the offender, unwanted emails were sent, a threat was sent digitally to the victim by the offender, a digital forgery or a digital burglary was committed by the offender before, during or after the offence. In this section, we summarize the findings related to digital involvement of crime in India. We focus on three aspects, namely, the offence itself, the suspects and victims and the investigation of the offence. We look for digital involvement from all these points of view.

5.1.1 Offence

In table 5.1, we list the percentage of cases of different types of offences in India which had a digital modus operandi. We find that 4.8% of all cases we studied in India had a digital aspect in the commission of the offence. It is clear from our statistics that only frauds (23.3%) had any digital characteristics out of the three offences we studied. As we can see, a very small number of residential burglaries (2.9%) in the Netherlands involve a digital aspect. We also find that a much higher number of frauds in the Netherlands (40.5%) have a digital modus operandi as compared to frauds in India (23.3%).

We have already listed the individual type of digital modus operandi followed by the offender by type of offence in the previous chapter (Table 4.5, Chapter 4). We find that digital forgery is the most common type of digital modus operandi found in India. We can also see from that table that most of

Table 5.1: Digital Modus Operandi for Crimes in India (N=291, in%)

Digital Modus Operandi by type of offence	India	Netherlands
Residential Burglary	0.0 ^{***}	2.9 ^{***}
Commercial Burglary	0.0 ^{***}	0.0 ^{***}
Fraud	23.3 ^{***}	40.5 ^{***}

^{***} p < .001 (significant).

the digital involvement was found either before or during the offences.

5.1.2 Suspects and Victims

We have observed that frauds in India have some suspects who are active on the Internet and this information has been recorded by the police and hence coded by us for our research (Table 4.9, Chapter 4). Again, we see that only frauds exhibit this characteristic out of all the three crimes. We find that hardly any offender found out about the plunder using the Internet. This can mean that the information on the Internet is not really used to identify targets for crime in India. At least, it is not mentioned by the police as being one of the sources where the offenders get their information. We found that 6.8% of the fraud suspects in India were active on social media and the Internet while as many as 25.3% had a profile on a social networking site or Skype, etc.

We also observe that the suspects mostly use social media before and during the offence (Table 16, Appendix H). However, the trends observed in that table are not statistically significant.

For victims, we find the similar situation where victims of frauds were found to be more active online as compared to other crimes. There can be two possible explanations for this. The first explanation is that the police investigated about the online activities of the victim as a digital aspect of the offence was found and recorded this information. Moreover, we also found during our research that a lot of victims of the fraud cases were employees in organizations such as banks and hence were more likely to be well versed with modern technology and the Internet. Although, we find that the use of social media is not that common for the victims in relation with the offence (Table 17, Appendix H).

5.1.3 ICT in Police Investigation

We have seen how much digital technology is influencing the offences and the victims as well as suspects. Another aspect of any crime is the investigation

performed by the police. We have seen in the previous chapter that the police have used confiscation of digital items such as camera images and phone data for their investigation (Table 4.11, Chapter 4). We again found that the police used the highest number of digital investigation resources to solve fraud cases as compared to commercial and residential burglaries. However, we do observe that a significant amount residential burglary cases involved confiscation of phone data (31.5%). This was due to the fact that a lot of the burglaries involved theft of mobile phones.

When we look at the factors leading to the arrest of the offender, we find that digital resources such as phone data, camera images, phone and Internet taps are used (Table 14, Appendix H). A significant number of offenders for both residential burglary (30%) and commercial burglary (13.9%) were apprehended with the help of phone data confiscation. 47.3% of the fraud offenders were caught with the help of confiscated camera footage. The fact that a significant number of frauds (17.7%) happened in ATMs contributes quite substantially to this number (Table 11, Appendix H).

Overall, we find that frauds involve the highest amount of ICT in both the commission of the offence as well as investigation. Even activities of suspects and victims are more dependent on ICT for fraud cases. This is congruent with our hypothesis which we mentioned in chapter 2. An unexpected observation was made regarding the use of ICT in investigation of burglaries. We found that a substantial number of burglary investigations were aided by using phone data by the police. This resulted in a larger than expected amount of ICT in police investigation of offences in India.

5.2 Comparison between India and the Netherlands

A major aim of this research was to compare and contrast different aspects of crime between India and the Netherlands. We summarize the comparison in different characteristics of the crimes between these two countries in this section. First, we focus on the digital aspect of crime and then move on to some other general differences.

5.2.1 Digital Aspect of Crime

When we compare India and the Netherlands in terms of digital modus operandi, we find that the Netherlands is ahead of India for all three types of offences (Table 4.5, Chapter 4). Digital characteristics of residential and commercial burglaries are minimal in both countries and frauds show the highest amount of digital dependence in both India and the Netherlands.

One interesting observation about the offences is regarding the plunder. A higher percentage of cases in India involve misappropriation of mobile phones as compared to the Netherlands (Table 12, Appendix H). We also find that

for commercial burglaries and frauds, the number of cases which involve gaining of electronic devices by the offender is higher in India as compared to the Netherlands. Thus, overall, it is not inaccurate to conclude that Indian offences involve more digital devices being gained by the offender as compared to the Netherlands.

We found that no burglaries in either country was committed on the Internet (Table 11, Appendix H). A much higher number of Dutch frauds (33%) were committed on the Internet as compared to Indian frauds (8.1%). This is along expected lines due to the difference in Internet penetration between the two countries as mentioned in chapter 2.

If we look at the Internet activities of suspects, we find that the Netherlands is much ahead of India in most aspects (Table 4.9, Chapter 4). However, we do find a larger number of fraud suspects in India having a profile on social media, YouTube, Skype, etc. If we look at the usage of social media for the offence however, we find that the numbers are similar for India and the Netherlands in the case of frauds (Table 16, Appendix H). For burglaries, both residential and commercial, suspects in the Netherlands show some digital characteristics where the Indian offenders do not.

Similarly, for victims, we find that the Netherlands is ahead of India in terms of Internet activity (Table 4.10, Chapter 4). However, it is important to mention that fraud victims in India have been found to be using the Internet more than their Dutch counterparts. It should also be mentioned that information about Internet activities was available for a very limited number of victims in India. The use of social media in different stages of the offence is almost similar in both countries (Table 17, Appendix H).

If we consider the digital resources being used for investigation, we have some interesting results (Table 4.11, Chapter 4). We find two specific aspects in which India is well ahead of the Dutch cases. One of these aspects is confiscation of phone data to investigate residential burglaries. This is due to the large number of cases where mobile phones are stolen in residential burglaries in India (33.3%) as compared to the Netherlands (16.9%) as well as commercial burglaries in both countries (Table 12, Appendix H). Another digital characteristic of investigation where we have a large difference is confiscation of camera images. For commercial burglaries, Netherlands (21.1%) is way ahead of India (0%). This is mainly due to the large number of commercial burglaries happening in businesses equipped with security cameras in the Netherlands. However, this trend is completely reversed for frauds. We find that a much higher number of frauds in India (41.5%) involve confiscation of camera images as compared to the Netherlands (2.1%). This can be attributed to the fact that 17.7% of the frauds in India happened in ATMs (table 11, Appendix H). ATM vestibules typically have security cameras and this becomes a useful investigation resource for the police in such cases.

Overall, we find that crime in the Netherlands has a higher involvement of ICT as compared to India with a few notable exceptions such as investigation tools like camera image confiscation and phone data confiscation which are

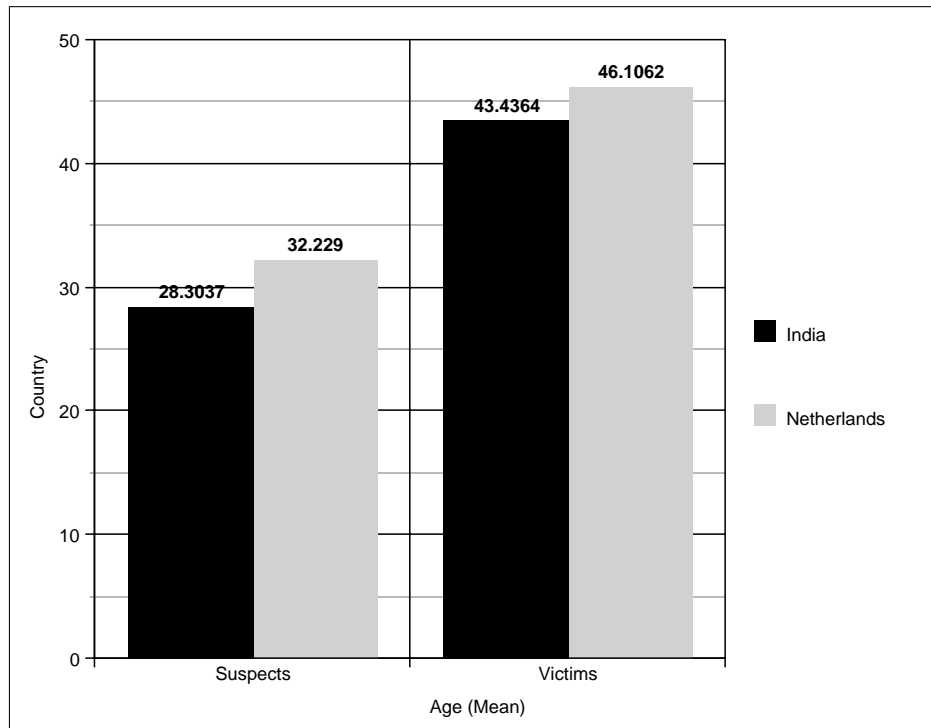


Figure 5.1: Comparing Age (mean) of Suspects and Victims

higher in India for some types of offences. Both suspects and victims in the Netherlands are found to be more active on the Internet as compared to their Indian counterparts.

5.2.2 Other Comparisons

After looking at how India and the Netherlands compare in the digital aspects of crime, here we highlight some of the differences we observed between crime in the two countries.

Age

Figure 5.1 shows the difference between the mean age of suspects and victims in both the countries. It is clear that India has a lower mean age for both suspects and victims. The mean age for suspects in India is 28.3 years while in the Netherlands it is 32.2 years. Similarly, for the victims, India has a mean age of 43.4 years whereas it is 46.1 years in the Netherlands. Thus, in both countries, we find that victims are older than the suspects. However, it should also be mentioned here that the number of victims in India for whom we had information about their age was very low ($N=55$).

This finding is consistent with our hypothesis mentioned in chapter 2. We noted earlier that the median age of India (26.7) is much lower than that of the

Netherlands (41.8). Hence, we expected both suspects and victims in India to be younger than in the Netherlands.

Gender

For both suspects (Table 3, Appendix H) and victims (Table 7, Appendix H), we find that India has a lower percentage of females for all the types of offences as compared to the Netherlands. This is also expected due to the difference in gender ratio between the two countries as mentioned earlier.

Location of Offence

A couple of interesting facts emerge when we look at the number for location where offence took place (Table 11, Appendix H). We find that as many as 66.1% of the frauds in India took place in either banks or ATMs. We did not find any of the Dutch frauds to have taken place in these locations.

Another interesting observation is that a significant amount of commercial burglaries (10.5%) took place in a place of worship in India. We did not observe this in the Netherlands. As mentioned before, this is due to the fact that temples in India store a lot of items made from precious metals and jewelery and hence become an attractive target for offenders.

We found that no burglaries were committed on the Internet in either India or the Netherlands. For frauds, the Netherlands had a higher number of cases (33%) where the offence was committed on the Internet as compared to frauds in India (8.1%).

Localization

We found that crimes in India were much more localized as compared to the Netherlands (Table 4.4, Chapter 4). This means that the radius of a criminal in which he/she can commit the offence is higher in the Netherlands as compared to India. The distance between the offender and the victim is larger in the Netherlands. We also found that a small number of Dutch crimes had an international element to them (2.8%) while this trend was absent for Indian crimes.

Our observation is that crimes in these two countries differ in many ways due to differences in digital and non-digital characteristics. Our research has enabled us to identify these differences and we have tried to highlight them in this chapter.

Chapter 6

Conclusions

Our research was aimed at understanding the extent to which Information and Communication Technologies (ICT) have permeated in the world of crime in India. Moreover, we looked at how this reliance on modern digital technology with respect to crime compares with the Netherlands.

We did not look for the digital element of crime by looking at traditional definitions of Cyber Crime described in academics or law. We attempted to define each particular offence by using our checklist (Appendix D) which contained many questions about the digital aspect of the offence as well as the offenders and the victims.

For our study, we looked at burglary (both residential and commercial) and fraud in the city of Kolkata. The data was obtained from the crime indexes maintained by the Kolkata Police with the cooperation and permission of the Kolkata Police Headquarters.

A major advantage of this research was the experience we had of working with the police in India. It was an extremely challenging task to obtain the requisite permissions for accessing their data. We started planning and discussing the project with the police authorities about 10 to 12 months before the actual data collection process began. Our experience tells us that any researcher who wishes to work with the police on similar research should devote a lot of time in preparing adequately for the project by reaching the right people and asking them for permissions. This is not trivial as the police is always busy in a country like India and is not initially inclined to entertain any requests for such studies. We spent a substantial amount of time in convincing them about our project and only after ensuring that the secrecy of their data will not be threatened did they provide us with access.

Another aspect of our research was that we always had the intention of comparing our findings with the Dutch data collected during the MO-IT project. This made it essential for us to use the same frame of reference for the offences as well the information about the cases as much as possible. Thus, we had to account for the differences in the legal systems as explained in chapter 2. These differences and challenges have resulted in some limitations of our research which

we will discuss in the following chapter.

Looking at our results, we found that ICT in crime in India is lower as compared to the Netherlands. However, the difference is perhaps not as high as we expected. We found that 10.5% of all Indian cases involved a digital modus operandi. In the Netherlands, the number is marginally higher (17.8%). In both countries, frauds contribute almost entirely to this number and burglaries have negligible digital modus operandi. In fact, we find that burglaries in India have no digital modus operandi at all while only 2.5% of residential burglaries in the Netherlands involved a digital modus operandi (Table 4.5, Chapter 4).

When we look at digital aspect of investigation, we find that 41.9% of Indian cases involved digital resources such as confiscation of camera images, digital data, digital traces of suspects, etc. Surprisingly, a lower number (24.1%) of Dutch cases involve digital resources for investigation. At first glance, this does look surprising and contrary to our expectations. However, if we look a little deeper, we find that India has a higher percentage of residential burglaries (31.5%) which involve digital resources of investigation as compared to the Netherlands (13.6%). We find that phone data confiscations contribute entirely to this number (31.5%) for residential burglaries in India (Table 4.11, Chapter 4). On the other hand, residential burglaries in the Netherlands use small number of all types of digital resources for investigation. The high number of cases where confiscation of phone data is used is closely related to the fact that mobile phones are gained in one-third (33.3%) of all residential burglaries in India (Table 12, Appendix H). On the other hand, mobile phones are stolen in only 16.9% of the residential burglaries in the Netherlands. This basically explained the high number of Indian residential burglary cases where phone data confiscations are used for investigations. Similarly, if we look at frauds, we find that the number of Indian cases which involve digital investigation resources (62.1%) is more than double the number of cases in the Netherlands (29.2%). This large disparity can also be attributed to a noticeable feature of frauds in India. We find that confiscation of camera images contributes heavily (41.5%) to this high number. In comparison, only 2.1% of frauds in the Netherlands involve confiscation of camera images. This can be further explained by the fact that 66.1% of Indian frauds took place in a bank or ATM which are equipped with CCTV cameras. Footage from these cameras are generally used by the police to try and identify the suspects in the event of any crime. None of the Dutch frauds we studied occurred in banks or ATMs and hence this possibility is not present for Dutch cases. Therefore, we observe that two particular investigation resources, namely, phone data confiscation for residential burglaries and camera image confiscation for frauds, are contributing heavily to the total number of digital investigation in Indian cases and hence inflating the figures as compared to the Netherlands.

Suspects as well as victims in the Netherlands were found to be more active on the Internet as compared to those in India (Table 4.9 and Table 4.10, Chapter 4). This is along expected lines as we have already discussed the difference in Internet penetration between the two countries in chapter 2 (Appendix A). However, we find that a higher number of fraud suspects in India (25.3%) have a profile on social media as compared to fraud suspects in the Netherlands (2.8%).

This is one exceptional observation from our research. It should also be noted that information about Internet activities of suspects and victims have to be mentioned by the police in the crime index for us to record it in our research.

Another observation was that the average age of suspects and victims was lower in India as compared to the Netherlands. This is also expected as the median age in India is much lower than in the Netherlands. Also, the number of female suspects and victims was negligible in India which can be attributed to a larger disparity in the gender ratio as compared to the Netherlands.

We also found that the crimes in India were much more localized and a higher number of cases there involved the suspect and victim to be in geographical proximity as compared to the Netherlands. In both countries, we found that offences with digital characteristics were more likely to have a larger distance between the suspect and the victim.

