

Combating crime in international electronic commerce

JA KOUAMO
23659777

Dissertation submitted in *partial* fulfillment of the requirements
for the degree *Magister Legum* in *Import and Export Law* at
the Potchefstroom Campus of the North-West University

LLM Import and Export Modules Passed:

LLMI 873

LLMI 886

LLMI 887

LLMI 892

LLMI 894

LLMI 895

Supervisor: Prof SPLR de la Harpe (NWU)

Co-Supervisor: Dr W Erlank (NWU)

November 2013

ABSTRACT

Electronic commerce, broadly defined as doing business online, has with the advent of the Internet and more importantly of the World Wide Web, developed at an unanticipated speed. Electronic transactions have been said to be very convenient, fast and limitless. This limitless character of electronic commerce does not only have advantages but also a number of disadvantages. E-commerce has opened very wide doors to criminals who take advantage of both the advancement in technology and the cross-border nature of the Internet to deceive other people. Over the years there have been attempts to find solutions to the increasing problem of cybercrime in general, and crime in international electronic commerce (IEC) in particular. To date, even though techniques have been developed, laws have been enacted and some initiatives are still ongoing, there seems to be much more to do in order to achieve a successful fight against online crime. E-commerce has been presented as an aspect of the broad cyber universe and the solutions so far provided are meant for cybercrime in general. Thus, it appears that e-commerce and more precisely crime in IEC is an aspect that should be given consideration to in the sense that specific laws need to be passed on the issue.

OPSOMMING

Elektroniese handel, wat beteken om besigheid aanlyn te doen, het met die ontstaan van die Internet en meer belangrik, die Wêreldwye Web, teen 'n ongekende spoed ontwikkel. Elektroniese transaksies is al as baie gerieflik, vinnig en sonder perke beskryf. Hierdie onbeperkte aard van elektroniese handel het voor- en nadele. Dit het deure vir misdadigers wyd oop gemaak om voordeel te trek uit die ontwikkeling van tegnologie en die internasionale aard van die Internet om ander mense te bedrieg. Oor die jare was daar pogings om oplossings te vind vir die toenemende probleem van kubermisdaad oor die algemeen, en misdaad in internasionale elektroniese handel in besonder. Tot op datum, selfs al is sekere tegnieke ontwikkel, wette in werking gestel en sommige inisiatiewe geloods, is daar nog baie wat gedoen moet word om aanlyn misdaad te bekamp. Elektroniese handel is aangedui as 'n aspek van die breë kuberruim, en die oplossings wat tot dusver gevind is, is bedoel vir kubermisdaad in die algemeen. Dit wil dus voorkom asof elektroniese handel en, meer spesifiek, internasionale elektroniese handel, 'n aspek is wat aandag moet geniet by die skryf van spesifieke wette oor die onderwerp.

KEYWORDS

Combating

Online crime

International

Electronic commerce

ACKNOWLEDGMENTS

I am truly grateful to God for all the graces he has bestowed on me for the past three years. I would also like to extend my sincere gratitude to the North-West University (Potchefstroom Campus) for equipping me both financially and materially for the completion of this research. To both my supervisors, thank you for being so patient with me and for your very constructive and unfailing support. Sincere words of gratitude go to Anita for her administration guided by a motherly touch. Last but not least, so many thanks to the precious and very supportive family God has blessed me with and to the wonderful friends I have.

TABLE OF CONTENTS

Abstract	i
Opsomming	ii
Keywords	iii
Acknowledgments	iv
List of abbreviations	viii
1 Introduction	1
2 The legal nature of crime with specific reference to e-commerce	8
<i>2.1 Introduction</i>	<i>8</i>
<i>2.2 The relationship between electronic and traditional crime</i>	<i>9</i>
<i>2.3 Brief overview of the common criminal activities encountered in IEC</i>	<i>11</i>
<i>2.3.1 Direct schemes generally amounting to crime in IEC</i>	<i>11</i>
2.3.1.1 Internet auction fraud	11
2.3.1.2 Travel and vacation business fraud	13
2.3.1.3 Health care fraud/Health insurance fraud	13
2.3.1.4 Chargebacks/denial of receiving service or product/distributed denial of service	14
2.3.1.5 Bogus returns	15
<i>2.3.2 Indirect criminal activities in IEC</i>	<i>15</i>
2.3.2.1 Phishing	15
2.3.2.2 Pharming	15
2.3.2.3 Advance fee scams	16
2.3.2.4 Identity theft and credit card fraud as consequences of indirect criminal activities	17
<i>2.4 Conclusion</i>	<i>18</i>
3 International and regional instruments against crime in international	19

electronic commerce	
3.1 Introduction	19
3.2 International instruments against online crime	20
3.2.1 <i>The United Nations and online crime</i>	20
3.2.1.1 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996) with additional article 5 bis as adopted in 1998	20
3.2.1.2 UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001)	21
3.2.1.3 United Nations Convention against Transnational Organised Crime and the Protocols Thereto (2000)	23
3.2.1.4 United Nations Convention against Corruption	24
3.2.1.5 The United Nations Convention on the Use of Electronic Communications in International Contracts (2005)	27
3.2.1.6 Other initiatives by the United Nations	28
3.2.2 <i>Other international instruments against crime in IEC</i>	36
3.2.2.1 The Council of Europe Convention on Cybercrime (2001)	36
3.3 Regional initiative against crime in IEC	40
3.3.1 <i>Draft African Union Convention on the Establishment of a credible Legal Framework for Cyber Security in Africa 2011</i>	40
3.4 Conclusion	43
 4 The South African legal position with regard to crime in international electronic commerce	 45
4.1 Introduction	45
4.2 The common law position	46
4.3 International Co-operation in Criminal Matters Act 75 of 1996	48
4.4 Prevention of organised Crime Act 121 of 1998	49
4.5 The Electronic Communications and Transactions Act 25 of 2002	50
4.6 Consumer Protection in South Africa	53
4.7 Conclusion	57

5 Conclusion and recommendations	59
Bibliography	62

LIST OF ABBREVIATIONS

ABLJ	American Business Law Journal
ACFE	Association of Certified Fraud Examiners
AIC	Australian Institute of Criminology
ASR	African Security Review
AU	African Union
B2C	Business-to-Consumer E-commerce
B2B	Business-to-Business E-commerce
B2G	Business-to-Government E-commerce
CCF	Credit Card Fraud
COE	Council of Europe
COECC	Council of Europe Convention on Cybercrime
CPA	Consumer Protection Act
DDoS	Distributed Denial of Service attack
EDPACS	The EDP Audit, Control, and Security Newsletter
ECC	Electronic Communications Convention
ECT Act	Electronic Communications and Transactions Act
E-commerce	Electronic Commerce
E-deal	Electronic deal
EDI	Electronic Data Interchange
E-platforms	Electronic Platforms
E-transactions	Electronic Transactions
E-signatures	Electronic signatures
FBI	Federal Bureau of Investigations
FTC	Federal Trade Commission
G2B	Government-to-Business E-commerce
GAO	United States General Accounting Office
GPRI	The Geneva Papers on Risk and Insurance
ICCM	International Co-operation in Criminal Matters Act
IEC	International Electronic Commerce

IJCLP	International Journal of Communications Law and Policy
IT	Information Technology
IJCSE	International Journal of Cyber Society and Education
IJEC	International Journal of Electronic Commerce
Interpol	International Criminal Police Organisation
JHTL	Journal of High Technology Law
JECM	Journal of Economic Crime Management
JICM	Journal of International Consumer Marketing
JILT	Journal of Information, Law and Technology
JWL	Journal of Workplace Learning
MAJ	Managerial Auditing Journal
MLEC	Model Law on Electronic Commerce
MLES	Model Law on Electronic Signatures
MUEJL	Murdoch University Electronic Journal of Law
NCC	National Consumer Commission
OECD	Organisation for Economic Co-operation and Development
PER	Potchefstroom Electronic Law Journal
PIN	Personal Identity Number
POCA	Prevention of Organised Crime Act
RICA	Regulation of Interception of Communications and Provision of Communications-Related Information Act
SALC	South African Law Commission
SALJ	South African Law Journal
SAMLJ	South African Mercantile Law Journal
SMS	Self-message Service
UN	United Nations
UNCAC	United Nations Convention against Corruption
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention against Transnational Organised Crime
US IFCC	United States Fraud Complaint Center
VAT	Value Added Tax

VJLT	Virginia Journal of Law and Technology
WWD	Women's Wear Daily
WWW	World Wide Web

1 Introduction

Electronic commerce (hereafter e-commerce) can broadly be defined as “doing business electronically”.¹ Dinodia and Tiwari² perceive e-commerce as “the buying and selling of products or services over electronic systems such as the Internet and other computer networks”. On their side, and in an attempt to limit the definition to their domain of research, Westland and Clark³ regard e-commerce as “the automation of commercial transactions using computer and communications technologies”. E-commerce in general comprises all the trading stages namely advertising online, exchanging information via computer networks, placing an order, paying for services rendered and receiving support for delivery.⁴ According to Rosen⁵ “e-commerce covers the range of online business activities for products and services, both business-to-business and business-to-consumer, through the Internet”. These different ways of approaching and defining e-commerce demonstrate that there is no generally agreed definition of the term. In trying to ascertain what it means, it should always be kept in mind that it is a developing concept that is to be defined according to the context at stake.⁶

The advent of the Internet and the World Wide Web (hereafter WWW)⁷ have resulted in e-commerce being perceived as the “way forward”,⁸ not only for the many advantages⁹ it has brought about, but also because it has given a completely new face to trade as a

1 Timmers *Electronic Commerce* XV.

2 Dinodia and Tiwari 2009 www.srdinodia.com.

3 Westland and Clark *Global Electronic Commerce* 1.

4 Timmers *Electronic Commerce* XV.

5 Rosen *E-commerce Question and Answer Book* 4.

6 Westland and Clark *Global Electronic Commerce* 1; see also Anonymous Date Unknown www.sagepub.com.

7 The Internet has come to streamline “e-transactions”. E-commerce before the Internet was restricted and not really common. EDI (Electronic Data Interchange) is one of the forms under which e-commerce was previously conducted and is still being conducted. See Timmers *Electronic Commerce* 3-4; see further Eiselen 1995 *SAMLJ* 1-18 for more regarding EDI in general.

8 Plant *Ecommerce* 2-3.

9 Advantages that, according to a Sagepub article, (SAGE is an international publisher of journals, books and electronic media for academic, educational and professional purposes) range from creation of a global market place to more efficient delivery processes, through connecting people worldwide and enabling them to transact from any location at any time to mention but a few. Anonymous Date Unknown www.sagepub.com.

whole. This picture of e-commerce can be justified by its impact on society.¹⁰ As an efficient and fast developing way of trading,¹¹ which is undoubtedly convenient and thus beneficial to all participants,¹² e-commerce has however also opened the door to a number of practices which, to a considerable extent, still hold it back.¹³ Put differently, the growth of e-commerce has given rise to several criminal activities that are perpetrated to deceive or defraud people relying on interconnected networks for their transactions.¹⁴ While some of these schemes are “age-old scams” that have been transplanted into electronic platforms (hereafter e-platforms), others have only seen the light with the development of e-commerce.¹⁵ They are generally regrouped under the umbrella of cybercrime which comprises among others of “attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, botnets, and various e-mail scams such as phishing.”¹⁶ Most writers sometimes simply use the word fraud to refer to all these illegal activities occurring online. E-commerce only being an aspect of the very broad cyberspace,¹⁷ the terms crime in international electronic commerce, online crime, and criminal activities perpetrated online would have precedence in this research paper over the terms cybercrime and fraud, as the author intends only to discuss illegal activities that may occur during an international e-commerce deal. However, and due to the fact that the solutions

10 That impact can be said to be overall positive, if consideration is given to the ease with which transactions are carried out electronically, and further to the number of transactions that take place via computer networks. See Albert 2002 *ABLJ* 578; see also Timmers *Electronic Commerce* 3-4; and Smith and Urbas 2001 www.aic.gov.au; see also Kariyawasam (ed) *The WTO* 39 for more regarding the influence of the Internet on e-commerce.

11 Timmers *Electronic Commerce* XV.

12 Baker 1999 *Internet Research* 358.

13 There might be countless advantages in trading online, but there are still a number of companies and individuals that are reluctant about engaging into any e-commerce deal. This, on the one hand, because they do not fully understand what it is all about, and more importantly, how to go about it, and on the other hand, for security purposes. Furthermore, fear exists about committing on a platform not well regulated or not regulated at all. See Timmers *Electronic Commerce* 8; see also Darch and Lucas 2002 *JWL* 151 for more regarding the barriers to e-commerce adoption; further, see Yang *South African SMME Owner/Manager's Perceptions* 23-24 for a full range of factors from different authors prompting some businesses and individuals to avoid e-commerce.

14 Brenner 2001 *MUEJL* 1.

15 Snyder 2002 www.nbcnews.com. According to this author, an example of an old scam that has been adapted to the digital world is credit card fraud; one example of a scam that has developed with technology, is the Distributed Denial of Service attack. See Brenner 2005 *IJCLP* 6.

16 Interpol Date Unknown www.interpol.int.

17 Murungi 2012 www.snailattorneys.com.

proposed for crime in IEC are the same proposed for cybercrime and fraud in general, cybercrime and fraud will in some instances be used.

To that end, illegal activities perpetrated online that relate to e-commerce, namely among others denial of service,¹⁸ phishing,¹⁹ pharming,²⁰ identity theft sometimes associated with credit card fraud,²¹ Internet auction fraud,²² travel and vacation business fraud,²³ health care fraud²⁴ and lastly, advanced fee scams²⁵ will be examined. More specifically, crime in e-commerce includes, but is not limited to: advertising or auctioning goods or services that do not exist, that are fake or simply substandard in a deceitful way.²⁶ It may also involve receiving payments and not rendering any services in return, or receiving goods and either refusing to pay, denying their reception or falsely claiming to have paid.²⁷ Another variation of online crime is using stolen credit cards to buy goods that are subsequently sold on auction sites. Online criminals may even require personal information from customers purporting to be from companies known to the customers, or direct customers to fake websites similar to the genuine ones.²⁸ They may also operate by tracing consumers' orders and misdirecting the seller on the

18 Attack that aims at rendering a web page or a system unavailable or unusable by rightful customers. See Singleton 2002 *EDPACS Newsletter* 9.

19 Scheme through which consumers are tricked into providing their personal information such as passwords and account numbers to people impersonating financial institutions. See ACFE 2011 www.acfe.com.

20 This attack consists of a consumer being driven into making available his personal data on a website that passes for the genuine website. ACFE 2011 www.acfe.com.

21 In this scheme, personal information is stolen and used for a range of illegitimate activities such as large online purchases, obtaining loans or opening several bank accounts with various addresses. See Standard Bank Date Unknown www.standardbank.co.za.

22 Internet auction is the process by which partakers bid against one another to buy products offered for sale on an Internet auction house. See Gregg and Scott 2006 *IJEC* 96.

23 See Better Business Bureau 2007 www.bbb.org. (BBB is an organisation based in America and Canada, founded in 1912, that aims at solving disputes between consumers and business, providing necessary information regarding ethical business practices and acting as an intermediary between consumers and businesses). According to the BBB, this variety of fraud is characterised by offers made to consumers in the form of travel packages that appear to offer massive bargains, but that turn out "too good to be true".

24 This scheme may comprise an untrue statement, a falsification or purposeful omission that is vital for the calculation of benefits. See ACFE 2011 www.acfe.com.

25 Smith, Holmes and Kaufmann 1999 *Trends and Issues in Crime and Criminal Justice* 1. These authors state that, in this scheme, people receive unrequested e-mails, faxes or letters containing unlawful proposals that may lead to considerable losses, if taken as the truth.

26 Smith and Urbas 2001 www.aic.gov.au.

27 Pathak 2004 *MAJ* 560-561.

28 These schemes are known as phishing and pharming.

delivery point or address.²⁹ Criminal operations in international e-commerce (hereafter IEC) may also be by interfering with and disturbing electronic payment systems or stealing other people's identity in order to impersonate them for financial benefit.³⁰ Crime in IEC thus takes different shapes according to the gain expected; the kind of addressee targeted and attained, and also on the type of transaction effected.³¹ Although it appears in different forms, the final outcome of each criminal activity carried out electronically will usually be to make financial profit.³²

Crime in IEC is neither easily traceable, nor easily prosecutable.³³ The nature of online crime renders these activities difficult ones to tackle.³⁴ One of the reasons being "...the low cost, the high speed, and the anonymity of the Internet".³⁵ The Internet makes it possible for information to be dispatched easily and inexpensively to a considerable audience. It thus becomes quite easy for people with evil intentions "to send credible looking messages" to potential victims.³⁶

Another difficulty in tackling online crime arises from the scarcity of appropriate regulatory measures, the inefficiency of existing regulations and most importantly, the international character of the Internet.³⁷ Information technology has thus increased the

29 Montague 2011 www.fraudpractice.com.

30 Smith and Urbas 2001 www.aic.gov.au.

31 Although there is one main way through which the crime is committed namely the Internet, the process of operation differs. See Smith 1998 www.aic.gov.au.

