Journal of Forensic Sciences &
Criminal Investigation

Juniper PUBLISHERS key to the Researchers

Research Article
Volume-4 Issue -2 August 2017
DOI: 10.19080/JFSCI.2017.04.555634

J Forensic Sci & Criminal Inves

Copyright © All rights are reserved by Gaurav Misra

A Cross-National Study on Cybercrime: Incident, Suspect and Victim Characteristics for Digital and Traditional Fraud in the Netherlands and Kolkata, India

Gaurav Misra*[1], Marianne Junger[2] and Lorena Montoya[3]

[1]Australian Centre for Cyber Security, University of New South Wales Canberra, Australia

[2]Department of Industrial Engineering and Business Information Systems, University of Twente Enschede, Europe

Submission: July 18, 2017; **Published:** August 01, 2017

***Corresponding author:** Gaurav Misra, Australian Centre for Cyber Security, University of New South Wales Canberra, Australia, Email: g.misra@adfa.edu.au

Abstract

Technological advances have impacted our society in various ways. For example, it has completely revolutionized the way we communicate with each other and has had a large impact on crime. The present research analyses fraud cases and classifies them as 'digital' or 'traditional' based on the use of Information and Communication Technology (ICT). The primary objective is to compare the characteristics of the offence as well as the victims and the offenders for digital and traditional (non-digital) frauds. This research was done in The Netherlands and later replicated as a pilot in Kolkata, India. The transfer of a methodology that was effective in a western country to Kolkata lead to two major problems, namely, getting the cooperation of the police and drawing a sample which traces back accurately to the original research in The Netherlands. Despite these problems, results were informative for traditional and digital fraud in both countries. 23% of all frauds have a digital aspect in Kolkata and 40% in The Netherlands.

Three trends were similar in both countries:

a. The digital offenders were relatively young,

b. The frauds were more often committed by single offenders, and

c. The proximity between suspects and victims was greater.

Trends in both countries differ with respect to the offenders' place of birth, employment status, criminal record and the relationship between suspect and victim. Practical issues on cross-cultural research are discussed. Despite limitations, cross-cultural studies give us an insight into how different factors involved in digital frauds in two very different settings compare.

Keywords: Cyber-crime; Fraud; Offender characteristics; Cross-national comparison

Abbreviation: ICT: Information and Communication Technology

Introduction

Computers and the internet have become essential in areas such as professional life, interpersonal communication, finances, and leisure. Most scholars agree that the Internet has had a major impact upon criminality [1,2]. The increased use of computers and the fact that internet connects (almost) everybody to (almost) everybody else in the world has made crime considerably easier to perpetrate [3-6]. It is plausible that criminal might have adapted to the increasingly digitized world and that this permeates traditional crime [2]. Many sources make claims about the prevalence of cybercrime, but do not clearly define what has been measured. The imprecision of victim surveys [7] and the non-standardized description of cybercrime incidents by commercial companies [8,9] and the police might explain the lack of valid figures [10].

The present work aims to measure the extent to which the internet infiltrates traditional crime. It focuses on the impact of ICT on frauds committed in The Netherlands and Kolkata, India. Internet use has grown more rapidly in developed nations during the last couple of decades. In The Netherlands, Internet use by the population has increased from 44.0% in 2000 to 93.0% in 2012 [11]. In developing countries the increase has been more modest. In India, the figures are 0.5% and 12.6% respectively [11]. Moreover, there is evidence that the differences in internet use between these two countries also apply to fields such as Smartphone adoption [12]. The widespread accessibility of the Internet has further facilitated computer-assisted offenses. It is therefore likely that cybercrime has become a relatively larger part of overall crime in developed countries compared to developing ones.

To the best of our knowledge, no prior research has compared offenders and victims of traditional crime against ICT-related crime across two different countries. The present research fills this gap by investigating the similarities and differences in the extent to which ICT plays a role in crime in The Netherlands and Kolkata, India by analysing not only the offense itself, but also victim and offender characteristics. To study cybercrime, the scientific community requires some agreement on definitions and measurement techniques [13]. A definition has consequences for the explanation of cybercrime and the study of how ICT changes crime. The measurement of the extent of cybercrime is typically done by defining cybercrime and then quantifying how many cases fit the definition. This approach was used by Domenie, Leukfeldt et al. [14], who investigated the amount of cybercrime by examining a representative sample of more than 30,000 crimes registered in the police records of two regions located in the eastern part of The Netherlands. To measure the amount of cybercrime, a search protocol for associated keywords such as 'computer', 'cyber' or 'digital' was used. They found that the amount of cybercrime varies between 0.3% and 0.5% [14].

However, [15] argues that measuring cybercrime as a "single phenomenon" is unlikely to yield accurate or effective cross-national comparisons. This is due to the differences in the "cybercrime" definitions used in the various recording systems and which causes many cybercrimes to be recorded as traditional crimes. Given such variations and the on-going evolution of the cybercrime definition, the digital modus operandi (MO) of traditional crime offers a different line of reasoning; i.e. most forms of cybercrime are not unique to the online world since they have long-established traditional (offline) counterparts [16,17]. Consequently, an alternative approach is to use traditional definitions of crime and quantify the amount of associated ICT that each offence contains.