Overall, we can conclude that crime in India differs from the Netherlands in terms of both digital and non-digital factors. Our research sheds light on some of these differences and it also helps us understand the role which ICT plays in crime in India. However, our findings need to be assimilated in the backdrop of some limitations which arise due to the complex nature of our methodology and research environment. We end our report by enlisting these limitations in some detail in the final chapter.

Chapter 7

Limitations

We end our report by mentioning some of the limitations of this research. It is important for us to explain these limitations so that the readers can understand the findings of our research in the proper context.

Source of Data

As we have explained in previous chapters, the source of our data is the crime indexes maintained by the concerned department (burglary and fraud) of the Kolkata Police headquarters. This introduces the greatest limitation to our research. Our study is totally dependent on the information documented by the police in these indexes and we have to complete our checklist using this information. In many cases, we found the description of the offence and/or the information about suspect and victim to be minimal. Specifically, the information about victims was found to be very less in most cases. For instance, the police have not recorded the online activities of victims in a lot of cases and this information is missing from our data. Information about the age of victims is also missing for a lot of cases. These gaps significantly impact our results and we have mentioned the total number of cases (N-value) which had legitimate values for the variables used in each table we have presented in the report. This gives the readers an idea of the sample size for each analysis and hence it can be put into proper context.

Another important aspect to remember is that most of the qualitative information for our study was found from the description of offence written in the crime indexes. These were written by the investigating officer of each particular case and the style of writing varies for different officers. The description does not follow a strict format for all cases. We have tried to use all the information we found in the crime indexes to describe each offence in our research and use that information for our analysis.

The original case files could not be obtained for the Indian part of the study as the majority of cases from the last three years (2010, 2011 and 2012), which was the scope of our study, are still in court. The judicial process in India is quite slow and once a case is in court, the files related to the case are not allowed

to be accessed by any external person except for the police, lawyers associated with the case and the court itself. We convinced the Kolkata Police to help us with the research but they were only legally able to grant us access to the case indexes and hence that became the source of our data.

For the Dutch study, original case files were studied. It is expected that the crime indexes accessed for the Indian study do not contain the same level of detail as the case files used in the Netherlands. As we have compared our findings, there is potentially an asymmetry of information in the comparison. We have tried to minimize this problem by filtering some data from the Dutch cases while comparing the results. This limitation manifests itself greatly when we analyze the results related to characteristics of victims. We see that there is a large disparity in the number of cases for which victim information is available between both countries. More specifically, for Indian cases, we found a lot of basic information such as the victim's age, employment, education, etc., to be missing while for most Dutch cases this information was present. We have indicated the number of cases with eligible values for a particular variable in all the tables we have displayed in the text as well as Appendix H in order to give the reader an idea about the difference in size of the available sample for each variable.

Lack of Randomness in Selecting Cases

Our entire research was in collaboration with the Kolkata Police headquarters and we used only their case indexes. This is not a police station in itself but actually receives cases from all local police stations in the metropolitan area of Kolkata. However, we were not able to make a random selection of the cases. We considered all the cases from the case index of the particular years (2010 - 2012 for frauds and 2011 - 2012 for burglaries) and considered all of them for our research.

The Kolkata Police headquarters is at the very top of the Kolkata Police hierarchy and receives cases from local police stations in different scenarios. The first scenario is if the local police station is not able to solve the case, it hands it over to the headquarters. Secondly, all sensitive cases (politically or otherwise) are handed over to the headquarters directly. These aspects suggest that our selection of cases may not be an accurate sampling of the crime of the entire city.

It is possible that the cases selected by the police have a certain degree of bias, admittedly unintentional, due to some situational factors [33]. It is widely accepted that the arrest practices of the police are dependent on certain extraneous factors, often beyond the context of the offences themselves. As our only source of data is the police, there is a strong possibility of it being biased. Selection bias is one of the major issues which influence the quality of cross-national research [12]. However, in our study, this is an unavoidable reality.

We had earlier contacted the Criminal Investigation Department (CID) of the state of West Bengal for cooperation in our research. However, they declared themselves unable to provide a sufficient number of cases and hence we

went on to work with the Kolkata Police. Working with the CID would have enabled us to sample cases from across the state of West Bengal which would have been a wider selection as compared to our current data.

Limited Area

Our research only focuses on crime in Kolkata. We have already seen in chapter 3 how the city of Kolkata compares with the rest of the country in terms of crimes and specifically in terms of the crimes we studied. Nevertheless, our research does not present a picture of the national situation and the results may not be necessarily extrapolated to the rest of the country.

The study focuses primarily on the digital aspect of crime. Use of digital technology is not consistent throughout a large country like India. There are many regional disparities and it would be extremely worthwhile to conduct a similar research in another city or region within the country to compare the findings. It will be interesting to find differences in all aspects including suspect characteristics, nature of commitment of offences, victim characteristics as well as police procedures.

Choice of Crimes

We studied only burglary (residential and commercial) and frauds and analyzed the digital aspect in these crimes in India. It may also be a good idea to perform similar studies for different offences to truly understand the effect of ICT on crime as whole.

As we have already stated earlier in our report, we were unable to include threats for our study in India as they are a non-cognizable offence in India and the police does not record information about them unless they are part of a larger conspiracy such as extortion, etc. As a result, we were unable to compare the findings of the Dutch threat cases with those in India.

Despite these considerable limitations, our research provides an insight into the use of digital technology in crime and investigation in an Indian environment. Moreover, we also compare our findings with that of the MO-IT study performed in the Netherlands and find some interesting differences. A follow-up study with a larger sample encompassing larger area in India would be extremely desirable in order to test our findings. We feel that any future research along this line will find our work to be a useful starting point.

Bibliography

- [1] Albanese and Jay S. “The Causes of Organized Crime Do Criminals Organize Around Opportunities for Crime or Do Criminal Opportunities Create New Offenders?” In: *Journal of Contemporary Criminal Justice* 16.4 (2000), pp. 409–423.
- [2] David Budgen and Pearl Brereton. “Performing systematic literature reviews in software engineering”. In: *Proceedings of the 28th international conference on Software engineering*. ACM. 2006, pp. 1051–1052.
- [3] K Chockalingham. “Criminal victimization in four major cities in Southern India”. In: *Forum on Crime and Society*. Vol. 3. 1-2. United Nations. 2003, pp. 117–126.
- [4] Ronald V Clarke. “Technology, criminology and crime science”. In: *European Journal on Criminal Policy and Research* 10.1 (2004), pp. 55–63.
- [5] Indian Law Commission. *Indian Penal Code*. The Lawbook Exchange, Ltd., 1838.
- [6] Derek B Cornish and Ronald V Clarke. “2. The rational choice perspective”. In: *Environmental criminology and crime analysis* (2008), p. 21.
- [7] Edwardes and Stephen Meredyth. *Crime in India*. Oxford university press, 1924.
- [8] Denise Gürer and Tracy Camp. “An ACM-W literature review on women in computing”. In: *ACM SIGCSE Bulletin* 34.2 (2002), pp. 121–127.
- [9] Debarati Halder and K Jaishankar. “Cyber crimes against women in India: Problems, perspectives and solutions”. In: *TMC Academic Journal* 3.1 (2008), pp. 48–62.
- [10] Debarati Halder and K Jaishankar. “Cyber Victimization in India: A Baseline Survey Report (2010)”. In: *Available at SSRN 1759708* (2010).
- [11] P. H. Hartel, M. Junger, and R. J. Wieringa. *Cyber-crime Science = Crime Science + Information Security*. Technical Report TR-CTIT-10-34. Enschede: Centre for Telematics and Information Technology University of Twente, 2010.
- [12] Simon Hug. “Selection bias in comparative research: The case of incomplete data sets”. In: *Political Analysis* 11.3 (2003), pp. 255–274.
- [13] Renée Colette Hulst and Rudolf Johannes Maria Neve. *High-tech crime, soorten criminaliteit en hun daders: een literatuurinventarisatie*. Wetenschappelijk Onderzoek-en Documentatiecentrum [host], 2008.

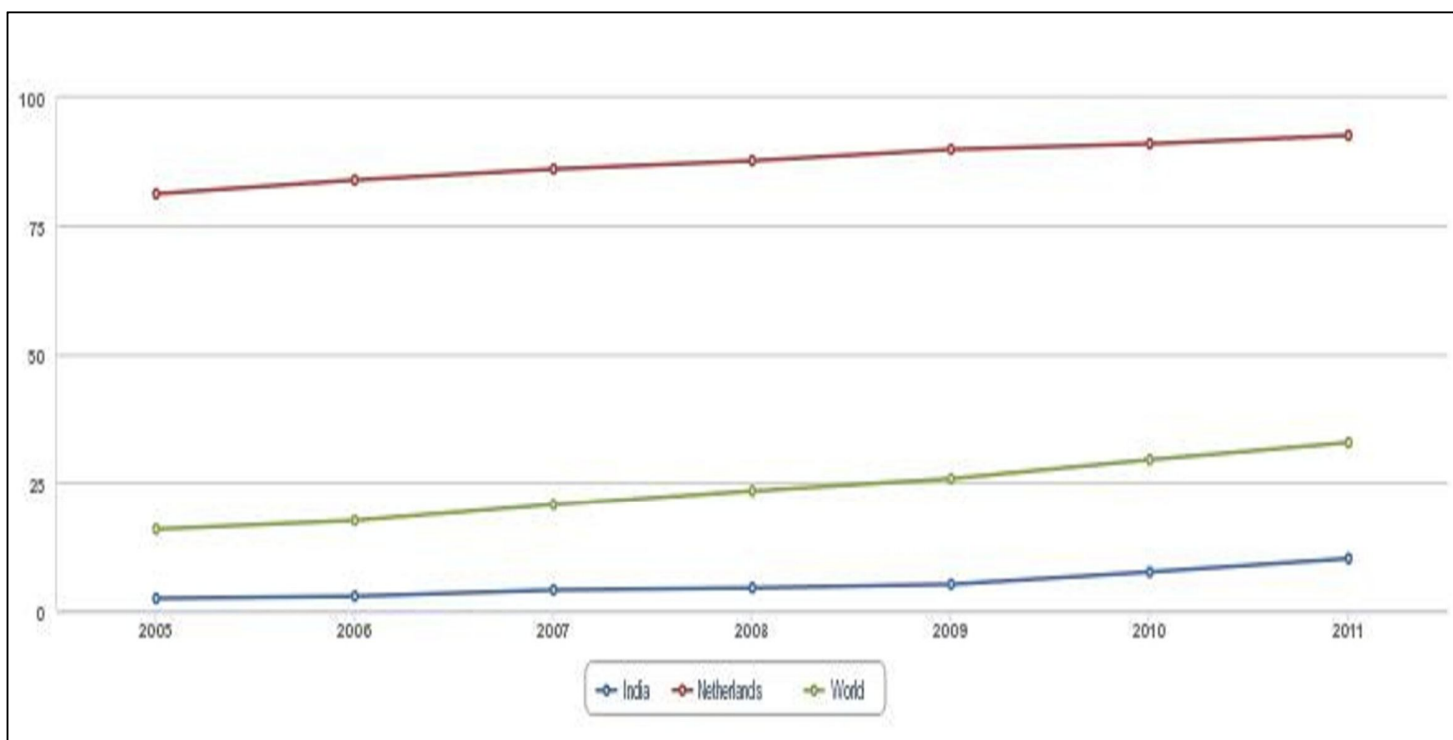
- [14] Karuppannan Jaishankar. "Establishing a Theory of Cyber Crimes". In: *International Journal of Cyber Criminology* 1.2 (2007), pp. 7–9.
- [15] J. Jansen, M. Junger, A. L. Montoya Morales, and P. H. Hartel. "Offenders in a digitized society". In: *Cybercrime and the police*. Ed. by W. P. Stol and J. Jansen. Safety & Security Studies. The Hague, The Netherlands: Eleven International Publishing, 2013, pp. 45–59.
- [16] Noel Klima and Belinda Wijckmans. "European cross-country crime statistics, surveys and reports". In: *European Crime Prevention Monitor* 1 (2012).
- [17] K Krishnamurthi. *Police Diaries, Statements, Reports, Investigation and Arrest*. Law Book Company, 1963.
- [18] M Vijaya Kumar and C Chandrasekar. "Spatial-Temporal Analysis of Residential Burglary Repeat Victimization: Case Study of Chennai City Promoters Apartments, INDIA". In: *International Journal of computer Technology and Applications* 2 (2011).
- [19] Manoj Kumar and Anuj Rani. "Computer crime IT laws in Ireland and India".
- [20] Surender Kumar and Sudesh Kumar. "Does modernization improve performance: evidence from Indian police". In: *European Journal of Law and Economics* (2013), pp. 1–21.
- [21] Harjinder Singh Lallie. "An overview of the digital forensic investigation infrastructure of India". In: *Digital Investigation* 9.1 (2012), pp. 3–7.
- [22] Rutger Leukfeldt, Sander Veenstra, and Wouter Stol. "High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands". In: *International Journal of Cyber Criminology* 7.1 (2013).
- [23] Gerrit Meijer, Y Th Sjoerd, et al. "Influence of the Code Civil in the Netherlands". In: *European journal of law and economics* 14.3 (2002), pp. 227–236.
- [24] A. L. Montoya Morales, M. Junger, and P. H. Hartel. "How 'Digital' is Traditional Crime?" In: *European Intelligence and Security Informatics Conference, EISIC 2013, Uppsala, Sweden*. Uppsala, Sweden: IEEE Computer Society, 2013.
- [25] NS Nappinai. "Cyber crime law in india: Has law kept pace with emerging trends? an empirical study". In: *Journal of International Commercial Law and Technology* 5.1 (2009), pp. 22–28.
- [26] Graeme R Newman. "Cybercrime". In: *Handbook on Crime and Deviance*. Springer, 2009, pp. 551–584.
- [27] Sudershan Pasupuleti, Eric G Lambert, Shanhe Jiang, Jagadish V Bhimarasetty, and K Jaishankar. "Crime, Criminals, Treatment, and Punishment An Exploratory Study of Views Among College Students in India and the United States". In: *Journal of Contemporary Criminal Justice* 25.2 (2009), pp. 131–147.
- [28] Am Psychol. "Reporting Standards for Research in Psychology". In: *Am Psychol* 63.9 (2008), pp. 839–851.

- [29] Nadia Qureshi, Muhammad Usman, and Naveed Ikram. “Evidence in software architecture, a systematic literature review”. In: *Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering*. ACM. 2013, pp. 97–106.
- [30] Nimmi Rangaswamy. “Regulating Indias Digital Public Cultures: A Grey or Differently Regulated Area”. In: *Usability and Internationalization. Global and Local User Interfaces*. Springer, 2007, pp. 183–192.
- [31] Rebecca Rees, Kathryn Oliver, Jenny Woodman, and James Thomas. “The views of young children in the UK about obesity, body size, shape and weight: a systematic review”. In: *BMC public health* 11.1 (2011), p. 188.
- [32] Mark Shaw, Jan Van Dijk, and Wolfgang Rhomberg. “Determining trends in global crime and justice: An overview of results from the United Nations surveys of crime trends and operations of criminal justice systems”. In: *Forum on crime and society*. Vol. 3. 1. United Nations. 2003, p. 2.
- [33] Douglas A Smith and Christy A Visher. “Street-level justice: Situational determinants of police arrest decisions”. In: *Social Problems* (1981), pp. 167–177.
- [34] S Tamilarasi. “Forensic Investigative Methodologies for Digital Crime”. In: *International Journal of Computer Science & Applications (TIJCSA)* 2.03 (2013).
- [35] Pierre Tremblay, Bernard Talon, and Doug Hurley. “Body switching and related adaptations in the resale of stolen vehicles. Script elaborations and aggregate crime learning curves”. In: *British Journal of Criminology* 41.4 (2001), pp. 561–579.
- [36] Alfred Vagts and Detlev F Vagts. “The balance of power in international law: A history of an idea”. In: *The American Journal of International Law* 73.4 (1979), pp. 555–580.
- [37] Lalit Wadhwa and Virender Pal. “Forensic Accounting And Fraud Examination In India”. In: *International Journal of Applied Engineering Research* 7.11 (2012).
- [38] Harshad S Wadkar, Makarand R Velankar, and Praful D Meshram. “A survey paper on Cyber crimes, Cyber Laws in India”. In: *International Journal of Advances in Computing and Information Researches* 1.2 (2012), pp. 24–28.
- [39] Jennifer Hardison Walters, Andrew Moore, M Stat, Marcus Berzofsky, and Lynn Langton. *Household Burglary, 1994-2011*. Tech. rep. U.S Department of Justice, 2013.

