National Journal of Cyber Security Law
Volume 1, Issue 2
www.stmjournals.com

Cyber Insecurity in E-Commerce Transactions in Cameroon: What Prospects for the Digital Economy

Ayuk Macbert Nkongho*
Research Scholar, Department of English Law, University of Dschang, Cameroon

Abstract

Today, the digital economy or developing the digital economy is the dream of every state government. Due to the success stories envisaged in some digital economies, cyber-attacks have emerged in the form of cybercrimes by cyber criminals. As a result, the advancement of e-commerce transactions has held back worldwide especially in Cameroon. Cyber criminality has become a major concern to the actors of E-commerce as cyber criminals feel more secured operating online without using guns. The global nature of cyber-attacks in e-commerce has made it inevitable for stakeholders to take action against its prevalence in online business but despite these efforts, there is little or no literature on cyber criminality in Cameroon per se. This paper attempt to explain some threats of cyber insecurity and its potential damaging effects in e-commerce transactions in Cameroon as the country is growing digitally. The paper also seeks to examine the legal mechanisms put in place by the government to build trust in electronic communication networks and information systems thereby filling the gap in the literature by critically examining the 2010 cyber-crimes and security law as well as the Budapest Convention of 2001 relating to cybercrimes. In achieving these, we applied the doctrinal approach in assembling information consonant to the research. The paper concludes with some robust recommendations that could be contributive in reducing the damaging effects in Cameroon in particular and the world at large, amongst them is streamlining data protection and cyber-crime laws on e-commerce transactions.

Keywords: *Cyber criminality, E-commerce, Criminals, Digital, Economy, Cameroon.*

Author for Correspondence E-mail: ayuk.macbert@yahoo.com

INTRODUCTION

The internet is still a fairly young technology in its own right, only having been really accessible on a major global scale since 1995. It existed before in the 1980s, but on a smaller scale, and its uses were mainly limited to government organizations and educational institutions. Ever since its commercial inception, the internet has exploded in popularity amongst commercial and private users (e-commerce transactions) [1]. It has become the medium of the 21st Century pre-occupation in terms of communication and digital commercialization. It is from the rise of the internet that the concept of e-commerce has really come to exist on its own. E-commerce has become so firmly established that certain individuals believe the next level for companies to do business must incorporate information technologies and without it they can face great difficulties as time goes on:

The internet has proven itself as a very useful medium and tool for corporations to conduct their business. The fact that internet is extremely dynamic and fast growing, has seen the rise of new areas for business development and the increase in potential wealth, invariably affected by the so-called cyber criminality. The internet has seen the rise of new companies and has observed older and more established firms expanding their business ventures. The following statement demonstrates the reality of it all:

"Although U.S. firms are considered world leaders in e-business, the rapid growth of the number of businesses that use the internet is a global phenomenon. Over the period of 1999 to 2001, Europe bridged the e-business gap with the United States by experiencing triple-digit growth in this area. By the end of 2000, European firms" e-retail revenues were estimated to be worth $8.5 billion, increasing to an estimated $19.2 billion by 2001, as compared to North America's figures of $40.5 billion for 2000" [2].

The economic benefits of e-commerce have been seen over the past few years, with the likes of companies such as Amazon and E-Bay (giant online companies specialized in facilitating the buying and selling of goods). The concept behind e-commerce is to make business flourish electronically, without the need for places or physical presence, i.e., stores. The fact that many are interested in cashing in on the e-commerce concept has led to a mass drive to establish an online presence, i.e., carry out business on the World Wide Web. Unfortunately, this leaves room for more undesirable issues to surface such as cybercrime, computer fraud, and copyright or trademark infringement. This has led to the need for countries and Cameroon in particular to establish laws aimed at protecting both companies and consumers, in order to avoid malicious, fraudulent and exploitative use of the internet and e-transactions.

The Cameroonian legislature in 2010 enacted the law on cybercrime and security due to the security challenges faced in electronic commercial transactions. Nevertheless, the internet (e-transaction) has provided numerous advantages ever since its inception, ranging from: e-government (facilitating administrative procedures); e-commerce (online sale and purchase of goods and services); e-finance (ease of interbank electronic payments in international trade). Cybercrime is a threat to the abovementioned electronic transactions. Therefore, cybercrime goes a long way to retard progress in this sector of internet business. The threats posed could be computer fraud, deceit, identity theft espionage, cyber scam, child pornography, hacking of encrypted data, forgery, spread of viruses, and unauthorized access to information. These cause huge loss to public and private investments in the global village and Cameroon is not an exception.

Due to e-commerce, customers do not need to drive, park, stand-in-line, and wait for shopping hours or inclement weather. Commodities can be purchased either locally or around the world 24 hours a day. Financial accounts (bank cards, credit cards, etc.) can be opened online and funds can be transferred around the world with the click of a mouse. The internet has transformed the world in a single and borderless e-Commerce marketplace [2]. Organizations all over the world are increasingly relying on e-commerce for their business transactions and growth. E-commerce is growing rapidly, accounting for $132 billion in retail sales in the U.S. in 2008 and £50 billion in purchases and sales in the U.K. in 2009. In the European Union (EU) countries, 15% of enterprises received orders online in 2007, 6% up from 2003. The EU average for online purchases grew from 13% in 2003 to 27% in 2007. As people conduct e-commerce and use cyberspace, enormous amounts of personal, financial, organizational, and commercial data are being collected, processed automatically, and stored electronically.

A GLOBAL EXAMINATION AND THE CATEGORIES OF E-COMMERCE

This Section of the paper examines e-commerce in a global scale as well as the various categories or types of e-commerce transactions in Cameroon.

A Global Examination of E-Commerce Transactions

There are different views of e-commerce transactions but within our present context. Andam defines e-commerce as "any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact" [3]. In other words, it is trade that involves goods crossing borders electronically, the production, advertising, sale and distribution of products via telecommunications network. Examples of products distributed electronically are books, music and videos transmitted through telephone lines or through the internet. E-Commerce can be between many groups. The sole problem retarding it development is that the internet/computer mediated network is flourished by scrupulous users who alternates its use for dubious and criminal intentions, which of course, is the call for concern in this paper. This form of internet/computer-mediated channel can operate between business and business, or between business and consumers, or can be between business and employees, and can be many more" [4].

