LEBANESE AMERICAN UNIVERSITY

Cyber Law in Lebanon:
Reasons That Burdened its Enactment and the Effect on Electronic Financial Transactions

By
Fatima Ali Soueid

A thesis
Submitted in partial fulfillment of the requirements for the degree of Masters of Business Law (L.L.M)

Adnan Kassar School of Business

March 2019

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS APPROVAL FORM

Student Name: Fatima Soueid I.D. #: 201606028

Thesis Title: Cyber Law in Lebanon: Reasons That Burdened its Enactment and the Effect on EFTs

Program: Masters of Law (L.L.M)

Department: Information Technology and Operations Management

School: Adnan Kassar School of Business

The undersigned certify that they have examined the final electronic copy of this thesis and approved it in Partial Fulfillment of the requirements for the degree of:

Masters in the major of Business Law

Thesis Advisor's Name: [redacted]

Signature: [redacted] Date: 19 / 3 / 19 (Day / Month / Year)

Committee Member's Name: Abbas Tarhini

Signature: [redacted] Date: 19 / 3 / 2019 (Day / Month / Year)

Committee Member's Name: Abdul-Nasser Kassar

Signature [redacted] Date: 19 / 3 / 2019 (Day / Month / Year)

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS COPYRIGHT RELEASE FORM

LEBANESE AMERICAN UNIVERSITY NON-EXCLUSIVE DISTRIBUTION LICENSE

By signing and submitting this license, you (the author(s) or copyright owner) grants the Lebanese American University (LAU) the non-exclusive right to reproduce, translate (as defined below), and/or distribute your submission (including the abstract) worldwide in print and electronic formats and in any medium, including but not limited to audio or video. You agree that LAU may, without changing the content, translate the submission to any medium or format for the purpose of preservation. You also agree that LAU may keep more than one copy of this submission for purposes of security, backup and preservation. You represent that the submission is your original work, and that you have the right to grant the rights contained in this license. You also represent that your submission does not, to the best of your knowledge, infringe upon anyone's copyright. If the submission contains material for which you do not hold copyright, you represent that you have obtained the unrestricted permission of the copyright owner to grant LAU the rights required by this license, and that such third-party owned material is clearly identified and acknowledged within the text or content of the submission. IF THE SUBMISSION IS BASED UPON WORK THAT HAS BEEN SPONSORED OR SUPPORTED BY AN AGENCY OR ORGANIZATION OTHER THAN LAU, YOU REPRESENT THAT YOU HAVE FULFILLED ANY RIGHT OF REVIEW OR OTHER OBLIGATIONS REQUIRED BY SUCH CONTRACT OR AGREEMENT. LAU will clearly identify your name(s) as the author(s) or owner(s) of the submission, and will not make any alteration, other than as allowed by this license, to your submission.

Name: Fatima Soueid

Signature: [redacted]

Date: 18 / 3 / 2019
Day Month Year

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

PLAGIARISM POLICY COMPLIANCE STATEMENT

I certify that:

1. I have read and understood LAU's Plagiarism Policy.
2. I understand that failure to comply with this Policy can lead to academic and disciplinary actions against me.
3. This work is substantially my own, and to the extent that any part of this work is not my own I have indicated that by acknowledging its sources.

Name: Fatima Soueid

Signature: [redacted] Date: 18 / 3 / 2019
Day Month Year

Dedication

I thank my family whom I consider the foundation of my strength and inspiration. I extend my deepest gratitude to my father; the sole reason behind me doing this, and my mother for her prayers, constant love, support, and encouragement.

Above all that, I thank Allah for providing me patience, guidance, and perseverance throughout this academic journey.

Acknowledgments

I would like to express my deepest appreciation and gratitude to all the people that have contributed to the completion of this thesis.

First of all, I would like to thank my advisors; Dr. Khodr Fakih and Dr. Abbas Tarhini, who have continuously supported and guided me throughout this academic journey. Also, I would like to thank Dr. Abdel Nasser Kassar for his valuable advices.