Appendix A

Internet users per 100 people (Netherlands vs India)

	2005	2006	2007	2008	2009	2010	2011
India	2.4	2.8	4.0	4.4	5.1	7.5	10.1
Netherlands	81.0	83.7	85.8	87.4	89.6	90.7	92.3
World	15.8	17.5	20.6	23.3	25.7	29.4	32.7

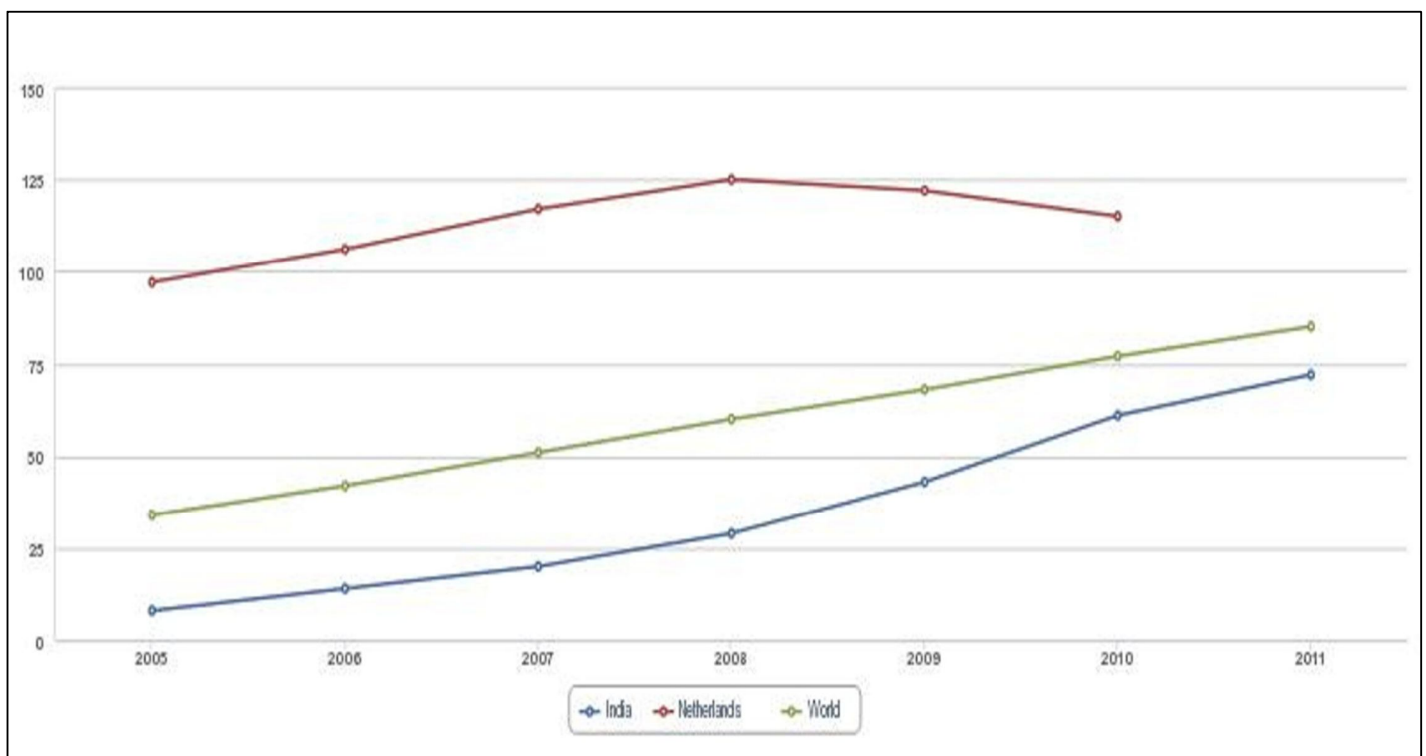


Online reference - <http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/IN-NL?display=graph>

Appendix B

Mobile connection per 100 people (Netherlands vs India)

	2005	2006	2007	2008	2009	2010	2011
India	8	14	20	29	43	61	72
Netherlands	97	106	117	125	122	115	..
World	34	42	51	60	68	77	85



Online reference - <http://data.worldbank.org/indicator/IT.CEL.SETS.P2/countries/IN-NL?display=graph>

Appendix C

Relevant Sections of the Indian Penal Code (IPC)

22. "Movable property".--The words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.

23.

"Wrongful gain".

23. "Wrongful gain".--"Wrongful gain" is gain by unlawful means of property to which the person gaining is not legally entitled.

"Wrongful loss".

"Wrongful loss".--"Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled.

Gaining wrongfully. Losing wrongfully.

Gaining wrongfully. Losing wrongfully.--A person is said to gain wrongfully when such person retains wrongfully, as well as when such person acquires wrongfully. A person is said to lose wrongfully when such person is wrongfully kept out of any property, as well as when such person is wrongfully deprived of property.

24.

"Dishonestly".

24. "Dishonestly".--Whoever does anything with the intention of causing wrongful gain to one person or wrongful loss to another person, is said to do that thing "dishonestly".

25.

"Fraudulently".

25. "Fraudulently".--A person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.

1. Ins. by Act 39 of 1920, s. 2.

2. Subs. by Act 40 of 1964, s. 2, for cl. Twelfth, ins. by Act 2 of 1958, s. 2.

3. Ins. by Act 39 of 1920, s. 2.

4. Explanation 4 ins. by Act 2 of 1958, s. 2, omitted by Act 40 of

1964, s. 2.

106

26.

"Reason to believe".

26. "Reason to believe".--A person is said to have "reason to believe" a thing, if he has sufficient cause to believe that thing but not otherwise.

27.

Property in possession of wife, clerk or servant.

27. Property in possession of wife, clerk or servant.--When property is in the possession of a person's wife, clerk or servant, on account of that person, it is in that person's possession within the meaning of this Code.

Explanation.--A person employed temporarily or on a particular occasion in the capacity of a clerk, or servant, is a clerk or servant within the meaning of this section.

28.

"Counterfeit".

28. "Counterfeit".--A person is said to "counterfeit" who causes one thing to resemble another thing, intending by means of that resemblance to practise deception, or knowing it to be likely that deception will thereby be practised.

1*[Explanation 1.--It is not essential to counterfeiting that the imitation should be exact.

Explanation 2.--When a person causes one thing to resemble another thing, and the resemblance is such that a person might be deceived thereby, it shall be presumed, until the contrary is proved, that the person so causing the one thing to resemble the other thing intended by means of that resemblance to practise deception or knew it to be likely that deception would thereby be practised.]

29.

"Document".

29. "Document".--The word "document" denotes any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may

Explanation 2.-The expression "women's or children's institution" shall have the same meaning as in Explanation 2 to sub-section (2) of section 376.

376D.

Intercourse by any member of the management or staff of a hospital with any woman in that hospital.

376D. Intercourse by any member of the management or staff of a hospital with any woman in that hospital.--Whoever, being on the management of a hospital or being on the staff of a hospital takes advantage of his position and has sexual intercourse with any woman in that hospital, such sexual intercourse not amounting to the offence of rape, shall be punished with imprisonment of either description for a term which may extend to five years and shall also be liable to fine.

Explanation.-The expression "hospital" shall have the same meaning as in Explanation 3 to sub-section (2) of section 376.]

Of unnatural offences

377.

Unnatural offences.

377. Unnatural offences.--Whoever voluntarily has carnal intercourse against the order of nature with any man, woman or animal, shall be punished with 1*[imprisonment for life], or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

Explanation.-Penetration is sufficient to constitute the carnal intercourse necessary to the offence described in this section.

CHAPTER XVII

OF OFFENCES AGAINST PROPERTY

CHAPTER XVII

OF OFFENCES AGAINST PROPERTY

Of theft

378.

Theft.

378. Theft.--Whoever, intending to take dishonestly any movable

property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft.

Explanation 1.-A thing so long as it is attached to the earth, not being movable property, is not the subject of theft; but it becomes capable of being the subject of theft as soon as it is severed from the earth.

1. Subs, by Act 26 of 1955, s. 117 and Sch., for "transportation for life".

187

Explanation 2.-A moving effected by the same act which effects the severance may be a theft.

Explanation 3.-A person is said to cause a thing to move by removing an obstacle which prevented it from moving or by separating it from any other thing, as well as by actually moving it.

Explanation 4.-A person, who by any means causes an animal to move, is said to move that animal, and to move everything which, in consequence of the motion so caused, is moved by that animal.

Explanation 5.-The consent mentioned in the definition may be express or implied, and may be given either by the person in possession, or by any person having for that purpose authority either express or implied.

Illustrations

(a) A cuts down a tree on Z's ground, with the intention of dishonestly taking the tree out of Z's possession without Z's consent. Here, as soon as A has severed the tree in order to such taking, he has committed theft.

(b) A puts a bait for dogs in his pocket, and thus induces Z's dog to follow it. Here, if A's intention be dishonestly to take the dog out of Z's possession without Z's consent, A has committed theft as soon as Z's dog has begun to follow A.

(c) A meets a bullock carrying a box of treasure. He drives the bullock in a certain direction, in order that he may dishonestly take the treasure. As soon as the bullock begins to move, A has committed theft of the treasure.

(d) A being Z's servant, and entrusted by Z with the care of Z's plate, dishonestly runs away with the plate, without Z's consent. A has committed theft.

(e) Z, going on a journey, entrusts his plate to A, the keeper of a warehouse, till Z shall return. A carries the plate to a goldsmith and sells it. Here the plate was not in Z's possession. It could not therefore be taken out of Z's possession, and A has not committed theft, though he may have committed criminal breach of trust.

(f) A finds a ring belonging to Z on a table in the house which Z occupies. Here the ring is in Z's possession, and if A dishonestly removes it, A commits theft.

(g) A finds a ring lying on the high-road, not in the possession

of any person. A, by taking it, commits no theft, though he may commit criminal misappropriation of property.

(h) A sees a ring belonging to Z lying on a table in Z's house. Not venturing to misappropriate the ring immediately for fear of search and detection, A hides the ring in a place where it is highly improbable that it will ever be found by Z, with the intention of taking the ring from the hiding place and selling it when the loss is forgotten. Here A, at the time of first moving the ring, commits theft.

(i) A delivers his watch to Z, a jeweller, to be regulated. Z carries it to his shop. A, not owing to the jeweller any debt for which the jeweller might lawfully detain the watch as a security, enters the shop openly, takes his watch by force out of Z's hand, and carries it away. Here A, though he may have committed criminal trespass and assault, has not committed theft, inasmuch as what he did was not done dishonestly.

188

(j) If A owes money to Z for repairing the watch, and if Z retains the watch lawfully as a security for the debt, and A takes the watch out of Z's possession, with the intention of depriving Z of the property as a security for his debt, he commits theft, inasmuch as he takes it dishonestly.

(k) Again, if A, having pawned his watch to Z, takes it out of Z's possession without Z's consent, not having paid what he borrowed on the watch, he commits theft, though the watch is his own property inasmuch as he takes it dishonestly.

(l) A takes an article belonging to Z out of Z's possession without Z's consent, with the intention of keeping it until he obtains money from Z as a reward for its restoration. Here A takes dishonestly; A has therefor committed theft.

(m) A, being on friendly terms with Z, goes into Z's library in Z's absence, and takes away a book without Z's express consent for the purpose merely of reading it, and with the intention of returning it. Here, it is probable that A may have conceived that he had Z's implied consent to use Z's book. If this was A's impression, A has not committed theft.

(n) A asks charity from Z's wife. She gives A money, food and clothes, which A knows to belong to Z her husband. Here it is probable that A may conceive that Z's wife is authorized to give away alms. If this was A's impression, A has not committed theft.

(o) A is the paramour of Z's wife. She gives a valuable property, which A knows to belong to her husband Z, and to be such property as she has not authority from Z to give. If A takes the property dishonestly, he commits theft.

(p) A, in good faith, believing property belonging to Z to be A's own property, takes that property out of B's possession. Here, as A does not take dishonestly, he does not commit theft.

379.

Punishment for theft.

379. Punishment for theft.--Whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

380.

Theft in dwelling house, etc.

380. Theft in dwelling house, etc.--Whoever commits theft in any building, tent or vessel, which building, tent or vessel is used as a human dwelling, or used for the custody of property, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

381.

Theft by clerk or servant of property in possession of master.

381. Theft by clerk or servant of property in possession of master.--Whoever, being a clerk or servant, or being employed in the capacity of a clerk or servant, commits theft in respect of any property in the possession of his master or employer, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

382.

Theft after preparation made for causing death, hurt or restraint in order to the committing of the theft.

382. Theft after preparation made for causing death, hurt or restraint in order to the committing of the theft.--Whoever commits theft, having made preparation for causing death, or hurt, or restraint, or fear of death, or of hurt, or of restraint, to any person, in order to the committing of such theft, or in order to the effecting of his escape after the committing of such theft or in order to the retaining of property taken by such theft, shall be punished with rigorous imprisonment for a term which may extend to ten years, and shall also be liable to fine.

Illustrations

(a) A commits theft on property in Z's possession; and, while committing this theft, he has a loaded pistol under his garment, having provided this pistol for the purpose of hurting Z in case Z should resist. A has committed the offence defined in this section.

189

(b) A picks Z's pocket, having posted several of his companions near him, in order that they may restrain Z, if Z should perceive what is passing and should resist, or should attempt to apprehend A. A has

this section.

(c) A finds a cheque payable to bearer. He can form no conjecture as to the person who has lost the cheque. But the name of the person, who has drawn the cheque, appears. A knows that this person can direct him to the person in whose favour the cheque was drawn. A appropriates the cheque without attempting to discover the owner. He is guilty of an offence under this section.

193

(d) A sees Z drop his purse with money in it. A pick up the purse with the intention of restoring it to Z, bu afterwards appropriates it to his own use. A has committed an offence under this section.

(e) A finds a purse with money, not knowing to whom it belongs; he afterwards discovers that it belongs to Z, and appropriates it to his own use. A is guilty of an offence under this section.

(f) A finds a valuable ring, not knowing to whom it belongs. A sells it immediately without attempting to discover the owner. A is guilty of an offence under this section.

404.

Dishonest misappropriation of property possessed by deceased person at the time of his death.

404. Dishonest misappropriation of property possessed by deceased person at the time of his death.--Whoever dishonestly misappropriates or converts to his own use property, knowing that such property was in the possession of a deceased person at the time of that person's decease, and has not since been in the possession of any person legally entitled to such possession, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine, and if the offender at the time of such person's decease was employed by him as a clerk or servant, the imprisonment may extend to seven years.

Illustration

Z dies in possession of furniture and money. His servant A, before the money comes into the possession of any person entitled to such possession, dishonestly misappropriates it. A has committed the offence defined in this section.

Of criminal breach of trust

405.

Criminal breach of trust.

405. Criminal breach of trust.--Whoever, being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law prescribing the mode in which such trust is to be

discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or wilfully suffers any other person so to do, commits "criminal breach of trust".

1*[2*[Explanation 1].-A person, being an employer 3*[of an establishment whether exempted under section 17 of the Employees' Provident Funds and Miscellaneous Provisions Act, 1952 (19 of 1952) or not] who deducts the employees' contribution from the wages payable to the employee for credit to a Provident Fund or Family Pension Fund established by any law for the time being in force, shall be deemed to have been entrusted with the amount of the contribution so deducted by him and if he makes default in the payment of such contribution to the said Fund in violation of the said law shall be deemed to have dishonestly used the amount of the said contribution in violation of a direction of law as aforesaid.]

4*[Explanation 2.-A person, being an employer, who deducts the employees contribution from the wages payable to the employee for credit to the Employees' State Insurance Fund held and administered by the Employees' State Insurance Corporation established under the Employees' State Insurance Act, 1948 (34 of 1948), shall be deemed to have been entrusted with the amount of the contribution so deducted by him and if he makes default in the payment of such contribution to the

-
1. Ins. by Act 40 of 1973, s. 9 (w.e.f. 1-11-1973).
 2. Explanation renumbered as Explanation 1 by Act 38 of 1975, s. 9 (w.e.f. 1-9-1975).
 3. Ins. by Act 33 of 1988, s. 27 (w.e.f. 1-8-1988).
 4. Ins. by Act 38 of 1975, s. 9 (w.e.f. 1-9-1975).
-

194

said Fund in violation of the said Act, shall be deemed to have dishonestly used the amount of the said contribution in violation of a direction of law as aforesaid.]

Illustrations

(a) A, being executor to the will of a deceased person, dishonestly disobeys the law which directs him to divide the effects according to the will, and appropriates them to his own use. A has committed criminal breach of trust.

(b) A is a warehouse-keeper, Z, going on a journey, entrusts his furniture to A, under a contract that it shall be returned on payment of a stipulated sum for warehouse-room. A dishonestly sells the goods. A has committed criminal breach of trust.

(c) A, residing in Calcutta, is agent for Z, residing at Delhi. There is an express or implied contract between A and Z, that all sums remitted by Z to A shall be invested by A, according to Z's direction. Z remits a lakh of rupees to A, with directions to A to invest the same in Company's paper. A dishonestly disobeys the directions and employs the money in his own business. A has committed criminal breach of trust.

(d) But if A, in the last illustration, not dishonestly but in good faith, believing that it will be more for Z's advantage to hold shares in the Bank of Bengal, disobeys Z's directions, and buys shares in the Bank of Bengal, for Z, instead of buying Company's paper, here, thought Z should suffer loss, and should be entitled to bring a civil action against A, on account of that loss, yet A, not having acted

dishonestly, has not committed criminal breach of trust.