Products and structures of e-commerce cover its three categories: consumer-oriented commerce, business-to-business commerce, and inter organizational business. All three are experiencing vigorous developments; with differing economic outcomes at this time [5]. The most highly touted applications of e-commerce are consumer-oriented. They include remote (or home) shopping, banking, and stock brokerage, accompanied by on-line advertising. Examples of e-commerce transactions include:

- An individual purchases a book on the internet;
- A government employee reserves a hotel room over the internet;
- A business calls a toll free number and orders a computer using the seller's interactive telephone system;
- A business buys office supplies on-line or through an electronic auction;
- A retailer orders merchandise using an electronic data interchange (EDI) network or a supplier's extranet;
- A manufacturing plant orders electronic components from another plant within the company using the company's intranet;
- An individual withdraws funds from an automatic teller machine (ATM).

Nowadays, many transactions are done through the internet, and as well, guaranteeing security for e-commerce users is a challenging issue, because there are a lot of cyber threats, malware, spam, phishing, social engineering, scare ware, identity theft, etc., are activated into use. Without ensuring a secure e-commerce environment, it is almost impossible to gain confidence and trust for customers and the entrepreneurs. Most governmental institutions, public and private corporations usually make use of e-commerce and there is need for cyber security in their various computer units. The private information breach is misused for different purposes such as opening new accounts; gaining control over victims" credit account; gaining benefits from government by using fake identity, etc. Unfortunately identity theft methods are hidden to the victim because there is lack of awareness to quickly discover and identify perpetrators and to report to law enforcement agencies. Usually victims spend billions of dollars annually to compensate the effects of identity theft and personal data breach. It is important that information, especially PII must be kept secured without being compromised; otherwise e-commerce will continue to face real challenges in the foreseeable future.

Categories of E-Commerce

There are different categories of e-commerce, according to Andam and Koponen [6], but those of prime importance include:

Business to Business (B2B)

B2B or business to business is an e-commerce transaction between companies for sale or purchase of products, services, or information. Forecasts are that B2B income will far exceed business-to consumers (B2C) income in the near future. B2B e-commerce can save or make your company money.

Business to Consumer (B2C)

B2C (Business to Consumer): refers to a business communicating with or selling to an individual rather than a company. It refers to businesses selling to the general public typically through catalogs utilizing shopping cart software. Doing business online no longer requires a huge investment by retailers, thanks to developments in template-based online stores which are based on packaged applications that are delivered over the internet. All online stores will require the same functions: catalogues, order baskets, payment processing, content management and member management.

Consumer to Business (C2B)

C2B is a business model in which consumers (individuals) offer products and services to companies and the companies pay them. This business model is a complete reversal of traditional business model where companies offer goods and services to consumers. This kind of economic relationship is qualified as an inverted business model. Blogs have paved the way for new C2B and C2C applications by giving the opportunity and tools to anyone to express themselves easily and to communicate inexpensively. Video casting, RSS and other blog related technologies help to provide opportunities to develop new economic

systems and to generate alternative revenues. Online Advertising sites like Google Ad sense, affiliation platforms like Commission Junction and affiliation programs like Amazon are the best examples of C2B schemes.

Business to Employee (B2E)

B2E (Business to Employee) e-commerce generally refers to the business between the company and its employees. The examples could be an e-store company where employees can buy the company goods and services at discounted prices. However, B2E has grown into technologies that allow the employee to access their employee records to update address information, shift investments, or maintain their internal resume.

Consumer-to-Consumer (C2C)

The C2C business is the one that originates from consumers and the destination is also consumers. The most famous and successful example of a consumer-to-consumer application is EBay. It is an online site that facilitates the trade of privately owned items between individuals. The website claims that through EBay, practically anyone can trade anything. EBay is now considered one of the most successful C2C e-businesses ever. There are many sites offering free classifieds, auctions, and forums where individuals can buy and sell thanks to online payment systems like PayPal where people can send and receive money online with ease. Consumer-to consumer applications are a growing area of e-commerce. As online business expands, peer-to-peer transactions will continue to grow in popularity and the industry will become highly profitable. All the above types of e-commerce are exposed to identity theft because they include remote (or home) shopping, banking, and stock brokerage, accompanied by on-line advertising and financial misuses are the common purpose of criminals.

Business-to-Government (B2G)

Business-to-government (B2G) commerce is generally defined as e-commerce between companies and the public sector. It refers to the use of the internet for public procurement, licensing procedures, and other government related operations. In B2G e-commerce, the public sector generally assumes the pilot role in establishing e-commerce in an effort to make its procurement system more efficient. The size of the B2G e-commerce market as a component of total e-commerce is still rather insignificant as government e-procurement systems still remain comparatively undeveloped [7].

LEGAL INSTRUMENTS APPLICABLE TO CYBER CRIMES IN E-COMMERCE TRANSACTIONS IN CAMEROON

This Section of the paper focuses on both national laws and international conventions drafted to harmonized aspects of cyber-crimes in Cameroon

National Instruments on Cyber Crimes in Cameroon

In the light of offenses committed with the use of the internet in E-commerce transactions, the Cameroonian legislator has enacted law No. 2010/12 of 21st December 2010 relating to cyber security and cyber criminality in Cameroon, hereinafter referred to as "the 2010 law" is very instructive as seen in its Section 1, as it seeks to build trust in electronic communication systems by establishing a legal regime of digital evidence, security, cryptography, and electronic certification activities, electronic signatures, protect basic human right particular, the right of human dignity, respect of privacy as well as the legitimate interest of corporate bodies. All these security mechanisms are managed by the regulatory agency known in French acronym as ANTIC (national agency for information and communication technology) under the ministry of telecommunication having specific missions provided in Section 7. The cybercrime law targets satellite, ground and electronic networks which are used to commit cybercrimes in electronic transaction as provided in its Section 3. Also, Article 6 provides that". The administration in charge of telecommunication shall formulate and implement the electronic communication security policy by taking into account technological developments and government priority in this domain. Accordingly, it shall:

-Promote the security of electronic communication network and formulation system and monitor the evolution of issues

related to security and certification activity;
-Coordinate activities that contribute to the security and electronic communication networks and information system at national level;

-Ensure the setting up of an electronic communication security frame work;
-Draw up the list of certification authorities;
-Represent Cameroon in international bodies in charge of activities related to the security and protection of electronic communication network and information system.

Offences and Sanctions Contained in the Cyber-Crime Law of Cameroon

The 2010 law on cyber-crimes and security has outlined exhaustive lists of offences and sanctions which constitutes cybercrimes in e-commerce transactions. These offences include:

Interception and Unauthorized access through Electronic Medium

Whoever, without any right or authorization, proceeds by electronic means to intercept or not during transmission, intended for, whether or not within an electronic communication network, an information system or a terminal device shall be punished with imprisonment for from 05 (five) to 10 (ten) years or a fine of from 5.000.000 (five million) to10.000.000 (ten million) CFA francs or both such fine and imprisonment as per Section 65. Also, any unauthorized access to all or part of an electronic communication network or an information system or a terminal device shall be liable to the same sanctions in accordance with Subsection 1 above. The penalties provided for in Subsection 1 above, shall be doubled where unauthorized access violates the integrity, confidentiality, availability of the electronic communication network or the information system. Sub (4) provides that whoever, without any right, allows access to an electronic communication network or an information system as an intellectual challenge shall be punished in accordance with Subsection 1 above.