Acknowledgements further go to all the people that participated in this research especially Mr. Jamal Al-Hout, Mr. Hassan Majed, Mr. Ziad Abu Tariyeh, and Dr. Mohammad Boudaher. Without their contribution, I wouldn't have been able to complete this work. Special thanks to Mr. Bassem Daouk for his constant support, guidance, and help.

Cyber Law in Lebanon:
Reasons That Burdened its Enactment and the Effect on Electronic Financial Transactions

Fatima Ali Soueid

Abstract

The last decade has seen a profuse growth in electronic financial transactions obliging banks to globalize and to constantly keep up with the latest technological developments while imperiling greater online exposure. As a result, the world has become an open medium for everything electronic. With the increasing rate of digital crimes, Lebanon was in need of a law addressing issues such as e-payments, e-signatures, e-transactions, and cyber-crimes that are often associated with electronic transaction cases.

The purpose of this paper is to determine the factors that burdened the enactment of a cyber-law governing cases associated with electronic financial transactions in Lebanon. The paper provides a definition of electronic financial transactions, electronic commerce, and electronic payment. It presents a brief about electronic threats and security as well as highlighting the most common cybercrimes in the financial sector. It then develops a framework for understanding the reasons behind not having a cyber-law after discussing the Lebanese financial transactions medium. Finally, it outlines issues in three interrelated areas that often need attention for the

development of an adequate legal structure. These issues are characterized in political stability, economic stability, and the socio-economic structure.

Key Words: Cyber Law, Electronic Financial Transactions, Laws and Regulations, Cyber Security, Lebanon

Table of Contents

List of Tables

List of Figures

List of Abbreviations

EFT	Electronic Financial Transaction
EFTs	Electronic Financial Transactions
E-commerce	Electronic commerce
ATMs	Automated Teller Machines
POS	Point of Sale
SWIFT	Society for the Worldwide Interbank Financial Telecommunication
DOS	Denial of Service
PIN	Personal Identification Number
E-security	Electronic Security
PCM	Presidency of the Council of Ministers
OMSAR	Office of the Minister of State for administrative Reform
MOIM	Ministry of Interior and Municipality
MOET	Ministry of Economy and Trade
MOD	Ministry of Defense
MOT	Ministry of Telecom
BDL	Banque du Liban/ Central Bank of Lebanon
MP	Member of Parliament
SIC	Special Investigation Commission
CEO	Chief Executive Office
GDP	Gross Domestic Product

Chapter One
Introduction

The first chapter embodies the foundation of the study and the aim behind doing it. It acquaints the reader to the subject matter discussed by presenting problematic research questions that lead to the main resolve. Consequently, it signifies the structure of the thesis.

1.1 Overview:

Since the introduction of the internet in 1969, it has advanced from its main purpose of being an academic tool to becoming a network of communication (Nehmzow, 1997). Recently, it has been hastily gaining recognition as a prospective medium for electronic commerce (Crede, 1995; Ooi, 1999).

Continuing advances in technology and its prominent role in commerce are leading financial institutions towards the internet in increasing numbers. The internet is now being considered as a tactical weapon revolutionizing the way banks function, provide, and compete against one another (Nehmzow, 1997; Seitz and Stickel, 1998).

With worldwide usage growing to almost two billion users, the internet has contributed in cost reduction, efficiency, and productive gains in capital; however, this rapid growth has created issues for the law makers of financial markets that weren't imagined before in the past years.

The internet has created huge areas of opportunity for computer hacking and identity theft and these new areas of cyber securities enforcement create novel and interesting legal challenges especially for the drafters of those acts (Trautman, Triche, and Wetherb, 2013). New legislative rules have been required to resolve the many ambiguities confronted when dealing with transactions in cyberspace.

1.2 Background of the Study:

The volume and variety of electronic financial services have increased significantly when the use of the electronic medium to do business has spread rapidly over the past decade. This incredible growth in open networks has created a permeable electronic atmosphere that facilitated the transmission of finances across the world with no limits or boundaries. Financial institutions are gradually depending on technology to process, save, and recover data, but improvements in computer hardware, software, and communication technology is increasing the financial industry's exposure to internal and external risks.