(e) A, a revenue-officer, is entrusted with public money and is either directed by law, or bound by a contract, express or implied, with the Government, to pay into a certain treasury all the public money which he holds. A dishonestly appropriates the money. A has committed criminal breach of trust.

(f) A, a carrier, is entrusted by Z with property to be carried by land or by water. A dishonestly misappropriates the property. A has committed criminal breach of trust.

406.

Punishment for criminal breach of trust.

406. Punishment for criminal breach of trust.--Whoever commits criminal breach of trust shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

407.

Criminal breach of trust by carrier, etc.

407. Criminal breach of trust by carrier, etc.--Whoever, being entrusted with property as a carrier, wharfinger or warehouse-keeper, commits criminal breach of trust, in respect of such property, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

408.

Criminal breach of trust by clerk or servant.

408. Criminal breach of trust by clerk or servant.--Whoever, being a clerk or servant or employed as a clerk or servant, and being in any manner entrusted in such capacity with property, or with any dominion over property, commits criminal breach of trust in respect of that property, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

409.

Criminal breach of trust by public servant, or by banker, merchant or agent.

409. Criminal breach of trust by public servant, or by banker, merchant or agent.--Whoever, being in any manner entrusted with property, or with any dominion over property in his capacity of a

public servant or in the way of his business as a banker, merchant, factor, broker, attorney or agent, commits criminal breach of trust in respect of that property, shall be punished with 1*[imprisonment for life], or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

1. Subs. by Act 26 of 1955, s. 117 and Sch., for "transportation for life".

195

OF THE RECEIVING OF STOLEN PROPERTY

410.

Stolen property.

410. Stolen property.--Property, the possession whereof has been transferred by theft, or by extortion, or by robbery, and property which has been criminally misappropriated or in respect of which 1***criminal breach of trust has been committed, is designated as "stolen property", 2*[whether the transfer has been made, or the misappropriation or breach of trust has been committed, within or without 3*[India]]. But, if such property subsequently comes into the possession of a person legally entitled to the possession thereof, it then ceases to be stolen property.

411.

Dishonestly receiving stolen property.

411. Dishonestly receiving stolen property.--Whoever dishonestly receives or retains any stolen property, knowing or having reason to believe the same to be stolen property, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

412.

Dishonestly receiving property stolen in the commission of a dacoity.

412. Dishonestly receiving property stolen in the commission of a dacoity.--Whoever dishonestly receives or retains any stolen property, the possession whereof he knows or has reason to believe to have been transferred by the commission of dacoity, or dishonestly receives from a person, whom he knows or has reason to believe to belong or to have belonged to a gang of dacoits, property which he knows or has reason to believe to have been stolen, shall be punished with 4*[imprisonment for life], or with rigorous imprisonment for a term which may extend to ten years, and shall also be liable to fine.

413.

Habitually dealing in stolen property.

413. Habitually dealing in stolen property.--Whoever habitually receives or deals in property which he knows or has reason to believe to be stolen property, shall be punished with 4*[imprisonment for life], or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

414.

Assisting in concealment of stolen property.

414. Assisting in concealment of stolen property.--Whoever voluntarily assists in concealing or disposing of or making away with property which he knows or has reason to believe to be stolen property, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Of cheating

415.

Cheating.

415. Cheating.--Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat".

Explanation.--A dishonest concealment of facts is a deception within the meaning of this section.

Illustrations

(a) A, by falsely pretending to be in the Civil Service, intentionally deceives Z, and thus dishonestly induces Z to let him have on credit goods for which he does not mean to pay. A cheats.

-
1. The words "the" and "offence of" rep. by Act 12 of 1891, s. 2 and Sch. I and Act 8 of 1882, s. 9, respectively.
 2. Ins. by Act 8 of 1882 s. 9.
 3. Subs. by Act 3 of 1951, s. 3 and Sch., for "the States".
 4. Subs. by Act 26 of 1955, s. 117 and Sch., for "transportation for life".
-

(b) A, by putting a counterfeit mark on an article, intentionally deceives Z into a belief that this article was made by a certain

celebrated manufacturer, and thus dishonestly induces Z to buy and pay for the article. A cheats.

(c) A, by exhibiting to Z a false sample of an article intentionally deceives Z into believing that the article corresponds with the sample, and thereby dishonestly induces Z to buy and pay for the article. A cheats.

(d) A, by tendering in payment for an article a bill on a house with which A keeps no money, and by which A expects that the bill will be dishonoured, intentionally deceives Z, and thereby dishonestly induces Z to deliver the article, intending not to pay for it. A cheats

(e) A, by pledging as diamond articles which he knows are not diamonds, intentionally deceives Z, and thereby dishonestly induces Z to lend money. A cheats.

(f) A Intentionally deceives Z into a belief that A means to repay any money that Z may lend to him and thereby dishonestly induces Z to lend him money, A not intending to repay it. A cheats.

(g) A intentionally deceives Z into a belief that A means to deliver to Z a certain quantity of indigo plant which he does not intend to deliver, and thereby dishonestly induces Z to advance money upon the faith of such delivery. A cheats; but if A, at the time of obtaining the money, intends to deliver the indigo plant, and afterwards breaks his contract and does not deliver it, he does not cheat, but is liable only to a civil action for breach of contract.

(h) A intentionally deceives Z into a belief that A has performed A's part of a contract made with Z, which he has not performed, and thereby dishonestly induces Z to pay money. A cheats.

(i) A sells and conveys an estate to B. A, knowing that in consequence of such sale he has no right to the property, sells or mortgages the same to Z, without disclosing the fact of the previous sale and conveyance to B, and receives the purchase or mortgage money from Z. A cheats.

416.

Cheating by personation.

416. Cheating by personation.--A person is said to "cheat by personation" if he cheats by pretending to be some other person, or by knowingly substituting one person for or another, or representing that he or any other person is a person other than he or such other person really is.

Explanation.--The offence is committed whether the individual personated is a real or imaginary person.

Illustrations

(a) A cheats, by pretending to be a certain rich banker of the same name. A cheats by personation.

(b) A cheats by pretending to be B, a person who is deceased. A cheats by personation.

417.

Punishment for cheating.

417. Punishment for cheating.--Whoever cheats shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

197

418.

Cheating with knowledge that wrongful loss may ensue to person whose interest offender is bound to protect.

418. Cheating with knowledge that wrongful loss may ensue to person whose interest offender is bound to protect.--Whoever cheats with the knowledge that he is likely thereby to cause wrongful loss to a person whose interest in the transaction to which the cheating relates, he was bound either by law, or by legal contract, to protect, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

419.

Punishment for cheating by personation.

419. Punishment for cheating by personation.--Whoever cheats by personation shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

420.

Cheating and dishonestly inducing delivery of property.

420. Cheating and dishonestly inducing delivery of property.--Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Of fraudulent deeds and dispositions of property

421.

Dishonest or fraudulent removal or concealment of property to prevent distribution among creditors.

421. Dishonest or fraudulent removal or concealment of property to prevent distribution among creditors.--Whoever dishonestly or fraudulently removes, conceals or delivers to any person, or transfers or causes to be transferred to any person, without adequate consideration, any property, intending thereby to prevent, or knowing it to be likely that he will thereby prevent the distribution of that property according to law among his creditors or the creditors of any other person, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

422.

Dishonestly or fraudulently preventing debt being available for creditors.

422. Dishonestly or fraudulently preventing debt being available for creditors.--Whoever dishonestly or fraudulently prevents any debt or demand due to himself or to any other person from being made available according to law for payment of his debts or the debts of such other person, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

423.

Dishonest or fraudulent execution of deed of transfer containing false statement of consideration.

423. Dishonest or fraudulent execution of deed of transfer containing false statement of consideration.--Whoever dishonestly or fraudulently signs, executes or becomes a party to any deed or instrument which purports to transfer or subject to any charge any property, or any interest therein, and which contains any false statement relating to the consideration for such transfer or charge, or relating to the person or persons for whose use or benefit it is really intended to operate, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

424.

Dishonest or fraudulent removal or concealment of property.

424. Dishonest or fraudulent removal or concealment of property.--Whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with

imprisonment of either description for a term which may extend to two years, or with fine, or with both.

Of mischief

425.

Mischief.

425. Mischief.--Whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits "mischief".

198

Explanation 1.-It is not essential to the offence of mischief that the offender should intend to cause loss or damage to the owner of the property injured or destroyed. It is sufficient if he intends to cause, or knows that he is likely to cause, wrongful loss or damage to any person by injuring any property, whether it belongs to that person or not.

Explanation 2.-Mischief may be committed by an act affecting property belonging to the person who commits the act, or to that person and others jointly.

Illustrations

(a) A voluntarily burns a valuable security belonging to Z intending to cause wrongful loss to Z. A has committed mischief.

(b) A introduces water in to an ice-house belonging to Z and thus causes the ice to melt, intending wrongful loss to Z. A has committed mischief.

(c) A voluntarily throws into a river a ring belonging to Z, with the intention of there by causing wrongful loss to Z. A has committed mischief.

(d) A, knowing that his effects are about to be taken in execution in order to satisfy a debt due from him to Z, destroys those effects, with the intention of thereby preventing Z from obtaining satisfaction of the debt, and of thus causing damage to Z. A has committed mischief.

(e) A having insured a ship, voluntarily causes the same to be cast away, with the intention of causing damage to the underwriters. A has committed mischief.

(f) A causes a ship to be cast away, intending thereby to cause damage to Z who has lent money on bottomry on the ship. A has committed mischief.

(g) A, having joint property with Z in a horse, shoots the horse, intending thereby to cause wrongful loss to Z. A has committed mischief.

(h) A causes cattle to enter upon a field belonging to Z,

1. Ins. by Act 8 of 1882, s. 10
 2. Subs, by Act 26 of 1955, s. 117 and Sch, for "transportation for life".
-

200

438.

Punishment for the mischief described in section 437 committed by fire or explosive substance.

438. Punishment for the mischief described in section 437 committed by fire or explosive substance.--Whoever commits, or attempts to commit, by fire or any explosive substance, such mischief as is described in the last preceding section. shall be punished with 1*[imprisonment for life]. or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

439.

Punishment for intentionally running vessel aground or ashore with intent to commit theft, etc.

439. Punishment for intentionally running vessel aground or ashore with intent to commit theft, etc.--Whoever intentionally runs any vessel aground or ashore, intending to commit theft of any property contained therein or to dishonestly misappropriate any such property, or with intent that such theft or misappropriation of property may be committed, shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

440.

Mischief committed after preparation made for causing death or hurt.

440. Mischief committed after preparation made for causing death or hurt.-- Whoever commits mischief, having made preparation for causing to any person death, or hurt, or wrongful restraint, or fear of death, or hurt, or of wrongful restraint, shall be punished with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.

Of criminal trespass

441.

Criminal trespass.

441. Criminal trespass.--Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property,

or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence,

is said to commit "criminal trespass".

442.

House-trespass.

442. House-trespass.--Whoever commits criminal trespass by entering into or remaining in any building, tent or vessel used as a human dwelling or any building used as a place for worship, or as a place for the custody of property, is said to commit "house-trespass".

Explanation.-The introduction of any part of the criminal trespasser's body is entering sufficient to constitute house-trespass.

443.

Lurking house-trespass.

443. Lurking house-trespass.--Whoever commits house-trespass having taken precautions to conceal such house-trespass from some person who has a right to exclude or eject the trespasser from the building, tent or vessel which is the subject of the trespass, is said to commit "lurking house-trespass".

444.

Lurking house-trespass by night.

444. Lurking house-trespass by night.--Whoever commits lurking house-trespass after sunset and before sunrise, is said to commit "lurking house-trespass by night".

445.

House-breaking.

445. House-breaking.--A person is said to commit "house-breaking" who commits house-trespass if he effects his entrance into the house or any part of it in any of the six ways hereinafter described; or if, being in the house or any part of it for the purpose of committing an offence, or having committed an offence therein, he quits the house or any part of it in any of it in such six ways, that is to say :-

First.-If he enters or quits through a passage made by himself, or by any abettor of the house-trespass, in order to the committing of the house-trespass.

1. Subs. by act. 26 of 1955, s. 117 and Sch., for "transportation for life".

201

Secondly.-If he enters or quits through any passage not intended by any person, other than himself or an abettor of the offence, for human entrance; or through any passage to which he has obtained access by scaling or climbing over any wall or building.

Thirdly.-If he enters or quits through any passage which he or any abettor of the house-trespass has opened, in order to the committing of the house-trespass by any means by which that passage was not intended by the occupier of the house to be opened.

Fourthly.-If he enters or quits by opening any lock in order to the committing of the house-trespass, or in order to the quitting of the house after a house-trespass.

Fifthly.-If he effects his entrance or departure by using criminal force or committing an assault, or by threatening any person with assault.

Sixthly.-If he enters or quits by any passage which he knows to have been fastened against such entrance or departure, and to have been unfastened by himself or by an abettor of the house-trespass.

Explanation.-Any out-house or building occupied with a house, and between which and such house there is an immediate internal communication, is part of the house within the meaning of this section.

Illustrations

(a) A commits house-trespass by making a hole through the wall of Z's house, and putting his hand through the aperture. This is house-breaking.

(b) A commits house-trespass by creeping into a ship at a port-hole between decks. This is house-breaking.

(c) A commits house-trespass by entering Z's house through a window. This is house-breaking.

(d) A commits house-trespass by entering Z's house through the door, having opened a door which was fastened. This is house-breaking.

(e) A commits house-trespass by entering Z's house through the door, having lifted a latch by putting a wire through a hole in the door. This is house-breaking.

(f) A finds the key of Z's house door, which Z had lost, and commits house trespass by entering Z's house, having opened the door with that key. This is house-breaking.

(g) Z is standing in his doorway. A forces a passage by knocking Z down, and commits house-trespass by entering the house. This is house-breaking.

(h) Z, the door-keeper of Y, is standing in Y's doorway. A commits house-trespass by entering the house, having deterred Z from opposing him by threatening to beat him. This is house-breaking.

446.

House-breaking by night.

446. House-breaking by night.--Whoever commits house-breaking after sunset and before sunrise, is said to commit "house-breaking by night".

447.

Punishment for criminal trespass.

447. Punishment for criminal trespass.--Whoever commits criminal trespass shall be punished with imprisonment of either description for a term which may extend to three months, or with fine which may extend to five hundred rupees, or with both.

448.

Punishment for house-trespass.

448. Punishment for house-trespass.--Whoever commits house-trespass shall be punished with imprisonment of either description for a term which may extend to one year, or with fine which may extend to one thousand rupees, or with both.

202

449.

House-trespass in order to commit offence punishable with death.

449. House-trespass in order to commit offence punishable with death.--Whoever commits house-trespass in order to the committing of any offence punishable with death, shall be punished with 1*[imprisonment for life], or with rigorous imprisonment for a term not exceeding ten years, and shall also be liable to fine.

450.

House-trespass in order to commit offence punishable with imprisonment for life.

450. House-trespass in order to commit offence punishable with imprisonment for life.--Whoever commits house-trespass in order to the committing of any offence punishable with 1*[imprisonment for life], shall be punished with imprisonment of either description for a term not exceeding ten years, and shall also be liable to fine.

451.

House-trespass in order to commit offence punishable with imprisonment.

451. House-trespass in order to commit offence punishable with imprisonment.--Whoever commits house-trespass in order to the committing of any offence punishable with imprisonment, shall be punished with imprisonment of either description for a term which may extend to two years, and shall also be liable to fine; and if the offence intended to be committed is theft, the term of the imprisonment may be extended to seven years.

452.

House-trespass alter preparation for hurt, assault or wrongful restraint.

452. House-trespass alter preparation for hurt, assault or wrongful restraint.--Whoever commits house-trespass, having made preparation for causing hurt to any person or for assaulting any person, or for wrongfully restraining any person, or for putting and person in fear of hurt, or of assault, or of wrongful restraint, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

453.

Punishment for lurking house-trespass or house-breaking.

453. Punishment for lurking house-trespass or house-breaking.--Whoever commits lurking house-trespass or house-breaking, shall be punished with imprisonment of either description for a term which may extend to two years, and shall also be liable to fine.

454.

Lurking house-trespass or house-breaking in order to commit offence punishable with imprisonment.

454. Lurking house-trespass or house-breaking in order to commit offence punishable with imprisonment.--Whoever commits lurking house-trespass or house-breaking, in order to the committing of any offence punishable with imprisonment, shall be punished with imprisonment of either description for a term which may extend to three years, and

shall also be liable to fine; and if the offence intended to be committed is theft, the term of the imprisonment may be extended to ten years.

455.

Lurking house-trespass or house-breaking after preparation for hurt, assault or wrongful restraint.