This approach was used by Montoya, Junger, Hartel, et al. [18], who measured the extent to which ICT permeates traditional crime for residential and commercial burglary, threats and fraud. They found the ICT incidence to be 2.9% for residential burglary, 0% for commercial burglary, 16.0% for threats and 41.0% for fraud. For three out of four studied crimes [19], the figures are much higher than the percentage of 0.3%-0.5% reported by Domenie et al. [14]. Taken together, these four types of crime represent 36% of the registered crime in the Netherlands [18]. The present study continued along this path using this methodology to study the differences in cybercrime between Kolkata and The Netherlands. The objective of the present research is to assess the amount of ICT in fraud in both The Netherlands and Kolkata, investigate the similarities and differences regarding how ICT permeates crime in both countries, and to analyse the differences between traditional and digital crimes in terms of characteristics of the offence, of the victims and of the offenders.

The cross-cultural replication of the Dutch research presented several challenges which have been abundantly discussed in the literature [20]. The main methodological challenges encountered were:

I. Getting permission to execute the study and

II. Drawing a representative sample of the population. Since data collection was in the hands of the researchers, it was possible to use the same coding instrument in both countries.

The biggest challenges with regards to the Kolkata study relates to the complexity of the police structure, which involves many different departments with varying areas of jurisdiction. The research was performed at the Kolkata Police Headquarters which is the main police station controlling the metropolitan area of Kolkata. In addition, there are several local police stations which are responsible for sub-areas. The Anti-Bank Fraud Department of the Kolkata Police Headquarters is the department which primarily handles all fraud cases at the headquarters. It also handles other types of fraud cases which are not necessarily bank frauds. The types of fraud encountered in our sample are explained in a later section. The Anti-Bank Fraud section has jurisdiction over a particular geographical area around the station. However, if any fraud cases remain unsolved at the local police stations in other parts of the city, these get forwarded to the headquarters for further investigation. This introduces some variability in the sample of cases available for analysis at this location.

Despite these challenges, the data from Kolkata (even though it is not representative of the entire population) gives an insight into the difference between the nature of crime and investigation in two diverse societies. This aspect, in itself, constitutes a useful contribution of this research. Many amendments were made to the structure of the questionnaire used for the data collection. More details are presented in the following section.

Method

This study is based on two fraud samples from The Netherlands and Kolkata, India. The aim of our research was to apply the same method in both countries although this was not fully possible. The present research can be considered as a pilot study that could lead to further examination in other cities of India using larger samples. The study methods used in each country are explained in the next sections.

Permission to Execute the Study

In The Netherlands, the research was funded by the Dutch police; therefore, their collaboration was readily available. On the other hand, the Kolkata Police Headquarters was approached with a detailed proposal of the project. This proposal also contained a report of the Dutch findings as well as a letter of endorsement of the project from the Dutch counterparts, which aimed at legitimizing the project. These documents helped to reduce the skepticism which the Kolkata police initially had. After spending a significant amount of time and effort to convince the top officials (Assistant Commissioner of Police) of the Kolkata police, the permission was granted to perform this research using the records available at the headquarters. It was not possible to choose from a larger sample of cases as that would have required additional permissions (presumably given by the individual police stations) which was deemed impossible to obtain in the limited time frame in which the data collection was performed. There seemed to be no procedure at the Kolkata police to apply for permission to carry out research involving data collection from police records. Accordingly, permission was granted based on personal judgment and discretion of the officials in charge. A series of meetings with various top ranking Kolkata Police officers over a period of approximately 6 weeks was required before permission was granted. It was also evident from these discussions that this type of research was uncommon and there was skepticism about the possibility of obtaining permission.

Sample

Cases for this research were chosen from those that have been registered by the police. As the data is collected from the police files directly, the cases which are unreported are not covered in this research. Due to the difference in police structures as well as in the crime registration across the two countries, the samples are not fully comparable. In The Netherlands, data on all fraud cases was stored electronically and hence the researchers were able to draw a random sample for examination. The dataset in Kolkata was much more limited as no computerized records were kept and only paper copies were available. Moreover, only the fraud cases in the anti-bank fraud department of the Kolkata Police headquarters were available for analysis. Due to the small number of the cases, randomization was not deemed to be feasible and all the cases that were available were considered for analysis. The samples in both countries are described in more detail below.

Dutch sample

In The Netherlands, the analysis consisted of 300 randomly selected fraud cases registered by the police in the eastern Dutch provinces of over Ijssel and Gelderland. Cases were selected from all 2011 fraud cases that were registered in the East-Netherlands. Data collection took place from March until June 2012. For more information, refer to Montoya et al. [19], Jansen et al. [21] and for the full report in Dutch refer to Junger et al. [18].