The most terrifying feature of the progression of technology is the scale of crimes that can be carried out quite rapidly. Without sturdy security panels, banks risk the possibility of monetary loss, legal responsibility, and reputational damage. Law enforcement officials have been concerned with the vulnerability of Electronic Financial Transaction (EFT) systems to cybercrime. The internet has created a lot of challenges for the regulators of financial markets. Cyber-fraud has become a major peril to the progression of the financial transactions market.

According to a report delivered by Kaspersky Security Bulletin in 2015, Lebanon ranks as the 10^{th} country with most of its computer users targeted by web attacks

(https://securelist.com/kaspersky-security-bulletin-2015-overall-statistics-for-2015/73038/). Despite that, the law addressing such issues wasn't passed until 2018. Lebanon faces the problem of being a country with a lot of political and economic issues. In the absence of significant improvements in those prospects, the possibility of a financial crisis and sovereign default is growing.

1.3 Objective of the Study:

The paper's target is to provide an abbreviated overview on Electronic Financial Transactions (EFTs) with a brief discussion on electronic threats and security.

It demonstrates the jurisdictional difficulties to the trial of internet fraud and wrongdoing regulators faced when there was no cyber law to comply by in Lebanon. Also, it displays the complications to address such difficulties especially when facing legal matters and protecting the rights of the different parties involved.

To gather information on the effect such absence possessed on electronic financial transactions, how such problems were handled (whether by courts, banks, or administrations), and the reason why the law addressing those matters was previously on hold is an addition.

1.4 Research Questions:

The paper will cover the mentioned topics by answering the following questions.

- Are the Lebanese people aware of the dangers and attacks associated with EFTs?

- Why did it take so long for Lebanon to pass a law governing cybercrime?

- What are the factors that have significant influence on delaying the enactment of a cyber-law in Lebanon?

- Will the implementation of cyber law help resolve the complexities in terms of usage and security?

Chapter Two
Literature Review

Chapter two is divided to several parts. The first part explains the definition of EFT and other terms such as electronic commerce. It also talks about EFTs in brief. The second part discusses EFT's threats and fears. It defines those threats and fears emphasizing the most common crimes. The final part talks about EFTs in Lebanon and the bouts that encountered its usage with the lack off a governing law.

2.1 Definition of EFT and other related terms

2.1.1 Electronic Commerce

One of the terms associated with EFTs and often used when talking about it is electronic commerce (e-commerce).

E-commerce is defined as transaction activities between firms and individuals which involve goods in the exchange of money (Hasan and Harris, 2009). Popular examples of e-commerce revolve around buying and selling online, but the e-commerce universe contains other types of activities as well. Any form of a business transaction conducted electronically is e-commerce including shipping, billing, and payment information. The benefits of e-commerce include decreasing costs, increasing business opportunities, reducing lead time, and providing a more personalized service to the consumers (Turban, 2008).

2.1.2 Electronic Financial Transaction

The term "electronic financial transaction" means any transaction whereby a commercial company or an electronic financial business operator offers financial products and services through electronic tools where users use them in a non-facing and mechanized manner without any direct interaction with employees of the said company or electronic financial business operator (Electronic Financial Transactions Act, Article 2).

It can be also defined as the electronic interchange or transmission of money from one account to another, either within a single financial establishment or across multiple ones, through computer constructed systems without the involvement of paper money. It consists of any transfer of funds initiated through an electronic terminal, including credit cards, automated teller machines (ATMs), Fed-wires, and point of sale transactions (POS).

2.1.3 Electronic Payment

Generally defined, electronic payment is a form of a financial exchange that takes place between the buyer and the seller facilitated by means of electronic communications. An e-commerce electronic payment is a financial exchange that takes place in an online environment (Kalakota and Whinston, 1997).