32 Smith and Urbas 2001 www.aic.gov.au.

33 Smith and Urbas are of the opinion that the cost of identification and prosecution of crime committed online is definitely a major problem. See Smith and Urbas 2001 www.aic.gov.au.

34 Smith and Urbas are of the view that the main difficulty in providing sound and appropriate response to fraud in e-commerce resides in the fact that transactions are not limited to one jurisdiction. They furthermore regard the multiplicity, complexity and difference in substance of rules that exist in various jurisdictions as barriers to the effective fight against fraud. See Smith and Urbas 2001 www.aic.gov.au.

35 Baker 1999 *Internet Research* 357; to the problem of anonymity, other writers add the "pseudonymity" of the Internet as one barrier to the detection and prosecution of fraud. See Brenner 2005 *IJCLP* 10.

36 Baker 1999 *Internet Research* 349.

37 Cassim 2009 *PER* 39. The Internet has certainly made e-commerce efficient and more practicable, but its openness goes beyond borders and it is this borderless aspect that hinders any effort made in trying to stop fraudulent behaviours perpetrated online. This does not mean that, within the territory of a country, tracing and prosecuting the crime is less strenuous, only that the matter is worsened when it has a cross-border effect. Cassim opines, regarding cybercrime in general, that existing laws

benefits of crime.³⁸ In a nutshell, online crime is not easily eradicable because of the Internet's interactive, decentralized, universal³⁹ and open⁴⁰ nature.

Weighing up the extra advantages that a crime free online trade could afford to society, techniques that can help minimise and possibly eradicate the risk of being victimised while transacting online, have been and are continually being developed.⁴¹

In an attempt to provide a solution to the concerns posed by cybercrime in general, it is said that each country should be able to give a broader sense to the "territorial notion" of jurisdiction so as to remove the barriers that give authority to a country to prosecute a crime only under particular circumstances.⁴² Several organisations⁴³ have tried to provide some solutions to the problem of cybercrime in general. The merits of all these initiatives reside in the fact that they have a broader scope compared to national legislation.⁴⁴ Although praiseworthy, all these initiatives have proven not to be sufficient or not to meet the challenges that online crime poses, both at local and international levels. Cassim⁴⁵ opines that their shortcomings come from the fact that they are made for specific countries. It may be inferred from this viewpoint that those instruments certainly do not take account of the realities in other countries and continents.

relating to cyberspace seem inefficient because of jurisdictional difficulties associated with sophisticated resources needed to trace, prosecute and convict criminals in other countries.

38 Lisanawati 2010 *IJCSE* 163.

39 Cassim 2009 *PER* 44.

40 Wopperer 2002 *GPRI* 393.

41 In order to ensure greater confidence in doing business online, security measures have been developed that aim at making web-based transactions safer for the stakeholders. The said security measures vary from raising "e-dealers'" awareness about the existing risks associated with online trade, to the features to find on a credible website etc. See Baker 1999 *Internet Research* 348.

42 Brenner and Koops 2004 *JHTL* 14.

43 The Council of Europe (COE) through its *Convention on Cybercrime* (adopted on November 8, 2001 and enacted on July 1, 2004), the Organisation for Economic Co-operation and Development through its *Guidelines for Consumer Protection in the Context of Electronic Commerce* (adopted on December 9, 1999 and entered into force in 2000). The United Nations on their side adopted in 2000 the *Convention against Transnational Organized Crime* which has a much larger scope than the others.

44 National legislation or domestic solutions which, according to Cassim, are unsound because "cyberspace has no geographic or political boundaries". See Cassim 2009 *PER* 66.

45 Cassim 2009 *PER* 67.

This research paper is concerned with crime in IEC⁴⁶ which happens either in business-to-consumer or consumer-to-consumer transactions.⁴⁷

Therefore, the aim of the research is to investigate and evaluate the measures, so far provided by some international instruments by the United Nations (UN),⁴⁸ the African Union (AU)⁴⁹ and the Council of Europe (COE)⁵⁰ to address the issue of crime in international e-commerce. Furthermore, the author's endeavour is to enquire into the efforts that have been made by South Africa⁵¹ to limit the effects of online crime in its territory. More specifically, are the solutions that have so far been proposed by these organisations and by South Africa, efficient enough to really curb crime in IEC? The choice of organisations is simply guided by their respective geographical capacity and also by the roles they have been playing in curtailing cybercrime in general.

In trying to provide an answer to the above question, it is of utmost importance to first define the borders of this research by exploring and understanding the legal nature of

46 United States General Accounting Office 2002 www.gao.gov. IEC is defined as trade via computer networks that cross borders. There might not be, as in the case of e-commerce, a general definition to IEC as mentioned by the US GAO, but being a component of e-commerce, IEC generally comprises an online dedication to sell, that results in the import or export of goods and services.

47 Business-to-consumer (commonly referred to as B2C) is a web-based platform via which a retail consumer willing to participate in a transaction interacts with an organisation. See Plant *Ecommerce* 24-28 for different definitions ascribed to e-commerce categories. Note is to be taken that the general and well-known distinction is made between business-to-consumer (B2C), business-to-business (B2B), business-to-government (B2G), government-to-business (G2B); and that the use of consumer-to-consumer in this paper is only a way to present other forms of criminal activities that arise within e-commerce, but that have nothing to do with businesses, or that take advantage of some B2C relationship.

48 Through the following instruments: *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* (1996) with additional article 5 *bis* as adopted in 1998, the *United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (2000), the *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment* (2001), the *United Nations Convention against Corruption* (2003), the *United Nations Convention on the Use of Electronic Communications in International Contracts* (2005), the *Handbook on Identity-related Crime* (2011) (UN Office on Drugs and Crime 2011 www.unodc.org) and finally, the *Draft Comprehensive Study on Cybercrime* (2013) (UN Office on Drugs and Crime 2013 www.unodc.org).

49 Through the *Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa* (2011).

50 Through the *Council of Europe Convention on Cybercrime* (2001).

51 Through its *International Co-operation in Criminal Matters Act* 75 of 1996, the *Prevention of Organised Crime Act* 121 of 1998, the *Electronic Communications and Transactions Act* 25 of 2002 and lastly, the *Consumer Protection Act* 68 of 2008.

crime, with specific reference to e-commerce (Chapter 2), before paying attention to the contributions of the United Nations, the Council of Europe and the African Union to the fight against cybercrime in general and crime in IEC in particular (Chapter 3). Thirdly, the focus will be on the South African legal position with regard to crime in IEC (Chapter 4). Lastly, in conclusion of this research, some solutions will be provided that can help curtail the pace at which crime in IEC is developing, to keep it within manageable limits and so make online trade a safer platform for all the stakeholders (Chapter 5).

2 The legal nature of crime with specific reference to e-commerce

2.1 Introduction

Crime as a basic concept has known considerable changes with web-based transactions.⁵² In other words, Information Technology has not only given crime new shapes and speed, but has also somehow made it difficult to prosecute successfully since on one side of the world, persons can victimise people on the other side without having to leave their desk or to know their victims.⁵³ As mentioned earlier, this paper focuses on IEC. However, it is important to emphasise that there is no real difference between the types of criminal activities committed within a particular country and those that go beyond borders. The main noticeable and distinguishing feature is that, when the crime has a cross-border effect, it becomes extremely difficult and sometimes impossible to trace and prosecute.⁵⁴ As the Internet, online crime has no borders.⁵⁵ The abuse of the Internet is to a considerable extent different from crime perpetrated offline. Although taxed as “old wine in new bottles”⁵⁶ there are substantive features that differentiate online crime from traditional crime. Brenner mentions that some authors see the difference between these two forms of crime as artificial since in the end it is all about crime.⁵⁷ Note is to be taken that many research papers to be used in this chapter are simply based on a comparison between online and offline fraud. However, and due to the fact that they make a clear distinction between an illegal activity perpetrated online and that perpetrated offline, the word crime will be mostly used instead of fraud. In the context they are usually the same. The purpose of this chapter is firstly to establish the relationship that exists between online and traditional crime and secondly, to briefly present some examples of behaviours that amount to crime in IEC.

52 Thomas et al 2004 www.eurecom.fr.

53 Cassim 2009 *PER* 38.

54 Clough *Principles* 185.

55 Brenner 2005 *IJCLP* 1.

56 Brenner 2005 *IJCLP* 4.

57 Brenner 2005 *IJCLP* 4.

2.2 *The relationship between electronic and traditional crime*

According to Thomas *et al*,⁵⁸ the main distinguishing factor between traditional and online crime is that, in the latter instance, crime feels less significant and more unidentified. They are of the view that the major types of traditional crime have their counterparts online.⁵⁹ They further argue that online crime is much easier to detect than traditional crime. The advancement of technology eases the process they opine. This latter assertion will certainly find justification depending on the types of criminal activities involved, or in some cases on the geographical area or areas involved.⁶⁰

Brenner⁶¹ establishes the main elements that set online crime apart from offline crime. She identifies four characteristics attached to traditional crime that are not found in cybercrime, namely “proximity, scale, physical constraints and patterns.”⁶²

Proximity has to do with the offenders being near their victims or potential victims. The scale of traditional crime is restricted as it mostly involves “one-to-one” crime, i.e. a single perpetrator and a single victim. There is usually a time span between the commission of a crime and the following attempt. Physical constraints concerns the preparation, planning and evaluation of all the aspects of the crime envisaged in order for the crime to be successful. Patterns refer to evidence that can be gathered easily, witnesses that may come forward, and the geographical area concerned that is easily delineable. According to her, the fact that the boundaries of the crime are controllable makes it easier to understand the “how”, “why” and “where” of the crime. This enables law enforcement to react positively as they have the possibility to reduce crime in view

58 Thomas *et al* 2004 www.eurecom.fr.

59 Brenner also shares this view regarding cybercrime in general. She compares hacking to burglary in the real world; spreading viruses, worms and other dangerous code to vandalism. See Brenner 2005 *IJCLP* 4.

60 Some other writers think the “ephemeral nature” of online information creates a huge gap between traditional and online crime in the sense that, in the latter case, perpetrators have the ability to wipe away data and walk free because they are henceforth known under new identities and may as well relocate. See Albert 2002 *ABLJ* 592; online offenders operate at a much faster rate with the information available online than traditional offenders, and are helped in their offences by the “automated” nature of the Internet. See Brenner 2005 *IJCLP* 9.

61 Brenner 2005 *IJCLP* 7-9.

62 Brenner 2005 *IJCLP* 7.

of their investigations. In brief, offline crime is committed in areas “geographically and demographically demarcated”.⁶³

Contrary to what she taxes as real-world crime, there is no need of proximity in cybercrime. Moreover, cybercrime knows no boundaries as the perpetrator and the potential victim can be miles apart from each other. Here, it suffices for the criminal to have access to the Internet where it becomes easier to get hold of sensitive information and act thereon.

Albert⁶⁴ is of the view that traditional ways of prosecution are not adequate for online crime. Brenner also suggests in this regard that reactive techniques that work for traditional crime are not similarly adequate. According to her, online crime needs more preventive than reactive strategies.⁶⁵ Brenner further raises the problem that an obstacle to successful prosecution in online crime is the fact that what is considered in one country as crime may not be an illegal act in another country.⁶⁶ Another point of difference between traditional crime and online crime is the cost of prosecution. Smith and Urbas⁶⁷ argue that prosecuting online crime is very costly. They submit that sophisticated infrastructures, well-trained investigators, and courts well aware of this type of crime are needed for successful prosecution of online crime. The threatening effect of online crime is among the many factors prompting some people to choose conventional ways of trading above web-based transactions.⁶⁸

In terms of volume, the number of cybercrime committed is far larger than that of conventional crime.⁶⁹ If a comparison is made regarding the damage caused, it appears again that cybercrime generates heavier damage than crime in the real world.⁷⁰ All

63 Brenner 2005 *IJCLP* 9.

64 Albert 2002 *AB LJ* 592.

65 Brenner 2005 *IJCLP* 1.

66 Brenner 2005 *IJCLP* 10.

67 Smith and Urbas 2001 www.aic.gov.au.

68 Tse and Yim 2001 *JICM* 142.

69 Brenner 2005 *IJCLP* 10.

70 Brenner 2005 *IJCLP* 5.

these views make traditional crime less strenuous in terms of detection, prosecution and knowledge compared to cybercrime.

2.3 *Brief overview of the common criminal activities encountered in IEC*

It is noteworthy that the types of crime that will be enumerated below are only illustrative and in no case an exhaustive list of all the types of illegal activities found in IEC. A distinction will be made between direct and indirect online schemes.

2.3.1 *Direct schemes generally amounting to crime in IEC*

Direct here refers to the types of online schemes that occur when the parties involved are aware of their dealings. It relates to those fraudulent activities that are committed when the parties know that they are involved in an electronic deal (hereafter e-deal) which results in deals of fraudulent nature. Although belonging to this category, some crimes mentioned here may also fit in the category of indirect crimes. Internet auction fraud, travel and vacation business fraud, health care fraud, denial of service, and bogus return are the many variants of illegal behaviour that can fit into this category.

2.3.1.1 Internet auction fraud

This involves items that are offered for sale on an Internet house through a process of bidding.⁷¹ Fraud may occur either during the bidding process or after the process has been finalised.⁷² It may be done through “non-delivery, misrepresentation, triangulation, fee stacking, black market goods, multiple bidding and shill bidding”.⁷³

Regarding non-delivery, the seller presents non-existent items for auction or if the items do exist, they are never delivered. The unavoidable consequence is that the buyer never receives the goods that he has purchased. If payment is done via credit card, the

71 Gregg and Scott 2006 *IJEC* 96.

72 Albert 2002 *AB LJ* 581-582.

73 US IFCC 2001 www.ifccfbi.gov.

dishonest seller ends up with personal information of the innocent buyer (for instance name and credit card number).⁷⁴ Another aspect of non-delivery is when a bidder receives the goods put up for sale and does not effect payment.⁷⁵

Misrepresentation occurs when the main aim of the seller is to delude or misinform the buyer regarding the qualities or characteristics of the goods. This results in the buyer receiving something that is worth far less than what he or she expected.⁷⁶

Triangulation implicates three parties namely the buyer, the seller and the deceiving party. The perpetrator of fraud, otherwise called the “man-in-the-middle” interferes in a session between seller and consumer in order to obtain the bank details of the cardholder. The card details are used to buy goods from the seller; goods that are subsequently sold to the buyer who then effect payment to the offender. Although the buyer may end up with the goods, he will in most cases be called to return them as a result of the seller (the real or original seller) not having received any payment for the goods in question. Both buyer and seller thus become victims of the scheme.⁷⁷

Fee stacking happens where the seller increases the price after the auction by adding unknown charges (administrative or even handling charges)⁷⁸ to the effect that the buyer pays a price substantially higher than what he originally bargained for.

Selling illegitimate goods such as pirated music CD’s or videos⁷⁹ on auction sites are part of black market goods and the people selling these are committing crime.

In order to obtain goods at very low prices, a buyer may use different identities to make a number of bids for the same item. The aim is to dissuade other people interested in

74 US IFCC 2001 www.ifccfbi.gov.

75 Kyo 2004 *JECM* 4.

76 Teck 2001 www.lawgazette.com.sg.

77 US IFCC 2001 www.ifccfbi.gov.

78 Teck 2001 www.lawgazette.com.sg.

79 US IFCC 2001 www.ifccfbi.gov.

buying the product from doing so. Some of the bids are high, others are low.⁸⁰ Shortly before the end of the auction, the high bids are revoked, giving the opportunity to the buyer to get away with the scheme, i.e. buying the item at a very low price.⁸¹

Lastly, shilling⁸² or shill bidding⁸³ is a type of scheme generated or perpetrated by sellers themselves, or other people in collaboration with sellers. The purpose is to raise the price of their own item that is up for bidding by making several simulated bids. The seller thus receives a very high price for an item that is not worth it.

2.3.1.2 Travel and vacation business fraud

This aspect of e-commerce crime takes effect where a consumer is offered a travel package purported to be a discount deal but ends up paying more than what a normal trip would have cost.⁸⁴ This encompasses getting accommodation under the expected standard, or travel only to find out that reservations were either never made or made with an unacceptable credit card.⁸⁵ Consumers may also come across certain charges unknown to them when the offer was made.⁸⁶

2.3.1.3 Health care fraud/health insurance fraud

This variant of online crime covers any scheme that involves the health care industry that is designed for illegitimate financial profit.⁸⁷ It has many aspects ranging from:

...billing for services not rendered, inflating the cost of the service provided, the deliberate performance of medically unnecessary services, and the payment of

80 US IFCC 2001 www.ifccfbi.gov.

81 Teck 2001 www.lawgazette.com.sg; see further Albert 2002 *ABLJ* 588 where she qualifies such practice as “bid shielding”.

82 Teck 2001 www.lawgazette.com.sg.

83 US IFCC 2001 www.ifccfbi.gov.

84 Teck 2001 www.lawgazette.com.sg.

85 Better Business Bureau 2007 www.bbb.org.

86 Teck 2001 www.lawgazette.com.sg.

87 FBI 1999 www.fbi.gov.

“kickbacks,” illegal payments designed to guarantee awarding of a contract or the exclusive right to provide a service.⁸⁸

On closer analysis, this type of scheme is more likely to happen within a country. It is however presented here because some people may have their medical cover outside their country of residence, and they can similarly become victims of these criminal behaviours.