Hacking

Section 66(1) provides that whoever causes disturbance or disruption of the functioning of an electronic communication network or a terminal device by introducing, transmitting, destroying, erasing, deteriorating, altering, deleting data or rendering data inaccessible shall be punished with imprisonment for from 02 (two) to 05 (five) years or a fine of from 1.000.000 (one million) to2.000.000 (two million) CFA francs or both of such fine an imprisonment. While Sub (2) maintained that whoever uses the deceptive or undesirable software to carry out operations on a user's terminal device without first informing the latter of the true character of the operation which the said software is likely to damage shall be punishable with the same penalties. Also, Sub (3) states that whoever uses potentially undesirable software to collect, try to collect or facilitate any of such operations in order to access information of the operator or supplier of an electronic network or services and commit a crime shall be punishable in accordance with Subsection1above. Also, Section 67stipulate that**,** Causing serious disturbance or disruption of the functioning of an electronic communication network or terminal equipment by introducing, transmitting, changing, deleting or altering data shall constitute a breach of the integrity of an electronic communication network or an information system and shall be punishable in accordance with Section 66 above. However, Section 72 goes further to state that, whoever without authorization and for financial gain uses any means to introduce, alter, erase or delete electronic data such as to cause damage to someone else's property shall be punished with the penalties provided for in Section 66 above.

Illegal Access

This shall mean whoever fraudulently gains access in full or in part of an electronic communication network or an information system by transmitting, destroying, causing serious disturbance or disruption to the functioning of the said system or network shall be punished with imprisonment for from 05 (five) to 10 (ten) years or a fine of from 10.000.000 (ten million) to 50.000.000 (fifty million) CFA francs or both of such fine and imprisonment as per Section 68(1) of the cyber code.

Child Pornography

Whoever uses electronic communications or an information system to design, carry or publish a child pornography message or a message likely to seriously injure the self-respect of a child shall be punished with imprisonment for from 5 (five) years to 10 (ten) years or a fine of from 5,000,000 (five million) to 10,000,000 CFA francs or both of such fine and imprisonment as per Section 76, 80, 81 of the 2010 cyber code.

Identity Theft

Identity theft is a crime that threatens cyber security. Identity theft involves personal identifiable information (PII) and concerns breach on Social Security numbers (SSNs), driver's license numbers, government identification numbers, alien registration numbers, email addresses, taxpayer identification numbers, telephones numbers, financial records, credit card numbers, passport numbers, employer identification number, electronic identification number, and criminal history [8]. It also includes unique biometric data (fingerprints, retina scans, facial geometry, iris images, and other unique physical representations), patient identification numbers, and medical records [9]. With this information, a thief is capable of charging merchandise to the victim's account and changing the billing address for the account so that the unauthorized purchases remain undetected [10]. Identity-theft is a relatively new phenomenon and there is no unique universally accepted definition yet. The definition by an author [11] commonly encountered for identity theft is "The use of another individual's personal identifying information without that individual's permission for purposes of committing a crime" [12]. An identity thief could be an individual criminal, a terrorist, or a crime ring as seen in the case of In R v Andrew Skelton (Bradford Crown Court 17 July 2015 Computer Misuse Act 1990), Section 2 in unauthorized access with intent to commit or facilitate commission of further offences where a senior internal auditor at Morrison's supermarket accessed and uploaded confidential personal data (including employees' names, addresses, national identity and bank details) of nearly 100,000 employees to newspaper and data sharing websites. The defendant was found guilty of fraud by abuse of position of trust, securing unauthorized access to computer material and disclosing personal data. Data breach cost the company more than £2m to rectify and was sentenced to eight years imprisonment. Also, in R v Gary Paul Kelly, Nicholas Webber, Ryan Thomas, Shakira Ricardo (Southwark Crown Court 2 March 2011)under the Computer Misuse Act 1990, s 3: Unauthorized modification. Conspiracy to defraud creators of Ghost Market forum used by thousands of their clients to trade unlawfully and obtained credit/debit card details, confidential personal information and malware tools. The accused pleaded guilty. All of them: Kelly sentenced to five years imprisonment, Webber five years, Thomas four years and Ricardo 18 months [13]. Also, in R v Adam Penny (Kingston Crown Court, 12 September 2016, Computer Misuse Act of England 1990 in Section 1 unauthorized access) whereby an unemployed hacker accessed a gold bullion firm's website to obtain names, addresses and tracking telephone numbers of customers to enable associates to intercept the gold deliveries. Pleaded guilty for conspiracy to steal, unauthorized access to a computer and blackmail and sentenced to five years and four months in jail. Identity theft opens the door to other crimes, such as gaining access to welfare and social security benefits, ordering new checks to a new address, obtaining new credit cards, obtaining the victim's paycheck, taking out loans in the victim's name, and using the victim's name upon arrest [14]. The risk posed by identity theft has affected online consumer behavior [15]. A 2004 survey conducted by the Identity Theft Resource Center (ITRC) reported that victims spent an average of 330 hours repairing the damage from identity theft. Identity thieves typically commit fraud in two steps. The first is to steal an identity or create a fake one. The second is to illegally use a fake identity to gain access to the victim's financial services or to commit crimes.

That notwithstanding, whoever uses any device to receive the privacy of another person by attaching, recording or transmitting private or confidential electronic data without the consent of their authors shall be punished with

imprisonment for from 01 (one) to 02 (two) years and a fine of from 1,000,000 (one million) to 5,000,000 (five million) CFA francs as per Section 74 (1) of the cyber code. Also, whoever, without authorization, intercepts personal data in the course of their transmission, from one information system to another, shall be punished in accordance with Subsection 2 above. The offender who even through, negligence processes or causes the processing of personal data in violation of the conditions precedent to their implementation shall be punished with imprisonment from 01 (one) to 03 (three) years and a fine of from 1,000,000 (one million) to 5000,000 (five million) or both of such fine and imprisonment as per Section 74(3). Also, Section 74(4), Whoever uses illegal means to collect the personal data of another in order to invade his or her privacy and undermine his or herself esteem shall be punishable with imprisonment for from 06 (six) months to 02 (two) years or a fine of from 1,000,000 (one million) to 5,000,000(five million) CFA francs or both of such fine and imprisonment. The penalties provided for in Section 4 above shall be doubled where anyone posts online, stores or has someone else store in a computerized memory, without the express consent of the person concerned, personal data which directly or indirectly discloses his/her tribal origin, political opinions, religious beliefs, trade union membership or values as per section74(5).