Reduced operational and payment processing costs, the growing medium of online commerce, and decreasing the costs of technology are the stimulating factors behind the development of electronic payment systems.

2.1.4 EFT Channels

Electronic financial transactions began in the early 1960's and were considered the oldest forms of electronic money transmittal.

The majority of global funds transferal is executed by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) that runs a network allowing financial establishments worldwide to send and obtain information about financial transactions in a safe, uniform, and trustworthy environment.

2.2 EFT Threats

The banking industry is witnessing a noticeable shift in the way customers deal with their transactions. There is a rapid increase in the usage of digital channels such as internet banking, digital wallets, mobile banking, and ATMs. This leads to the increase in exposure and thereby cyber-attacks which further may lead to financial and reputational losses.

Cyber Security has become a main concern for those interested in the welfare of banking procedures due to the expansion of modern electronic expertise and innovations linked with them. This tremendous development has paved the way to create novel methods of scam and fraud that rely mostly on the use of information technology and thus are considered a part of what we call cybercrime which is considered the biggest threat that is facing EFTs.

2.2.1 Definition of Cybercrime

Cybercrime is generally defined as illegal activity that use advanced information technology such as computer, network, and so forth. There are various types of cybercrime including illegal entry (such as hacking), illegal seizure, data and system intrusion, misuse of devices, forgery (ID theft), electronic fraud, and so forth (Moore, 2005).

2.2.2 Cybercrime Categories

Bantekas, Nash, and Cyber Forensics argue that cybercrime can be categorized into the following five classes as cited in Zhang Y., Xiao, Ghaboosi, Zhang J., and Deng (2011). We draw the classification below in Figure 1.

- The computer or network is used as a tool: in this case computers or networks are used mainly as tools. Examples include spamming and criminal copyright violations.

- The computer or network is the target**:** in which computers or networks are the targets of criminal activities. Unauthorized access, viruses, denial of service (DOS) attacks, and hacking attacks are examples.

- The computer or network is a place: here computers or networks are mainly the places of criminal activities. Theft of services (in particular telecommunication frauds) is considered an example in addition to certain financial frauds.

- The computer or the network is the facility: this category includes crimes such as phishing, identity theft, child pornography, securities fraud, and so forth.

- Other information crimes: There are also some information crimes, such as trade secret theft and industrial or economic espionage, which are considered to be cyber-crimes when facilitated by Computers or networks.

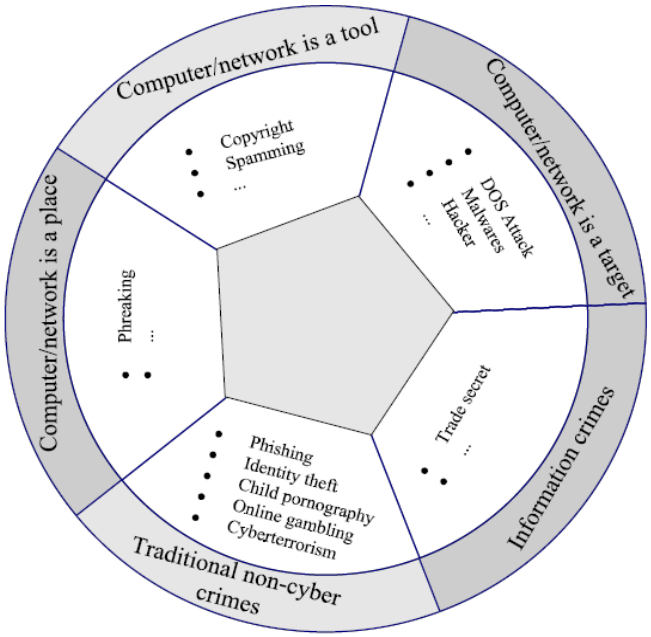

Figure 1: Categorization of cyber-crime (Zhang Y., Xiao, Ghaboosi, Zhang J., and Deng, 2011)

2.2.3 Most Common Crimes in Financial Institutions

In this part, the research will be dealing with the most common and traditional cybercrimes; regardless of their category, that occur in financial institutions defining the terminology of each one of them.