455. Lurking house-trespass or house-breaking after preparation for hurt, assault or wrongful restraint.--Whoever commits lurking house-trespass, or house-breaking, having made preparation for causing hurt to any person, or for assaulting any person, or for wrongfully restraining any person, or for putting any person in fear of hurt or of assault or of wrongful restraint, shall be punished with imprisonment of either description or a term which may extend to ten years, and shall also be liable to fine.

456.

Punishment for lurking house-trespass or house-breaking by night.

456. Punishment for lurking house-trespass or house-breaking by night.--Whoever commits lurking house-trespass by night, or house-breaking by night, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

457.

Lurking house-trespass or house-breaking by night in order to commit offence punishable with imprisonment.

457. Lurking house-trespass or house-breaking by night in order to commit offence punishable with imprisonment.--Whoever commits lurking house-trespass by night, or house-breaking by night in order to the committing of any offence punishable with imprisonment, shall be punished with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine; and, if the offence intended to be committed is theft, the term of the imprisonment may be extended to fourteen years.

458.

Lurking house-trespass or house-breaking by night after preparation for hurt, assault, or wrongful restraint.

458. Lurking house-trespass or house-breaking by night after preparation for hurt, assault, or wrongful restraint.--Whoever commits lurking house-trespass by night, or house-breaking by night, having made preparation for causing hurt to any person or for assaulting any

person, or for wrongfully restraining any person, or for putting any person in fear of hurt, or of assault, or of wrongful restraint, shall be punished with imprisonment of either description for a term which may extend to fourteen years, and shall also be liable to fine.

1. Subs. by Act 26 of 1955, s. 117 and Sch., for "transportation for life".

203

459.

Grievous hurt caused whilst committing lurking house-trespass or house-breaking.

459. Grievous hurt caused whilst committing lurking house-trespass or house-breaking.--Whoever, whilst committing lurking house-trespass or house-breaking, causes grievous hurt to any person or attempts to cause death or grievous hurt to any person, shall be punished with 1*[imprisonment for life], or imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

460.

All persons jointly concerned in lurking house-trespass or house-breaking by night punishable where death or grievous hurt caused by one of them.

460. All persons jointly concerned in lurking house-trespass or house-breaking by night punishable where death or grievous hurt caused by one of them.--If at the time of the committing of lurking house-trespass by night or house-breaking by night, any person guilty of such offence shall voluntarily cause or attempt to cause death or grievous hurt to any person, every person jointly concerned in committing such lurkking house-trespass by night or house-breaking by night, shall be punished with 1*[imprisonment for life], or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

461.

Dishonestly breaking open receptacle containing property.

461. Dishonestly breaking open receptacle containing property.--Whoever dishonestly or with intent to commit mischief, breaks open or unfastens any closed receptacle which contains or which he believes to contain property, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

462.

Punishment for same offence when committed by person entrusted with custody.

462. Punishment for same offence when committed by person entrusted with custody.--Whoever, being entrusted with any closed receptacle which contains or which he believes to contain property without having authority to open the same, dishonestly, or with intent to commit mischief, breaks open or unfastens that receptacle, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

CHAPTER XVIII

OF OFFENCES RELATING TO DOCUMENTS AND TO PROPERTY MARKS

CHAPTER XVIII

OF OFFENCES RELATING TO DOCUMENTS AND TO 2****PROPERTY MARKS

463.

Forgery.

463. Forgery.--Whoever makes any false document or part of a document with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

464.

Making a false document.

464. Making a false document.--A person is said to make a false document-

First.-Who dishonestly or fraudulently makes, signs, seals or executes a document or part of a document, or makes any mark denoting the execution of a document, with the intention of causing it to be believed that such document or part of a document was made, signed, sealed or executed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed or executed, or at a time at which he knows that it was not made, signed, sealed or executed; or

Secondly.-Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document in any material part thereof, after it has been made or executed either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly.-Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document, knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or the nature of the alteration.

1. Subs. by Act 26 of 1955, s. 117 and Sch., for "transportation for life".
 2. The words "Trade or" omitted by Act 43 of 1958, s. 135 and Sch. (w.e.f. 25-11-1959).
-

204

Illustrations

(a) A has a letter of credit upon B for rupees 10,000, written by Z. A, in order to defraud B, adds cipher to the 10,000, and makes the sum 1,00,000 intending that it may be believed by B that Z so wrote the letter. A has committed forgery.

(b) A without Z's authority, affixes Z's seal to a document purporting to be a conveyance of an estate from Z to A, with the intention of selling the estate to B and thereby of obtaining from B the purchase-money. A has committed forgery.

(c) A picks up a cheque on a banker signed by B, payable to bearer, but without any sum having been inserted in the cheque. A fraudulently fills up the cheque by inserting the sum of ten thousand rupees. A commits forgery.

(d) A leaves with B, his agent, a cheque on a banker, signed by A, without inserting the sum payable and authorizes B to fill up the cheque by inserting a sum not exceeding ten thousand rupees for the purpose of making certain payments. B fraudulently fills up the cheque by inserting the sum of twenty thousand rupees. B commits forgery.

(e) A draws a bill of exchange on himself in the name of B without B's authority, intending to discount it as a genuine bill with a banker and intending to take up the bill on its maturity. Here, as A draws the bill with intent to deceive the banker by leading him to suppose that he had the security of B, and thereby to discount the bill, A is guilty of forgery.

(f) Z's will contains these words-"I direct that all my remaining property be equally divided between A, B and C." A dishonestly scratches out B's name, intending that it may be believed that the whole was left to himself and C. A has committed forgery.

(g) A endorses a Government promissory note and makes it payable to Z for his order by writing on the bill the words "Pay to Z or his order" and signing the endorsement. B dishonestly erases the words "Pay to Z or his order", and thereby converts the special endorsement into a blank endorsement. B commits forgery.

(h) A sells and conveys an estate to Z. A afterwards, in order to defraud Z of his estate, executes a conveyance of the same estate to B, dated six months earlier than the date of the conveyance to Z, intending it to be believed that he had conveyed the estate to B before he conveyed it to Z. A has committed forgery.

(i) Z dictates his will to A. A intentionally writes down a

different legatee named by Z, and by representing to Z that he has prepared the will according to his instructions, induces Z to sign the will. A has committed forgery.

(j) A writes a letter and signs it with B's name without B's authority, certifying that A is a man of good character and in distressed circumstances from unforeseen misfortune, intending by means of such letter to obtain alms from Z and other persons. Here, as A made a false document in order to induce Z to part with property, A has committed forgery.

(k) A without B's authority writes a letter and signs it in B's name certifying to A's character, intending thereby to obtain employment under Z. A has committed forgery inasmuch as he intended to deceive Z by the forged certificate, and thereby to induce Z to enter into an express or implied contract for service.

205

Explanation I.-A man's signature of his own name may amount to forgery.

Illustrations

(a) A signs his own name to a bill of exchange, intending that it may be believed that the bill was drawn by another person of the same name. A has committed forgery.

(b) A writes the word "accepted" on a piece of paper and signs it with Z's name, in order that B may afterwards write on the paper a bill of exchange drawn by B upon Z, and negotiate the bills as though it had been accepted by Z. A is guilty of forgery; and if B, knowing the fact, draws the bill upon the paper pursuant to A's intention, B is also guilty of forgery.

(c) A picks up a bill of exchange payable to the order of a different person of the same name. A endorses the bill in his own name, intending to cause it to be believed that it was endorsed by the person to whose order it was payable; here A has committed forgery.

(d) A purchases an estate sold under execution of a decree against B. B, after the seizure of the estate, in collusion with Z, executes a lease of the estate to Z at a nominal rent and for a long period and dates the lease six months prior to the seizure, with intent to defraud A, and to cause it to be believed that the lease was granted before the seizure. B, though he executes the lease in his own name, commits forgery by antedating it.

(e) A, a trader, in anticipation of insolvency, lodges effects with B for A's benefit, and with intent to defraud his creditors; and in order to give a colour to the transaction, writes a promissory note binding himself to pay to B a sum for value received, and antedates the note, intending that it may be believed to have been made before A was on the point of insolvency. A has committed forgery under the first head of the definition.

Explanation 2.-The making of a false document in the name of a fictitious person, intending it to be believed that the document was made by real person, or in the name of a deceased person, intending it to be believed that the document was made by the person in his lifetime, may amount to forgery.

Illustration

A draws a bill of exchange upon a fictitious person, and fraudulently accepts the bill in the name of such fictitious person with intent to negotiate it. A commits forgery.

465.

Punishment for forgery.

465. Punishment for forgery.--Whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

466.

Forgery of record of Court or of public register, etc.

466. Forgery of record of Court or of public register, etc.--Whoever forges a document, purporting to be a record or proceeding of or in a Court of Justice, or a register of birth, baptism, marriage or burial, or a register kept by a public servant as such, or a certificate or document purporting to be made by a public servant in his official capacity, or an authority to institute or defend a suit, or to take any proceedings therein, or to confess judgment, or a power of attorney, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

206

467.

Forgery of valuable security, will, etc.

467. Forgery of valuable security, will, etc.--Whoever forges a document which purports to be a valuable security or a will, or an authority to adopt a son, or which purports to give authority to any person to make or transfer any valuable security, or to receive the principal, interest or dividends thereon, or to receive or deliver any money, movable property, or valuable security, or any document purporting to be an acquittance or receipt acknowledging the payment of money, or an acquittance or receipt for the delivery of any movable property or valuable security, shall be punished with 1 *[imprisonment for life], or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

468.

Forgery for purpose of cheating.

468. Forgery for purpose of cheating.--Whoever commits forgery, intending that the document forged shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

469.

Forgery for purpose of harming reputation.

469. Forgery for purpose of harming reputation.--Whoever commits forgery, intending that the document forged shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

470.

Forged document.

470. Forged document.--A false document made wholly or in part by forgery is designated "a forged document".

471.

Using as genuine a forged document.

471. Using as genuine a forged document.--Whoever fraudulently or dishonestly uses as genuine any document which he knows or has reason to believe to be a forged document, shall be punished in the same manner as if he had forged such document.

472.

Making or possessing counterfeit seal, etc., with intent to commit forgery punishable under section 467.

472. Making or possessing counterfeit seal, etc., with intent to commit forgery punishable under section 467.--Whoever makes or counterfeits any seal, plate or other instrument for making an impression, intending that the same shall be used for the purpose of committing any forgery which would be punishable under section 467 of this Code, or, with such intent, has in his possession any such seal, plate or other instrument, knowing the same to be counterfeit, shall be punishable with 1*[imprisonment for life], or with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

473.

Making or possessing counterfeit seal, etc., with intent to commit forgery punishable otherwise.

473. Making or possessing counterfeit seal, etc., with intent to commit forgery punishable otherwise.--Whoever makes or counterfeits any seal, plate or other instrument for making an impression, intending that the same shall be used for the purpose of committing any forgery which would be punishable under any section of this Chapter other than section 467, or, with such intent, has in his possession any such seal, plate or other instrument, knowing the same to be counterfeit, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

474.

Having possession of document described in section 466 or 467, knowing it to be forged and intending to use it genuine.

474. Having possession of document described in section 466 or 467, knowing it to be forged and intending to use it genuine.--Whoever has in his possession any document, knowing the same to be forged, and intending that the same shall fraudulently or dishonestly be used as genuine, shall, if the document is one of the description mentioned in section 466 of this Code, be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine; and if the document is one of the description mentioned in section 467, shall be punished with 1*[imprisonment for life], or with imprisonment of either description, for a term which may extend to seven years, and shall also be liable to fine.

1. Subs. by Act 26 of 1955. s. 117 and Sch., for "transportation for life".

207

475.

Counterfeiting device or mark used for authenticating documents described in section 467, or possessing counterfeit marked material.

475. Counterfeiting device or mark used for authenticating documents described in section 467, or possessing counterfeit marked material.--Whoever counterfeits upon, or in the substance of, any material, any device or mark used for the purpose of authenticating any document described in section 467 of this Code, intending that such device or mark shall be used for the purpose of giving the appearance of authenticity to any document then forged or thereafter to be forged on such material, or who, with such intent, has in his possession any material upon or in the substance of which any such device or mark has been counterfeited, shall be punished with 1*[imprisonment for life], or with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Appendix D

Checklist for Data Collection

1.	Name	Label	Choice	Notes
2.				<u>77=Something different</u> <u>88=Inapplicable</u> <u>99=Unknown</u>
3.	Time	How long did it take to fill in this coding list		
4.	General data			
5.	Name coder		1.... 2.... 3....	
6.	Date	Date of entering data by the coder		
7.	Type of offence	What was the main offence	1.Burglary of house 2.Burglary of business 3. Threat 4.Forgery	
8.	The offence			
9.	Case number			
10.	Crime scene	In what place/town did the offence took place		
11.	Kind of location	On what kind of location did the crime take place. (Where was the suspect at the time of the crime)	1.House 2.School 3.Youth club 4.On the street 5.Business 6.Internet 7.Catering facility 8.Public place 9.Sports facility	
12.	Beginning date of offence	What is the date of the beginning of the offence		
13.	Ending date of offence	What is the date of the ending of the offence	1..... 0.Ending date = beginning date	
14.	Date of cognizance	What is the date of cognizance of the offence		
15.	Police district	At what police district did the crime take place	1.... 2.... 3....	
16.	Second offence	Was there another crime committed in addition to the main offence	1.Burglary of house 2.Burglary of business 3. Threat 4.Forgery 5.No 77. Something different, being	

17.	Attempt	Was it an attempt, meaning did the criminal activity fail?	0.No 1.Yes 99.Unknown		
18.	<u>Threat</u>	Were the following threats used at this offence:			
19.		Physical threat	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
20.		Publishing information (dutch = Openbaarmaking gegevens)	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	Na het delict 0.No 1.Yes 88.Inapplicable 99.Unknown
21.		Intimidation/harassment	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	Na het delict 0.No 1.Yes 88.Inapplicable 99.Unknown
22.		Sexual verbal harassment	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	Na het delict 0.No 1.Yes 88.Inapplicable 99.Unknown
23.		Relative threatened	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
24.		Unwanted e-mails sent	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
25.		Unwanted mail sent	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
26.		Harassed by means of a formal complaint	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

27.		Racism	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
28.		Property damage	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
29.		Stalking	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
30.	Form	Was the threat digital	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
31.		Was the threat in writing	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
32.		Was the threat verbal	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
33.	<u>Forgery</u>	Kind	1.Capital 2.Identity 77.Something different, being ... 88.Inapplicable		
34.		Was the forgery digital	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
35.		Was the forgery in writing	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
36.	Kind of burglary	What was the kind of burglary that took place	1.Burglary of house 2.Burglary of business		

			88.Inapplicable		
37.		Has personal data been stolen?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
38.		Was the burglary in physical form	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
39.		Was the burglary in digital form	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
40.	Confiscation digital	Was digital data (like youtube-movies, chats, fora berichten) confiscated for research?	0.No 1.Yes 99.Unknown		
41.	Confiscation camera surveillance	Were there camera images confiscated for research of the crime	0.No 1.Yes 99.Unknown		
42.	Confiscation Phone data	Is there Phone data (like Phone locations, numbers, etc.) confiscated by the police	0.No 1.Yes 99.Unknown		
43.	Forensic investigation	Did forensic investigation take place on the crime scene	0.No 1.Yes 99.Unknown		
44.	Physical traces	Did they find physical traces of the suspect?	0.No 1.Yes 99.Unknown		
45.	Digital traces	Were digital traces of the suspect found?	0.No 1.Yes 99.Unknown		
46.	Witness	How many witness statements of the offence were taken			
47.	Arrest	Was the suspect arrested	1.Yes 99.Unknown		
48.		Did wiretaps/phone taps lead to the arrest of the suspect(s)	1.Yes 99.Unknown		
49.		Did statements of the suspect lead to the arrest of the suspect(s)	1.Yes 99.Unknown		
50.		Did statements of other suspect's lead to the arrest of the suspect(s)	1.Yes 99.Unknown		
51.		Did witness statements lead to the arrest of the suspect(s)	1.Yes 99.Unknown		
52.		Did statements of the victim(s) lead to the arrest of the suspect(s)	1.Yes 99.Unknown		

53.		Did DNA traces lead to the arrest of the suspect(s)	1.Yes 99.Unknown	
54.		Did camera footage lead to the arrest of the suspect(s)	1.Yes 99.Unknown	
55.		Did a found plunder lead to the arrest of the suspect(s)	1.Yes 99.Unknown	
56.		Did the suspect(s) get caught in the act, what lead to the arrest	1.Yes 99.Unknown	
57.		Did CIE information lead to the arrest of the suspect(s)	1.Yes 99.Unknown	CIE = Criminal Intelligence Unit
58.		Did internet taps lead to the arrest of the suspect(s)	1.Yes 99.Unknown	
59.		Did phone data lead to the arrest of the suspect(s)	1.Yes 99.Unknown	
60.		Did other elements lead to the arrest of the suspect(s)	1.Yes 99.Unknown	
61.	Plunder	Was there money gained at the offence	0.No 1.Yes 99.Unknown	
62.		Was there jewelry gained at the offence	0.No 1.Yes 99.Unknown	
63.		Were there electronics gained at the offence (except mobile phones)	0.No 1.Yes 99.Unknown	
64.		Were there mobile phones gained at the offence	0.No 1.Yes 99.Unknown	
65.		Was there valuable information gained at the offence	0.No 1.Yes 99.Unknown	
66.	Value	The total value of the plunder in Euro's		
67.	Used Language	Did the suspect(s) speak Dutch	0.No 1.Yes 88.Inapplicable 99.Unknown	
68.		Did the suspect(s) speak German	0.No 1.Yes 88.N.v.t 99.Unknown	
69.		Did the suspect(s) speak English	0.No 1.Yes 88. Inapplicable 99.Unknown	
70.		Did the suspect(s) speak French	0.No 1.Yes 88.Inapplicable 99.Unknown	
71.		Did the suspect(s) speak an East-European language	0.No 1.Yes 88.Inapplicable 99.Unknown	
72.		Did the suspect(s) speak	0.No	