2.3.1.4 Chargebacks/denial of receiving service or product/distributed denial of service

There seems to be two different types of denial of service which do not have a single thing in common. The first and most common is called a distributed denial of service (DDoS) attack. This kind involves:

An attack tactic that is intended to nullify the ability of a website to service legitimate client requests, swamping a target computer by inundating it with packets of information sent over the Internet. The objective can be achieved by various means, such as flooding the system with too many requests for it to handle or by subverting the normal protocol between clients and servers.⁸⁹

This aspect of denial of service is neither fraud nor theft, because the perpetrator does not take anything from the victim.⁹⁰

The other aspect which is more relevant to this research is denial of receiving products or services. After the seller has performed his part of the contract which is mainly to deliver the goods, the buyer (the scheme perpetrator), negates ever taking delivery of the goods, concluding the contract and even placing the order.⁹¹ All this is done in order to avoid paying for the service rendered by the seller.

88 FBI 1999 www.fbi.gov.

89 Singleton 2002 *EDPACS Newsletter* 9.

90 Brenner 2005 *IJCLP* 6.

91 Curry 2000 www.scambusters.org.

2.3.1.5 Bogus returns

A customer may aver (after receipt of the goods he/she has ordered), that he/she was unsatisfied with the quality and have returned the said goods to the seller, but the goods in question never reach the seller. Sometimes the trickster buyer will send back only one or a few items, but will allege to have sent more and ask for full reimbursement.⁹²

Other forms of scams that may be described as indirect are those aiming at the commission of another crime, and most of the time the victims are not aware that they are being victimised.

2.3.2 *Indirect criminal activities in IEC*

Direct schemes perpetrated online are opposed to indirect schemes where the real crime is discovered only at a later stage. The schemes are themselves fraudulent in nature but become real crime in IEC only because they facilitate the commission of purely e-commerce crime. Phishing, pharming and advance fee scams are the three most common indirect forms identified.

2.3.2.1 Phishing

Phishing is “a scheme that solicits Internet users’ personal and financial data by using e-mails falsely representing legitimate banks”.⁹³ The e-mail or whatever means of communication used will be shaped and designed as if originating from a company (most of the time financial institution) known to the consumer because he/she is the client of such institution.

2.3.2.2 Pharming

Pharming is defined as:

⁹² Curry 2000 www.scambusters.org.

⁹³ Ellis 2004 *WWD* 2.

...an attack in which a user is fooled into entering sensitive data (such as password or credit card number) into a malicious website that impersonate a legitimate website.⁹⁴

Pharming is sometimes described as “phishing without a lure”.⁹⁵ Unlike phishing where specific people may be targeted, pharming has a broader domain of operation, as a larger number of people may be instantaneously victimised.

2.3.2.3 Advance fee scams

Also known as 419 Nigerian scams,⁹⁶ this scam is characterised by the dispatching of unwanted letters, e-mails or faxes making unlawful offers to someone.⁹⁷ Substantially, through those channels, and through cellphones also nowadays, fraudsters request help from the addressee in order to move a huge sum of money out of the country (Nigeria). It may also be that the addressee has inherited a large amount of money from a deceased estate and is invited to liaise with the fraudster to receive their legacy. Another approach is to send documents ascertaining some contractual arrangements made on behalf of the prospective victim with Nigerian officials or other businessmen. Someone may receive a text message about being the lucky winner of a competition held in any country for example in the United Kingdom.⁹⁸ No matter what the proposal and the means used may be, the next step is generally to request the recipient’s bank information for the transaction. The addressee is promised a substantial commission in return for the assistance. Once the information is supplied, the recipients are asked to pay a certain sum upfront for various reasons (State taxes, administration fees, bank transfers etc.) all destined at facilitating the transaction.⁹⁹ Upon payment of the requested sum, the criminal either vanishes or sudden complications occur that render

94 ACFE 2001 www.acfe.com.

95 Knight 2005 *IEE Review* 29.

96 419 being the number of the Nigerian Statute prohibiting this offence.

97 Smith, Holmes and Kaufmann 1999 *Trends and Issues in Crime and Criminal Justice* 2.

98 When sms or text messages are used in order to get personal information from people, this is called Smishing or Tishing. See in this regard ACFE 2013 www.acfe.com.

99 Smith, Holmes and Kaufmann 1999 *Trends and Issues in Crime and Criminal Justice* 3.

the transfer impossible or more complicated.¹⁰⁰ The people so targeted may even be requested to make further transfers to help solve the complications that purportedly occurred. There seems to be evidence to the fact that some people, in trying to recover their money, have been subject to intimidation, threats, kidnapping and some have even been murdered.¹⁰¹ This type of scheme is relevant to this study in the sense that the personal data supplied by the victims may subsequently be used for identity theft or credit card fraud.

2.3.2.4 Identity theft and credit card fraud as consequences of indirect criminal activities

It should be noted that phishing, pharming and advance fee scam are not the only steps that lead to identity theft and credit card fraud. There are many other ways through which these crimes can be committed.¹⁰²

Identity Theft is defined as “the unlawful use of another’s personal identifying information”.¹⁰³ More succinctly, identity theft occurs when someone illegally obtains someone else’s personal information and uses it for unlawful purposes.¹⁰⁴ A criminal may simply steal someone’s identity and obtain several loans, knowing that it will never be repaid by him/her.

Credit card fraud (hereafter CCF) takes place whenever somebody, manages to get hold of someone else’s card or card details and utilises it to purchase goods online

100 Standard Bank Date Unknown www.standardbank.co.za.

101 Smith, Holmes and Kaufmann 1999 *Trends and Issues in Crime and Criminal Justice* 3.

102 The card information, for example, may fall into the hands of a criminal in a variety of ways, namely: “Intercepting of e-mails containing newly issued cards, copying and replicating of card information through skimmers or gathering sensitive information through phishing (cloned websites) or from unethical employees of credit card companies.” The man-in-the-middle attack referred to above, is one of the many ways that this fraud is being committed, i.e. a third party interfering into an exchange session between the buyer and the seller. See Quash and Sriganesh 2008 *Expert Systems with Applications* 1721.

103 Bellah 2002 *Law and Order* 222.

104 Standard Bank Date Unknown www.standardbank.co.za.

without the card holder's knowledge.¹⁰⁵ In these instances criminals normally make large purchases as payment will be made from the real account.

2.4 Conclusion

This chapter aimed at establishing the relationship that exists between online and traditional crime, and at briefly enumerating some major types of criminal behaviour that overwhelm the e-commerce world. It appears that proximity, scale, physical constraints, patterns, cost and ways of prosecution, nature, and availability of evidence are different aspects that set online crime apart from offline crime. Though it is said that the difference between the two forms of crime is not substantial, one thing is clear, namely that online crime has some specific aspects that are inexistent with real-world crime. Online crime covers a very wide field. That is why, to avoid confusion and delineate the topic, it was important to stick to the most common criminal activities that directly or indirectly affect IEC. Although this research is concerned with IEC, there seems to be no difference between the types of crime in e-commerce within a country and those crossing borders.

105 Quash and Sriganesh 2008 *Expert Systems with Applications* 1721.

3 International and regional instruments against crime in international electronic- commerce

3.1 *Introduction*

In their never-ending attempt to make the world a better place, several organisations have provided their respective member states with certain instruments; international, regional and sub-regional in scope, aimed at finding solutions to the numerous problems facing society. Among these organisations are the United Nations (UN), the African Union (AU) and the Council of Europe (COE). They may differ in size, objective, capacity, domain of expertise, achievements and prominence, but one thing they certainly have in common, is their determination to curtail crime and promote a fair, just and equitable society. It should be emphasised that the choice of organisations is simply guided by their respective geographical domain of application.

The above mentioned organisations have not only enacted a single comprehensive instrument that pertains to online crime, but have released several instruments that provide not only a starting point but also comprehensive guidelines to fight online crime. An IEC transaction, as its name implies, involves parties in different countries. Online crime raises several concerns: How to deal with such a situation with regard to jurisdiction and the nature of the crime; which authority to turn to for the purpose of reporting the crime; which remedies (legal or personal initiatives) are immediately available for the person confronted with a situation where he/she has been a victim of crime because of an online transaction? Is the cost of following up on a matter concerning online crime affordable for an individual? All these questions raise the problem of applicable legal instruments to govern criminal activities carried out electronically. The instruments to be examined below, to a certain extent provide answers to these questions.

The aim of this chapter is to ascertain, the limits within which the said instruments provide¹⁰⁶ a solution to the still emerging issue of online crime. The analysis of the international instruments will precede that of the regional instrument.

3.2 International instruments against online crime

3.2.1 The United Nations and online crime

Up to now, the UN has no specific Convention dealing with online crime. However, it has released a *Handbook on Identity-related crime*,¹⁰⁷ and more recently a *Comprehensive Study on Cybercrime*.¹⁰⁸ These initiatives demonstrate the UN's involvement in the fight against online crime. The two instruments will be discussed later under the title of other initiatives by the UN against crime in IEC. For present purposes the focus will be on the *Model Law on Electronic Commerce*,¹⁰⁹ the *UN Convention against Transnational Organized Crime*,¹¹⁰ the *Model Law on Electronic Signatures*,¹¹¹ the *UN Convention against Corruption*,¹¹² and finally, the *UN Convention on the Use of Electronic Communications in International Contracts*.¹¹³

3.2.1.1 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996) with additional article 5 bis as adopted in 1998 (MLEC)

Conducting business electronically has given a completely new face to international trade. Consequently, several concerns arose regarding the force, impact, effect and consequences of online performance of sales transactions. The MLEC is a model

106 Although not all specifically or expressly relating to crime in IEC.

107 UN Office on Drugs and Crime 2011 www.unodc.org.

108 UN Office on Drugs and Crime 2013 www.unodc.org.

109 *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* (1996) with additional article 5 bis as adopted in 1998.

110 *United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (2000).

111 *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment* (2001).

112 *United Nations Convention against Corruption* (2003).

113 *United Nations Convention on the Use of Electronic Communications in International Contracts* (2005).

providing guidance to solve some of the concerns posed by electronic transactions. It is more precisely a set of proposed rules establishing and acknowledging the effectiveness of electronic transactions (hereafter e-transactions) on society. The MLEC is a starting point for states members to develop their own law regarding e-commerce transactions.¹¹⁴ It is furthermore an alternative to existing laws that are not adequate or appropriate for e-transactions.¹¹⁵ Its purpose is to facilitate or enable the use of electronic commerce.¹¹⁶ With regard to the topic currently under discussion, namely crime in IEC, there are no express provisions in the MLEC that directly refer to or can help to curtail electronic-crime. However, note should be taken that the mere fact that the Model Law exists is a weapon against crime in IEC as it is a way of harmonising laws in this domain. This creates certainty with regard to e-transactions.

3.2.1.2 UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001)

In furtherance of their previous works that led to the adoption of the Model Law on e-commerce, the UN Commission on International Trade sought to give further guidance to e-commerce transactions by releasing the *Model Law on Electronic Signatures* (MLES). The MLES is meant to harmonise electronic signatures used in electronic deals, as described in article 7 of the Model Law on e-commerce.¹¹⁷ The MLES is moreover an attempt by the UN to promote certainty by harmonising rules relating to the recognition and acceptance of methods of assessing signatures in e-transactions that have a cross-border effect.¹¹⁸ This latter objective of the MLES is to be achieved by its incorporation into the legal systems of member states.¹¹⁹

Electronic signatures in IEC transactions have a very important role to play. Given the anonymity of the Internet, it is crucial to be able to identify parties to a transaction by

¹¹⁴ Introductory notes of the MLEC.

¹¹⁵ Paragraph 3 of the *Guide to Enactment* to the MLEC.

¹¹⁶ Paragraph 6 of the *Guide to Enactment* to the MLEC.

¹¹⁷ Introductory notes of the MLES.

¹¹⁸ Article 12 of the MLES.

¹¹⁹ Paragraph 26 of the *Guide to Enactment* to the MLES.

their signatures. The methods of identifying signatures are matters of preference, and parties to a contract may decide which of the several techniques available best suit them or their transaction.¹²⁰ Being able to have recourse to a trustworthy method used to identify a person and to attest that person's assent of the information contained in a data message¹²¹ is definitely a very important and quite efficient way to limit online crime. Smith and Urbas,¹²² nevertheless point out that one element that weakens this security measure is the fact that the different documents that are generally required for identification in the process may unfortunately be forged.

Furthermore, the ACFE¹²³ emphasises that encryption is a costly solution that is not affordable to everyone wishing to use it. It is in response to this problem of cost effectiveness, says the ACFE, that the use of smart card technology has been developed. According to this association, "smart card technology offers a solution to the major secure transactions requirements, namely data integrity, user authentication and non-repudiation of data."¹²⁴ The ACFE specifically regards the use of non-repudiation¹²⁵ as an efficient tool with regard to the problem of crime in IEC.¹²⁶ The ACFE is of the view that it can be an efficient way to prevent some parties performing electronic transactions from denying ever being part of such transactions. Both signatures' authentication and the use of "non-repudiation of data" as presented by the ACFE, are probably the best solutions to prevent and effectively combat the crime of denial of service as defined above for the purposes of this research paper.

120 The *Guide to Enactment* of the MLES establishes a distinction between electronic signatures based on techniques other than public-key cryptography (such as authentication through biometric device based on handwritten signatures, use of personal identification numbers (PINs) etc.) and digital signatures based on public-key cryptography. See para 33 and para 36-62 for a detailed explanation regarding both types of digital signatures.

121 Paragraph 63 of the *Guide to Enactment* to the MLES.

122 Smith and Urbas 2001 www.aic.gov.au

123 ACFE 2011 www.acfe.com.

124 ACFE 2011 www.acfe.com.

125 Which refers to parties involved in an electronic-commerce transaction that cannot escape liability by denying ever taking part to the said transaction because the specific method utilized for the particular transaction prevent them from doing so. Like user authentication techniques, it is a way to identify parties to a deal to one another. See ACFE 2013 www.acfe.com.

126 ACFE 2011 www.acfe.com.

3.2.1.3 United Nations Convention against Transnational Organized Crime and the Protocols Thereto (2000) (UNTOC)

The UNTOC has the merit of not limiting itself to a specific category of organised crime and is applicable to any type of transnational organised crime,¹²⁷ provided the characteristics of the “organized criminal group” as defined in article 2 (a) of UNTOC are met. Although this study focuses on criminal activities perpetrated online in a business-to-consumer or consumer-to-consumer relationship, some specific types of electronic crime, such as the Nigerian advance fee scams discussed above, are generally perpetrated by organised groups. Those types of groups generally operate in different countries and have an apparently well-established and well-functioning network in order to achieve as many schemes as possible. Viewed from this angle, the UNTOC could be largely instrumental to fight crime in IEC. Provisions such as those relating to the criminalization of the laundering of proceeds of crime,¹²⁸ international cooperation for purposes of confiscation,¹²⁹ extradition,¹³⁰ mutual legal assistance,¹³¹ special investigative techniques¹³² and collection, exchange and analysis of information on the

127 Crimes such as money-laundering, corruption, illicit trafficking in endangered species of wild flora and fauna, offences against cultural heritage are counted in the list. See introductory words of the *United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (2000) (UNTOC) 2.

128 Article 6 of the UNTOC. Under this article, conducts such as conversion or transfer of property, concealment or disguise of property, acquisition, possession and use of property with the knowledge of their unlawful origin and participation in any other capacity in the process are criminalised.

129 Once an offence covered by the UNTOC has been established and a request has been made by one state to another, the requested state is expected “to the greatest extent possible”, to present the request to its competent authority (in order to obtain a confiscation order) and further to take such steps as may be appropriate to “identify, trace and freeze or seize proceeds of crime, property, equipment or other instrumentalities...” In order to achieve greater results in this aspect of international cooperation, member states are required to conclude bilateral and multilateral agreements with one another. See aa 13(1)(a), 13(2), 13(9) of the UNTOC.

130 Provided that the offence which has given rise to a request for extradition is punishable both under the law of the requesting and the requested state, a state can request another state to extradite a person alleged to have committed a crime and who is located in the territory of the requested state. See a 16(1) of the UNTOC.

131 Once again, states’ parties to the UNTOC are called to afford one another “the widest measure of legal assistance in investigation, prosecutions and judicial proceedings” with regard to the offences established by the UNTOC. Furthermore, reference is made to affording one another mutual legal assistance to the “fullest extent possible under relevant laws, treaties, agreements and arrangements...” when offences involving an organised group is committed. See a 18(1)(2) of the UNTOC.

132 Article 20 of the UNTOC. Among other responsibilities, it is a state party’s choice within the limits prescribed by domestic law to make the necessary efforts to enable the use by its competent

nature of organized crime¹³³ can also be utilized to combat online crime. It also appears that each member state is called to provide its law enforcement personnel¹³⁴ with adequate training programmes in building techniques to fight organised crime.¹³⁵ The nature of online criminal activities calls for very technical approaches in dealing with those crimes. As such, there needs to be interaction between states in very diverse and technical respects to ensure timely and sound responses to crimes committed via computer networks. Above all, each country needs to have specific bodies dealing exclusively and extensively with those types of crime. In the process, these bodies are expected, according to the UNTOC, to help governments and citizens to understand online criminal activities. This is commonly referred to as “awareness raising” which definitely helps to counter and considerably reduce online crime.