2.2.3.1 Phishing

The term phishing is a short form of "password harvesting fishing". It refers to the attempts to criminally and fraudulently gain sensitive information by means of some public entities that run on electronic systems such as online banks, PayPal, and eBay (Felix and Hauck, 1987).

Typically, phishers use email or instant messaging to access user's detailed information. The email will typically direct the user to visit a website where he is asked to update personal information such as a password, credit card, social security, or bank account number that the legitimate organization already has. The website however is bogus and will capture and steal any information the user enters on the page.

In these years, phishing related reports increased dramatically. Such crimes have been more likely to target customers of banks and payment services (Zhang Y., Xiao, Ghaboosi, Zhang J., and Deng, 2011). Efforts have been made to protect people from phishing; including legislation, user training, and technical measures.

2.2.3.2 Hacking

In the context of security, a hacker is someone who tries to explore systems or obtain unauthorized access to others' computers through specific skills and knowledge. There are usually three kinds of hackers: black hat hackers, white hat hackers, and gray hat hackers. When talking about the term "hacker" people always refer it to black hat hackers that are malicious or criminal. White hat hackers are ethical hackers who specialize in penetration testing that ensure the security of an organization's information systems. Those ambiguous in ethics are called gray hat hackers (Zhang Y., Xiao, Ghaboosi, Zhang J., and Deng, 2011).

2.2.3.3 Identity Theft

Identity theft is a term used to describe fraud in which the criminal pretends to be someone else to steal money or get other benefits. It is also considered a crime to pretend to be someone else even if the act does not lead to stealing (Leyden, 2007).

Mostly, such crimes are related to computer theft, loss of backups, and compromised information systems that intend to reap financial benefits or to conceal illegal activities by using a legal identity (Paget, 2007).

According to the United States Federal Trade Commission, approximately 10 million people are victims of identity fraud every year (ITRC, 2017). Figure 2 shows the steps in which a fraud can be implemented through the help or use of a computer accessing the bank account and leading eventually to the transfer of money and information of the victim user.

Figure 2: How the fraud works (Kaspersky Lab)

2.2.3.4 Denial of Service

Denial of service attack is another painful crime that faces financial institutions and can cost them money and reputation. Such attacks happen when the planner directs a number of computers to send communication to a bank's web server. This floods the server with so much traffic that it cannot fulfill the user's main requests. Consequently, the site becomes inaccessible to customers shutting down the business (Karake-Shalhoub and Al Qasimi, 2010).

2.2.3.5 ATM Frauds

Skimming, peeping, and having an imposter are few types of fraud crimes associated with automatic teller machines. Skimming is a scam that consists of illegally reading

the magnetic data on the credit card in order to make a counterfeit copy of it. This only steals the information of the card and it's usually not noticed by the victim until cash is withdrawn from the account. According to Bruene; as cited in Karake-Shalhoub and Al Qasimi (2010), a skimming device is installed on the ATM to electronically record the card's number while a camera attached to it works on videotaping the keyboard to get the password. Criminals then download the information and send it via email account to fraudsters.

Peeping involves cases where the user's personal identification number (PIN) is stolen either by peeping from behind the ATM or through a camera that is secretly placed. As for the imposter ATM scam, the fraudster impersonates a bank clerk or guard to deceive a customer who is using an ATM. Typical cases is when the imposter pretends to help an elderly user operate an ATM and asks for the PIN (Karake-Shalhoub and Al Qasimi, 2010).

2.2.3.6 Insider Threat

This type of crime is considered the most dangerous and often neglected threat that financial institutions face. What makes it hazardous is the fact that these people are trusted. They know exactly what to look for and where to look at while evading existing security measures. They have an understanding of the system, access, and are often allowed to act in the company's name. An appropriate check for employees' backgrounds and balances might help reduce this threat.

This kind of threat is real and not so uncommon that a large scale of bank frauds and many of its criminal attacks involve insiders (Karake-Shalhoub and Al Qasimi, 2010).