Indian sample

The Indian data consisting of 62 fraud cases was collected at the Kolkata Police Headquarters in Kolkata, during March and April, 2013 [22]. The researchers were given access to the crime indexes of the Anti-Bank Fraud Squad of the Detective Department at the Kolkata Police Headquarters which handles all the traditional and digital fraud cases. A crime index is a journal of information about cases handled by a particular department during a calendar year. Each entry contains information about the place where the crime was committed, date of crime, date of cognizance, suspects' details (names, address, age, occupation, etc.) and details about the complainant. All crime indexes corresponding to 2010, 2011 and 2012 were included in this study.

Data collection

In both countries, the data collection was done at the police stations since the files couldn't leave the premises. A checklist was used to extract and translate the information present in the police files. Data from the Kolkata police was coded using an adaptation of the Dutch checklist. The checklist was kept as identical as possible but some local adaptations had to be made, e.g. names of Indian cities were added to the "location" field. In The Netherlands, six trained research assistants participated in the coding and seventy cases were double coded to assess inter-rater reliability. Overall, Kappa values showed good reliability [19]. In Kolkata, the coding was done by the first author of this article.

In both countries, the case records were entered by the investigating officer of a particular case and there was therefore often a difference in the level of information across cases. Each entry in the crime index also contains a small description of the offence itself. After initial information is recorded, the investigating officer updates the information and registers how the investigation proceeds. This includes the addition of details about newly acquired evidence, witness accounts, court hearing details, etc. The difference between the Dutch and Kolkata records is that the latter ones do not contain information about all the victims, but only about the complainant, who - based on our reading of the files, are also the victim. Hence, all data labelled as “victim” refers to data about the complainant. A considerable amount of basic information about the suspects is also missing in several Indian cases.

Concepts

In The Netherlands, fraud cases involve deception/scams, forgery/counterfeiting of documents and welfare/insurance fraud [18]. In Kolkata, the fraud cases involve counterfeiting/forgery of documents, cheating and deception by fraudulently inducing the victim and criminal breach of trust. These offences are defined in detail in the Indian Penal Code [23].

Information about the following concepts was collected from the police records:

a) Characteristics of the offence: Details such as location, date of offence, date of cognizance and police district. The *number of offenders* in a case was coded as ‘alone’ or ‘more than one offender’. The *relationship between offender and victim* consisted of different categories: a professional relationship, family, acquaintances, neighbours, ex-partners, partners, criminal contacts, online social network, fellow gamers, chat friends or another relationship. *Location* relates to whether at the moment of the crime execution, the victim and offender were:

i. Both in the Eastern region of The Netherlands or in West Bengal (Kolkata is the capital of this province),

ii. Either of them in the Eastern region of The Netherlands (or in West Bengal for the Indian cases), iii) either of them abroad, and

iii. Both of them elsewhere in The Netherlands (or in India but outside West Bengal for the Indian cases).

Information such as the value of the loss (in Euros), items acquired during the offence and whether personal information was stolen was noted. Finally, the coders filled out a brief description of each offence.

b) Digital Modus Operandi - A fraud offence was classified as “digital” if its commission included one or more of the following characteristics:-

i. Unwanted email sent to the victim at some stage (e.g. a phishing or spam email to lure the victim).

ii. Digital forgery: the suspect hacked into the victim’s email or other account or impersonated him online.

iii. Digital burglary: victim’s credentials were stolen by the suspect.

c) Information About Suspects and Victims

1. A. *Sex* although in some cases the victim or offender was a business.

B. *Age*: either younger or older than 40 years.

C. *Nationality*: country of birth (i.e. Dutch, Indian or other).

D. *Being employed*: having a legal occupation.

E. Criminal record: ‘present’ or ‘absent’.

F. The *relationship between offender and victim* consisted of different categories: a professional relationship, family, acquaintances, neighbours, ex-partners, partners, criminal contacts, online social network, fellow gamers, chat friends or another relationship.

G. As mentioned above, for the cases in Kolkata, the coder did not find any particular case where the ‘complainant’ was not the ‘victim’.

Analysis

The data was analysed using contingency tables and Chi Squares. However, since several authors warn against relying exclusively on statistical significance testing and argue in favour of investigating the size of relationships [24,25], odds ratios (OR) and 95 % confidence intervals of the ORs were also computed. Because information was not always available, the number of cases for the analyses varies. Accordingly, the number of cases corresponding to each variable is mentioned in each table. Because the aim of our study was to compare digital and traditional frauds but also compare across countries, we looked at statistical significance but also noted non-significant trends in the data. Mention will be explicitly made each time a non-significant finding is discussed (i.e. a ‘trend’). In order to protect the offender and victim’s privacy, information was anonymized.

Results

Offences

Information was available for 274 fraud cases (281 suspects and 278 victims) in The Netherlands and 62 fraud cases (203 suspects and 62 victims) in Kolkata. The results are summarised below.

Digital Aspects of Fraud

There are two main types of fraud modus operandi (Table 1). 23.3% of frauds in Kolkata were digital whilst this number is higher in The Netherlands (40.1%; p<.001). The more common digital modus operandi is digital forgery. This usually means that some form of hacking has occurred (14 cases) or some form of online shopping fraud has taken place. Digital forgeries occur mostly before or during the actual commission of the fraud. Digital burglaries were also observed during the analysis but there were less of them compared to digital forgeries. Digital burglaries refer to incidents such as stealing passwords or other credentials. 3.2% of digital frauds in Kolkata involved digital burglaries whereas this number is marginally higher (5.1%) in The Netherlands. In Kolkata, a higher number of digital burglaries were observed before the commission of the fraud whereas in The Netherlands, it was more often found to be during the commission of the fraud.