		Moroccan/Turkish	1.Yes 88.Inapplicable 99.Unknown	
73.		Did the suspect(s) speak a language not mentioned before	0.No 1.Yes 88.Inapplicable 99.Unknown	
74.	Police report	Has a police report been established and sent to the Prosecutor	0.No 1.Yes 99.Unknown	
75.	Suspect(s)			
76.	Suspect(s)	How many suspect's were involved in the incident		
77.	Internet	How many suspect's were active on the internet		
78.	Suspect 1			
79.	Gender	Gender of the suspect	1.male 2.female	
80.	Age	Year of birth of the suspect		
81.	Nationality	Nationality of the suspect	1. Dutch 2. Marroccan 3. Turkish 4. Antillian 5. German 6. Eastern European 77.Something different	
82.	Country of birth	The country of origin of the suspect	1.Dutch 2.Marroccan 3.Turkish 4.Antillian 5.German 6.Eastern European 77.Something different	
83.	Education	Highest level of education of suspect	1.Middelbaar-laag 2.Middelbaar-hoog 3.MBO 4.HBO 5.Universitair	
84.	Kind of education	Did the suspect take a digital program, namely an education in ICT	0.No 1.Yes 99.Unknown	
85.	Employment	Does the suspect have paid legal work	0.No 1.Yes 99.Unknown 77.Different	
86.	Kind of employment	The paid or unpaid work of the suspect, a qualitative description		

87.	Family background	Are the parents of the suspect divorced	0.No 1.Yes 99.Unknown	
88.		Is/are (a) parent(s) of the suspect an alcoholic	0.No 1.Yes 99.Unknown	
89.		Is/are (a) parent(s) of the suspect deceased	0.No 1.Yes 99.Unknown	
90.		Is/are (a) parent(s) of the suspect working in ICT	0.No 1.Yes 99.Unknown	
91.		Are the parents of the suspect known by the police, are they listed in the administration of the police	0.No 1.Yes 99.Unknown	
92.	Current residence	Where is the current residence of the suspect		
93.	Residential distance	What is the distance between suspect and victim	1.They both live in the east of the Netherlands 2.Suspect or victim lives in the east of the Netherlands, the other doesn't 3.International	When there are more victims, pick the distance of the most affected victim
94.	Antecedents	Does the suspect have a history in the administration of the police	0.No 1.Yes 99.Unknown	
95.	Offences	The offences of which the suspect is registered in the administration of the police		
96.	Relationship with the victim	Were the suspect and the victim business partners	0.No 1.Yes 99.Unknown	
97.		Were the suspect and the victim related	0.No 1.Yes 99.Unknown	
98.		Were the suspect and the victim acquaintances	0.No 1.Yes 99.Unknown	
99.		Were the suspect and the victim residents	0.No 1.Yes 99.Unknown	
100.		Were the suspect and the victim ex-partners	0.No 1.Yes 99.Unknown	
101.		Were the suspect and the victim partners	0.No 1.Yes 99.Unknown	
102.		Were the suspect and the victim criminal contacts	0.No 1.Yes 99.Unknown	
103.		Were the suspect and the victim friends on a social network	0.No 1.Yes 99.Unknown	

104.		Were the suspect and the victim fellow gamers	0.No 1.Yes 99.Unknown	
105.		Were the suspect and the victim chat friends	0.No 1.Yes 99.Unknown	
106.		Is there a relationship not mentioned before between the suspect and the victim	0.No 1.Yes 99.Unknown	
107.	Contact between suspect and victim	Has there been contact between the suspect and the victim, a week before the offence took place	0.No 1.Yes 99.Unknown	
108.	Motivation	Is the reason for commitment of the offence economic	0.No 1.Yes 99.Unknown	
109.		Is the reason for commitment of the offence addiction	0.No 1.Yes 99.Unknown	
110.		Is the reason for commitment of the offence a game of tension	0.No 1.Yes 99.Unknown	
111.		Is the reason for commitment of the offence revenge	0.No 1.Yes 99.Unknown	
112.		Is the reason for commitment of the offence opportunity	0.No 1.Yes 99.Unknown	
113.		Is the reason for commitment of the offence activism	0.No 1.Yes 99.Unknown	
114.		Is the reason for commitment of the offence piracy	0.No 1.Yes 99.Unknown	
115.		Is the reason for commitment of the offence other than mentioned before	0.No 1.Yes 99.Unknown	
116.	Influence	Was the suspect under the influence of alcohol during commitment of the offence	0.No 1.Yes 99.Unknown	
117.		Was the suspect under the influence of drugs during commitment of the offence	0.No 1.Yes 99.Unknown	
118.		Was the suspect under the influence of group pressure during commitment of the offence	0.No 1.Yes 99.Unknown	
119.		Did the suspect have an internet addiction during commitment of the offence	0.No 1.Yes 99.Unknown	

120.		Did the suspect have a game addiction during commitment of the offence	0.No 1.Yes 99.Unknown	
121.		Was the suspect under the influence of other addictions/resources not mentioned before during commitment of the offence	0.No 1.Yes 99.Unknown	
122.	Debts	Did the suspect have financial debts during commitment of the offence	0.No 1.Yes 99.Unknown	
123.	Debt	What is the extent of any possible debt		
124.	Expected plunder	Was the suspect aware of the plunder through family	0.No 1.Yes 99.Unknown	
125.		Was the suspect aware of the plunder through friends	0.No 1.Yes 99.Unknown	
126.		Was the suspect aware of the plunder through acquaintances	0.No 1.Yes 99.Unknown	
127.		Was the suspect aware of the plunder through neighbors	0.No 1.Yes 99.Unknown	
128.		Was the suspect aware of the plunder through his/her work	0.No 1.Yes 99.Unknown	
129.		Was the suspect aware of the plunder through social media	0.No 1.Yes 99.Unknown	
130.		Was the suspect aware of the plunder through Funda	0.No 1.Yes 99.Unknown	
131.		Was the suspect aware of the plunder through Ebay	0.No 1.Yes 99.Unknown	
132.		Was the suspect aware of the plunder through chat	0.No 1.Yes 99.Unknown	
133.		Was the suspect aware of the plunder through	0.No 1.Yes 99.Unknown	
134.		Was the suspect aware of the plunder through other internet sites	0.No 1.Yes 99.Unknown	
135.		Was the suspect aware of the plunder through coincidence	0.No 1.Yes 99.Unknown	
136.	Role	Was the suspect's role the one of an informant	0.No 1.Yes 99.Unknown	

137.		Was the suspect's role the one of driver	0.No 1.Yes 99.Unknown		
138.		Was the suspect's role the one of burglar	0.No 1.Yes 99.Unknown		
139.		Was the suspect's role the one of leader	0.No 1.Yes 99.Unknown		
140.		Was the suspect's role the one of helper	0.No 1.Yes 99.Unknown		
141.		Was the suspect's role the one of fraud perpetrator	0.No 1.Yes 99.Unknown		
142.		Was the suspect's role the one of deceiver	0.No 1.Yes 99.Unknown		
143.		Was the suspect's role one that hasn't been mentioned before	0.No 1.Yes 99.Unknown		
144.	Marital status	Marital status of suspect	1.Married 2.Unmarried 3.Devorced 4.Living together 77.Different		
145.	Assistance	Is the suspect known by probation	0.No 1.Yes 99.Unknown		
146.		Is the suspect known with addiction treatment	0.No 1.Yes 99.Unknown		
147.		Is the suspect known with a social aid agency	0.No 1.Yes 99.Unknown		
148.		Is the suspect known with other assistance agency's	0.No 1.Yes 99.Unknown		
149.	Treats	Did the suspect apply extreme threats(death threats and physical violence with weapons)	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
150.	Form of violence	Has a shot been fired during the commitment of the offence	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
151.		Has maltreatment been applied during the commitment of the offence	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

152.		Has imprisonment been applied at commitment of the offence?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
153.		Has tying down been applied at commitment of the offence?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
154.		Has holding hostage been applied at commitment of the offence?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
155.		Has sexual abuse been applied at commitment of the offence?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
156.		Has verbal abuse been applied at commitment of the offence?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
157.		Has violence via a social network been applied at commitment of the offence?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
158.		Has violence via MSN been applied at commitment of the offence?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
159.		Has violence via email been applied at commitment of the offence?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
160.		Has another form of violence been applied at commitment of the offence?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
161.	Digital media	Was the suspect active on social media?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
162.		Was the suspect active on real estate sites?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

163.		Was the suspect active on 'Marktplaats'?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
164.		Was the suspect active on a site he/she owned?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
165.		Was the suspect active on YouTube?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
166.		Was the suspect active on Skype?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
167.		Was the suspect active on a form of digital media, not mentioned before?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
168.	Did the suspect make use of	Email	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
169.		Google Streetview	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
170.		Searching for information on the internet	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
171.		Searching for products/ product information on the internet	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
172.		Make purchases on the internet	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
173.		Watching short movies on the internet (eg. via YouTube)	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

174.		Watching movies or programs online	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
175.		Downloading and using of software	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
176.		Downloading of music or films	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
177.		Visiting gambling sites	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
178.		Visiting porn sites	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
179.		Internetbanking	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
180.		Online gaming	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
181.		Reading news/magazines online	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
182.		Reading newsgroups	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
183.		Chatting (eg. via MSN)	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
184.		Visiting forums and internet communities	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

185.		Internetdating	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
186.		Webcam which is always on	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
187.		Does the suspect always ask others with whom he is chatting/"Skyping" to turn on the webcam.	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
188.	Did the suspect have a profile on	Datingsites	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
189.		Dropbox	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
190.		Facebook	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
191.		Flickr	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
192.		Hyves	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
193.		LinkedIn	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
194.		Twitter	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
195.		Sugababes	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

196.		Superdudes	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
197.		Waarbenjij.nu	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
198.		Youtube	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
199.		Skype	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
200.		Google plus	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
201.		Others	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
202.	Communication tools	Did the suspect communicate with his friends using a laptop?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
203.		Did the suspect communicate with his friends using a smartphone?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
204.		Did the suspect communicate with his friends using an iPad?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
205.		Did the suspect communicate with his friends using a desktop computer?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
206.	Communication channels	Did the suspect communicate with his friends using Whatsapp?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

207.		Did the suspect communicate with his friends using Ping?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
208.		Did the suspect communicate with his friends using sms?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
209.		Did the suspect communicate with his friends using imessage?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
210.		Did the suspect communicate with his friends using social media?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
211.		Did the suspect communicate with his friends using email?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
212.		Did the suspect communicate with his friends using another not mentioned channel?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
213.	Did the suspect have an	Up to date version of Windows/Linux/MacOs	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
214.		Up to date Anti-virus software	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
215.		Undesired contacts blocked	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
216.		Up to date spam-filter	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
217.		Protected profiles	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

218.	The victims			
219.	Number	How many victims were involved in the incident		
220.	Internet	How many victims were active on the internet		
221.	Victim 1			
222.	Gender	Gender of the victim	1.Male 2.Female	
223.	Age	Year of birth of the victim		
224.	Nationality	Nationality of the victim	1. Dutch 2. Marroccan 3. Turkish 4. Antillian 5. German 6. Eastern European 77.Something different	
225.	Country of birth	The country of origin of the victim	1.Dutch 2.Marroccan 3.Turkish 4.Antillian 5.German 6.Eastern European 77.Something different	
226.	Education	Highest level of education of victim	1.Middelbaar-laag 2.Middelbaar-hoog 3.MBO 4.HBO 5.Universitair	
227.	Kind of education	Did the victim take a digital program, namely an education in ICT	0.No 1.Yes 99.Unknown	
228.	Employment	Does the victim have paid legal work	1.Yes 2.No 99.Unknown 77.Different	
229.	Kind of Employment	The paid or unpaid work of the victim, a qualitative description		

230.	Family background	Are the parents of the victim divorced	0.No 1.Yes 99.Unknown		
231.		Is/are (a) parent(s) of the victim an alcoholic	0.No 1.Yes 99.Unknown		
232.		Is/are (a) parent(s) of the victim deceased	0.No 1.Yes 99.Unknown		
233.		Is/are (a) parent(s) of the victim working in ICT	0.No 1.Yes 99.Unknown		
234.		Are the parents of the victim known by the police, are they listed in the administration of the police	0.No 1.Yes 99.Unknown		
235.	Current residence	Where is the current residence of the suspect			
236.	Living situation	What is the current living situation of the victim	1.Living alone 2.With partner 3.With family 77. Different 99.Unknown		
237.	Antecedents	Does the victim have a history in the administration of the police	0.No 1.Yes 99.Unknown		
238.	Offences	The offences of which the victim is registered in the administration of the police			
239.	Digital media	Was the victim active on social media?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
240.		Was the victim active on selling houses sites?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
241.		Was the victim active on 'Marktplaats'?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
242.		Was the victim active on a site he/she owned?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
243.		Was the victim active on YouTube?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

244.		Was the victim active on Skype?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
245.		Was the victim active on a form of digital media, not mentioned before?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
246.	Did the victim make use of	Email	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
247.		Google Streetview	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
248.		Searching for information on the internet	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
249.		Searching for products/ product information on the internet	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
250.		Make purchases on the internet	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
251.		Watching short movies on the internet (eg. via YouTube)	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
252.		Watching movies or programs online	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
253.		Downloading and using of software	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
254.		Downloading of music or films	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

255.		Visiting gambling sites	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
256.		Visiting porn sites	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
257.		Internetbanking	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
258.		Online gaming	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
259.		Reading news/magazines online	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
260.		Reading newsgroups	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
261.		Chatting (eg. via MSN)	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
262.		Visiting forums and internet communities	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
263.		Internetdating	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
264.		Webcam which is always on	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
265.	Did the victim have a profile on	Datingsites	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

266.		Dropbox	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
267.		Facebook	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
268.		Flickr	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
269.		Hyves	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
270.		LinkedIn	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
271.		Twitter	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
272.		Sugababes	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
273.		Superdudes	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
274.		Waarben jij.nu	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
275.		Youtube	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
276.		Google plus	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

277.		Skype	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
278.		Others	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
279.	Communication tools	Did the victim communicate with his/her friends using a laptop?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
280.		Did the victim communicate with his/her friends using a smartphone?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
281.		Did the victim communicate with his/her friends using a iPad?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
282.		Did the victim communicate with his/her friends using a desktop computer?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
283.	Communication channels	Did the victim communicate with his/her friends using Whatsapp?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
284.		Did the victim communicate with his friends using Ping?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
285.		Did the victim communicate with his friends using sms?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
286.		Did the victim communicate with his friends using imessage?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
287.		Did the victim communicate with his friends using social media?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown

288.		Did the victim communicate with his friends using email?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
289.		Did the victim communicate with his friends using another not mentioned channel?	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
290.	Did the victim have an	Up to date version of Windows/Linux/MacOs	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
291.		Up to date Anti-virussoftware	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
292.		Undesired contacts blocked	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
293.		Up to date spam-filter	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
294.		Protected profiles	Prior to the offence 0.No 1.Yes	During the offence 0.No 1.Yes	After the offence 0.No 1.Yes 88.Inapplicable 99.Unknown
295.	Summary of the offence				
296.	Did the police miss opportunities during the interrogation of the victim and / or the suspect (s)? If they did, what?				