Whoever keeps information in works or in figures beyond the legal time-limit specified in the application for a prior opinion or declaration for use of .data processing shall be punished with imprisonment for from 06 (six) months to 02 (two) years or a fine of from 5,000,000 (five million) to 50,000,000 (fifty million) CFA francs or both of such fine and imprisonment as per Section 74 (7) of the cyber code. Finally, whoever discloses personal information that undermines the consideration due to the victim shall be punished with the penalties provided for Section 74 (8).
Also, law No. 2016/07 of 12 July 2016 amending law No. 67/LF/1 12 June 1967governing the penal code of Cameroon provides in Article 7 the application of criminal law in space. This applies to the principle of territoriality of cybercrimes as it makes it difficult for anyone country to detect the origin of cyber-attacks.

International Instruments

The Constitution of 18th January 1996 provides in its Article 45 for the application of treaties and international agreement approved and ratified by Cameroon. This provision gives power for reference to the Budapest Convention relating to cybercrimes. Cybercrime poses everyday threat to everyone anywhere, engaged in online activities. These internet crimes are classifications of the Council of Europe's Budapest Convention on cybercrime which seems to be the only international instrument in force as well, used as a model for national legislation in much domestic legislation such as Cameroon. The Budapest Convention has three objectives:

- To harmonize the domestic criminal substantive law elements of offences and related provisions in the field of cyber-crimes;
- To provide for domestic criminal procedural authorities necessary for the investigation and prosecution of cyber-criminal offences as well as gathering electronic evidence related to cybercrimes;
- To set up an expeditious and effective international cooperation regimes.

Under the Budapest Convention certain computer crimes are defined, for instance, Article 2, illegal access means "…that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system, Article 7 of the Budapest Convention like that of the Cameroonian 2010 law on cyber security and cybercrime in Article 73 defines electronic forgery as offence committed intentional and without right, the input, alteration, deletion, or suppression of computer data, resulting in unauthentic data with the intent that it can be considered or acted upon for legal purpose as if it were authentic, regardless of whether or not the data is directly readable and intelligible. Electronic fraud is defined in

Article 8 as an offence committed intentional and without right, the custody of loss of property to another person by:

- Any input, alteration, deletion or suppression of electronic data (computer information);
- Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring without right, an economic benefit for oneself or another person. The offence of electronic forgery and electronic fraud constitute the major threats to the smooth functioning of electronic commerce transactions as bank accounts and credit cards are been compromised online by cyber thieves. Article 10 provides for intellectual property right offences in electronic commerce transactions. That is, offences of copyright and related rights infringement on commercial scale and by the means of a computer system provided that it has undertaken obligations pursuant to the Paris Act of 24 July 1971 revising the Berne Convention for The Protection of Literary and Artistic Works, the agreement on Trade-Related Aspect of Intellectual Property Right Treaty but excepting moral rights conferred by the Convention.

The Budapest Convention, being the fundamental cybercrime instrument, provides for the following categories of cyber threats to electronic business:

1. Offences against the confidentiality, integrity and availability of computer data and systems, this includes: Illegal access, into classified information or stock system, for example, by means of hacking, deception or otherwise; Illegal interception of computer data; Data interference, including intentional damaging, deletion, deterioration, alteration or suppression of computer data without right; System interference, including intentional serious hindering of the functioning of a computer system, for example, by means of distributed attacks against the key information infrastructure; Misuse of devices, i.e., production, sale, procurement of devices, computer programs, computer passwords or access codes for the purpose of committing cybercrime offences;
2. Computer-related offences, including forgery and fraud committed with the use of computers;
3. Content-related offences, including child pornography, racism and xenophobia;
4. Offences related to infringements of copyright and related rights, including illegal reproduction and use computer software, audios/videos and other digital products as well as databases and books.

At the same time, in terms of criminal motivation, cybercrime offences may be arbitrarily divided into the following categories:

- Cyber fraud for gaining illegal possession of funds;
- Cyber fraud for gaining illegal possession of information (for personal use or further sale);
- Interference with operation of information systems for accessing management information systems (for intentionally damaging them for fee/payment or for inflicting losses on competitors);
- Other offenses.

The first category includes criminal offences committed for stealing i.e., gaining illegal possession of funds. The most widespread offences fall into the second and third categories. These offences involve database hacking and damaging government and corporate computer systems as well as theft of innovative solutions and technologies.

In particular, accessing funds of banking institutions customers is currently the most popular type of cybercrime offence. The most widespread offences that fall into this category are as follows:

1. Internet (online) fraud, including: online Ponzi/pyramid schemes;) is a fraudulent investment operation where the operator, an individual or organization, pays returns to its investors from new capital paid to the operators by new investors, rather than from profit earned through legitimate sources; internet sales fraud and online auction fraud; production of malware for stealing financial, commercial and personal

information (setting up dummy websites, distribution of computer viruses and Trojans, traffic interception, etc.);
2. Remote (online/distant) banking fraud, including: production of computer viruses and Trojans for establishing covert control over customer's computer with installed online banking software; opening accounts, carrying out unauthorized transactions and withdrawing cash as a result of such unauthorized transactions in online banking systems; receipt of payments via SWIFT from foreign originators as a result of interference with operation of computers and online banking systems of customers, of foreign banking institutions.
3. Counterfeit payment card and ATM fraud: Use of lost/stolen/ counterfeit payment cards; Theft of payment card details, inter alia, with the application of card cloning devices; skimming production, sale and installation of devices on ATMs for reading/copying data off a payment card's magnetic stripe and stealing PIN-codes; use of white plastic for cloning (counterfeiting) payment cards, withdrawing cash from ATMs, etc.

Jurisdiction of Courts in Cyber Crime Litigations

This Section of the paper examines both international and national jurisdictions in cyber-crime cases. Ever since Cain and Abel existed, crime is a well-known phenomenon to humankind [16].

International Jurisdiction of Courts in Cyber Crimes Litigation

As far as international jurisdiction is concerned in cybercrime cases, analyses are in accordance with Article 22 of the Budapest Convention of 23 December 2001 of member states. Considering the provision of Article 22 of the Convention, it provide for the jurisdictional principles of territoriality, nationality and universality.