How to cite this article: Gaurav M, Marianne J, Lorena M. A Cross-National Study on Cybercrime: Incident, Suspect and Victim Characteristics for Digital and Traditional Fraud in the Netherlands and Kolkata, India. J Forensic Sci & Criminal Inves. 2017; 4(2): 555634. DOI: 10.19080/JFSCI.2017.04.555634.

Table 1: ICT component (modus operandi) of fraud case in The Netherlands (N=274) and Kolkata (N=62), (in % of N for each sample).A crime script consisting of three stages in the execution of an offense was used: the preparation of the offense (i.e. 'before'), the event itself (i.e. 'during') and after the event has taken place (i.e. 'after').

	Digital Forgery			Digital burglary		
	Kolkata	The Netherlands	Pearson Chi-Square	Kolkata	The Netherlands	Pearson Chi-Square
Before the offence	16.7	9.5	2.64	3.2	0	8.89**
N	10	26		2	0	
During the offence	23.3	38.7	5.04*	1.6	5.1	1.45
N	14	106		1	14	
After the offence	5.0	2.9	0.67	0	0	-
N	3	8		0	0	
Total	23.3	40.1	5.96*	3.2	5.1	0.40
N	14	110		2	14	

*p < .05, ***p < .001

Proximity between suspects and victims

Traditional frauds in both countries are more localized compared to digital frauds (Table 2). In Kolkata, in a large majority (93.6%) of traditional frauds, the suspect and the victim resided in West Bengal in contrast to 54.0% of digital frauds. In The Netherlands, 57.5% of traditional frauds involved both a suspect and victim from the Eastern region in contrast to 19.4% of digital frauds. In both countries, digital frauds are less local than traditional frauds. Regarding international offences, only 2% of the digital frauds in Kolkata had an international component while this was not observed in any traditional frauds. The Dutch frauds show a similar proportion (i.e. 12.3% of traditional and 13.9% of digital frauds). Few cases are international; in India only 2% of the digital frauds whilst in The Netherlands 12.3% of the traditional frauds and 13.9% of the digital frauds.

Table 2: Proximity between the suspect and victim for traditional and digital frauds in The Netherlands (N=274) and Kolkata (N=62), (in % of N for each sample).

Proximity of suspect and victim	Kolkata, India		Netherlands	
	Traditional	Digital	Traditional	Digital
Both in local 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 and 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

All results in this table are significant with p<.001

Number of suspects and victims

In Kolkata, there is no significant difference between traditional and digital frauds in terms of the number of suspects (Tables 3 & 4), although there is a trend for digital frauds (35.7%) to be more often committed by a single suspect compared to traditional frauds (29.3%). In The Netherlands, digital frauds have more often a single suspect (82.4%) compared to traditional frauds (94.4%). We noted that overall, in The Netherlands much more fraud seems to be committed by single offenders compared to India. Suspect and victim characteristics are reported in Table 3 and summarised below.

How to cite this article: Gaurav M, Marianne J, Lorena M. A Cross-National Study on Cybercrime: Incident, Suspect and Victim Characteristics for Digital and Traditional Fraud in the Netherlands and Kolkata, India. J Forensic Sci & Criminal Inves. 2017; 4(2): 555634. DOI: 10.19080/JFSCI.2017.04.555634.

Table 3: Suspect and victim characteristics for traditional and digital fraud in India and The Netherlands (in %).

Suspect and victim characteristics	Kolkata, India			Netherlands		
	Traditional	Digital	p	Traditional	Digital	p
Gender						
Suspects (% of women)	6.9	2.0		18.9	19.1	
Victims (% of women)	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	**
Country of Origin (% of local born)						
Suspects	97.9	84.0	***	71.6	96.0	**
Victims	93.5	100.0		86.1	92.4	
Paid/Legal Employment						
Suspects	80.0	18.2	***	11.8	6.3	
Victims	96.6	90.0		16.9	13.4	
Suspects (above 18)	79.4	18.2	***	16.2	26.9	
Victims (above 18)	85.7	43.8		22.2	13.5	
Criminal record						
Suspects	0.0	6.0	**	8.8	11.7	
Victims	0.0	0.0		0.6	0.0	
Number of suspects/victims						
Suspects (single suspect)	29.3	35.7		82.4	94.4	*
Victims (single victim)	100.0	100.0		95.2	93.8	*

The numbers of cases on which these percentages are based are presented in the appendix (table 1).

*p<.05.**p<.01. ***p<.001

Table 4: Number of cases Suspect and victim characteristics for traditional and digital fraud in India and The Netherlands (in %).