Appendix E

Total Incidents of Cognizable Crimes in 2012

TABLE-1.6 (Concluded)
Incidence & Rate of Total Cognizable Crimes (IPC) In States, UTs & Cities During 2012

Sl. No.	City	Incidence of Total Cognizable Crimes	Percentage Contribution to All-City Total	Population* (In Lakhs)	Rate of Total Cognizable Crimes
(1)	(2)	(3)	(4)	(5)	(6)
CITIES:					
1	AGRA	6537	1.4	17.46	374.4
2	AHMEDABAD	21347	4.5	63.52	336.1
3	ALLAHABAD	2788	0.6	12.17	229.1
4	AMRITSAR	1964	0.4	11.84	165.9
5	ASANSOL	3897	0.8	12.43	313.5
6	AURANGABAD	3659	0.8	11.89	307.7
7	BENGALURU	29297	6.2	84.99	344.7
8	BHOPAL	11732	2.5	18.83	623.0
9	CHANDIGARH (CITY)	3372	0.7	10.26	328.7
10	CHENNAI	19881	4.2	86.96	228.6
11	COIMBATORE	10357	2.2	21.51	481.5
12	DELHI (CITY)	47982	10.1	163.15	294.1
13	DHANBAD	1613	0.3	11.95	135.0
14	DURG-BHILAINAGAR	6244	1.3	10.64	586.8
15	FARIDABAD	5023	1.1	14.05	357.5
16	GHAZIABAD	5254	1.1	23.59	222.7
17	GWALIOR	7561	1.6	11.02	686.1
18	HYDERABAD	15992	3.4	77.49	206.4
19	INDORE	16526	3.5	21.67	762.6
20	JABALPUR	7212	1.5	12.68	568.8
21	JAIPUR	18678	3.9	30.73	607.8
22	JAMSHEDPUR	3192	0.7	13.37	238.7
23	JODHPUR	4531	1.0	11.38	398.2
24	KANNUR	2707	0.6	16.43	164.8
25	KANPUR	4558	1.0	29.20	156.1
26	KOCHI	17324	3.7	21.18	817.9
27	KOLKATA	25370	5.4	141.13	179.8
28	KOLLAM	7074	1.5	11.10	637.3
29	KOTA	3972	0.8	10.01	396.8
30	KOZHIKODE	4156	0.9	20.31	204.6
31	LUCKNOW	9147	1.9	29.01	315.3
32	LUDHIANA	3065	0.6	16.14	189.9
33	MADURAI	3261	0.7	14.62	223.1
34	MALAPPURAM	2091	0.4	16.99	123.1
35	MEERUT	4404	0.9	14.25	309.1
36	MUMBAI	30508	6.4	184.14	165.7
37	NAGPUR	8277	1.7	24.98	331.3
38	NASIK	4390	0.9	15.63	280.9
39	PATNA	10749	2.3	20.47	525.1
40	PUNE	12308	2.6	50.50	243.7
41	RAIPUR	5997	1.3	11.23	534.0
42	RAJKOT	4319	0.9	13.91	310.5
43	RANCHI	3990	0.8	11.27	354.0
44	SRINAGAR	2614	0.6	12.73	205.3
45	SURAT	9246	2.0	45.85	201.7
46	THIRUVANANTHAPURAM	7253	1.5	16.87	429.9
47	THRISSUR	6231	1.3	18.55	335.9
48	TIRUCHIRAPALLI	2926	0.6	10.22	286.3
49	VADODARA	6440	1.4	18.17	354.4
50	VARANASI	2282	0.5	14.35	159.0
51	VASAI VIRAR	2312	0.5	12.21	189.4
52	VIJAYAWADA	7686	1.6	14.91	515.5
53	VISHAKHAPATNAM	4626	1.0	17.30	267.4
TOTAL (CITIES)		473922	100.0	1607.24	294.9

* As per actual Census-2011 Population (Provisional)

Note : Percentage less than 0.05 is also shown as 0.0

Appendix F

Total Incidents of Burglary and Fraud in 2012

TABLE-1.15 (Continued)

Sl. No.	State/City	Preparation & Assembly for Dacoity (Sec. 399 – 402 IPC)	Robbery (Sec. 392 – 394, 397 & 398 IPC)	Burglary (Sec. 449 – 452, 454, 455, 457 – 460 IPC)	Theft (Sec. 379 – 382 IPC)			Riots (Sec. 143, 145, 147, 151, 153, 153A, 153B, 157, 158, 160 IPC)	Criminal Breach of Trust (Sec. 406 – 409 IPC)	Cheating (Sec. 419, 420 IPC)	Counter-Feiting (Sec. 231-254, 489A-489D IPC)
					Total	Auto theft	Other theft				
(1)	(2)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)
MAHARASHTRA											
1	AURANGABAD	8	178	292	822	419	403	168	19	245	2
2	AMRAVATI	7	54	232	778	195	583	77	35	59	8
3	MUMBAI	29	1131	2500	10851	4075	6776	374	564	1827	48
4	NAGPUR	29	491	883	2339	1334	1005	169	50	264	7
5	NASIK	13	163	356	1070	615	455	94	28	139	17
6	NAVI MUMBAI	7	417	596	1513	772	741	124	80	455	15
7	PUNE	50	731	1019	4181	2604	1577	532	92	756	18
8	SOLAPUR	1	98	187	557	335	222	132	6	106	2
9	THANE	15	757	1199	2435	1239	1196	280	82	867	35
PUNJAB											
1	AMRITSAR	14	25	158	416	149	267	0	13	266	1
2	JALANDHAR	3	18	195	443	192	251	0	8	171	2
3	LUDHIANA	21	19	196	504	225	279	0	45	281	2
RAJASTHAN											
1	AJMER	2	5	59	234	163	71	2	4	457	1
2	BHARATPUR	1	15	18	675	559	116	0	0	272	0
3	BIKANER	0	10	41	143	58	85	0	3	324	0
4	JAIPUR	3	257	975	5292	4121	1171	71	231	2725	7
5	JODHPUR	0	39	174	1043	717	326	0	7	722	3
6	KOTA	7	27	86	596	408	188	0	21	756	0
7	UDAIPUR	2	30	144	460	291	169	38	11	625	4
TAMIL NADU											
1	CHENNAI	0	85	546	2169	263	1906	95	50	769	137
2	COIMBATORE	0	101	125	544	205	339	16	9	132	59
3	MADURAI	0	79	68	459	201	258	26	7	294	21
4	SALEM	0	39	31	162	102	60	32	2	35	1
5	THIRUNELVELI	0	38	18	58	8	50	0	2	64	21
6	TIRUCHIRAPALI	0	56	42	253	52	201	7	0	103	5
UTTAR PRADESH											
1	AGRA	5	136	296	3070	2504	566	227	130	272	10
2	ALIGARH	1	54	135	1095	720	375	115	78	271	6
3	ALLAHABAD	5	22	135	914	732	182	39	48	190	7
4	BAREILLY	0	31	90	526	306	220	62	63	261	3
5	GHAZIABAD	11	63	160	2177	1753	424	32	85	227	4
6	GORAKHPUR	0	29	133	780	605	175	85	66	257	7
7	KANPUR	1	89	165	1104	913	191	71	130	379	1
8	LUCKNOW	0	43	399	2265	1586	679	135	377	839	6
9	MEERUT	2	133	173	1624	1240	384	117	71	285	7
10	MORADABAD	0	50	73	613	420	193	54	24	94	1
11	VARANASI	0	11	73	610	411	199	21	109	273	24
WEST BENGAL											
1	ASANSOL	44	75	21	947	254	693	212	20	15	3
2	KOLKATA	20	44	96	4960	659	4301	397	428	2100	26
CHANDIGARH UT											
1	CHANDIGARH (CITY)	7	55	226	1437	836	601	47	32	230	2
DELHI UT											
1	DELHI (CITY)	13	522	1483	20218	13196	7022	72	302	2271	59

Appendix G

Percentage Increase in Burglaries and Frauds from 2011 to 2012

TABLE-1.13 (Continued)

Sl. No.	City	Robbery (Sec.392-394, 397, 398 IPC)			Burglary (Sec.449-452,454,455,457-460 IPC)		
		2011	2012	% Variation	2011	2012	% Variation
(1)	(2)	(36)	(37)	(38)	(39)	(40)	(41)
CITIES:							
36	AGRA	134	136	1.5	240	296	23.3
37	AHMEDABAD	720	603	-16.3	831	701	-15.6
38	ALLAHABAD	54	22	-59.3	134	135	0.7
39	AMRITSAR	12	25	108.3	117	158	35.0
40	ASANSOL	23	75	226.1	9	21	133.3
41	AURANGABAD	152	178	17.1	380	292	-23.2
42	BENGALURU	783	670	-14.4	1313	1240	-5.6
43	BHOPAL	149	187	25.5	850	870	2.4
44	CHANDIGARH (CITY)	62	55	-11.3	265	226	-14.7
45	CHENNAI	219	85	-61.2	766	546	-28.7
46	COIMBATORE	48	101	110.4	105	125	19.0
47	DELHI (CITY)	473	522	10.4	1226	1483	21.0
48	DHANBAD	9	8	-11.1	63	67	6.3
49	DURG-BHILAINAGAR	59	26	-55.9	441	333	-24.5
50	FARIDABAD	37	34	-8.1	356	347	-2.5
51	GHAZIABAD	75	63	-16.0	171	160	-6.4
52	GWALIOR	155	155	0.0	678	610	-10.0
53	HYDERABAD	40	57	42.5	693	647	-6.6
54	INDORE	194	254	30.9	862	1043	21.0
55	JABALPUR	61	72	18.0	348	400	14.9
56	JAIPUR	179	257	43.6	889	975	9.7
57	JAMSHEDPUR	20	30	50.0	134	131	-2.2
58	JODHPUR	17	39	129.4	173	174	0.6
59	KANNUR	57	31	-45.6	71	59	-16.9
60	KANPUR	133	89	-33.1	319	165	-48.3
61	KOCHI	38	25	-34.2	76	90	18.4
62	KOLKATA	34	44	29.4	63	96	52.4
63	KOLLAM	16	62	287.5	105	132	25.7
64	KOTA	15	27	80.0	120	86	-28.3
65	KOZHICODE	48	65	35.4	136	92	-32.4
66	LUCKNOW	52	43	-17.3	410	399	-2.7
67	LUDHIANA	10	19	90.0	183	196	7.1
68	MADURAI	85	79	-7.1	106	68	-35.8
69	MALAPPURAM	11	8	-27.3	61	38	-37.7
70	MEERUT	131	133	1.5	154	173	12.3
71	MUMBAI	467	1131	142.2	2745	2500	-8.9
72	NAGPUR	198	491	148.0	734	883	20.3
73	NASIK	154	163	5.8	516	356	-31.0
74	PATNA	121	88	-27.3	425	469	10.4
75	PUNE	546	731	33.9	1192	1019	-14.5
76	RAIPUR	47	33	-29.8	466	391	-16.1
77	RAJKOT	36	43	19.4	187	198	5.9
78	RANCHI	66	71	7.6	157	162	3.2
79	SRINAGAR	33	18	-45.5	280	251	-10.4
80	SURAT	78	68	-12.8	356	333	-6.5
81	THIRUVANANTHAPURAM	79	101	27.8	175	154	-12.0
82	THRISSUR	28	28	0.0	75	55	-26.7
83	TIRUCHIRAPALLI	30	56	86.7	55	42	-23.6
84	VADODARA	83	112	34.9	295	333	12.9
85	VARANASI	18	11	-38.9	46	73	58.7
86	VASAI VIRAR	127	144	13.4	311	461	48.2
87	VIJAYAWADA	35	60	71.4	232	221	-4.7
88	VISHAKHAPATNAM	28	27	-3.6	283	366	29.3
TOTAL (CITIES)		6479	7655	18.2	21378	20841	-2.5

TABLE-1.13 (Continued ...)

Sl. No.	City	Riots (Sec.143-145,147-151, 153, 153A, 153B,157,158,160 IPC)			Criminal Breach of Trust (Sec. 406-409 IPC)			Cheating (Sec. 419,420 IPC)		
		2011	2012	% Variation	2011	2012	% Variation	2011	2012	% Variation
(1)	(2)	(51)	(52)	(53)	(54)	(55)	(56)	(57)	(58)	(59)
CITIES:										
36	AGRA	417	227	-45.6	139	130	-6.5	330	272	-17.6
37	AHMEDABAD	156	159	1.9	312	298	-4.5	288	246	-14.6
38	ALLAHABAD	45	39	-13.3	67	48	-28.4	155	190	22.6
39	AMRITSAR	0	0	@	16	13	-18.8	261	266	1.9
40	ASANSOL	99	212	114.1	10	20	100.0	76	15	-80.3
41	AURANGABAD	154	168	9.1	21	19	-9.5	194	245	26.3
42	BENGALURU	390	551	41.3	152	145	-4.6	3155	3092	-2.0
43	BHOPAL	80	80	0.0	17	24	41.2	75	174	132.0
44	CHANDIGARH (CITY)	64	47	-26.6	24	32	33.3	246	230	-6.5
45	CHENNAI	160	95	-40.6	22	50	127.3	767	769	0.3
46	COIMBATORE	30	16	-46.7	6	9	50.0	171	132	-22.8
47	DELHI (CITY)	44	72	63.6	287	302	5.2	2403	2271	-5.5
48	DHANBAD	68	61	-10.3	46	31	-32.6	27	52	92.6
49	DURG-BHILAINAGAR	35	21	-40.0	14	13	-7.1	137	110	-19.7
50	FARIDABAD	173	188	8.7	160	118	-26.3	42	46	9.5
51	GHAZIABAD	67	32	-52.2	112	85	-24.1	304	227	-25.3
52	GWALIOR	67	60	-10.4	34	32	-5.9	129	125	-3.1
53	HYDERABAD	220	354	60.9	75	71	-5.3	1864	2131	14.3
54	INDORE	72	52	-27.8	36	29	-19.4	205	186	-9.3
55	JABALPUR	67	25	-62.7	11	6	-45.5	81	125	54.3
56	JAIPUR	137	71	-48.2	271	231	-14.8	2756	2725	-1.1
57	JAMSHEDPUR	83	95	14.5	70	61	-12.9	53	219	313.2
58	JODHPUR	4	0	-100.0	18	7	-61.1	684	722	5.6
59	KANNUR	310	412	32.9	2	2	0.0	41	44	7.3
60	KANPUR	177	71	-59.9	208	130	-37.5	510	379	-25.7
61	KOCHI	343	393	14.6	9	8	-11.1	618	630	1.9
62	KOLKATA	336	397	18.2	333	428	28.5	1625	2100	29.2
63	KOLLAM	602	293	-51.3	14	6	-57.1	83	90	8.4
64	KOTA	2	0	-100.0	16	21	31.3	499	756	51.5
65	KOZHIKODE	446	353	-20.9	30	19	-36.7	188	164	-12.8
66	LUCKNOW	123	135	9.8	374	377	0.8	703	839	19.3
67	LUDHIANA	0	0	@	32	45	40.6	361	281	-22.2
68	MADURAI	25	26	4.0	10	7	-30.0	183	294	60.7
69	MALAPPURAM	144	129	-10.4	1	3	200.0	76	79	3.9
70	MEERUT	126	117	-7.1	64	71	10.9	298	285	-4.4
71	MUMBAI	379	374	-1.3	553	564	2.0	1946	1827	-6.1
72	NAGPUR	148	169	14.2	68	50	-26.5	294	264	-10.2
73	NASIK	111	94	-15.3	31	28	-9.7	197	139	-29.4
74	PATNA	292	294	0.7	12	6	-50.0	598	599	0.2
75	PUNE	478	532	11.3	93	92	-1.1	769	756	-1.7
76	RAIPUR	98	56	-42.9	41	23	-43.9	204	189	-7.4
77	RAJKOT	67	74	10.4	67	84	25.4	42	43	2.4
78	RANCHI	82	102	24.4	46	31	-32.6	179	249	39.1
79	SRINAGAR	147	107	-27.2	17	15	-11.8	126	101	-19.8
80	SURAT	64	65	1.6	34	24	-29.4	191	177	-7.3
81	THIRUVANANTHAPURAM	526	629	19.6	30	11	-63.3	397	304	-23.4
82	THRISSUR	362	443	22.4	7	13	85.7	636	366	-42.5
83	TIRUCHIRAPALLI	10	7	-30.0	0	0	@	57	103	80.7
84	VADODARA	78	92	17.9	31	24	-22.6	170	175	2.9
85	VARANASI	13	21	61.5	97	109	12.4	220	273	24.1
86	VASAI VIRAR	75	107	42.7	9	17	88.9	91	191	109.9
87	VIJAYAWADA	2	16	700.0	101	123	21.8	430	416	-3.3
88	VISHAKHAPATNAM	3	12	300.0	57	68	19.3	244	252	3.3
TOTAL (CITIES)		8201	8145	-0.7	4307	4173	-3.1	26379	26935	2.1

TABLE-1.13 (Continued)