2.2.4 EFTs and Security

Electronic security (e-security) has been an increasing area of distress for banks and other financial service suppliers while handling daily operational risks. Because of the fast progress of wireless technology and its constant use in providing financial services in evolving markets, there is an increased request for a careful look at topics associated to electronic security. Banks and vendors with fragile security controls are subject to business disturbances, theft of data, sabotage, corruption of key records, and fraud. The expansion of wireless Internet admittance will enable foreign governments, terrorists, criminals, and hackers, to operate in countries that do not have the advanced or adequate security protocols in place (Glaessner, Kellermann, and McNevin, 2002).

In the context of electronic financial transactions, threats can be made either through network and data transaction attacks or through unauthorised access to the accounts by means of false or defective authentication. Financial institutions are exposed to undetected, global, and virtually instantaneous attacks on internal systems and proprietary information originating from either foreign governments and terrorists or hackers originating domestically. In the past it would have taken months or perhaps even years for highly organized criminals to steal 50,000 credit card numbers. Today, one criminal can hack into a database and rob that number of identities in seconds using devices that are easily available on the Web. These are the factors that cause e-security to be taken very earnestly.

The rate of economic crime is clearly increasing throughout the years and across the world and that is shown clearly in figures 3 and 4.

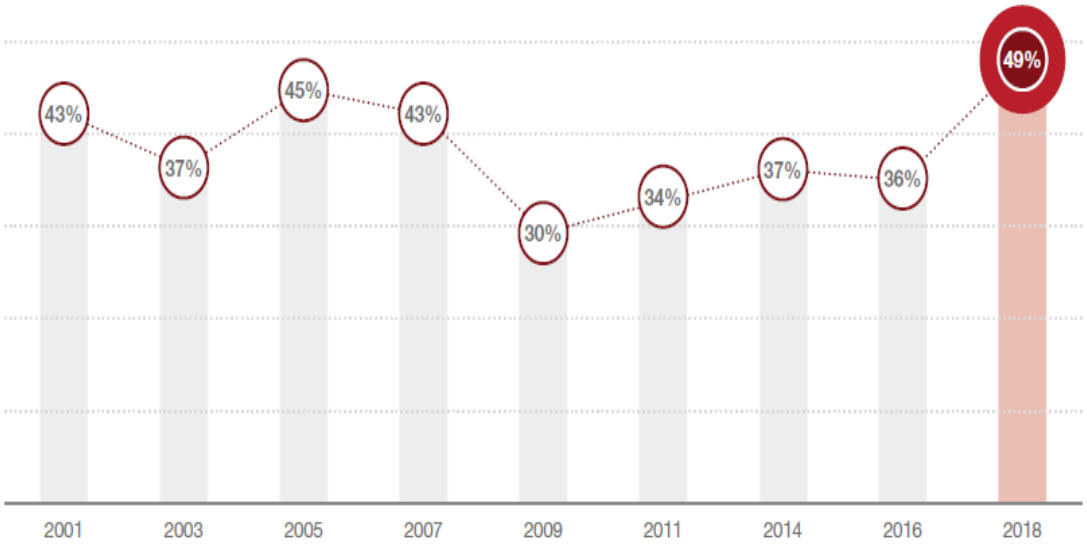

Figure 3: The reported rate of economic crime increase over the years

(PwC's 2018 Global Economic Crime and Fraud Survey)