Suspect and victim characteristics	Kolkata, India		Netherlands	
	Traditional	Digital	Traditional	Digital
Gender				
Suspects	145	50	122	47
Victims	44	14	113	103
Age				
Suspects	122	49	74	26
Victims	4	2	110	105
Country of Origin				
Suspects	145	50	74	25
Victims	46	14	108	105
Paid/legal employment				
Suspects	40	11	170	111
Victims	29	10	166	112
Paid/legal employment (above 18 years)				
Suspects (above 18)	34	11	69	25
Victims (above 18)	7	16	108	104
Criminal record				

Suspects	146	50	170	111
Victims	46	14	166	112
Number of suspects involved	41	14	136	72
Number of victims involved	46	14	163	111

Suspect Characteristics

a) Gender: In both countries there are more male suspects. Regarding female offenders, in both countries there are no differences between traditional and digital frauds. Overall, there seems to be more female fraud suspects in The Netherlands compared to Kolkata.

b) Age: In Kolkata, digital fraud suspects are younger than traditional fraud ones: 89.8% versus 63.3% of the suspects respectively are below the age of 40 ($p<.001$). A similar but non-significant trend is observed in The Netherlands where 73.0% of the digital fraud suspects are below the age of 40, compared to 62.2% for traditional frauds.

c) Country of origin: More traditional fraud suspects (97.9%) are Indian-born compared to those of digital frauds (84.0%). However, an opposite relationship is evident in The Netherlands; more digital fraud suspects (96.0%) are locals compared to traditional frauds (71.6%).

d) Employment: In Kolkata, more traditional fraud suspects (80.0%) are employed. For digital frauds, the number is very low (18.2%, $p<.001$). In The Netherlands, no significant differences are found between suspects of digital and traditional fraud.

e) Criminal record. In Kolkata, 6% of digital fraud suspects had previous police records while no traditional fraud suspects had such records ($p < .01$). In The Netherlands, no significant differences are found between digital and traditional fraud with respect to the number offenders with previous police records.

Victim characteristics

a) Sex: There are no significant differences between traditional and digital frauds in either Kolkata or The Netherlands in terms of sex of the victim.

b) Age: In Kolkata, no digital fraud victims are younger than 40 but there was one of traditional fraud. In The Netherlands, digital fraud victims (45.7% younger than 40) are younger compared to traditional frauds (28.2% younger than 40, $p<.01$).

c) Country of origin: In Kolkata, all digital fraud victims were Indians but some of traditional frauds (6.5%) were foreigners. In The Netherlands, the amount of local born digital fraud victims (92.4%) is higher than that of traditional frauds (86.1%). In both countries these differences are non-significant.

d) Employment: In Kolkata, no statistical differences are found with respect to the employment of victims. However, the number of victims who are employed seems to be higher in Kolkata, with 96.6% for traditional fraud and 90.0% for digital frauds, compared to The Netherlands, where the number of employed digital fraud victims is 13.4% and 16.9% for traditional frauds.

e) Criminal record: There are no victims with previous police records in the Indian sample whilst in The Netherlands only 0.6% of traditional fraud victims had previous police records compared to none of digital frauds. In both countries these differences are non-significant.

Relationship between suspect and victim

Table 5: Number of cases Suspect and victim characteristics for traditional and digital fraud in India and The Netherlands (in %).

Suspect and victim characteristics	Kolkata, India		Netherlands	
	Traditional	Digital	Traditional	Digital
Gender				
Suspects	145	50	122	47
Victims	44	14	113	103
Age				
Suspects	122	49	74	26
Victims	4	2	110	105
Country of Origin				
Suspects	145	50	74	25

Victims	46	14	108	105
Paid/legal employment				
Suspects	40	11	170	111
Victims	29	10	166	112
Paid/legal employment (above 18 years)				
Suspects (above 18)	34	11	69	25
Victims (above 18)	7	16	108	104
Criminal record				
Suspects	146	50	170	111
Victims	46	14	166	112
Number of suspects involved	41	14	136	72
Number of victims involved	46	14	163	111

In The Netherlands, the suspect and the victim were business partners in 47.3% of the traditional frauds compared to 24.0% of digital frauds (Table 5). There were also some noticeable but non-significant trends. More traditional frauds (7.0%) involve acquaintances compared to digital frauds (1.8%). There were also some traditional frauds (3.5%) among ex-partners but no such digital fraud cases were found. In Kolkata, the suspect and the victim were business partners in 50.7% of the traditional frauds compared to 24.0% of digital frauds (results were non-significant). There were some instances (18.5%) of traditional frauds involving acquaintances. This number was somewhat lower for digital frauds (12.0%). 4.1% of the traditional frauds were labelled as “other relationship”. For example, in one case, the suspect was a caretaker of the hostel where the victim was living. No fraud cases involved family members, partners, ex-partners, criminal contacts, friends on social network, fellow gamers or chat friends.

Investigation and Confiscation

Table 6: Comparison of traditional and digital frauds in terms of digital investigation and confiscation in The Netherlands (N=274) and Kolkata (N=62), (in % of N for each sample).