The UNTOC is supplemented by three protocols. The first appears in Annex II,¹³⁶ the second in Annex III,¹³⁷ and the third one is the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition. No state can be part of any of the protocols unless it is primarily part of the UNTOC,¹³⁸ and no state party can be held to any of the protocols unless it has become a party to the said protocol.¹³⁹ These protocols do not have a direct impact on IEC.

3.2.1.4 United Nations Convention against Corruption (UNCAC)

Due to the fact that corrupt activities adapt to the advancement in technology and that such adaptation has now made it to be considered a transnational crime,¹⁴⁰ this Convention is mentioned here because of that transnational character and also because

authorities of special investigative techniques such as electronic or other forms of surveillance and undercover operations.

133 Article 28 of the UNTOC.

134 Personnel referred to may include prosecutors, investigating magistrates, customs personnel and any other personnel tasked with prevention, detection and control of the offences condemned by the UNTOC.

135 Article 29 of the UNTOC.

136 *Protocol to Prevent, Suppress and Punish Trafficking in persons, Especially Women and Children.*

137 *Protocol against the Smuggling of Migrants by Land, Sea and Air.*

138 Article 37(2) of the UNTOC.

139 Article 37(3) of the UNTOC.

140 Preamble of the *United Nations Convention against Corruption* (2003) (UNCAC).

of the link between corruption and other forms of unlawful activities such as fraud.¹⁴¹ Regarding the transnational character of corruption, one of its various aspects that has easily found a home online and that also has a cross-border effect, is money laundering. Although money laundering is not a direct form of crime as defined for the purposes of this research, it is indirectly linked to IEC. This indirect link originates from the fact that not only money illegally acquired from corrupt activities can be laundered, but also the proceeds of deceitful activities carried out by means of electronic sales transactions. Whatever the source of money transferred in order to be hidden may be, the UNCAC has a very consistent approach to fight money laundering¹⁴² in all its facets. One very important point of the said approach is the paramount role to be played by banks in cases of suspicious transactions. In this regard, the UNCAC states as follows:

...each State Party shall empower its courts or other competent authorities to order that bank, financial or commercial records be made available or seized. A State Party shall not decline to act under the provisions of this paragraph on the ground of bank secrecy.¹⁴³

Banks are specifically exhorted to scrutinise each and every transaction and keep the necessary records in case doubtful transactions require investigations.¹⁴⁴ This step is a security measure that contributes to the detection of online criminal activities. Furthermore, and despite not being all appropriate, a substantial number of the UNCAC provisions could well be used to fight unlawful activities arising out of an IEC transaction. The UNCAC is particularly fitting as it provides a number of measures

141 Considering the fact that most criminal activities perpetrated online are done fraudulently, the UNCAC may also serve as an instrument to combat online crime in general. Some organisations such as the ACFE refer to the UNCAC as an international instrument to fight both fraud and corruption. Whereas some writers regard corruption as an aspect of fraud, others rather look at it the other way round. It is, however, important to point out that, whatever the nexus between fraud and corruption, they remain two distinct crimes belonging each to their own category. See respectively ACFE 2011 www.acfe.com; Hansen *et al* 2005 www.pactworld.org; and Snyman *Criminal Law* 376, 520.

142 Article 14 of the UNCAC.

143 Article 31(7) of the UNCAC.

144 Article 52 of the UNCAC.

varying from preventive¹⁴⁵ to implementation mechanisms¹⁴⁶ through international cooperation,¹⁴⁷ criminalization and law enforcement,¹⁴⁸ assets recovery¹⁴⁹ and finally, technical assistance and information exchange.¹⁵⁰ Thus, taken from an IEC point of view, the UNCAC would definitely have a positive impact on society in terms of crime reduction and transparency.

145 Chapter II of the UNCAC. It is common knowledge that prevention is better than cure. The UNCAC proposes a very broad list of preventative measures which, in the author's view, is consistent and could easily be applied to the online era. The diverse character of those measures demonstrates the determination of the UN to make the fight against corruption a common call, involving all sectors of society. See respectively aa 5, 6, 10(c), 12(2)(a), 13, 14 of the UNCAC, for more regarding the proposed preventive measures.

146 Chapter VII of the UNCAC. The UNCAC thus establishes in a 63(1) "a Conference of the States Parties" which has as duty the improvement of capacity and cooperation between states in order to meet the goals of the Convention and ensure its proper implementation.

147 Chapter IV of the UNCAC. Under this heading of international cooperation, there are a number of important provisions relating to extradition (a 44) subject to the principle of dual criminality as the case may be, and mutual legal assistance (a 46) that, as mentioned earlier, would definitely bear positive results if applied in case of online crime. As in the case of the UNTOC, member states are once again called to offer "the widest measure" of assistance to one another and further, "to the fullest extent possible".

148 Chapter III of the UNCAC. This chapter of the Convention deals, amongst others, with the need of member states to adopt and ensure the implementation of techniques to uncover and prevent the laundering of the proceeds of crime. Freezing and seizure and confiscation of the proceeds of crime are also outstanding in the Convention. States are furthermore exhorted to consider the cooperation of offenders in their fight against corruption. This article of the Convention sees the cooperation between law enforcement agencies and criminals as an efficient approach. Here the authorities are furnished with more information regarding crime, and the offenders may have their punishment mitigated or be granted immunity from prosecution. It does not suffice to cooperate in any manner; the cooperation the Convention talks about must be useful or substantial for the authorities to act on it. A cooperation of this nature is crucial to combat crime in IEC. Online criminals seem to always be one step ahead of law enforcement agencies and regulatory instruments. When one of their ways of operation is discovered, they quickly move to another. They appear to be faster in developing new schemes than law enforcement agencies are in regulating and prosecuting those types of crime. The nature of the crime thus makes such cooperation indispensable, because authorities and society will gain by being provided with information concerning different techniques and means of operation. See aa 23, 24, 31, 36, 37, 39, 40, 41 of the UNCAC; see also Pinguelo and Muller 2011 *VJLT* 88.

149 Chapter V of the UNCAC. Presented as fundamental principle of the Convention, all the articles under the broad assets recovery title suggest mechanisms to recover illegally acquired assets through international cooperation. Depending on each particular case, special cooperation is also suggested. Amongst other, the Convention caters for the return of property or properties so confiscated to the lawful owners - lawful owners that might either be the requesting state or an individual known as the "prior legitimate owner" - or provide compensation to such owner(s). Returning the proceeds of crime to the rightful owners in IEC or compensating them for their loss would be a relieving step for people defrauded online.

150 Chapter VI of the UNCAC. A 60(2) reads as follows: "States parties shall, according to their capacity, consider affording one another the widest measure of technical assistance, especially for the benefit of developing countries, in their respective plans and programme to combat corruption, including material support and training in the areas referred to in paragraph 1 of this article, and training and assistance and the mutual exchange of relevant experience and specialized knowledge, which will facilitate international cooperation between States Parties in the areas of extradition and mutual legal assistance."

3.2.1.5 The United Nations Convention on the Use of Electronic Communications in International Contracts (2005) (Electronic Communications Convention or ECC)

“The purpose of the Electronic Communications Convention is to offer practical solutions for issues related to the use of electronic means of communication in connection with international contracts.”¹⁵¹ Article 1 of ECC opens the Convention for application to “electronic communications in connection with the formation or performance of a contract between parties whose places of business are in different states.”¹⁵² Very often electronic deals occur between parties located in different countries, which makes the Convention applicable in the case of this study. However, the ECC excludes contracts concluded for personal, family or household purposes.¹⁵³ This research paper focuses on business-to-consumer and consumer-to-consumer transactions and does not differentiate whether consumers purchase goods for commercial, “personal, family or household purposes.”¹⁵⁴ According to the article-by-article remarks adduced to the ECC, the main reason for this exclusion is that “a number of rules in the Convention would not be appropriate in their context.”¹⁵⁵ They take as example article 10 (2) of the ECC which determines the time for reception of an electronic communication as the time when the electronic communication becomes capable of being retrieved by the addressee. The explanation given is that such a rule might not be appropriate in the context of consumers’ contracts as “consumers could not be expected to check their electronic mail regularly nor be able to distinguish easily between legitimate commercial messages and unsolicited mail (“spam”).”¹⁵⁶ Though convincing to a certain point, this position does not necessarily hold true today. Many are able to distinguish between spam and real commercial messages and are also

151 Paragraph 3 of the explanatory note by the UNCITRAL Secretariat on the *United Nations Convention on the Use of Electronic Communications in International Contracts* (2005) (ECC).

152 Article 2(1) of the ECC.

153 Article 2(1)(a) of the ECC.

154 Article 2(1)(a) of the ECC.

155 Paragraph 71 of the article-by-article remarks adduced to the ECC.

156 Paragraph 72 of the article-by-article remarks adduced to the ECC. Further examples justifying the exclusion are also found in para 73 of the article-by-article remarks.

aware of the ways to avoid them. Moreover, even though consumers may not be used to checking their e-mails regularly, they would surely do so when they are in the process of concluding an online deal.

Even without this exclusion, there seems to be no express provisions that are suitable to fight online crime in the Convention, as its main focus is the formation of contracts in electronic form; how and when an electronic contract is deemed to have come into existence, and what to do in case of 'input errors', amongst others. Once again however, the existence of the Convention improves the knowledge of countries and their citizens of the contours of electronic trade platforms and so provides a substantive idea of what the electronic environment is all about.

3.2.1.6 Other initiatives by the United Nations

3.2.1.6.1 Handbook on Identity-related Crime (2011)

This document's main aim, as explained in its introduction is:

...to lay out a range of options and considerations to be taken into account when addressing domestic criminal justice matters (typology of crimes/criminalization approaches/protection of victims), specific challenges in the field of international cooperation in criminal matters or the potential of synergies and partnerships between the public and the private sector, mainly in the area of prevention of identity-related crime.¹⁵⁷

The Handbook is the result of a project conducted by the Corruption and Economic Crime Branch of the United Nations Office on Drugs and Crime (UNODC). This document makes a detailed, although not complete,¹⁵⁸ analysis of the concept of identity-related crime,¹⁵⁹ the different types of information targeted¹⁶⁰ and the ways

157 UN Office on Drugs and Crime 2011 www.unodc.org iii.

158 See Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 5-8 regarding the aspects not covered by the study.

159 See Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 25-27 for the different definitions usually ascribed to the concept of identity theft.

160 Among others the main information sought by offenders are accounts information and passwords. See Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 14.

through which those types of information are obtained¹⁶¹ and subsequently used.¹⁶² It also evaluates the challenges posed when it comes to investigation.¹⁶³ The Handbook further elaborates on international¹⁶⁴ and national¹⁶⁵ approaches to the issue of identity violation. One very interesting element that is raised in the Handbook is the legal base for the restoration of victims' identities.¹⁶⁶ It is a very relevant aspect that tries to look into what can be done in order to repair the wrong that is caused to a victim by the illegitimate use of his/her identity.

The Handbook is also an exposition of the ways of preventing,¹⁶⁷ detecting and gathering of evidence, and investigating identity theft crime.¹⁶⁸ It also serves as an

161 Gercke makes an exposition of the methods through which information can be obtained and among others, this may happen through the redirection of mail, mail theft of sources of personal information, dumpster diving (searching bins to get hold of documents containing identity-related information), insider attacks, usage of publicly available information, scams related to digital information and malware. Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 15-18.

162 Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 20. Once personal information has been obtained, it may subsequently be used to perpetrate economic crimes such as taking over existing accounts or creating new accounts with the information obtained. It can also be used to make transfers or buy goods through those accounts. The information may also be sold and so used to devise "sophisticated identity documents or exploit weaknesses in insurance schemes, deceiving or corrupting authorities, in order to obtain genuine documents", which in turn may be marketed to some other people for further offences such as illicit travel and illegal migration, among others. Such information may furthermore be used by offenders to conceal their real identity and they may in this respect use a victim's account to launder money.

163 Many factors hinder a successful fight against identity theft and cybercrime in general, among others, the aptitude to recourse to anonymous means of communications, the ease with which digital information may be influenced and also the aptitude to act globally and to reproduce large databases in a very short time span. The Handbook suggests for the challenges posed by such forms of crime and even other forms, a strong and very close cooperation between law enforcement agencies and service providers. See respectively Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 21-23; Callanan in UN Office on Drugs and crime 2011 www.unodc.org 208.

164 Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 38-41.

165 Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 41-43.

166 Lawson in UN Office on Drugs and Crime 2011 www.unodc.org 129. As example of the said legal basis cited, Parts II.A.4 and VI of the *OECD Guidelines for Protecting Consumer Victims of Fraudulent and Deceptive Commercial Practices Across Borders* (2003), which respectively provide that Member States should: "[establish] effective mechanisms that provide redress for consumer victims of fraudulent and deceptive commercial practices" and should "jointly study the role of consumer redress in addressing the problem of fraudulent and deceptive commercial practices, devoting special attention to the development of effective cross-border redress system."

167 Callanan in UN Office on Drugs and Crime 2011 www.unodc.org 191. The Javelin Strategy and Research as referred to by the author, proposes six measures that, in their view, are the top identity safety tips and that are also efficient against fraud in general. Those measures require personal initiatives and are the following:

Be vigilant – Monitor your accounts regularly online at bank and credit card websites, ATMs or by phone and set up alerts that can be sent both online and to a mobile device.

evaluation of some legal responses that have been enacted against identity-related offences,¹⁶⁹ and an exposition of certain measures¹⁷⁰ provided in those instruments that are appropriate to curtail identity-related crime and their limits and strengths thereof.

The Handbook is divided into five parts. The first one deals with legal approaches to criminalize identity theft.¹⁷¹ The second part elaborates on typology and criminalization approaches to identity-related crime¹⁷² and the identity-related crime victim issues: A discussion paper forms the third part of the Handbook.¹⁷³ Fourthly, identity-theft: An inventory of best practices on public-private partnerships to prevent economic fraud and identity-related crime, is dealt with.¹⁷⁴ The last part of the Handbook is a practical guide regarding international cooperation to combat identity-related crime.¹⁷⁵ This last part specifically examines the different aspects of identity theft by presenting it under the umbrella of case studies and provision of some guidelines regarding how requests can

Keep personal data private – Do not provide sensitive financial information over the Internet or phone, including social security numbers, passwords, personal identification numbers (PINs) or account numbers, unless you initiated the interaction to a verified and trusted location, such as the number or web address on the back of a credit card, debit card or statement...

Online is safer than offline when consumers use available security controls – Consumers should install and regularly update anti-virus and anti-spyware software, and keep operating systems and browsers updated...

Be aware of those around you - Be mindful of your environment and others who may be in proximity of overhearing sensitive financial or personal information or watching you text. This includes purchases over the phone or use of your social security number for identification...

Ensure credit and debit cards are protected – Obtain credit and debit cards from financial institutions that provide zero liability if a card is ever lost, stolen or used without authorisation...

Learn about identity protection services – There are additional services for those consumers who want extra protection and peace of mind...

The author nevertheless acknowledges that, though these initiatives that should be carried out daily are efficient against a number of identity theft crime, they are ineffective against attacks directed at large databases and lost or stolen laptops containing personal information. See further Javelin Strategy and Research 2009 www.javelinstrategy.com.

168 Callanan in UN Office on Drugs and Crime 2011 www.unodc.org 205.

169 Examples of such instruments are the *UN Convention against Transnational Organised Crime* (2000), and the OECD works: *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* (1999); *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Practices across Borders* (2003); *OECD Scoping Paper on Online Identity Theft* (2008) and the *OECD Policy Guidance on Online Identity Theft* (2008).

170 Measures such as extradition and international cooperation. See in this regard Gercke and Simion in UN Office on Drugs and Crime 2011 www.unodc.org 245-249.

171 Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 1.

172 Almeida in UN Office on Drugs and Crime 2011 www.unodc.org 55.

173 Lawson in UN Office on Drugs and Crime 2011 www.unodc.org 107.

174 Callanan in UN Office on Drugs and Crime 2011 www.unodc.org 169.

175 Gercke and Simion in UN Office on Drugs and Crime 2011 www.unodc.org 235.

be made, and how and why it is important to choose and identify the correct legal instruments applicable.

The briefing given about the preventive measures that have been developed against identity crime and some other aspects that need to be developed in order to reach certainty in fighting identity-related crime, seems to be the part of the Handbook that has consistent information relating to this research paper. Substantially, what is briefly summarised under the title “Aspects not covered by the study”¹⁷⁶ appears to be the solution to the main enquiry of this paper. Thus, as preventive measures that have been developed, there is restriction of the publication of critical identity-related information, data breach requirements¹⁷⁷ and the enhancement of protective measures designed for large databases.¹⁷⁸

The summary that can be made from this part of the Handbook is that more security measures (such as Personal Identification Number (PIN)) and biometric information¹⁷⁹ are needed, and investigation techniques also need to be enhanced.¹⁸⁰ International cooperation (in terms of entering into agreements with one another) is a way of facilitating and sharpening the weapons to fight identity-related crime as it overcomes barriers such as national sovereignty.¹⁸¹ The importance of education is also emphasised in the Handbook, as it helps to inform all the interested parties about the constant presence of risks and raises their awareness on the steps to be taken to protect themselves.¹⁸² According to the Handbook, education can therefore help to, for instance, curtail phishing schemes which by nature are a step towards the commission

176 Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 5-8.