Sl. No.	City	Counterfeiting (Sec.231-254, 489A-489D IPC)			Arson (Sec.435,436,438 IPC)		
		2011	2012	% Variation	2011	2012	% Variation
(1)	(2)	(60)	(61)	(62)	(63)	(64)	(65)
CITIES:							
36	AGRA	35	10	-71.4	1	0	-100.0
37	AHMEDABAD	10	21	110.0	6	16	166.7
38	ALLAHABAD	11	7	-36.4	2	5	150.0
39	AMRITSAR	3	1	-66.7	4	6	50.0
40	ASANSOL	0	3	@	0	1	@
41	AURANGABAD	5	2	-60.0	26	24	-7.7
42	BENGALURU	60	41	-31.7	4	0	-100.0
43	BHOPAL	0	6	@	15	10	-33.3
44	CHANDIGARH (CITY)	0	2	@	7	9	28.6
45	CHENNAI	99	137	38.4	7	10	42.9
46	COIMBATORE	19	59	210.5	23	21	-8.7
47	DELHI (CITY)	44	59	34.1	33	72	118.2
48	DHANBAD	2	1	-50.0	0	1	@
49	DURG-BHILAINAGAR	9	1	-88.9	22	17	-22.7
50	FARIDABAD	1	2	100.0	9	9	0.0
51	GHAZIABAD	2	4	100.0	0	0	@
52	GWALIOR	2	1	-50.0	11	11	0.0
53	HYDERABAD	44	25	-43.2	50	101	102.0
54	INDORE	3	6	100.0	37	51	37.8
55	JABALPUR	0	0	@	13	14	7.7
56	JAIPUR	3	7	133.3	24	20	-16.7
57	JAMSHEDPUR	0	4	@	15	2	-86.7
58	JODHPUR	4	3	-25.0	12	13	8.3
59	KANNUR	0	10	@	18	29	61.1
60	KANPUR	35	1	-97.1	3	0	-100.0
61	KOCHI	0	2	@	5	3	-40.0
62	KOLKATA	63	26	-58.7	0	0	@
63	KOLLAM	0	1	@	17	14	-17.6
64	KOTA	1	0	-100.0	2	3	50.0
65	KOZHIKODE	1	0	-100.0	10	12	20.0
66	LUCKNOW	19	6	-68.4	4	0	-100.0
67	LUDHIANA	2	2	0.0	7	5	-28.6
68	MADURAI	20	21	5.0	2	8	300.0
69	MALAPPURAM	0	1	@	1	10	900.0
70	MEERUT	7	7	0.0	4	1	-75.0
71	MUMBAI	81	48	-40.7	46	86	87.0
72	NAGPUR	22	7	-68.2	22	32	45.5
73	NASIK	14	17	21.4	21	16	-23.8
74	PATNA	19	3	-84.2	1	0	-100.0
75	PUNE	34	18	-47.1	27	48	77.8
76	RAIPUR	3	8	166.7	33	36	9.1
77	RAJKOT	7	11	57.1	12	8	-33.3
78	RANCHI	1	0	-100.0	5	4	-20.0
79	SRINAGAR	4	2	-50.0	23	21	-8.7
80	SURAT	42	14	-66.7	4	3	-25.0
81	THIRUVANANTHAPURAM	0	0	@	14	10	-28.6
82	THRISSUR	0	0	@	10	7	-30.0
83	TIRUCHIRAPALLI	8	5	-37.5	2	3	50.0
84	VADODARA	10	5	-50.0	5	5	0.0
85	VARANASI	25	24	-4.0	2	0	-100.0
86	VASAI VIRAR	2	1	-50.0	6	6	0.0
87	VJAYAWADA	6	6	0.0	24	33	37.5
88	VISHAKHAPATNAM	4	6	50.0	11	10	-9.1
TOTAL (CITIES)		786	654	-16.8	662	826	24.8

Appendix H

Tables for the Results

TABLES

Table 1: Is it an attempt, that is the criminal activity fails? # 17 (N = 843, in%)

Was it an attempt?	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
No	100.0	81.6	100.0	70.0	98.4	81.4	99.7	78.5
Yes	0.0	18.4	0.0	30.0	1.6	18.6	0.3	21.5
N	174	136	57	140	62	274	293	550
Pearson Chi-Square	34.791***		21.734***		11.170**		70.288***	

Note: df = 1, **p < .01, ***p < .001,

Table 2: Number of suspects in the crime in question # 77 (N = 766, in%)

Number of Suspects involved	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
1	87.4	79.8	77.2	53.3	31.6	86.5	74.3	75.1
2	9.2	14.7	15.8	29.2	21.1	11.5	12.8	17.5
3	2.3	3.1	7.0	11.7	12.3	1.9	5.2	5.1
4	0.6	1.6	0.0	2.2	8.8	0.0	2.1	1.1
5	0.6	0.8	0.0	2.9	1.8	0.0	0.7	1.1
6	0.0	0.0	0.0	0.0	8.8	0.0	1.7	0.0
7	0.0	0.0	0.0	0.7	5.3	0.0	1.0	0.2
8	0.0	0.0	0.0	0.0	3.5	0.0	0.7	0.0
9	0.0	0.0	0.0	0.0	1.8	0.0	0.3	0.0
10	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
11	0.0	0.0	0.0	0.0	1.8	0.0	0.3	0.0
12	0.0	0.0	0.0	0.0	3.5	0.0	0.7	0.0
N	174	129	57	137	57	208	288	474
Pearson Chi Square	3.398		10.857		115.535***		30.968***	

Note: df = 11, ***p < .001.

Table 3: Gender of suspect # 79 (N=999, in%)

Gender of offender	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
Female	1.0	16.8	0.0	8.5	5.6	18.9	2.3	14.3
Male	99.0	83.2	100.0	91.5	94.4	81.1	97.3	85.7
N	203	155	74	200	198	169	475	524
Pearson Chi-Square	30.391***		6.706**		15.779***		41.564***	

Note: df = 1, **p < .01, ***p < .001.

Table 4: Age of Suspects #80 (N=882, in%)

Age of Offender	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
Below 18	1.5	10.8	2.8	9.3	0.0	7.0	1.1	9.3
18 – 29	77.0	47.3	57.7	42.3	41.6	38.0	60.0	43.0
30 – 39	13.8	21.6	25.4	21.6	28.9	20.0	21.6	21.3
40 – 49	6.1	16.2	14.1	20.1	17.3	19.0	11.8	18.6
50 and above	1.5	4.1	0.0	6.7	12.1	16.0	5.5	7.9
N	196	148	71	194	173	100	440	442
Pearson Chi-Square	38.049***		11.649*		14.734**		48.688***	

Note: df = 4, *p < .05, **p < .01, ***p < .001.

Table 5: The country of origin of the suspect # 82 (N=913, in%)

Nationality of offender	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
Local ¹	98.5	71.9	100.0	77.7	94.4	77.8	97.1	75.8
Born Elsewhere	1.5	28.1	0.0	22.3	5.6	22.2	2.9	24.2
N	203	146	74	193	198	99	475	438
Pearson Chi-Square	349.000***		267.000***		297.000***		913.000***	

Note: ¹Local means that for Indian crimes, the offender is born in India and for Dutch crimes, the offender is born in Netherlands.

df = 28, ***p < .001.

Table 6: Did the suspect undergo digital training, ie training in eg IT? #84 (N=691, in%)

Did the suspect take digital education?	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
No	100.0	100.0	100.0	98.5	88.0	99.6	93.2	99.4
Yes	0.0	0.0	0.0	1.5	12.0	0.4	6.8	0.6
N	16	162	3	204	25	281	44	647
Pearson Chi-Square	-		0.045		24.128***		15.793***	

Note: df = 1, ***p < .001.

Table 7: Gender of victims # 222 (N=695, in%)

Gender of victim	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
Female	23.0	51.1	15.8	19.6	13.3	41.7	19.6	42.1
Male	77.0	48.9	84.2	80.4	86.7	58.3	80.4	57.9
N	174	137	57	51	60	216	291	404
Pearson Chi-Square	26.488***		0.271		16.461***		38.907***	

Note: df = 1, ***p < .001.

Table 8: Age of victims #83 (N=453, in%)

Age of Victim	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
Below 39	42.5	41.0	55.6	34.7	16.7	36.7	41.8	37.9
40 – 49	22.5	22.4	33.3	18.4	50.0	20.9	27.3	21.1
50 and above	35.0	36.6	11.1	46.9	33.3	42.3	30.9	41.0
N	40	134	9	49	6	215	55	398
Pearson Chi-Square	0.037		4.054		3.033		2.257	

Note: df = 2

Table 9: Nationality of victims #224 (N=689, in%)

Nationality of victim	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
Local *	100.0	91.8	100.0	83.7	95.2	89.2	99.0	89.4
Born Elsewhere	0.0	8.2	0.0	16.3	4.8	10.8	1.0	10.6
N	174	134	57	49	62	213	293	396
Pearson Chi-Square	308.000***		106.000***		275.000***		689.000***	

Note: df = 21, ***p < .001.

Table 10: Relationship between suspect and victim # 97 - # 106 (N=1134, in%)

Relationship	Residential Burglary			Commercial Burglary			Fraud			Total		
	India	Netherlands	Chi-Square	India	Netherlands	Chi-Square	India	Netherlands	Chi-Square	India	Netherlands	Chi-Square
Business Partners	0.5	4.1	5.793*	0.0	6.9	5.348*	2.5	33.2	67.486***	1.3	17.5	78.346***
Related	0.0	7.6	16.084***	0.0	0.0	-	0.0	1.1	2.123	0.0	2.4	11.740***
Acquaintances	0.5	8.2	14.370***	1.4	2.0	0.111	2.0	4.9	2.803	1.3	4.9	11.069***
Residents	0.0	2.9	6.052*	0.0	0.5	0.362	0.5	1.1	0.506	0.2	1.4	4.235*
Ex-Partners	0.0	2.9	6.052*	0.0	0.0	-	0.0	2.1	4.272*	0.0	1.7	8.035**
Partners	0.0	0.0	-	0.0	0.0	-	0.0	0.0	-	0.0	0.0	-
Criminal Contacts	0.0	0.0	-	0.0	0.0	-	0.0	0.0	-	0.0	0.0	-
Friends on Social network	0.0	0.0	-	0.0	0.0	-	0.0	0.7	1.412	0.0	0.3	1.449
Fellow Gamers	0.0	0.0	-	0.0	0.0	-	0.0	0.0	-	0.0	0.0	-
Chat Friends	0.0	0.0	-	0.0	0.0	-	0.0	0.7	1.412	0.0	0.3	1.449
Other Relationship	2.0	3.5	4.527	14.9	6.8	8.280*	3.0	3.5	1.580	4.4	4.6	7.920*
Relationship – total	3.0	29.4	50.753***	16.2	21.1	0.809	8.0	43.8	72.563***	7.1	33.0	107.249***
Contact between victim and offender	2.0	5.9	3.919*	12.3	9.8	0.381	36.4	11.0	36.199***	14.4	9.3	6.451**
N	203	170		74	204		199	283		476	657	

Note: df = 1, *p < .05, **p < .01, ***p < .001.

Table 11: In what location the offense took place # 11 (N=801, in%)

Kind of Location	Residential Burglary		Commercial Burglary		Fraud	
	India	Netherlands	India	Netherlands	India	Netherlands
House	98.9	97.1	0.0	0.0	3.2	26.6
School	0.0	0.0	7.0	0.0	0.0	0.0
Youth hostel	0.6	0.0	1.8	0.0	0.0	0.0
On the street	0.0	2.2	1.8	0.0	1.6	9.4
Business	0.0	0.7	68.4	93.5	6.5	23.2
Internet	0.0	0.0	0.0	0.0	8.1	33.0
Catering facility	0.0	0.0	0.0	6.5	0.0	3.0
Public space	0.0	0.0	0.0	0.0	8.1	4.7
Sports facilities	0.0	0.0	0.0	0.0	0.0	0.0
Public Transport	0.0	0.0	0.0	0.0	0.0	0.0
Bank	0.0	0.0	0.0	0.0	48.4	0.0
ATM	0.0	0.0	0.0	0.0	17.7	0.0
Hospital	0.0	0.0	7.0	0.0	0.0	0.0
Place of Worship	0.0	0.0	10.5	0.0	0.0	0.0
Other	0.5	0.0	3.6	0.0	6.4	0.0
N	174	136	57	139	62	233
Pearson Chi-Square	6.706		50.540***		206.139***	

Note: df = 10, ***p < .001.

Table 12: Plunder (N=843, in%)

Plunder	Residential Burglary		Commercial Burglary		Fraud	
	India	Netherlands	India	Netherlands	India	Netherlands
Money gained ***	63.2	30.1	49.1	25.0	95.2	55.5
Jewellery gained ***	51.1	25.7	26.3	1.4	12.9	0.4
Electronics gained*	21.3	35.3	26.3	12.9	1.9	1.1
Mobile phones gained***	33.3	16.9	21.1	5.7	1.9	0.4
Information gained	4.6	6.6	10.5	2.1	4.8	1.8
N	174	136	57	140	62	274

Note: df = 1, *p < .05, ***p < .001.

Table 13: Is anyone arrested? #47 (N=843, in%)

Was the suspect arrested?	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
No	1.7	41.9	1.8	20.0	22.6	85.8	6.1	58.2
Yes	98.3	58.1	98.2	80.0	77.4	14.2	95.9	41.8
N	174	136	57	140	62	274	293	550
Pearson Chi-Square	78.985***		10.742***		105.197***		215.526***	

Note: df = 1, ***p < .001.

Table 14: Factors leading to arrest of suspect #48 to #60 (N=763, in%)

Factor leading to Arrest of Suspect	Residential Burglary			Commercial Burglary			Fraud		
	India	Netherlands	Chi-Square	India	Netherlands	Chi-Square	India	Netherlands	Chi-Square
Wiretaps/Phone taps	0.0	1.0	2.027	0.0	0.0	-	14.3	0.0	6.939**
Statement of suspect	0.0	1.0	2.027	0.0	5.8	4.365**	0.0	18.6	35.109***
Statement of other suspect	0.0	7.1	14.480***	0.0	7.6	5.748*	7.1	2.3	1.383
Witness statements	9.5	15.2	2.099	91.7	34.9	65.529***	33.5	18.6	3.683
Statement of victim(s)	100.0	17.2	228.255***	100.0	11.5	168.752***	46.2	7.0	22.511***
DNA traces	0.0	6.1	12.369***	0.0	5.2	3.912*	0.0	7.0	12.869***
Camera footage	0.0	3.0	6.122*	0.0	14.5	11.660***	47.3	4.7	26.508***
Plunder found	100.0	12.1	247.885***	98.6	5.8	197.082***	35.8	0.0	22.542***
Suspect(s) get caught in the act	0.0	36.4	82.682***	0.0	37.8	37.090***	0.0	39.5	77.834***
CIE information ¹	0.0	0.0	-	0.0	0.0	-	2.2	2.4	5.178
Internet taps	0.0	0.0	-	0.0	0.0	-	4.4	0.0	1.960
Phone data	30.0	2.0	31.542***	13.9	0.0	24.910***	9.3	0.0	4.345*
Other elements	0.0	16.2	34.151***	0.0	12.8	10.122***	4.9	25.6	18.290***
Digital evidence – total	30.0	6.1	22.063***	13.9	14.5	0.017	58.9	4.7	40.625***
N	200	99	-	72	172	-	182	43	-

Note: ¹ CIE – Criminal Intelligence Unit, in Indian cases, the Criminal Investigation Department (CID) was involved.

df = 1, ***p < .001

Table 15: How many suspects are active on the Internet? #77 (N=565, in%)

No. of suspects active on the Internet	Residential Burglary		Commercial Burglary		Fraud	
	India	Netherlands	India	Netherlands	India	Netherlands
None	100.0	84.8	100.0	90.2	14.3	76.9
1	0.0	12.7	0.0	8.9	14.3	23.1
2	0.0	2.5	0.0	0.9	14.3	0.0
3	0.0	0.0	0.0	0.0	14.3	0.0
4	0.0	0.0	0.0	0.0	14.3	0.0
7	0.0	0.0	0.0	0.0	14.3	0.0
8	0.0	0.0	0.0	0.0	7.1	0.0
12	0.0	0.0	0.0	0.0	7.1	0.0
N		79		112	14	39
Pearson Chi-Square	-		-		34.935***	

Note: df = 7, ***p < .001.

Table 16: Role of Social Media for suspects (N=712, in%)

Was the suspect active on social media?	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
Before the offence	0.0	4.0	0.0	2.3	10.3	2.3	3.3	2.9
During the offence	0.0	2.0	0.0	0.6	7.4	2.3	2.9	1.3
After the offence	0.0	3.2	0.0	1.2	2.3	2.3	0.7	1.9
Total	0.0	5.1	0.0	2.9	10.3	2.3	3.3	3.5
N	200	99	72	172	126	43	398	314
Pearson Chi-Square	10.723***		2.137		2.695		0.030	

Note: df = 1, ***p < .001.

Table 17: Role of Social Media for victims (N=851, in%)

Was the victim active on social media?	Residential Burglary		Commercial Burglary		Fraud		Total	
	India	Netherlands	India	Netherlands	India	Netherlands	India	Netherlands
Before the offence	0.0	0.7	0.0	0.0	5.5	0.4	1.0	0.4
During the offence	0.0	0.0	0.0	0.0	5.2	0.7	1.0	0.4
After the offence	0.0	0.0	0.0	0.0	3.4	0.4	0.7	0.2
Total	0.0	0.7	0.0	0.0	5.5	0.7	1.0	0.5
N	174	146	57	141	55	278	286	565
Pearson Chi-Square	1.196		-		6.961**		0.728	

Note: df = 1, **p < .01.