Principle of Territoriality

The principle that jurisdiction is determined by the place where the offence is committed, in whole or in part (territoriality theory) derives from the Westphalia treaty model of sovereignty [17] which is said to include three fundamental principles: exclusive control over the nations territory, non-interference, and of equality between States [18]. Although discussed and opposed [2], the model seems to have, at least, a general acceptance in what concerns these principles, even if the equality between the States is most often only of formality. Given that the State has sovereignty over the territory, it will obviously have jurisdiction over any misconduct which occurs in that territory, whether perpetrated or not by one of its nationals [19]. A complex case of application of the territoriality theory is *Bavaria v.* Felix Somm, tried at the Amtsgericht of Munich, Germany, in 1999. As managing director of Computer server Information Services GmbH, Felix Bruno Somm, a citizen from Switzerland, was charged in Germany for being responsible for the access in Germany to violent, child, and animal pornographic representations stored on the computer server's placed in the USA. The court considered it had jurisdiction over Mr. Somm because, even though he was Swiss, he lived in Germany and sentence to two years imprisonment.

Nationality Theory

The "nationality theory" is also called "active personality theory" because it deals primarily with the nationality of the person who committed the offence [20]. Being widely recognized that a country has almost unlimited control over its nationals [21], the said country is considered to have the right to exercise jurisdiction over those individuals, wherever they are and whatever they do as a means of protection against criminal behavior. Also, an act can be considered legal in the territory where it was committed, whereas it can be considered a crime in the person's homeland. The case of *United States v. Galaxy Sports* seems to be a good example of the application of this theory. World Sports Exchange, together with its President Jay Cohen, was one of the defendants. The company targeted customers in the United States, advertising its business all over America by radio, newspaper, and television. Its advertisements invited clientele to bet with the company either by toll-free telephone or through the internet [22]. Because the company was Antigua-based, the court was unable to assert jurisdiction over it. The companies' president,

however, was a citizen of the USA and could, therefore, be taken to court. Mr. Cohen was on August 10, 2000, after a jury trial presided by Judge Thomas P. Griesa, sentenced to a term of twenty-one months imprisonment of which he seems to have served 17 months [22]. Dealing with the appeal to this sentence, the Second Circuit Court of Appeals affirmed the judgment of the district court without even discussing the assumption of jurisdiction [23].

Universality Principle

The "universality theory" is based on the international character of the offence and contrary to the other theories, allows every State to claim jurisdiction over offences, even if those offences have no direct effect on the asserting state [20]. Therefore, demanding no nexus between the state assuming jurisdiction and the offence itself. Two requirements are necessary for assuming jurisdiction: the State assuming jurisdiction must have the defendant in custody [24] and the crime must be especially offensive to the international community [25].

National Jurisdiction of Courts in Cyber Crimes Litigation

Section 7(1)(2) of the Cameroon Penal Code provides that: (1) Criminal law of the Republic shall apply to any act committed on its territory; Sub (2) proceeds that included in the territory of the Republic, territorial waters and airspace over that territory and its waters and vessels and aircraft registered in the Republic. From the above provision, cybercrimes committed in Cameroon automatically accord jurisdiction to Cameroonian courts. The provisions of Section 52(1) of the cyber security and cybercrime law 2010 of Cameroon states that "In case of any cyber offence, Criminal Investigation Officers with general jurisdiction and authorized officials of the Agency shall carry out investigations, in accordance with the provisions of the Harmonized Criminal Procedure Code of 27th July 2005". Also Section 294 of the Code equally makes provision as far as jurisdiction of the courts in criminal cases is concerned. It states that a court shall have jurisdiction over a case when it is: (a) The court of the place of the commission of the offence; or (b) The court of the place of residence of the accused; or (c) The court of the place of arrest of the accused. These courts include ordinary courts such as court of first instance and the high court though some case may likely go on appeal and the appeal court.

EFFECTS OF CYBER INSECURITY ON THE CAMEROON NATIONAL ECONOMY

This Section of the paper discusses the effects of cyber criminality on the national economy though other state faces same. The effects are financial loss, loss or theft of information, breach of electronic contracts by means of deceits, publication of obscenity to the society such as cyber pornography (child pornography, cyber harassment, i.e., defamation of one's person by posting obscene images of individual privacy, cyber prostitution i.e. exchange of address to clients by prostitutes for further crimes. Nevertheless these effects include:

Effects on E-Businesses

Cyber-crimes through hacking have resulted into loss of business confidential information and the line between business confidential information and intellectual property is inexact. Business confidential information can include trade secrets or "know how". These categories are similar to intellectual property and their loss imposes serious and similar costs. We distinguish between intellectual property information that makes it easier to produce a competing product and business confidential information. While it may take years for stolen intellectual property to show up in a competing product, there is no delay in monetizing stolen confidential business information. Theft of oil exploration negotiation data or even, insider stock trading information can be used immediately by the acquirer. The damage to individuals and companies are enormous. Measuring this category of loss is very difficult since the victim may not know the reason they were underbid, a negotiation went badly, or a contract was lost.

A more insidious form of hacking is the equivalent of insider trading. In this case, the individual extracting non-public information about a future financial transaction is not an

insider, but the effect is the same. Insider trading, or its hacking equivalent, may look like a victimless crime but it reduces social welfare and harm financial markets [26].

Moreover, there can be a risk to the information system of a company or even the entire State. In this case, confidentiality will not be enforced, and hackers could even take control of the information contained in their websites. A report by ASSONGMONECDEM states that Cameroon is a country vulnerable to cyber criminality. ASSONGMONECDEM further proceeds that Cameroon is not safe in a world where 16 pieces of data are stolen every second. It could start with an e-mail which should have been opened, or counterfeit software which opens the door to all kinds of threats. ANTIC even reminds that over 90% of software and operating systems used in Cameroon are hacked.

Effects on Financial Institutions

This Section of the paper discusses the effects of cybercrime in the banking sector and its impact on the banks' finances. It also examines the different types of cybercrimes which plague the banking sector and the motives of the cyber criminals behind such acts. Through information communication technology (ICT), cybercrimes have seriously affected the banking sectors, and such attacks include ATM frauds, phishing, identity theft, and denial of service. The financial loss in the banking sector is huge across the globe both in terms of combating the cyber-attacks and on development of systems to prevent such attacks in the future. But that notwithstanding, cybercriminals have developed advanced techniques to not only cause theft of finances and finances information but also to espionage businesses and access important business information indirectly impacting the banks' finances. In global terms, $114 billion is lost nearly every year due to cybercrimes, and the cost spend to combat cybercrimes is double in amount, i.e., $274 billion. On an average analysis, banking facilities take 10 days to fully recover from a cyber-act which further adds to the cost of operation. Comparing the financial losses faced by the Indian Banking Sector, it is nearly 3.5% of the loss in cash in comparison to global loss. $4 billion is lost in recovering from the crime and $3.6 billion is spent to combat such crimes from happening in future [27].The main issue of concern here is that there is absence of effective compilation of service in the banking sector which can identify the trends in cyber-crime and compile a model according to it thus; worsening the situation. However, in the last few months, banks all across the globe have perceived cybercrime as among their top five risks [28].