177 Requirement that makes it compulsory for entities and institutions that undergo data breach to inform persons whose sensitive information was compromised by the said breach.

178 Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 5.

179 Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 6.

180 One aspect of this improvement process concerns the interrogation of identity theft suspects. This way of proceeding to find best solutions in the fight has been said to be beneficial to the extent that “it gives scholars a glimpse into the lived experiences of offenders and thereby offers insights into why they chose to engage in illicit behaviors”. See Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 6; see also Copes and Vieraitis 2009 *Criminology and Public Policy* 238.

181 Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 6-7.

182 Gercke in UN Office on Drugs and Crime 2011 www.unodc.org 7.

of identity-related crimes.¹⁸³ In this respect, banks generally inform their customers never to act on an e-mail or self-message service (sms) purporting to originate from them requesting customers' personal identification number (PIN) or any other sensitive information.¹⁸⁴ Education is also a way to counter Nigerian advance fee scams. In essence, if one is aware of how these criminals operate, namely sending sms, e-mail or mail, which is most commonly used, one will never bother to act on these messages, informing one of winning the lottery or a competition which one has never participated in, or that one has inherited something from a relative one has never heard of. It is also mentioned in the Handbook that international cooperation may however be limited by factors such as human rights and national security.¹⁸⁵

In the end, public-private partnerships which are seen as "a strategic alliance or relationship between two or more strategic organizations"¹⁸⁶ are said to be the key approach in building up barriers against online offenders.¹⁸⁷ These types of partnerships revolve around "knowledge and skills sharing"¹⁸⁸ and "independent coordination".¹⁸⁹ Lastly, and as mentioned in the Handbook, "there is a need for updated legislation, international initiatives, international coordination of law enforcement and agreed industry self-regulation and code of practice."¹⁹⁰

183 Phishing is described in chapter 2 as a form of indirect scheme perpetrated online that is merely a step to commit crimes such as credit card fraud or identity theft.

184 This initiative can fall under the term "end-user training" used in the handbook and that is said to be founded on mass media warnings, leaflets distributed by retail banking outlets or by service providers. See Callanan in UN Office on Drugs and Crime 2011 www.unodc.org 195.

185 Callanan in UN Office on Drugs and Crime 2011 www.unodc.org 225-228.

186 Callanan in UN Office on Drugs and Crime 2011 www.unodc.org 188.

187 Callanan in UN Office on Drugs and Crime 2011 www.unodc.org 188.

188 Regarding this particular aspect, in putting together or combining knowledge, skills and experience from varied entities including but not limited to industry, government, human rights, law enforcement and the legislature, this would lead to more and more effective initiatives. See Callanan in UN Office on Drugs and Crime 2011 www.unodc.org 231.

189 Effective and well defined international coordination is said to be important as it is a way of promoting sharing, broadening the partnership so as to involve new entities and further, making known the deeds of the said partnership. See Callanan in UN Office on Drugs and Crime 2011 www.unodc.org 231.

190 Callanan in UN Office on Drugs and Crime 2011 www.unodc.org 232.

3.2.1.6.2 Draft Comprehensive Study on Cybercrime (2013)

The Comprehensive Study on Cybercrime (hereafter the study) examines all the factors pertaining to online crime and builds on the elements that make online crime a real challenge for the entire society. It looks into the efficiency of existing legal measures to fight cybercrime and proposes a range of options for more efficient results.¹⁹¹ The study further acknowledges that these forms of criminal activities developing with advancement in technology require “fundamental changes in law enforcement approach, evidence gathering, and mechanisms of international cooperation in criminal matters.”¹⁹² The study was released following responses provided to some questionnaires prepared¹⁹³ and handed out to different countries¹⁹⁴ on different continents¹⁹⁵ and to several organisations.¹⁹⁶ It reflects recent challenges faced by role players and constitutes consistently well-based findings that have very constructive, informative and broad evaluation of online crime, and does not reflect the reality of only one state or one continent, but that of the global community.

The study is more precisely:

...a comprehensive study of the problem of cybercrime and responses to it by member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with the view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.¹⁹⁷

191 UN Office on Drugs and Crime 2013 www.unodc.org X.

192 UN Office on Drugs and Crime 2013 www.unodc.org X.

193 The questionnaires were prepared by an open-ended intergovernmental expert group established by the Commission on Crime Prevention and Criminal Justice on request of the General Assembly Resolution 65/230.

194 69 (sixty nine) countries in total responded to the questionnaire. See UN Office on Drugs and Crime 2013 www.unodc.org X.

195 Africa (11 countries), Americas (13 countries), Asia (19 countries), Europe (24 countries) and Oceania (2 countries). See UN Office on Drugs and Crime 2013 www.unodc.org X and Annex Five adduced to the Study.

196 According to the Study, the draftsmen gathered information from 40 (forty) private organisations, 16 (sixteen) academic organisations and 11 (eleven) intergovernmental organisations. See UN Office on Drugs and Crime 2013 www.unodc.org Annex Five.

197 UN Office on Drugs and Crime 2013 www.unodc.org IX.

As is evident from the above quote, the study is about “examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.”¹⁹⁸ Thus, it balances different practices adopted by different countries, bilateral and multilateral agreements and, based on the responses provided by the participating countries and organisations, states which practices would work well against cybercrime.¹⁹⁹

3.2.1.6.2 Findings of the study²⁰⁰

According to the study the challenges encountered in fighting cybercrime arise from the fact that there exists a certain “fragmentation at the international level, and diversity of national cybercrime laws”.²⁰¹ This constitutes a barrier to the effective fight in the sense that each legal framework has its own focus, approach and scope of application. Such discrepancies between procedural powers and international cooperation provisions are not appropriate for the nature of cybercrime, according to the study.

Secondly, the study acknowledges the limits of traditional means of formal international cooperation in effectively and efficiently providing timely responses required to the gathering of electronic evidence that is by nature volatile. It also appears that the concept of evidence “location” needs to be rethought so as to allow law enforcements authorities’ access to extraterritorial data. Furthermore, the study emphasises the insufficiency of harmonisation regarding the fundamental “cybercrime offences, investigative powers, and admissibility of electronic evidence.” Another point concerns the judiciary. It is said that law enforcement authorities, prosecutors, and judiciary in developing countries are in need not only of any type of support, but of “long-term, sustainable, comprehensive technical support” in their fight against cybercrime. As one of the key findings of the study, it appears that:

198 UN Office on Drugs and Crime 2013 www.unodc.org X.

199 Among other examples of such evaluation, the Study balances, for instance, the pros and cons of formal and informal international cooperation. See UN Office on Drugs and Crime 2013 www.unodc.org 197-215.

200 UN Office on Drugs and Crime 2013 www.unodc.org XI-XII.

201 UN Office on Drugs and Crime 2013 www.unodc.org XI.

Cybercrime prevention activities in all countries require strengthening, through a holistic approach involving further awareness raising, public-private partnerships, and the integration of cybercrime strategies with a broader cybersecurity perspective.²⁰²

3.2.1.6.2.2 Proposed options²⁰³

The purpose of the study is to strengthen already existing mechanisms and suggest new legal and other responses to cybercrime. Four options, derived from answers provided by participating countries, are proposed as the way forward in the fight against cybercrime. Those options include:

- Development of international model provisions
- Development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters
- Development of a comprehensive multilateral instrument on cybercrime
- Delivery of enhanced technical assistance for the prevention and combating of cybercrime in developing countries.²⁰⁴

The study is split into eight chapters namely connectivity and cybercrime (Chapter one), the global picture (Chapter two), legislation and frameworks (Chapter three), criminalization (Chapter four), law enforcement and investigations (Chapter five), electronic evidence and criminal justice (Chapter six), international cooperation (Chapter seven), and prevention (Chapter 8).

This study may only be a draft or may not bear any legal force, but what can be said is that it is a topical document that consistently evaluates almost all aspects relating to the global fight against cybercrime. Its specificity is a result of the fact that it is compiled following responses given by different organisational groups reflecting realities from all over the world. This may be seen as a huge step towards reaching more appropriate,

202 UN Office on Drugs and Crime 2013 www.unodc.org XII.

203 UN Office on Drugs and Crime 2013 www.unodc.org XII-XV.

204 UN Office on Drugs and Crime 2013 www.unodc.org XII.

more universal responses and most importantly, a common understanding and common purpose in curtailing cybercrime in general. The options proposed to strengthen the fight clearly reveal that the study is one that really has the answers to the many concerns caused by cybercrime in terms of suggestion of new approaches. It is however important to note that some of these proposed options seem too optimistic to find implementation in the near future. The aspect that talks of “development of a comprehensive multilateral instrument on cybercrime” for instance appears to be one of those goals that, although it would be of great assistance if realised, would take many years of negotiations to be able to operate. Even once consensus is reached by the participating countries, for one reason or another, many participants or signatories would make some reservations, justifiably taking into account the reality of their national abilities and capabilities, and this would once again restrict the reputation of the instrument. On the other hand, it might sound easier for European, American and Asian countries for instance to implement such instrument, because they are well equipped to respond effectively to the solutions that may be proposed by such an instrument. Though it is also acknowledged that developing countries need enhanced technical assistance, one thing is clear; the same standard cannot be set for developed and developing countries; even with the help provided. Like the UN, some other organisations such as the Council of Europe have not remained insensitive to the threat posed by crime in IEC.

3.2.2 Other international instruments against crime in IEC

3.2.2.1 The Council of Europe Convention on Cybercrime (2001) (COECC)

Internationally recognised for the effect it has had in the development of regulatory instruments to attend to the issue of crime perpetrated via the Internet and other computer networks, the COECC, also known as the Budapest Convention, stands out as the first international and binding²⁰⁵ instrument to tackle cybercrime. Adopted in 2001, it came into force in 2004. The COECC is supported in its purposes by a protocol

205 Council of Europe 2013 www.coe.int.

concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.²⁰⁶

Acknowledging the nature of cybercrime, and conscious about the fact that efficient responses against it need to be enhanced and speeded up through appropriate international cooperation,²⁰⁷ the COECC sees itself as an indispensable instrument:

...to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both domestic and international levels and by providing arrangements for fast and reliable international co-operation.²⁰⁸

The COECC contains three principal parts. Firstly, it imposes the duty to enact certain conduct as constituting criminal offences under their criminal legal systems on signatory states.²⁰⁹ Secondly, the Convention provides for procedural measures to follow in the detection, investigation,²¹⁰ collection of electronic evidence, and prosecution of computer-related crimes and any other crime.²¹¹ The said procedural steps entail prompt preservation of stored computer data,²¹² timeous preservation and partial disclosure of traffic data,²¹³ production orders,²¹⁴ search and seizure of stored computer data,²¹⁵ real-time collection of traffic data²¹⁶ and lastly interception of content data.²¹⁷ It

206 The Protocol was adopted in 2003 and came into force in 2006.

207 Preamble of the *Council of Europe Convention on Cybercrime* (2001) (COECC).

208 Preamble of the COECC. Note is to be taken that in the recent *Comprehensive Study on Cybercrime* released by the UN, some countries when asked about the best options to strengthen the fight against cybercrime, recommended the accession to the COECC as a way to promoting international cooperation and harmonisation of national cybercrime laws. See in that respect UN Office on Drugs and Crime 2013 www.unodc.org XIII.

209 Such offenses are respectively illegal access (a 2), illegal interception (a 3), data interference (a 4), system interference (a 5), misuse of devices (a 6), computer-related forgery (a 7), computer-related fraud (a 8), offences related to child pornography (a 9) and offences related to the infringement of copyright and related rights (a 10).

210 Article 14(1) of the COECC.

211 Article 14(b)(c) of the COECC.

212 Article 16 of the COECC.

213 Article 17 of the COECC.

214 Article 18 of the COECC.

215 Article 19 of the COECC.

216 Article 20 of the COECC.

should, however be emphasised that safeguarding measures must be put in place for the “protection of human rights and liberties”, and in consideration of the principle of proportionality.²¹⁸ Furthermore, it is member states’ duty to enact legislative and other measures in order to establish jurisdiction upon offences recognised by the Convention. This is to be done in order to rule over offences that are committed in their territory, on board a ship flying the flag of that party, or on board an aircraft registered under the laws of that party by one of its nationals if committed outside the jurisdiction of any state.²¹⁹

Thirdly, looking into the nature of cybercrime, measures such as extradition,²²⁰ mutual assistance,²²¹ spontaneous information²²² and 24/7 Network²²³ are provided. Gathered under the broad concept of international co-operation, these measures appear to be the best available in this regard and the principles underlying them justify their use.

To enlighten member States in their understanding and implementation of the Convention and taking into account new developments, the Council of Europe (through its Cybercrime Convention Committee (T-CY)), has recently published several draft

217 Article 21 of the COECC.

218 Article 15(1) of the COECC. Note should also be taken that dual criminality may not be required as a condition to act regarding these provisional measures. See a 29(3) of the COECC.

219 Articles 22(1)(a), (b), (c) and (d) of the COECC.

220 Extradition as presented by the Convention can only occur subject to the principle of dual criminality. That is, in order to have effect, the offence for which the demand for extradition is made, must be punishable both under the law of the requesting and the requested state. See a 24(1)(a) of the COECC.

221 One outstanding aspect of this measure is that, because formal process of mutual legal assistance have been said to be lengthy and time consuming, and thus not really adequate for the investigation and prosecution of cybercrime offences, there have been a development in this regard. The COECC provides in its a 25(3) for the possibility to circumvent the normal process and so proceed with faster ways of communications such as fax or e-mail. However, formal proceedings are to follow if required by the requested state. See respectively UN Office on Drugs and Crime 2013 www.unodc.org 207. See further a 25(3)(5) of the COECC. Subparagraph 5 relaxes to a certain extent, the principle of dual criminality.

222 Article 26 of the COECC. A party to the Convention may provide another party with information that it deems helpful for engaging proceedings or enlightening proceedings already engaged to the other state party without having been requested to do so.

223 This article provides that each member state shall elect a point of contact available on a twenty-four hour, seven-day-a-week basis that can be used to provide timely assistance to the offences established by the Convention. The said assistance may pertain to facilitating or carrying out the provision of technical advice, the preservation of data, the collection of evidence, the provision of legal information and locating of suspects. See a 35(1)(a), (b) and (c) of the COECC.

Guidance Notes respectively on computer system,²²⁴ botnets,²²⁵ identity theft,²²⁶ DDoS attack,²²⁷ critical infrastructure attack,²²⁸ and on malware.²²⁹ As a further effort to ensure the proper enforcement of its provisions, given the nature of cybercrime offences, the government of Japan and the COE came together and organised a workshop in May 2013 regarding the effective international cooperation in the area of cybercrime investigation and prosecution.²³⁰ International cooperation was once again seen as the key method through which cybercrime can be curbed and it was further acknowledged that making use of already developed frameworks and providing assistance in the making and shaping of criminal justice systems were indispensable in the enhancement of international cooperation.²³¹

There are nevertheless divergent views about the real impact of the COECC. While some see it as just what the world needed and more importantly a “clear and comprehensive solution” to the problem of cybercrime,²³² others are reluctant to accept it as global standard.²³³ Both positions are very consistent in their argumentation, and what is left to say is that the COECC may not be a perfect instrument in the sense

224 Guidance note # 1 on computer system.

225 Guidance note # 2 on botnets.

226 Guidance note # 4 on identity theft.

227 Guidance note # 5 on DDoS attack.

228 Guidance note # 6 on critical infrastructure attack.

229 Guidance note # 7 on malware.

230 Council of Europe 2013 www.coe.int.

231 These are the remarks made by Osamu Imai from Japan, ambassador in charge of cyber policy, ministry of foreign affairs in his opening words. See Council of Europe 2013 www.coe.int.

232 The Council of Europe Secretary-General, Thorbjørn Jagland, so expressed himself at the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador, Brazil, 12-19 April 2010 (Jagland *Secretary-General's Contribution*). He is of the view that, having received support from the Asia-Pacific Economic Cooperation, the European Union, Interpol, the Organisation of American States and other organisations and initiatives as well as the private sector, the Convention really meets the standard. Furthermore, he takes as proof the fact that many legal instruments against cybercrime are based on the COECC. According to him, the Convention appears as a “model law”, or the basis for enacting national legislation, whether the country later becomes party to the Convention or not.