Confiscation and investigation	**Kolkata, India**			**Netherlands**		
	Traditional	**Digital**	**p**	**Traditional**	**Digital**	**p**
Digital data (YouTube videos, etc.) confiscated	0.0	0.0		0.0	12.6	***
Camera images confiscated	35.3	60.0	**	3.5	0.0	*
Phone data confiscation	10.0	22.0	*	2.4	3.6	
Digital traces of suspect found	8.7	38.0	***	5.9	56.8	***
Digital investigation and confiscation (total)	50.0	98.0	***	10.6	57.7	***
N	150	50		70	111	

*p<.05.**p<.01. ***p<.001

No cases in Kolkata involved digital data confiscated by the police whilst in The Netherlands, 12.6% of the digital frauds did (Table 6). In Kolkata, 35.3% of traditional frauds involved confiscated camera images compared to 60.0% of digital frauds (p < .01). However, camera image confiscation is not prevalent in The Netherlands since only 3.5% of traditional frauds and none of the digital fraud cases involved it (p < .001). In Kolkata, more digital frauds (22.0%) involve phone data confiscation compared to traditional frauds (10.0%). Although phone data confiscation is also minimal in The Netherlands, digital frauds (3.6%) have marginally more compared to traditional frauds (2.4%). This trend, however, was found to be non-significant. In Kolkata, digital frauds (38.0%) involve more investigations with digital traces of the suspect compared to traditional frauds (8.7%). In The Netherlands, a similar trend is observed as 56.8% of digital frauds involved digital traces of the suspect compared to only 5.9% of traditional frauds (p < .001).

Discussion

The primary objective of this research was to assess the amount of information and communication technologies (ICT) in fraud in both The Netherlands and Kolkata, India with the aim of investigating the similarities and differences to establish how ICT permeates crime. To this end, offence, suspect and victim characteristics were analysed to understand how technology has influenced crime. Below the main findings are summarized. The focus was on suspect characteristics since victim information is incomplete for Kolkata. The exploratory nature of this study should be emphasized. To maximize possible conclusions, this research did not focus solely on statistically significant differences between digital and traditional crimes; non-significant findings are also pointed out.

Traditional vs. Digital

23% of the frauds are digital in Kolkata and 40% are digital in The Netherlands. Three trends were similar in both countries. First, digital offenders were younger than traditional offenders. In The Netherlands, however, this is a non-significant difference. Previous research has also reported that offenders of digital crime are younger than traditional offenders [26]. Second, in both countries, digital crimes are committed more often by single offenders (the finding is non-significant for India).

No research seems to have so far reported information on a comparison of these characteristics between digital and traditional offenders. However, the UNODC states that most cybercrime is organised crime. Although our findings can't report on the offender as being part of a larger organised crime network, the present findings are not supportive of the UNODC [15] study. Finally, for digital frauds, the proximity between suspects and victims increases. Less digital frauds were found among suspects and victims from the same province compared to traditional frauds. However, in both countries international fraud was relatively rare. Again, no research seems to have presented data on this feature of crime and compared digital with traditional crimes. However, as many studies argued [26] cybercrimes can be carried out remotely. However, the UNODC also argued that a considerable amount of cybercrime is international, which is not supported by the findings in India nor in The Netherlands.

With regard to the relationship between suspect and victim, findings differ between the two countries. In Kolkata, more traditional frauds involved the suspects and victim being business partners compared to digital frauds. This also includes situations where the suspect sold a commodity/service to the victim. However, an opposite trend was observed in The Netherlands since more digital frauds involved business partners compared to traditional ones. This seems to point to the medium of the transaction. In The Netherlands, online trade (e.g. Markplaats) is prevalent while this is not yet so common in Kolkata, where most fraudulent transactions involved forgery of documents and were thus classed as traditional frauds. Again, we did not find previous research to compare our findings. We observed that 'insider crime' [27] is difficult to study by doing research within organisations, and that studying police records allows to collect some information on this special category of crime.

Diverging trends were found for four characteristics. In Kolkata, more digital offenders are born outside India, are unemployed and have a criminal record. Traditional and digital offenders in The Netherlands do not differ with respect to these characteristics, except for the nationality of suspects: more Dutch digital suspects are Dutch nationals. Finally, the findings differ with respect to the relationship between suspect and victim: less digital suspects in Kolkata are business partners compared to traditional offenders, whilst in The Netherlands the opposite is the case. These finding show that the characteristics of digital fraud versus traditional fraud are not consistent across the two countries. Our second objective was to discuss the theoretical implication of these findings.

The main findings of this research were:

a. Digital offenders in both countries are younger compared to traditional offenders,

b. Digital crimes involve more single offenders and,

c. Only 6% of the digital suspects in Kolkata have a criminal record and no differences were found in The Netherlands.

The above mentioned trends seem to fit the Routine Activities Theory (RAA) [28]. The RAA focuses on the circumstances in which criminal offences are carried out rather than on the characteristics of the offenders. Future research could focus more explicitly on the RAA to explain differences between digital and traditional offenders. As expected, digital frauds in both countries require the police to perform more confiscation of digital items compared to traditional frauds. It is surprising that the Kolkata police use more investigation and confiscation than the Dutch police. A large share of the digital confiscations in Kolkata involved camera images. This can be explained by the large number of ATM frauds involved. This is due to the usual police request for CCTV footage of the ATM machine and surrounding areas in such crimes.