High-profile banks in the UK like Barclays and Standard Charter Bank were targeted by hackers who stole personal information of nearly 2.9 million credit cards of customers by hacking the software maker system of these banks, which led them to incur huge losses. However, the scenario is not restricted to UK; in US as well such attacks have surfaced in the past years and in order to curb the effect, they launched the program Quantum Dawn 2, which tests the efficacy of systems installed in banks in response to cyber-attacks [28]. A solid defense system to resolve attacks are considered on the popular saying prevention is better than cure [29]. Telephone calls fraud is also rampant in Cameroon. In 2015, the mobile phone sector lamented losses of over FCfA 3 billion for operators; another FCfA 4 billion for the State. According to the 2014 report from the National Anti-Corruption Commission, cyber-criminality cost was FCfA 3.5 billion to Cameroon between November and December 2013 [29].

Effect on Society

Cybercrime creates social costs, public indecency, and promotes riots in the society. A website hosting child pornography or advocating terrorism imposes real costs on the society. The Congressional Budget Office of the United States estimated that the costs of implementing a law to fight child pornography are roughly at $30 million a year. This estimate does not of course measure the psychological trauma and "spillover" costs that these activities generate. Intangible costs arise from the suffering of the victims. Companies are not persons, although employees or shareholders may suffer as a result of damage from malicious cyber actions (if they are aware that this is the cause). Efforts to estimate the cost of intangible

suffering for other crimes such as stolen property offenses, vandalism, forgery and counterfeiting, embezzlement, and fraud suggest another caveat.

SECURITY MEASURES FOR COMBATING CYBER CRIMINALITY IN CAMEROON AND WORLDWIDE

The threats and challenges plaguing the information and communication system have been so devastating that certain security measures are put in place to mitigate their effects on economy and the society as a whole. These security measures are both national and international.

National Security Measures

Cameroonian legislators have provided certain preemptive security measures, even though there are not exhaustive, conventional security mechanisms are however available for the fight against cyber criminality as well as ensure confidentiality of information in e-commerce trans actions.

Pre-emptive security measures include the following:

Electronic Signature

According to Section 17 of the 2010 Cyber Crime Law, "The advanced electronic signature shall have the same legal value as handwritten signature and produce the same effects as the latter. Furthermore, Section 18 provides guidelines and conditions to be met for it to constitute an advanced electronic signature:

- The data related to signature creation shall be exclusively linked to the signatory and be under his exclusive control;
- Each modification shall be easily detectable;
- It shall be created using a protected device whose technical characteristics shall be defined by an instrument of the Ministry in charge of telecommunications;
- The certificate used to generate signatures shall be a qualified certificate. An instrument of the ministry in charge of telecommunications shall determine the criteria of the qualification of certificates.

Electronic Certificate

Section 15(1) of the cyber-crime law provides that "Qualified electronic certificates shall be valid only for the objects for which they were issued. Sub (2) states that devices used to design and verify qualified certificates shall, from the technological standpoint, be neutral, standardized, certified and inter-operable. Also, Section 16(1) provides that certification authorities shall be responsible for prejudice caused to people who relied on the certificates they presented as qualified in the case where:

- the information contained in the certificate on the date of its issuance was inaccurate;
- the data prescribed such that certificate could be considered as qualified was incomplete;
- the issuance of the qualified certificate did not give rise to the verification that the signatory holds the private Convention corresponding to the public Convention of the certificate;
- Certification authorities and certification service providers, as the case may be, have not registered the repeal of the qualified certificate and placed this information at the disposal of third parties. Sub (2) precedes that certification authorities shall not be responsible for the prejudice caused by the use of the qualified certificate that exceeds the limits fixed for its use or the value of transactions for which it can be used, provided that such limits appear in the qualified certificate and are accessible to users and Sub (3) concludes that certification authorities must justify adequate financial guarantee, allocated particularly for the payment of sums they may owe people who relied logically on the qualified certificates they issue, or an insurance that guarantees the pecuniary consequences of their civil professional responsibility.

Data Encryption

In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not of itself prevent interference but denies the intelligible content to a would-be interceptor or cyber-criminal. In an encryption scheme, the intended information or message, referred to as

plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users or cyber criminals.

Nevertheless, apart from pre-emptive security measures there are also conventional security mechanisms or software security measures put in place to fight against cyber-crimes. These measures include:

Firewalls

In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules [30]. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the internet, that is assumed not to be secure or trusted [31]. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks; they are either software appliances running on general purpose hardware, or hardware-based firewall computer appliances while Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine [32]. Firewall appliances may also offer other functionality to the internal network they protect, such as acting as a DHCP server or VPN server for that network [33].

Password

A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which is to be kept secret from intruders. The use of passwords is known to be ancient. In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc. A typical computer user has passwords for many purposes: logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites, and even reading the morning newspaper online. Some passwords are formed from multiple words and may accurately be called a passphrase. The terms pass code and passkey are sometimes used when the secret information is purely numeric, such as the personal identification number (PIN) commonly used for ATM access. Passwords are generally short enough to be easily memorized and typed. Most organizations specify a password policy that sets requirements for the composition and usage of passwords, typically dictating minimum length, required categories (e.g. upper and lower case, numbers, and special characters), prohibited elements (e.g. own name, date of birth, address, telephone number). Some governments have national authentication frameworks that define requirements for user authentication to government services, including requirements for passwords.

Anti-virus

Anti-virus or anti-virus software (AV), sometimes known as anti-malware software is computer software used to prevent, detect and remove malicious software [33]. Antivirus software was originally developed to detect and remove computer viruses. However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern antivirus software can protect from: malicious browser helper objects (BHOs), browser hijackers, ransom ware, key loggers, backdoors, root kits, Trojan horses, worms, malicious LSPs, dialers, fraud tools, adware and spyware [34]. Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, advanced persistent threat (APT) and botnet DDoS attacks.