233 Many are those who argue that, having been drafted by and for European countries, it does not really reflect other regions' realities. They are of the opinion that, to be perceived as a global standard, the Convention needed to have been drafted by a higher number of countries than those that actually drafted it, and that even in its present state, the Convention needed to be signed and ratified by more countries. Others opine that the Convention as it stands is outdated. Some other detractors go on to say that it “undermines individual privacy rights and expands surveillance powers too far.” See Archick 2004/2006 www.ncpc.org 3; see also Harley 2010 www.stlr.org for further critics; see further Schjolberg and Ghernaouti-Helie *Global Treaty* ii.

wanted by several countries, but the fact remains that it is unique in its genre and the constant work of the cybercrime Convention committee (T-CY) proves that the COE acknowledges its limits and is progressively working towards meeting the daily challenges imposed by cybercrime.²³⁴

3.3 Regional initiative against crime in IEC

3.3.1 Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa 2011 (Draft Convention)

As a regional organisation, the African Union has also taken steps towards reaching a regional legal instrument to counter cybercrime. This reaffirms the AU's self-determination to help out its member states to make Africa a better place.²³⁵ Despite being a draft, the Convention contains important provisions for the global issue of cybercrime. Africa is said to be a safe haven for cybercriminal attacks because enforcement agencies are not adequately armed "in terms of personnel, intelligence and infrastructure".²³⁶ It is also said that the "lack of IT knowledge by the public and the absence of suitable legal frameworks to deal with cybercrime at national and regional levels"²³⁷ are the reasons why Africa is an easy target. The draft was released in 2011 and its main aim is to find a compromise between "African cyber legislations on electronic commerce organization, personal data protection, cyber security promotion and cyber crime control."²³⁸ It is therefore not too much to acknowledge that trying to reach comprehensive legislation for the sake of Africa in the context of cyber security is indeed a praiseworthy step.

234 Note is also to be taken that, as mentioned by the Council of Europe Secretary General, once a country becomes party to the Convention, it thus becomes a participant to the Cybercrime Convention Committee. This means that if a country did not take part to the negotiations, once it has become member to the treaty, it participates to work toward further development of the Convention in order to fit it into each country's reality. See Jagland *Secretary-General's Contribution* para 52.

235 Murungi 2012 www.snailattorneys.com.

236 Cassim 2009 *PER* 65.

237 Cassim 2009 *PER* 66.

238 Summary of the Draft *African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa* (2011) (Draft Convention).

Praiseworthy to the extent that, although not properly structured and not easily understandable, it is an attempt by the AU to respond in its way to the scourge of cybercrime. The first part of the African draft deals with the organization of electronic commerce, the second part is concerned with the protection of personal data. Combating cyber crime is the content of part three, followed by common and final provisions forming part four.

Considering the limits of this research paper, one's enquiry will be limited to part three which is concerned with how the AU intends to fight cybercrime in its member states. Apart from inviting its member states to each put in place a "cyber security policy" and strategies to implement the said policy,²³⁹ the draft Convention also obliges them to criminalise certain conduct and to ensure that the offenders are found, accordingly prosecuted and punished.²⁴⁰ It is further member states' obligation to establish or develop existing institutions which deal particularly with cyber security issues,²⁴¹ to ensure that their respective laws on cybercrime "reflect international best practices" and work together towards enhancing "the possibility of regional harmonization of the said legal measures."²⁴² Moreover, African states are called to cooperate with one another through their respective established organisations designated for instance in exchanging information based on bilateral or multilateral agreements.²⁴³ Some other steps that constitute each member state's responsibility, are among others involving different groups in the fight against cybercrime through "public-private partnership",²⁴⁴ "education and training"²⁴⁵ programs, and also through "public awareness-raising".²⁴⁶ More measures include Article III-1-14 of the draft convention which reads as follows:

239 Articles 1 and 2 of the Draft Convention.

240 Article III-1-1 of the Draft Convention.

241 Article III-1-2 of the Draft Convention.

242 Article III-1-5 of the Draft Convention.

243 Article III-1-7 of the Draft Convention. Note is to be taken that a broader form of cooperation is provided for in a III-1-23 and involves not only cooperation among member states, but also "with the greatest possible number of... regional and world institutions".

244 Article III-1-10 of the Draft Convention.

245 Article III-1-11 of the Draft Convention.

246 Article III-1-12 of the Draft Convention.

Each Member State shall adopt such measures as it deems necessary to establish appropriate institutions to combat cyber crime, conduct surveillance in response to cyber crime incidents and early warning, for coordination of national and cross-border cyber security problems and for global cooperation.²⁴⁷

One outstanding aspect is that the draft Convention imposes on the member states the adoption of a prison sentence of one (1) to five (5) years for the offences covered by the Convention.²⁴⁸ This stands out in the sense that it is generally rare to find a prescribed sentenced period in an instrument against cybercrime. Whether this is realistic or insufficient will depend on future developments of the Convention.

Murungi²⁴⁹ questions whether it was really necessary for the AU to initiate the process of adopting a Convention against cybercrime. He poses the question whether it would not have been better for the AU to recommend the adoption and accession of the Council of Europe's *Convention on Cybercrime* to its member states, and therefore, try to adjust the said Convention according to the reality of Africa. He sees in the draft Convention not only an instrument that was not properly scrutinized before being drafted,²⁵⁰ but also an unrealistic and unnecessarily broad²⁵¹ instrument that places the stakes too high and undermines member states' sovereignty by leaving little or no room at all for "domestic legislative leeway". He backs this position by stating that in prescribing definitive propositions of law, the draft Convention runs the risk of being in contradiction with some aspects of domestic laws in more than one country, and in these circumstances, none of the said countries will be ready to adopt it once it has been finalised. He further is of the opinion that, although the objective of the draft convention is well defined in the preamble, the Convention gets it wrong when it limits itself to e-commerce. He argues that cyber space is broader than e-commerce.

247 Article III-1-14(1) of the Draft Convention.

248 Article III-31 of the Draft Convention.

249 Murungi 2012 www.snailattorneys.com.

250 Murungi is of the view that it is inconceivable, considering the global nature of cybercrime, to try and produce an instrument only by and for African countries.

251 Murungi finds that there was no need to draft such a long text. It sufficed to build the paper around the most important principles of international cooperation that are applied worldwide and that can simply be adjusted according to each country's rules of law, but that remain within the spirit that cybercrime is a universal problem.

These views do have merit, but is it not better to draft an instrument within the reality of Africa by those who live and share those experiences? Are the standards, or rather “minimum standards” proposed by the international community, affordable (not necessarily in terms of financial ability) by each and every African state? On the other hand however, does the speed at which cybercrime is developing allow wasting time in trying to develop rules applicable to a continent? Whatever the answer to these questions may be, it is important to remember that the spirit is there; measures for national and international cooperation identified as the best ways to combat cybercrime are provided, surely not as well-defined and structured as apparent in other instruments, but sight should not be lost that the draft instrument shows that Africa is indeed responding positively to the global call to legislate in order to combat cybercrime.

3.4 Conclusion

To sum up, this chapter was concerned with ascertaining the limits within which some specific instruments pertaining directly or indirectly to IEC enacted by organisations such as the UN, the COE and the AU, provided solutions to the issue of crime in IEC. Common measures found in these instruments are raising of awareness, international cooperation, public-private partnerships, law enforcement capacity, cybercrime legislation, harmonisation and lastly criminal justice capacity.²⁵² Each and every one of these measures is seen as a step towards making the fight a common one, and to reach a global understanding and global ways of dealing with cybercrime, which by nature knows no bounds.

There may not be an official convention by the UN against cybercrime, but given all the instruments referred to above, it seems appropriate to say that indeed, as an international organisation, the UN is fulfilling its role. The *Comprehensive Study on Cybercrime* is particularly edifying as it brings together concerns and prospects of solutions that are the results of answers provided by various countries from various

²⁵² These provisions found in some instruments, are also mentioned as responses provided by different countries as forming part of national strategies to curtail cybercrime. See UN Office on Drugs and Crime 2013 www.unodc.org 228.

continents. It remains each member state's responsibility to take heed of these propositions and to make the necessary changes to their national laws and build relationships with other countries in order to evaluate how to reach consensus for an international instrument, well understood, properly drafted, that takes into consideration the limits and strengths of all participants and thus providing realistic approaches for all.

The well-known work of the COE is also lauded as it has had a very positive impact worldwide. Although the COECC has been criticised of being outdated and purely European, it has the merit of being the first binding international instrument against cybercrime that can be used as a guideline by other countries, and can be adjusted according to each country's legal reality.

The AU still hasn't officially provided its Member states with a proper Convention. The draft convention also reveals its willingness and commitment to take steps for the wellbeing of its member states.

Indeed, all these initiatives are commendable but the bottom line remains, how effective and efficient are they? This question raises the issue of implementation of the measures provided. In order to be really involved in the fight against cybercrime, which begins with national legislation and ends with the main channel, which is international cooperation, each state has to be well equipped; technically, capacity wise and financially. If these "basic steps" are easily met by European, American and Asian states, can the same be said or expected of African states?

4 The South African legal position with regard to crime in international electronic commerce

4.1 Introduction

South Africa, like any other country in the world, is also vulnerable to online crime.²⁵³ Cyber criminals operate worldwide and every country can be the target of online criminal activities. That is why over the years it has become an obligation for each and every country to enact laws that can protect their citizens against online criminal activities.²⁵⁴ South Africa has not remained behind in this international call to legislate against cybercrime. That is why, taking into account the inability of common law and statutory provisions to deal appropriately with online matters,²⁵⁵ the *Electronic Communications and Transactions Act* (hereafter ECT Act),²⁵⁶ and later the *Consumer Protection Act* (hereafter CPA)²⁵⁷ were passed. Before them, laws on international co-operation in criminal matters²⁵⁸ and on organised crime²⁵⁹ already existed which, by their nature had something to offer regarding cross-border issues. The present chapter is an enquiry into how well these instruments provide a solution to the cross-border problem of crime in international e-commerce. Before scrutinizing the different legal instruments that have been given effect to in order to ascertain the extent to which they contribute to the fight against online crime, it is important to look at the common law position as it was before the coming into operation of the mere legislative instrument on electronic communications in South Africa, namely the ECT Act.

253 See Camerer 1997 ASR 45-46 in which she discusses the reasons for South Africa being an easy target to organised crime in general.

254 See Collier "Criminal Law and the Internet" 319 in which the need of enacting new laws is mentioned as one of the exigencies of new technology. See also UN Office on Drugs and Crime 2013 www.unodc.org 51-72 for details regarding the importance of national and international laws in curtailing online crime.

255 Collier "Criminal Law and the Internet" 320-321. Reference is made in this book to a law commission that was put in place in order to evaluate whether there was any need to introduce in South Africa new types of crimes by way of legislation. The commission's report was that it found it extremely difficult to extend the definitions of common law crimes to what are commonly known and called computer crimes. The commission thus suggested that passing laws in this regard had to be taken seriously. In a nutshell, its findings were that "existing laws cannot accommodate computer crime".

256 *Electronic Communications and Transactions Act* 25 of 2002.

257 *Consumer Protection Act* 68 of 2008.

258 *International Co-operation in Criminal Matters Act* 75 of 1996.

259 *Prevention of Organised Crime Act* 121 of 1998.

4.2 The Common Law position

The common law²⁶⁰ represents that system of law that has its roots in Roman-Dutch Law.²⁶¹ More precisely it refers to:

Those rules of law not contained in an Act of parliament or of legislation enacted by some other subordinate legislature, such as a provincial legislature, but which are nevertheless as binding as any legislation.²⁶²

Before the ECT Act was passed, the common law and statutory law could be interpreted as broadly as possible to also cover the arrest and prosecution of law offenders operating online.²⁶³ This is seen as a privilege recognised in South African law, which enables the constant development of the common law in order to adjust it to suit new developments in the legal domain.²⁶⁴ However, the extent to which the common law responds effectively to online crime is still questionable.²⁶⁵ It is submitted that, even in its adaptive capacity, the common law cannot respond to the pressure brought about by online schemes, and that it was a wise decision by South Africa to take steps to enact the ECT Act.²⁶⁶

Snyman²⁶⁷ provides two reasons why the Roman-Dutch law impact on South African criminal law has decreased namely: first of all courts' tendency over the years to overlook old sources of law,²⁶⁸ and secondly, the "technological age" within which we live that is very demanding and is symbolised by problems substantively different from their old counterparts.

260 As generally opposed to statute law. See Hutchison (ed) *Wille's Principles* 20.

261 Gibson *Wille's Principles* 23.

262 Snyman *Criminal Law* 8.

263 Snail 2009 *JILT* 2; see also Hutchison (ed) *Wille's Principles* 20 for more regarding the capacity of South African courts to interpret common law rules so as to make them very practical and able to suit modern conditions.

264 Van der Merwe "Criminal Law" 65.

265 Van der Merwe "Criminal Law" 66.

266 Van der Merwe "Criminal Law" 69.

267 Snyman *Criminal Law* 9.

268 The importance of the said historical sources of law is not contested, but the difficulty lies in dealing properly with new problems, says Snyman. See Snyman *Criminal Law* 9.

It is thus common cause that because conventional crime deals with tangibles, and information technology (IT) crime deals with intangibles, the common law could not efficiently address IT crime.²⁶⁹ It is in this respect that Burchell said that “the common law is, therefore, not suited to punish conduct such as unauthorized access to computer systems and altering computer data.”²⁷⁰ Furthermore, and in spite of the fact that common and statutory law could be applied to offences such as child pornography and cyber fraud, it could not provide a solution to crimes such as theft, spamming and phishing, to mention a few.²⁷¹

To the question whether computer crime could properly be dealt with in terms of South African criminal law and whether there was any need to pass new laws for those specific forms of crime, the Law Commission project team,²⁷² found that it was not easy to broaden the definitions of common law crimes so as to cover computer crime. It consequently recommended that bringing about new types of offences through legislation had to be taken seriously. The Commission looked at for instance the crime of malicious injury to property, which is defined as the unlawful and intentional damaging of property belonging to another.²⁷³ It considered all the features of the crime, namely: damage (destruction, loss, permanent character of the loss, loss which reasonably requires repair or replacement, causation), property (the damaged property must be corporeal), and culpability (intent to perpetrate an act, and to cause the ensuing damage).²⁷⁴ In the end, it was found that it is improbable that courts will be prepared to apply these features to incorporeal properties such as information stored on a computer.

269 Cassim 2009 *PER* 55-56. Note is to be taken that criminal activities perpetrated online appear under various denominations. While some will tax them as IT crimes, others will use computer crime and some others will use cybercrime, computer fraud amongst others.

270 Burchell 2002 *SALJ* 585.

271 Cassim 2009 *PER* 56.

272 As referred to by Collier “Criminal Law and the Internet” 320-321 (*SALC Discussion Paper* 99).

273 Snyman *Criminal Law* 535.

274 See respectively the *SALC Discussion Paper* 99 5-6 and Collier “Criminal Law and the Internet” 329.

Before the enactment of the legislative instrument regulating electronic transactions (namely the ECT Act), several instruments existed that by nature had, and still have to a certain extent something to offer in the fight against crime in IEC, more precisely based on their international character.

4.3 International Co-operation in Criminal Matters Act 75 of 1996 (ICCM Act)

The ICCM Act is meant to enhance evidence gathering and the enforcement of sentences in trans-border criminal matters where South Africa is either the requesting or the requested state.²⁷⁵ The ICCM Act also has as main goal the regulation of the confiscation and restitution of the proceeds of crime between South Africa and other states.²⁷⁶ Prior to the coming into being of the ICCM Act, South Africa had already, as far back as 1962, passed the *Extradition Act*.²⁷⁷ This latter Act's aim revolves around legislating "the extradition of persons accused or convicted of certain offences and for incidental matters."²⁷⁸ Extradition treaties can be entered into by South Africa and any other country according to section 2 (1) of the *Extradition Act*.²⁷⁹

Like extradition, which is seen as an aspect of international co-operation²⁸⁰ the ICCM Act, in accordance with section 27(1), enables the conclusion by South Africa of agreements to fight criminal activities that have a cross-border effect. In this regard South Africa has concluded several agreements²⁸¹ that aim to provide mutual legal

275 Introductory words of the *International Co-operation in Criminal Matters Act 75 of 1996 (ICCM Act)*.

276 Introductory words of the ICCM Act.

277 *Extradition Act 67 of 1962*.

278 Introductory words of the *Extradition Act 67 of 1962*.

279 South Africa has entered into several extradition agreements with Botswana, Lesotho, the United States of America, Canada, Australia, Israel, Egypt and India, among others. For more information regarding agreements in which South Africa has entered for extradition purposes, see Department of Justice 2010 www.justice.gov.za.

280 Enhancing international co-operation among states has been said to be the best tool in the fight against cybercrime. This is what was said by Osamu Imai from Japan, ambassador in charge of cyber policy, ministry of foreign affairs at the workshop organised by both the COE and the Government of Japan in May 2013, available at Council of Europe 2013 www.coe.int.

281 Among which the *Mutual Legal Assistance in Criminal Matters Treaty between the Republic of South Africa and the French Republic* that was ratified in 2002 and entered into force in 2004; the *Mutual Legal Assistance in Criminal Matters Treaty between the Republic of South Africa and the Hong Kong Special Administrative Region of the People's Republic of China* that came into force in 2011;

assistance in prosecution and sanctioning of criminal activities among the states to the agreements. Although no reference is made to electronic issues in the Act,²⁸² what can be said is that this is the type of co-operation that is needed to fight online crime. If the ICCM Act is concerned only with real-world criminal activities that have a trans-border character, the legislature should probably consider revising the agreements it entered into so as to incorporate electronic criminal activities. This can be done in accordance with section 27 (1) of the ICCM Act. Otherwise, this can be made possible by way of interpretation given the modern world within which we live nowadays.