Cross-National Comparison

Some differences were found between the two countries such as with respect to proximity between suspect and victim. Both traditional and digital frauds seem to be much more localized in India compared to The Netherlands. Contextual factors might also explain this difference since the Eastern state of West Bengal has its own language. Since most of the Indian states have their own language(s), this might create a barrier for criminals, especially for traditional frauds since many involve forging documents. These contextual differences support Crime Science approaches, such as the RAA (see above) and the Rational Choice model of crime [29,30] that emphasize the importance of context to explain the occurrence and the type of crime that takes place in various environments. Although the findings are new for Kolkata, some limitations need to be mentioned.

All the data was collected from the Kolkata Police Headquarters due to logistical reasons since it was easier to persuade the top hierarchy of the Kolkata police to participate in this research rather than approaching individual police stations. However, this limited the sample size. Ideally, randomly selected cases for our study should have been selected from a large pool of case files. Since only 62 fraud cases were registered with the Anti-Bank Fraud Squad of the Kolkata Police Headquarters in 2010, 2011 and 2012, all of them were included in the research. The Kolkata Police Headquarters is the only police station in the metropolitan area of Kolkata which has a specialized team to deal with fraud cases. Therefore, they receive most of the fraud cases that have not been solved by the subordinate police stations.

Since in India the access to case files is denied as long as a case is in court, there was only access to the crime indexes maintained by the police as most of the cases studied were “sub-judice” and the case files were inaccessible. These crime indexes contain an abstract view of the case and the quality and quantity of the content differs across cases. Another deficiency relates to the information about victims. Only information about the complainant is recorded in the crime indexes, hence no information was available on victims. For some variables, information was available for a small number of the victims. In addition, only a small sample of cases in one city of India was studied. Replication of the study elsewhere in India would enable the investigation of whether the results can be extrapolated and generalized nationally. It would also be interesting to study the effect of ICT on crimes other than frauds to identify whether in India some crimes are more affected by ICT than others.

In The Netherlands, the sample consists of cases reported to the police in East Netherlands. Regional disparities exist and thus the extent to which these numbers are representative of the country as a whole must be determined. Residents of large cities are often victims of crime twice as often compared to those living in the countryside [31]. Internet use also differs by region. Residents of large cities are online more hours than those of rural areas [32]. The information is based on victim reports as registered by the police and doubt exists as to how accurate these are particularly in relation to the digital nature of crimes. However, based on our reading of the files [19], it appears likely that the police do not accurately register digital modus operandi (MO). This could imply that the figures of digital crime might actually be higher. Another limitation is that, in some crimes the MO is unknown. For instance, sometimes police officers found that burglars used Google Maps and information from websites to identify and burgle wealthy houses. The present study did not find evidence of this type of digital preparation. However, even if offenders used these digital MO’s, it is unlikely that the victims were aware of it, which means that it went unnoticed unless an apprehension occurred. Despite these research limitations, we believe that the results provide a good insight into how ICT affects fraud in two countries with differing levels of technological penetration.

Conclusion

The present research compared 62 fraud cases from 2010 through 2012 registered by the Anti-Bank Fraud Squad of the Kolkata Police Headquarters and 274 fraud cases from 2011 registered by the Dutch National Police. These cases were analysed with the aim of identifying how differences between digital and traditional frauds illustrate how ICT has influenced crime. The research had several methodological challenges which led to limitations regarding the interpretation and generalization of the results. These limitations have been enumerated in this article. However, despite the identified limitations, we believe that this cross-country comparison provides valuable insights into some differences between digital frauds in these two countries.

References

1. Petee TA, Corzine J, Huff-Corzine L, Clifford J, Weaver G (2010) Defining ‘Cyber-Crime’: Issues in Determining the Nature and Scope of Computer-related Offenses. Paper presented at the Proceedings of the Futures Working Group, University of Twente, Europe, p.1-7.
2. Wall DS (2010) The Internet as a Conduit for Criminal Activity (Revised March 2010). The Internet as a Conduit for Criminal Activity p. 1-17.
3. Albanese, SJ (2000) The Causes of Organized Crime Do Criminals Organize Around Opportunities for Crime or Do Criminal Opportunities Create New Offenders? Journal of Contemporary Criminal Justice 16(4): 409-423.

4. Clarke RV (2004) Technology, criminology and crime science. European Journal on Criminal Policy and Research 10(1): 55-63.

5. Felson M (1998) Crime and everyday life. Thousand Oaks, Pine Forge Press, CA, USA.

6. Felson M (2006) Crime and nature: Sage publications, USA.

7. Anderson R, Barton C, Boehme R, Clayton R, J G van Eeten, et al. (2012) Measuring the cost of cybercrime. Paper presented at the 11th Workshop on the Economics of Information Security, Berlin, Germany, p. 1-31.

8. Trustwave (2013) 2013 Trustwave Global Security Report. In Trustwave , London, UK.

9. Verizon (2012) 2012 Data Breach Investigations Report. Verizon, new jersey, USA, p. 1-92.

10. Bureau of Justice Statistics (2012) IC3 2011 Internet Crime Report. FBI National Press Office Washington DC, USA.

11. Bank TW (2014) Internet Users (per 100 people). World Development Indicators Internet Users (per 100 people), World Development Indicators p.1-3.