Secure Socket Layer (SSL)

Secure Socket Layer is a protocol that encrypts data between the shopper's computer and the site's server. When an SSL protected page is requested, the browser identifies the server as

a trusted entity and initiates a handshake to pass encryption key information back and forth. Now, on subsequent requests to the server, the information flowing back and forth is encrypted so that a hacker sniffing the network cannot read the contents. SSL allows transferring data in an encrypted form. All information that a customer might want to keep private are transmitted via SSL. Such information must include credit card number and related information, and may, depending on the type of business, include customer's name, address, and the list of products that the customer is buying. It should also include the customer's password and order ID E-commerce. The SSL certificate is issued to the server by a certificate authority authorized by the government. Whenever a request is made from the shopper's browser to the site's server using https://, the shopper's browser checks if this site has a recognized certificate before replying.

The Payment Card Industry Standard Compliance

In 2004, five different credit card security programs merged to form the Payment Card Industry Security Standards Council (PCI DSS) with the purpose of creating an extra level of protection for card issuers making sure that merchants (both online and brick and mortar) meet basic levels of security when storing, processing, and transmitting cardholder's data. To set a minimum level of security, the Payment Card Industry set twelve requirements for compliance that fall into one of six groups called control objectives. The control objectives consist of: build and maintaining a secure network; protect cardholder data; maintain a vulnerability management program; implement strong access control measures; regularly monitor and test networks; maintain an information security policy. Companies that fail to comply with the PCI DSS standards risk losing the ability to process credit card payments and may be subjected to audits and fines. Credit card details can be safely sent with SSL, but once stored on the server they are vulnerable to outsiders hacking into the server and accompanying network. A PCI (peripheral component interconnect) hardware card is often added for protection; therefore another approach altogether is adopted [5].

International Measures to Mitigate Cyber Criminality

At the international sphere, different groups universal and regionally, have contributed in devising mechanisms for combating cyber threats in e-commerce in order to enable electronic trade flourish within their respective economic or political grouping. The universal groups include inter alia:

The Group of Eight Countries (G8)

Group of Eight is made up of the heads of eight industrialized countries: the U.S., the United Kingdom, Russia, France, Italy, Japan, Germany, and Canada. In 1997, G8 released a Ministers' Communiqué that includes an action plan and principles to combat cybercrime and protect data and systems from unauthorized impairment. G8 also mandates that all law enforcement personnel must be trained and equipped to address cybercrime, and designates all member countries to have a point of contact on a 24 hours a day/7 days a week basis.

United Nations

In 1990 the UN General Assembly (GA) adopted a resolution dealing with computer crime legislations. In 2000, the UN GA adopted a resolution for combating the criminal misuse of information technology. In 2002, the UNGA adopted a second resolution on the criminal misuse of information technology. In May 2011, the United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU) signed a memorandum of understanding for developing regulatory frameworks and legal mechanisms to counter the threats. With the view of mitigating threats and reducing exposure of the information environment to such threats, the ITU, being the UN specialized agency, developed: Global Cyber Security Agenda; Guideline on Child Online Protection; Guidelines for Parents, Guardians and Educators on Child Online Protection; Guidelines for Industry on Child Online Protection; Guidelines on Child Online Protection; Guideline for Policy Makers on Child Online Protection; and Elements for Creating a Global Culture of Cyber security.

Council of Europe
Council of Europe is an international organization focusing on the development of human rights and democracy in its 47 European member states. In 2001, the Convention on Cybercrime, the first international Convention aimed at internet criminal behaviors, was co-drafted by the Council of Europe with the addition of USA, Canada, and Japan and signed by its 46 member States, Cameroon is yet to ratify the Convention. It aims at providing the basis of an effective legal framework for fighting cybercrime, through harmonization of cyber-criminal offences qualification, provision for laws empowering law enforcement and enabling international cooperation.

That said, apart from universal groupings there are also regional groupings with security mechanisms aiming at combating cyber-crimes worldwide. These groups include:

Asia-Pacific Economic Cooperation (APEC)
Asia-Pacific Economic Cooperation (APEC) is an international forum that seeks to promote open trade and practical economic cooperation in the Asia-Pacific Region. In 2002, APEC issued Cyber Security Strategy, which is included in the Shanghai Declaration. The strategy outlined six areas for co-operation among member economies including legal developments, information sharing and co-operation, security and technical guidelines, public awareness, and training and education.

Organization for Economic Co-operation and Development (OECD)
The Organization for Economic Cooperation and Development (OECD) is an international economic organization of 34 countries founded in 1961 to stimulate economic progress and world trade. In 1990, the Information, Computer and Communications Policy (ICCP) Committee created an Expert Group to develop a set of guidelines for information security that was drafted until 1992 and then adopted by the OECD Council. In 2002, OECD announced the completion of "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" against cyber threats in information and communication technologies.

European Union
In 2001, the European Commission published a communication titled "Creating a Safer Information Society by improving the Security of information Infrastructures and Combating Computer-related Crime". In 2002, EU presented a proposal for a "Framework Decision on Attacks against Information Systems". The Framework Decision taken note of Convention on Cybercrime but concentrates on the harmonization of substantive criminal law provisions that are designed to protect infrastructure elements.

Commonwealth
In 2002, the Commonwealth of Nations presented a model law on cybercrime that provides a legal framework to harmonize legislation within the Commonwealth and enable international cooperation. The model law was intentionally drafted in accordance with the Convention on Cyber Crime.

Economic Community of West African States (ECOWAS)
ECOWAS is a regional group of West African Countries founded in 1975 with fifteen member states. In 2009, ECOWAS adopted the Directive on Fighting Cyber Crimes that provided a legal framework for the member states, which includes substantive criminal law as well as procedural law.

ECCAS and CEMAC
About a hundred telecommunications experts, legal specialists, parliamentarians, members of security forces, and other stakeholders in the cyber-security sector in Central Africa have recommended that member states of ECCAS and CEMAC continue to formulate and implement national policies and strategies for a transition to a sustainable and inclusive knowledge society by creating safe and trustworthy environment for the use of Information and Communication Technologies (ICTs) and to make proposals on the African Union's draft Convention on the implementation of a legal framework to build confidence in e-transactions on the continent.

CONCLUSION AND RECOMMENDATIONS

The paper concludes by stating clearly a brief history and understanding of the advent of the

internet and its role played in our daily lives and economic benefits which of course concerns electronic commerce transactions. Even though, it facilitates trade globally through the use of information and communication technologies, it has been threatened by cyber criminals who wreak havoc on the internet, hence causing adverse effect on ecommerce transactions and the society as a whole. To this effect, some measures were put in place both nationally and internationally to combat such threats thereby guaranteeing confidentiality of information and protecting properties. Nevertheless, these measures are insufficient thus, the following recommendations is hoped to go a long way to combat cyber-crimes in Cameroon and the world at large. Some of these recommendations include:

Providing Proper Training and Equipment's

Law enforcement personnel, police and private investigators, prosecutors, and judges should get appropriate training on a regular basis. Training assists individuals and institutions to keep up with the advances in the computer and online business industry. To adequately address the cybercrime problem, individuals should have information about the new technology. Training provides opportunity to individuals to learn the ever-updating technology.