4.4 Prevention of Organised Crime Act 121 of 1998 (POCA)

Among other objectives, the main goals of the POCA are “to introduce measures to combat organised crime, money laundering and criminal gang activities;...to provide for the recovery of the proceeds of unlawful activity;...to provide for the establishment of a Criminal Assets Recovery Account;...”²⁸³ The POCA was also enacted to fill the gap left by common and statutory law.²⁸⁴ When looking at the definitions provided in Chapter one, proceeds of unlawful activities are defined as:

Any property or any service advantage, benefit or reward which was derived, received or retained, directly or indirectly, in the Republic or elsewhere, at any time before or after the commencement of this Act, in connection with or as a result of any unlawful activity carried on by any person, and includes any property representing property so derived;

This definition, by referring to “in the Republic or elsewhere” gives an international scope to the POCA to the extent that it provides for what is to be done to deal with the proceeds illegally acquired in the Republic or “elsewhere”, which means in another territory. This broad definition indeed shows that South Africa is prepared to efficiently engage in a process of investigation in order to seize and restore to the rightful owners

the *Southern African Development Community Protocol on Mutual Legal Assistance in Criminal Matters* that was ratified in 2003 and entered into force in 2007, to mention a few.

282 If limited to the definition of evidence given in the ICCM Act, it does not include electronic evidence.

283 Objectives of the *Prevention of Organised Crime Act 121 of 1998 (POCA)* as described in its introductory words.

284 Preamble of POCA.

ill acquired properties.²⁸⁵ The words “in the Republic or elsewhere” are further found in the definition of “unlawful activity”²⁸⁶ given in the Act. The POCA is more or less in the same line with the ICCM Act in that it empowers South African courts to deal extensively with proceeds of unlawful activities. This is done through investigations, preservation of information, seizure and confiscation of such proceeds in order to use such proceeds to fight crime. To this effect, the POCA establishes in chapter 7 a criminal assets recovery account in which all moneys deriving from the fulfillment of confiscation and forfeiture orders and the execution of foreign confiscation orders must be deposited.²⁸⁷ Although the POCA merely adopts a civil approach to its proceedings, they appear wide enough to involve electronic transactions and thus online cross-border crime.

4.5 *The Electronic Communications and Transactions Act 25 of 2002*

In response to the fast growing issue of cybercrime, South Africa released the ECT Act which aims at facilitating the use of electronic communications in transactions and provides diversified answers to the questions arising from the use of electronic communications. The chapter in the ECT Act dealing with cybercrime is chapter XIII that is made up of sections 85 to 89. The ECT Act is to be supplemented by common law and statutory provisions in case it does not provide for a specific criminal activity or sanctions thereto.²⁸⁸ The ECT Act considers as an offence any access or interception of data without authority or permission,²⁸⁹ and any interference with data tempering in any way with the data.²⁹⁰ A person who “unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component”, with the primary intent to circumvent security

285 Watney 2012 *PER* 297. It is submitted in this article, regarding mutual legal assistance and extradition in general, that so far South Africa has proven to be ready to engage positively and efficiently in cross-border criminal matters.

286 This is defined by s 1 of POCA as “conduct which constitutes a crime or which contravenes any law whether such conduct occurred before or after the commencement of this Act and whether such conduct occurred in the Republic or elsewhere”.

287 Section 64 of POCA.

288 Section 3 of the *Electronic Communications and Transactions Act 25 of 2002* (ECT Act).

289 Section 86(1) of the ECT Act.

290 Section 86(2) of the ECT Act.

measures pertaining to the protection of data, and any person who uses such device, are guilty of an offence.²⁹¹ If all of this is done with the intention to interfere into a system in such a manner as to prevent legitimate users' access to such service, again, that person is guilty of an offence.²⁹² In order to obtain any "unlawful proprietary advantage" or any other unlawful advantage, if a person performs or threatens to perform any of the acts described in section 86,²⁹³ or by causing fake data to be produced with the full knowledge that it will be acted upon, that person is also guilty of an offence.²⁹⁴ A person who attempts,²⁹⁵ aids and abets²⁹⁶ someone to commit any of the offences mentioned in sections 86 and 87 of the ECT Act, is liable to either a fine or imprisonment for a period not exceeding 12 months,²⁹⁷ or to a fine or imprisonment for a period not exceeding five years.²⁹⁸

These penalties have been criticised²⁹⁹ for not being harsh enough when compared to those provided by the *Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002* (the RICA).³⁰⁰

Section 90 of the ECT Act which deals with jurisdiction empowers a court within South Africa to try an offence where:

- (a) the offence was committed in the Republic;

291 Sections 86(3) and (4) of the ECT Act.

292 Section 86(5) of the ECT Act.

293 Section 87(1) of the ECT Act.

294 Section 87(2) of the ECT Act.

295 Section 88(1) of the ECT Act.

296 Section 87(2) of the ECT Act.

297 Section 89(1) of the ECT Act. This penalty is applicable to offences described in ss 86(1), (2) and (3) of the ECT Act.

298 Section 89(2) of the ECT Act. The penalty of this sub-section applies specifically to the offences described in ss 86(4), (5) and 87 of the ECT Act.

299 Van der Merwe "Criminal Law" 78.

300 Cassim and Van der Merwe take as example s 51 of the *Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002* (RICA) that prescribes fines not exceeding R 2 000 000 or imprisonment not exceeding ten years. Cassim 2009 *PER* 59; Van der Merwe "Criminal Law" 78.

- (b) any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic; or
- (c) the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or
- (d) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

This means that even for offences committed in another country but which have an effect in the Republic, South African courts will have jurisdiction. According to Cassim,³⁰¹ this particular provision of section 90 (b) stands out in the sense that it makes it easy to engage in the prosecution of overseas based hackers and offenders who devise and spread viruses overseas. The nationality of an offender is also a ground which will give jurisdiction to South African courts. It is submitted³⁰² that section 90 (d) contradicts section 28 (1) (d) of the *Magistrate's Courts Act*,³⁰³ which rather requires the "whole cause of action" to occur inside a particular court or district. According to Cassim, another difficulty may arise if cybercrime is committed across South African borders but the offender is prosecuted in SA. In these circumstances, it becomes a problem to effectively ascertain the regional or district court having jurisdiction to rule over the matter.

One very important chapter of the ECT Act is Chapter XII which establishes cyber inspectors with a number of powers among which the power to inspect, search and seize.³⁰⁴ The establishment of bodies with such empowerment has been said to be a very important step toward providing timely and sound responses to the problem of cybercrime as a whole, because such bodies have the ability to monitor and inspect any

301 Cassim 2009 *PER* 60.

302 Cassim 2009 *PER* 60.

303 *Magistrates' Courts Act* 32 of 1944.

304 Section 82 of the ECT Act.

website, search premises or information systems, prevent the deletion or alteration of information by preserving data, to mention but a few.³⁰⁵

It is further said that sections 81 to 83 of the ECT Act are in contradiction with section 14 of the Constitution,³⁰⁶ which recognises the right of privacy to everyone.

Overall, it can be seen that conduct such as spamming, distributed denial of service attack, hacking and interference with data, are catered for in the ECT Act. It is however important to stress that most of these measures are more “cyber security” related and there seems to be a need for legislation regarding the specific aspect of international electronic commerce which merely deals with sale of goods and other services. The Act deals to a considerable extent with protection of electronic systems and data without concretely regulating on the issue of e-commerce.

4.6 Consumer protection in South Africa

In South Africa consumers are protected both under the ECT Act³⁰⁷ and the *Consumer Protection Act* (CPA).³⁰⁸ Without the need of entering into details in order to see under what conditions someone may have the standing of a consumer,³⁰⁹ it is nevertheless useful to state that a consumer, as defined by the ECT Act, is “any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier.”³¹⁰ The nature of electronic

305 See the cyber inspectors’ powers as described by ss 81 and 82 of the ECT Act.

306 *Constitution of the Republic of South Africa*, 1996.

307 Chapter VII of the ECT Act.

308 *Consumer Protection Act* 68 of 2008 (the CPA).

309 Eiselen points out the fact that, even though Chapter VII of the ECT Act makes the Act applicable to electronic transactions, the chapter deals in reality only with transactions where one of the parties is a consumer. He further explains that the chapter thus excludes transactions between legal or artificial persons, and those between a web-trader and a natural person where the latter is not taking the goods or services as the end-user, but for business purposes. See Eiselen “E-commerce” 181-182; note is to be taken that, unlike Chapter VII of the ECT Act, the CPA expands the definition of consumer so as to include natural and small to medium sized juristic persons whose asset value or annual turnover at the time of the transaction is less than the monetary threshold of two million rand. See Papadopoulos “Online Consumer Protection” 66. See further the definition of “person”, which includes a juristic person as given by s 1 of the CPA.

310 Section 1 of the ECT Act.

transactions compared to real-world transactions makes consumer protection a very crucial aspect, and so poses challenges to the legislature which has acknowledged this difference in the level of protection needed.³¹¹ The issue of consumer protection arises where the consumer is preparing to conclude a contract or has already concluded such contract and seeks to either evade the negative consequences brought by such conclusion, or lean on the rights flowing from it.³¹²

The CPA, like Chapter VII of the ECT Act, both aim at affording South African consumers the greatest possible protection by defining the obligations and rights under which online and offline traders are to operate. Though Chapter VII of the ECT Act deals particularly with transactions carried out electronically, both Acts will be assessed simultaneously in order to ascertain the extent to which each provides an answer to the main enquiry of this paper.

Under the ECT Act, a web trader has the duty to provide the customer with all information relating to himself (his business) and to the goods or services he provides. He must further indicate the full price of the goods or services and any other administrative fees, and also make use of a secure payment system for the transaction.³¹³ This secure method of payment concerns not only the transmission of information in the relationship web trader-consumer and web trader-payment institution, but also the manner in which the said information is stored after the transaction.³¹⁴ On the other hand, the consumer is among others entitled to rectify mistakes made in an order, cancel an order, withdraw from a transaction,³¹⁵ a cooling-off period,³¹⁶ examine the goods,³¹⁷ and may also return them³¹⁸ within well-defined deadlines. Consumers are extensively protected against deceptive and misleading trading schemes.³¹⁹ Taken from

311 Eiselen "E-commerce" 181.

312 Eiselen "E-commerce" 182.

313 Section 43 of the ECT Act.

314 Eiselen "E-commerce" 187.

315 These rights and obligations flow from ss 43 and 44 of the ECT Act; see also s 17 of the CPA.

316 See s 16 of the CPA, which does not apply if the transaction is governed by the similar s 44 of the ECT Act.

317 Section 18 of the CPA.

318 Section 20 of the CPA.

319 Sections 29, 40, 41, 42 of the CPA.

this angle, unsatisfied consumers have an opportunity to sue before the National Consumer Commission (NCC)³²⁰ a web trader who fails to comply with its obligations under Chapter VII of the ECT Act.³²¹ It appears that within South Africa it would be easier to prevent and stop conducts such as internet auction fraud in all its different facets as described in Chapter 2 above; chargeback/denial of service, bogus returns and travel, and holiday business fraud to mention a few. One question however remains: is the cost of seizing the national consumer commission conducive for all, or at least, worth it sometimes?³²²

Under the CPA an unsatisfied consumer has remedies such as seeking a court's order warning a supplier against pursuing an offending conduct, award of damages, payment of fines, or even imprisonment for up to 10 years, or both fine and imprisonment.³²³

Due to the fact that both Acts regulate consumer protection, there have been some debates about the extent to which one Act applies and the other one does not, and under what circumstances.³²⁴ So, to solve this issue of what applies where and to what extent, the CPA provides the following solution. In case of inconsistency between this Act and any other Act, the provisions of both Acts, to the extent possible are to be applied concurrently and if it is not possible to so apply them, then the provision that affords the consumer greater protection must prevail over the other.³²⁵ Referring

320 Established in accordance with s 49 of the ECT Act and which is defined by s 1 of the CPA.

321 Schedule 1, part B. para 15 which amends s 1 of the ECT Act.

322 This simple example can justify the enquiry. The author remembers ordering a computer online where the total cost (VAT and postage charges included) amounted to R3 200; she added to the order a school bag on the same website which cost R300. The total cost for the notebook and the bag was thus R3 500. Payment was effected through an electronic funds transfer. Upon reception of the order, there was no bag attached to the notebook. Checking the receipt, the notebook amounted to R3 300 and the shipping cost to R200. After enquiring at the e-mail address provided by the website, there was no satisfying answer. The author had thus lost R300 and thought it would be a waste of time to engage any proceeding to recover such amount. There it can be said that the consumer has made the choice not to exercise her rights. This example is only to show that some web traders out there do not fully comply with the requirements of the Acts and suing them may not always be worth it in all cases. They probably use this situation to their advantage.

323 Sections 76, 111 and 112 of the CPA.

324 Papadopoulos "Online Consumer Protection" 82.

325 Sections 2(8), (9) and (10) of the CPA.

specifically to the ECT Act, there are some specific provisions of the CPA that are not applicable if the right to be enforced are governed by the ECT Act.³²⁶

Trade within SA, be it online or offline, is thus regulated such as to leave little opportunity to criminals to benefit from the fruit of their unlawful labour. However, if these measures are lauded for offline and online transactions within national borders, can the same be said about IEC? It has been submitted³²⁷ that consumer protection measures in SA have been drafted following the example of the *European Distance Selling Directive*.³²⁸ There seems however to be no legal instrument to date in SA catering for e-commerce between SA and other countries.³²⁹

Despite being contemplated by the interpretation clause of the CPA³³⁰ and other sections³³¹ of the same Act, foreign and international law (measures) do not seem to be adequately present throughout the Act. Note should however be taken of section 97(3)(4) of the CPA which allows the co-operation between the NCC and similar foreign or international agencies or authorities dealing with the same issue for information exchange purposes or in respect of existing international agreements relating to consumer protection. One assumes from the latter section that abuses happening online, under the varied forms presented by the CPA, may indeed lead to the seizure of the NCC³³² that may in turn seize a similar organ in another country in seeking redress for the conducts so prohibited in the CPA. The extent to which this inference may lead to the effective fight against misleading and dishonest behaviour arising from

326 Section 16 of the CPA vs s 44 of the ECT Act; s 19 of the CPA vs s 46 of the ECT Act; s 23 of the CPA vs s 43 of the ECT Act; s 26 of the CPA vs s 43 of the ECT Act; s 33 of the CPA vs Chapter VII of the ECT Act.

327 Eiselen "E-commerce" 180; see also Papadopoulos "Online Consumer Protection" 64-65.

328 *European Distance Selling Directive* (EC) 97/7 on the protection of consumers in respect of distance contracts [1997] OJ L144/19.

329 See Eiselen "E-commerce" 180 regarding the lack of legal instruments governing distance selling.

330 Section 2(2)(a) of the CPA.

331 Section 5(3)(b), 5(8)(a) and 97(3)(4) of the CPA.

332 Collier suggests that, when a person is victimised online, he/she should approach the South African Police Service Computer Crime Unit, or a 24/7 network (The National Association of Attorneys General) or even the cybercrime unit of the International Chamber of Commerce. See Collier "Criminal Law and the Internet" 345.

international online trade remains to ascertain and heavily depends on the NCC's ability to answer effectively to this type of call.

4.7 Conclusion

This chapter sought to appreciate the efforts so far made by South Africa to combat criminal activities perpetrated online. More precisely, the endeavour of the research was to evaluate or appreciate how efficient the efforts of South Africa nationally, and mostly internationally regarding crime in IEC, have been. It appears that its efforts are commendable if one limits itself to the ICCM Act, the ECT Act, the POCA and the CPA. The ICCM, the POCA and the *Extradition Act* 67 of 1962 have so far been of great use in helping South Africa to provide and receive help to and from other countries for mutual legal assistance and extradition in criminal matters.³³³ However, can the same be said about crime in IEC? Though the ECT Act and the CPA also contemplate international co-operation and deal consistently with electronic transactions, and despite having had a considerable impact nationally, the fact remains that they are not fully helpful for international problems arising from electronic sale of goods and other services. The ECT Act tries to extend its scope of application by giving South African courts jurisdiction under a number of circumstances, but this attempt still does not substantively solve the fact that the Act has a national scope. That is why, to be part of the global fight against cybercrime in general (and by inference against crime in IEC), it has been recommended³³⁴ that South Africa needs to ratify the Council of Europe *Convention on Cybercrime* to prevent its territory from becoming a safe haven for international cybercriminal activities. Indeed, there is a need for South Africa to do so as it participated in the drafting of the Convention, this means that it understands better than non-participatory countries the principles underlying the Convention, and this fact makes it easier to use the Convention as a guideline. Furthermore, South Africa should probably consider entering other agreements that specifically deal with IEC or electronic

333 Watney 2012 *PER* 292-318 for more details regarding cases of extradition and mutual legal assistance in which South Africa has provided its help to other states.

334 Cassim 2009 *PER* 68.

distance selling as it is a very important aspect of a country's economic growth nowadays.