12. Ahonen T (2011) Smartphone penetration rates by country. We Have Good Data (finally). Luetta vissa.

13. Skogan W (1999) Proceedings from the Police Research Institute Meetings. National Institute of Justice p. 37-54.

14. Domenie M, Leukfeldt E, Toutenhoofd-Visser M, Stol W (2009) Werkaanbod cybercrime bij de politie: een verkennend onderzoek naar de omvang van het gereg is treerde werkaanbod cybercrime. Lectora at Cyber safety, Noordelijke Hoge school Leeuwarden, Netherlands, p. 1-48.

15. UNODC (2013) Comprehensive Study on Cybercrime. Draft Comprehensive Study on Cybercrime. Draft. Vienna, Austria: Organized Crime Branch, Division for Treaty Affairs, New York, USA, pp. 1-320.

16. Grabosky PN (2001) Virtual criminality: old wine in new bottles? Social & Legal Studies 10(2): 243-249.

17. Jordan T, Taylor PA (2004) Hacktivism and cyber wars: rebels with a cause?: Psychology Press. pp. 1-193.

18. Junger M, Montoya L, Hartel P, Karemaker M (2013) Modus Operandi onderzoek naar door Informatie en Communicatie Technologie (ICT) ge faciliteerde criminaliteit.

19. Montoya L, Junger M, Hartel PH (2013) How `Digital' is Traditional Crime? Paper presented at the European Intelligence and Security Informatics Conference, EISIC 2013, Uppsala, Sweden, Europe.

20. Liamputtong P (2008) Doing Research in a Cross-Cultural Context: Methodological and Ethical Challenges. In P Liamputtong (edn.), Doing Cross-Cultural Research, Springer, Netherlands 34: 3-20.

21. Jansen J, Junger M, Montoya L, Hartel PH (2013) Offenders in a Digitized Society. In: WP Stol, J Jansen (Eds.), Cybercrime and the police. The Hague, Eleven International Publishing, Netherlands, p. 45-59.

22. Misra G (2013) Permeance of ICT in Crime in India. University of Twente, Enschede, The Netherlands, Europe.

23. Indian Law Commission (1838) The Law book Exchange, Ltd. Indian Penal Code, India.

24. Carver RP (1978) The Case Against Statistical Significance Testing. Harvard Educational Review, 48(3): 378-399.

25. Schmidt FL, Hunter JE (1997) Eight common but false objections to the discontinuation of significance testing in the analysis of research data. What if there were no significance tests 37-64.

26. Leukfeldt R, Veenstra S, Stol W (2013) High Volume Cyber Crime and the Organization of the Police: The Results of Two Empirical Studies in the Netherlands International Journal of Cyber Criminology 7(1): 1-17.

27. Samonas S (2013) Insider fraud and routine activity theory. p.1-32.

28. Cohen LE, Felson M (1979) Social change and crime rate trends: A routine activity approach. American sociological review 44(3): 588-608.

29. Cornish DB, Clarke RV (2008) The Rational Choice Perspective. In R Wortley, L Mazerolle (eds.), Environmental Criminology and Crime Analysis. Willan Publishing, Cullompton, UK.

30. Wortley R, Mazzerole L (2008) Environmental Criminology and Crime Analysis: Situating the Theory, Analytic Approach and Application. In R Wortley, L Mazzerole (eds.), Environmental Criminology and Crime Analysis, Willan Publishing, Cullompton, UK.

31. Eggen ATJ, Kessels RJ (2011) Criminaliteit en rechtshandhaving 2010. Ontwikkelingen en samenhangen. In SN Kalidien, NEd Heer-de Lange (eds.), Den Haag, the Netherlands: Boom Juridische Uitgevers, CBS, WODC, USA, p. 53-87.

32. van Den Broek A, Koen B, De Haan J, Harms L, Huysmans F (2006) Thuis op het platteland: de leefsituatie van platteland en de stad vergeleken. In A Steenbekkers, C Simon, V Veldheer (eds.), Den Haag: Sociaal Cultureel Planbureau, Netherlands, pp. 289-316.

This work is licensed under Creative Commons Attribution 4.0 License

DOI: 10.19080/JFSCI.2017.04.555634

Your next submission with Juniper Publishers will reach you the below assets

- Quality Editorial service
- Swift Peer Review
- Reprints availability
- E-prints Service
- Manuscript Podcast for convenient understanding
- Global attainment for your research
- Manuscript accessibility in different formats

(Pdf, E-pub, Full Text, Audio)

- Unceasing customer service

Track the below URL for one-step submission

https://juniperpublishers.com/online-submission.php

How to cite this article: Gaurav M, Marianne J, Lorena M. A Cross-National Study on Cybercrime: Incident, Suspect and Victim Characteristics for Digital and Traditional Fraud in the Netherlands and Kolkata, India. J Forensic Sci & Criminal Inves. 2017; 4(2): 555634. DOI: 10.19080/JFSCI.2017.04.555634.