Increasing Data and Reporting

In order to assess and address the cyber-related crime, electronic transaction problem, more comprehensive information is needed. Without detailed information, it is difficult to depict the trends in computer-related crime.

Cooperation between Public and Private Sectors

The criminal law system cannot address the cybercrime problem alone. Entire criminal law system (law enforcement personnel, prosecutors, and judges) needs support of high-tech industry. This cooperation whether regional, national or international, may encourage institutions and industries to report computer crime incidents.

Streamlining Data Protection and Cyber Crime Laws

The development and adoption of legal frameworks for protecting personal data and for combating cybercrime at the national level to ensure confidence and trust in the use of the internet should not be done in isolation. Harmonization of laws and policies is required at the regional and international levels. Also, the establishment of minimum standards helps to ensure cross border coordination on the design and implementation of relevant legislation and stronger enforcement institutions as well as establishment of computer emergency response teams/computer security incident response teams.

Strengthening the Capacity of the Judiciary

The judiciaries in many developing countries need to be trained in the area of cyber laws. Legal issues around e-commerce are still relatively new. Several international and regional organizations, including the Commonwealth secretariat, the International Telecommunication Union, UNCITRAL, UNCTAD, the United Nations Office on Drugs and Crime and the Council of Europe can provide assistance to countries and regions in the different legal areas. Increasingly, these agencies are joining forces to maximize their actions.

REFERENCES

1. John C., *Business Week*, Aug. 28, 2000, 210pp.
2. Christopher C. J., Wayne P. "Libya and the aerial incident at Lockerbie: What lessons for international extradition law". *Michigan Journal of International Law.* Winter 1993; 14: 256, 257pp.
3. Andam Z. R. "E-Commerce and E-Business". United Nations Development program-Asia Pacific Development Information Program. 2003.
4. Sharma R. K. Innovation in Telecommunications. 2012.
5. Zwass V. "Electronic commerce: Structures and issues". *International Journal of Electronic Commerce.* 1996.
6. Koponen A. E-commerce, electronic payments. *Innovation in Telecommunications*. 2006; 26pp.
7. Huang Z. Bwoma P. O. An overview of critical issues of e-government. *Issues of Information Systems*. 2003; 4(1): 164-170pp.
8. Kenneally E. Boyond Whiffle-Ball bats:

Addressing identity crime in an information economy. *John Marshalls Journal of Computer & Information Law. 2012*; 200: 26(47).
9. McAllister E. "Guide to protecting the confidentiality of personally identifiable information". *Diane Publishing.* 2010.
10. Pannah E. Cyber security in electronic commerce, effect of safeguarding personal data on identity theft, *University of Maryland University College, 2011pp.*
11. Eisenstein E.M. "Identity theft: An exploratory study with implications for marketers". *Journal of Business Research.* 2008; 61(11): 1160-1172pp.
12. Collins J. M. Investigating identity theft: A guide for businesses, law enforcement and victims; *Wiley.* 2006.
13. Wang W. J., Yuan Y., Archer N. A contextual framework for combating identity theft. Security & Privacy; *IEEE*; 2006; 4(2): 30-38pp.
14. Arnold S. Internet users at risk: The identity/privacy target zone. *Searcher-MedfordNJ;* 2001; 9(1): 24-41pp.
15. Strategy J. Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance Necessary. Feb. 2007; 35pp.
16. Susan W. B., Joseph J. S. "Cybercrime havens: Challenges and solutions"; *Business Law Today.* Nov/Dec 2007; 17; 49pp.
17. Christopher H., Lim C. L. "Renegotiating westphalia: Essays and commentary on the European and conceptual foundations of modern international law. The Hague/Boston/London". *MartinusNijhoff Publishers.*1999.
18. Joan F. "Sovereignty, territoriality, and the rule of law"; *Hastings International and Comparative Law Review.*, 2002; 25: 304,310pp.
19. Francisco Ferreira D'Almeida. Droit Publique Internationale ; 2 ed; 2003; 15pp.
20. Christopher L. B. "Jurisdictional issues and conflicts of jurisdiction". 1988; 26pp.
21. August A.Y. "International cyber-jurisdiction: A comparative analysis", *American Business Law Journal.* Summer 2002; 39; 539p.
22. Bennet K. "Crystal ball. Gov: Predicting cyber policy in 2008". *Journal of Internet Law,* Mar 2008; 11: 21p.
23. Kathryn B. C. "Betting on the wrong horse: The detrimental effect of non-compliance in the internet gambling dispute on the General Agreement on Trade in Services (GATS)". *William and Mary Law R*eview; 2007; 49: 946pp.
24. Cherifbassiouni M. Crimes against Humanity in International Criminal Law. Dordrecht: *Martinus Nijhoff Publishers*. 1992, 511-513pp.
25. Kenneth C. R. "Universal Jurisdiction under International Law", *Texas* Law Review. Mar 1988; 66; 788p.
26. Center for Strategic and International Studies July 2013 Report. P.10 on www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf. Last accessed on 10 May 2017.
27. Asherry B.P. "Cyber security in Tanzania: Prevention and Detection of Cybercrimes", *Create Space Independent Publishing Platform.* 2017.
28. Osman N.S. "Criminal Justice Responses to Emerging Computer Crime Problems", University of North Texas, unpublished. 2001.
29. McCullagh A., Caelli W. Who goes there? Internet banking: A matter of risk and reward; Paper presented at the Information Security and Privacy; 2005; 177p.
30. Boudriga N. Security of Mobile Communications, Boca Raton: *CRC Press*; 2010; 32-33pp.
31. Oppliger R. Internet security: "Firewalls and beyond". *Communications of the ACM*; 1997; 40(5): 94p.
32. Vacca J. R. Computer and Information Security Handbook, Amsterdam: *Elsevier; 2009*; 355p.
33. Andrés S. et al. Security Sage's Guide to Hardening the Network Infrastructure. Rockland, MA: *Syngress*, 2004, 94-95pp.
34. Henry A. "The difference between antivirus and anti-smalware (and which to use)", *ohn Marshalls Journal of Computer & Information Law,* 2008, 12pp.

Cite this Article
Ayuk Macbert Nkongho. Cyber Insecurity in E-Commerce Transactions in Cameroon: What Prospects for the Digital Economy. *National Journal of Cyber Security Law*. 2018; 1(2): 16-32p.