5 Conclusion and recommendations

Online crime has developed and continues to develop at an unexpected speed along with new developments in technology. At the beginning of this work, the aim was to enquire about the solutions so far provided by organisations such as the UN, the COE and the AU, and further by the South African government regarding criminal activities perpetrated in electronic commerce transactions between business-to-consumer and consumer-to-consumer. However, due to the fact that the solutions provided are meant for cybercrime in general, the author ended up including and often using cybercrime.

Throughout the instruments studied for the purpose of providing an answer to this research's main enquiry (which revolved around what has been done by the above organisations; and by South African law through some specific instruments to curb crime in IEC), there are six main measures that are found in all the instruments that cater for this type of crime. It has been said that international co-operation (that includes, among others, mutual legal assistance and extradition agreements, technical assistance and information exchange), awareness raising, private-public partnership, law enforcement capacity, cybercrime legislation and criminal justice capacity, are the way forward in finding appropriate weapons against the scourge of cybercrime as a whole.

Though the focal point was business-to-consumer and consumer-to-consumer transactions, it appears in the end that most solutions that would work or that are suitable for crime in IEC, are "State based". This means that only governments have the ability and necessary resources to properly challenge online crime. Consumers and businesses (who may be named private parties as opposed to the State), nevertheless have a crucial role to play.

Businesses are called to watch out for "weird" orders generally made in late hours, via free/anonymous e-mail services, and that request express shipping.³³⁵ Furthermore,

335 Curry 2000 www.scambusters.org.

merchants should be wary of huge quantity orders, several attempts to order on the same card, and frequent calls from customers, amongst others.³³⁶

On the other hand, consumers are called to be very cautious in the sense that they should not fool themselves regarding online offers that appear too good to be true.³³⁷ The United States of America (USA) Federal Trade Commission (FTC) as presented by Albert,³³⁸ while acknowledging that law enforcement activities are crucial, suggests that consumers should be enabled to take steps for their own protection in dealing with these new types of crime. The FTC thus urges consumers to make good use of states' initiatives by educating themselves on the patterns of online crime, and under such circumstances they will have more control over their transactions. Regarding the particular scheme of Internet auction fraud, Albert³³⁹ suggests that Internet auction sites should be subjected to financial liability for fraudulent activities perpetrated on their websites.

It is the view of Smith and Urbas³⁴⁰ that it cannot be possible to avoid all online risks, but that good knowledge and appropriate use of existing technologies can help to reduce the problem. They further are of the opinion that good partnerships between agencies and organisations and broad information sharing across nations are the key initiatives to effectively fight electronic crime. Uniform procedural and evidentiary laws are needed because of the nature of online crime they submit. According to these authors there is no better response to online fraud than being well informed of the existing risks and to know how to avoid them. Though traditional approaches to controlling of crime are inadequate for online crime, the combination thereof with "sophisticated technological solutions" can help to deal effectively with such types of crime.³⁴¹

336 Curry 2000 www.scambusters.org.

337 Baker 1999 *Internet Research* 357.

338 Albert 2002 *ABLJ* 594.

339 Albert 2002 *ABLJ* 595-596.

340 Smith and Urbas 2001 www.aic.gov.au.

341 Smith and Urbas 2001 www.aic.gov.au.

Overall, though it can be said that the world community through different organisations is really working towards barring the road to the escalating issue of online crime, there seems to be a crucial need for legal instruments dealing specifically with crime in IEC and that needs to be developed taking into account different countries' and regions' capacities and abilities.

BIBLIOGRAPHY

Albert 2002 *ABLJ*

Albert MR "E-buyer Beware: Why Online Auction Fraud Should Be Regulated"
2002 *ABLJ* 575-643

Baker 1999 *Internet Research*

Baker RC "An Analysis of Fraud on the Internet" 1999 *Internet Research* 348-360

Bellah 2002 *Law and Order*

Bellah J "Training: Identity Theft" 2001 *Law and Order* 222-226

Brenner 2001 *MUEJL*

Brenner S "Cybercrime Investigation and Prosecution: The Role of Penal and
Procedural Law" 2001 *MUEJL* 1-16

Brenner 2005 *IJCLP*

Brenner SW "Distributed Security: Moving Away from Reactive law Enforcement"
2005 *IJCLP* 1-43

Brenner and Koops 2004 *JHTL*

Brenner S and Koops B-J "Approaches to Jurisdiction" 2004 *JHTL* 1-46

Burchell 2002 *SALJ*

Burchell J "Criminal Justice at the Crossroads" 2002 *SALJ* 579-602

Camerer 1997 *ASR*

Camerer L "International Fraud Trends: South Africa at Risk" 1997 *ASR* 45-51

Cassim 2009 *PER*

Cassim F “Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study” 2009 *PER* 36-79

Clough *Principles*

Clough J *Principles of Cybercrime* (Cambridge University Press Cambridge 2010)

Collier “Criminal Law and the Internet”

Collier D “Criminal Law and the Internet” in Buys R and Cronjé F (eds) *Cyberlaw@SA II: The Law of the Internet in South Africa* 2nd ed (Van Schaik Pretoria 2004)

Copes and Vieraitis 2009 *Criminology and Public Policy*

Copes H and Vieraitis LM “Bounded Rationality of Identity Thieves: Using Offender-based Research to Inform Policy” 2009 *Criminology and Public Policy* 237-262

Darch and Lucas 2002 *JWL*

Darch H and Lucas T “Training as an E-commerce Enabler” 2002 *JWL* 148-155

Ellis 2004 *WWD*

Ellis K “Ashcroft Attacking E-commerce Fraud” 2004 *WWD* 1-2

Eiselen 1995 *SAMLJ*

Eiselen S “The EDI Interchange Agreement” 1995 *SAMLJ* 1-18

Eiselen “E-commerce”

Eiselen S “E-commerce” in Van der Merwe D *et al Information and Communications Technology Law* (LexisNexis Durban 2008)

Gibson *Wille’s Principles*

Gibson JTR *Wille's Principles of South African Law* 6th ed (Juta Cape Town 1970)

Gregg and Scott 2006 *IJEC*

Gregg DG and Scott JE "The Role of Reputation Systems in Reducing On-Line Auction Fraud" 2006 *IJEC* 95-120

Hutchison (ed) *Wille's Principles*

Hutchison D (ed) *Wille's Principles of South African Law* 8th ed (Juta Cape Town 1991)

Jagland *Secretary-General's Contribution*

Jagland T *Secretary-General's Contribution* (Unpublished paper delivered at the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador, Brazil, 12-19 April 2010)

Kariyawasam (ed) *The WTO*

Kariyawasam R (ed) *The WTO, Intellectual Property, E-commerce and the Internet* Volume II (Edward Elgar Cheltenham 2009)

Knight 2005 *IEE Review*

Knight W "Caught in the Net" 2005 *IEE Review* 26-30

Kyo 2004 *JECM*

Kyo MD "Internet Auction Fraud: The Silent Victims" 2004 *JECM* 1-22

Lisanawati 2010 *IJCSE*

Lisanawati G "Electronic Funds Transfer in Money Laundering Crime: Regulation Needed in Response to Meeting of Technology and Crime in Indonesia" 2010 *IJCSE* 163-170

Papadopoulos "Online Consumer Protection"

Papadopoulos S "Online Consumer Protection" in Papadopoulos S and Snail S (eds) *Cyberlaw@SA III The Law of the Internet in South Africa* (Van Schaik Pretoria 2012)

Pathak 2004 *MAJ*

Pathak J "A Conceptual Risk Framework for Internal Auditing in E-commerce" 2004 *MAJ* 556-564

Pinguelo and Muller 2011 *VJLT*

Pinguelo FM and Muller BW "Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals" 2011 *VJLT* 117-188

Plant *Ecommerce*

Plant RT *Ecommerce: Formulation of Strategy* (Prentice Hall Upper Saddle River 2000)

Quash and Sriganesh 2008 *Expert Systems with Applications*

Quash JTS and Sriganesh M "Real-time Credit Card Fraud Detection using Computational Intelligence" 2008 *Expert Systems with Applications* 1721-1732

Rosen *E-commerce Question and Answer Book*

Rosen A *The E-commerce Question and Answer Book: A Survival Guide for Business Managers* 2nd ed (AMACOM New York 2002)

SALC *Discussion Paper 9*

South African Law Commission *Discussion Paper 99, Project 108: Computer-related Crime: Preliminary Proposals for Reform in respect of Unauthorised Access to Computers, Unauthorised Modification of Computer Data and Software Applications and Related Procedural Aspects* (The Commission Pretoria 2001)

Schjolberg and Ghernaouti-Helie *Global Treaty*

Schjolberg S and Ghernaouti-Helie S *A Global Treaty on Cybersecurity and Cybercrime: A Contribution for Peace, Justice and Security in Cyberspace* 2nd ed (Cybercrime data Oslo 2011)

Singleton 2002 *EDPACS Newsletter*

Singleton T "Managing Distributed Denial-of-Service Attacks" 2002 *EDPACS Newsletter* 7-20

Smith, Holmes and Kaufmann 1999 *Trends and Issues in Crime and Criminal Justice*

Smith RG, Holmes MN and Kaufmann P "Nigerian Advance Fee Fraud" July, 1999 *Trends and Issues in Crime and Criminal Justice* 1-6

Snail 2009 *JILT*

Snail S "Cyber Crime in South Africa: Hacking, Cracking, and Other Unlawful Online Activities" 2009 *JILT* 1-13

Snyman *Criminal Law*

Snyman CR *Criminal Law* 4th ed (Lexis Nexis Butterworths Durban 2002)

Timmers *Electronic Commerce*

Timmers P *Electronic Commerce: Strategies and Models for Business-to-Business Trading* (Wiley Chichester 2000)

Tse and Yim 2001 *JICM*

Tse ACB and Yim F "Factors Affecting the Choice of Channels: Online vs Conventional" 2001 *JICM* 137-152

Van der Merwe "Criminal Law"

Van der Merwe D "Criminal Law" in Van der Merwe D *et al Information and Communications Technology Law* (LexisNexis Durban 2008)

Watney 2012 *PER*

Watney M “A South African Perspective on Mutual Legal Assistance and Extradition in a Globalised World” 2012 *PER* 292-318

Westland and Clark *Global Electronic Commerce*

Westland JC and Clark THK *Global Electronic Commerce: Theory and Case Studies* (MIT Press Cambridge 1999)

Wopperer 2002 *GPRI*

Wopperer W “Fraud Risks in E-commerce Transactions” 2002 *The Geneva Papers on Risk and Insurance* 383-394

Yang *South African SMME Owner/Manager’s Perceptions*

Yang PP *South African SMME Owner/Manager’s Perceptions of E-commerce Related Risks* (MTech-dissertation Cape Peninsula University 2007)

Register of legislation

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Electronic Communications and Transactions Act 25 of 2002

Extradition Act 67 of 1962

International Co-operation in Criminal Matters Act 75 of 1996

Magistrate’s Courts Act 38 of 1944

Prevention of Organised Crime Act 121 of 1998

Regulation of Interception of Communications and Provision of Communications Related Information Act 70 of 2002

Register of international instruments

Council of Europe Convention on Cybercrime (2001)

Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (2011)

European Distance Selling Directive (EC) 97/7 on the protection of consumers in respect of distance contracts [1997] OJ L144/19

OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999)

OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Practices across Borders (2003)

OECD Policy Guidance on Online Identity Theft (2008)

OECD Scoping Paper on Online Identity Theft (2008)

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996) with Additional Article 5 (as adopted in 1998)

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001)

United Nations Convention against Corruption (2003)

United Nations Convention against Transnational Organized Crime and the Protocols Thereto (2000)

United Nations Convention on the Use of Electronic Communications in International Contracts (2005)

Register of internet sources

ACFE 2011 www.acfe.com

Association of Certified Fraud Examiners 2011 *Fraud Examiners Manual*
www.acfe.com [date of use 8 Feb 2013]

ACFE 2013 www.acfe.com

Association of Certified Fraud Examiners 2013 *Financial Transactions and Fraud Schemes Computer and Internet Fraud* [date of use 3 Nov 2013]

Anonymous Date Unknown www.sagepub.com

Anonymous Date Unknown *Introduction to E-commerce* www.sagepub.com/upm-data/9598_019964Ch1.pdf [date of use 8 Feb 2013]

Archick 2004/2006 www.ncpc.org

Archick K 2004/2006 *Cybercrime: The Council of Europe Convention* www.ncpc.org/cms-upload/ncpc/File/cybercrime.pdf [date of use 8 Feb 2013]

Better Business Bureau 2007 www.bbb.org

Better Business Bureau 2007 *Homepage* www.bbb.org [date of use 28 Nov 2012]

Council of Europe 2013 www.coe.int

Council of Europe 2013 *Homepage* www.coe.int [date of use 17 Aug 2013]

Curry 2000 www.scambusters.org

Curry S 2000 *An Inside Look at E-commerce Fraud Prevention and Solutions* www.scambusters.org/ecommercefraud.pdf [date of use 21 Nov 2012]

Department of Justice 2010 www.justice.gov.za

Department of Justice 2010 *International Legal Relations-Extradition and Mutual Legal Assistance in Criminal Matters Treaties* www.justice.gov.za/ilr/mla.html [date of use 8 Feb 2013]

Dinodia and Tiwari 2009 www.srdinodia.com

Dinodia P and Tiwari A 2009 *E-commerce – International Approach* www.srdinodia.com/wp-content/uploads/2013/01/E-Commerce-International-Approach.pdf [date of use 21 Nov 2012]

FBI 1999 www.fbi.gov

Federal Bureau of Investigations 1999 *Health Care Fraud: National and Local Perspective on a Growing Trend* www.fbi.gov/contact/fo/norfolk/hcf.htm [date of use 28 Nov 2012]

Hansen et al 2005 www.pactworld.org

Hansen R et al 2005 *Fraud Prevention Handbook* www.pactworld.org [date of use 8 Feb 2013]

Harley 2010 www.stlr.org

Harley BA 2010 *Global Convention on Cybercrime? The Columbia Science and Technology Law Review Webpage* www.stlr.org/2010/03/a-global-convention-on-cybercrime/ [date of use 8 Feb 2013]

Interpol Date Unknown www.interpol.int

International Criminal Police Organisation Date Unknown *Homepage* www.interpol.int [date of use 10 Sep 2013]

Javelin Strategy and Research 2009 www.search.org

Javelin Strategy and Research 2009 *Identity Fraud Survey Report: Consumer Version – Prevent – Detect – Resolve* www.search.org/files/pdf/IdentityFraudSurveyConsumerReport.pdf [date of use 15 Aug 2013]

Montague 2011 www.fraudpractice.com

Montague D 2011 *The Fraud Practice* www.fraudpractice.com [date of use 17 Nov 2012]

Murungi 2012 www.snailattorneys.com

Murungi MM 2012 *Comments on the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (Version-1/01.2011)*

www.snailattorneys.com/Comments%20on%20The%20Draft%20African%20Union%20Convention%20on%20the%20Establishment%20of%20a%20Credible%20Legal%20Framework%20for%20Cyber%20Security%20in%20Africa.pdf [date of use 17 May 2013]

Smith 1998 www.aic.gov.au

Smith RG 1998 *Best Practice in Fraud Prevention*
www.aic.gov.au/publications/current%20series/tandi/81-100/tandi100.aspx [date of use 8 Feb 2013]

Smith and Urbas 2001 www.aic.gov.au

Smith RG and Urbas G 2001 *Controlling Fraud on the Internet: A CAPA Perspective: A Report for the Confederation of Asian and Pacific Accountants*
www.aic.gov.au/publications/current%20series/rpp/21-40/rpp39.aspx [date of use 8 Feb 2013]

Snyder 2002 www.nbcnews.com

Snyder A 2002 *Age-old Scams Find New Home on Net*
www.nbcnews.com/id/3078800/ [date of use 8 Feb 2013]

Standard Bank Date Unknown www.standardbank.co.za

Standard Bank Date Unknown *Homepage* www.standardbank.co.za [date of use 29 Nov 2012]

Teck 2001 www.lawgazette.com.sg

Teck KL 2001 *Fraud in E-commerce* www.lawgazette.com.sg/2001-9/Sep01-focus4.htm [date of use 21 Nov 2012]

Thomas *et al* 2004 www.eurecom.fr

Thomas B et al 2004 *A Comparison of Conventional and Online Fraud*
www.eurecom.fr/en/publication/1556/download/ce-dacima-041025.pdf [28 Mar 2012]

UN Office on Drugs and Crime 2011 www.unodc.org

UN Office on Drugs and Crime 2011 *Handbook on Identity-related Crime*
www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf [date of use 28 Nov 2012]

UN Office on Drugs and Crime 2013 www.unodc.org

UN Office on Drugs and Crime 2013 *Draft Comprehensive Study on Cybercrime*
www.unodc.org/documents/organised-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [date of use 28 Nov 2012]

United States General Accounting Office 2002 www.gao.gov

United States General Accounting Office 2002 *International Electronic Commerce - Definitions and Policy Implications* www.gao.gov/products/GAO-02-404 [date of use 21 Nov 2012]

US IFCC 2001 www.ifccfbi.gov

United States Internet Fraud Complaint Center 2001 *Internet Auction Fraud*
www.ifccfbi.gov [date of use 28 Nov 2012]