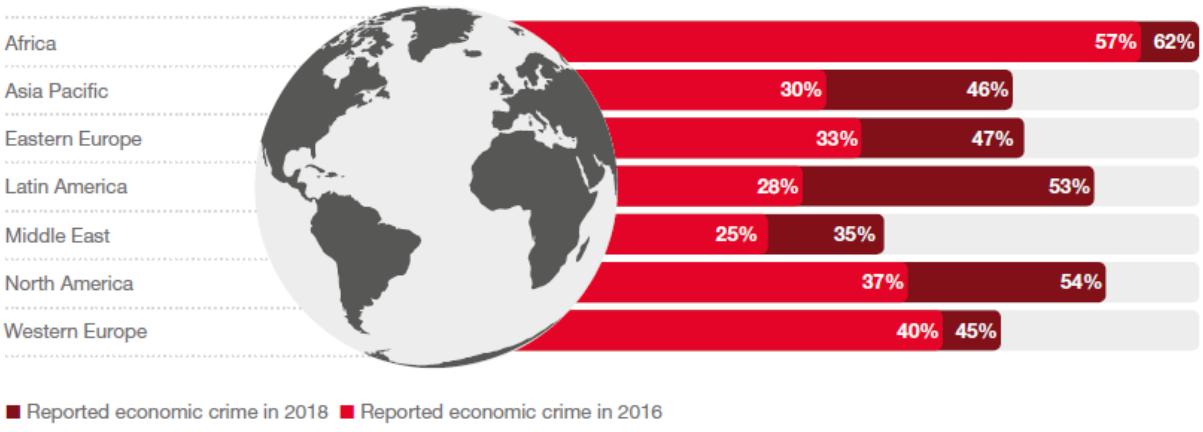

Figure 4: The reported rate of economic crime increase across the world

(PwC's 2018 Global Economic Crime and Fraud Survey)

The Internet Data Corporation (www.idc.com) recently reported that more than 57 % of all hack attacks were initiated in the financial sector (Glaessner, Kellermann, and McNevin, 2002). The United Kingdom is annually burdened about £1.3 billion from ID related fraud that includes: tax fraud for £215 million, credit fraud for £215 million, money laundering for £400 million, and immigration fraud (forging passports) for £584 million (Whitley, Hosein, Angell, and Davies, 2007).

Cyber criminals are another factor threatening the security of financial transactions. Nahshon Even Chaim (also known as Phoenix) was the first computer intruder prosecuted by evidence from remote computer intercepts. In the 1980's, he attacked the US defense and nuclear research computer systems (Sterling, 1993).

Jonathan James became the youngest person imprisoned for cybercrime in the USA. He was sentenced to prison at the age of 16 because he downloaded software related to the International Space Station's life sustaining elements, which was worth $1.7m. Before he became a public speaker and author, Kevin Mitnick spent more than 4 years in jail and was once known as "the most wanted man in cyberspace". Robert T. Morris created the first worm when he was still a student at Cornell University, Jason Burks was famous for writing malicious software, Neidorg stole secret documents from BellSouth through online means, Brian Scalcedo hacked the Low's for credit card numbers, and Smith launched the Melissa Worm (Zhang Y., Xiao, Ghaboosi, Zhang J., and Deng, 2011).

All these names prove that such criminals existed a long time ago and that throughout the years their number is increasing possessing a serious threat on electronic financial transactions.

2.3 Lebanon Being the Case

A series of innovative challenges encounter the controllers of financial institutions especially in Lebanon. Cybercrime has become a key threat to the progression of these markets. A few of the creative gears obtainable to today's cybercriminals include: the relative ease of data theft; the transferal of money in a flash through borders; and stolen identities assisting market manipulation (Trautman and Altenbaume, 2011).

The global nature and increasing use of cyberspace; along with the internet's cost-effective ability to reach an almost unlimited audience, poses unique and challenging questions to jurisdiction over internet financial transactions. Cyberspace defies traditional geographic concepts of boundaries since it is a place that is nowhere and everywhere (Westerlind, 2000).

Previously and in the absence of a cybercrime and electronic evidence legislation, Lebanon didn't have any specific jurisprudence concerning those matters. The existing legislations were traditional with legal rules that were scattered in different laws. The framework for all cybercrime investigations was the Penal Code in association with the Code of Criminal Procedure. It did not take into consideration the specificities of crimes related to information and communication technology. Lebanon was in need of a definitive law that governs the previous matters.

2.3.1 EFTs in Lebanon

The Lebanese banking sector has played a major role in fuelling the economic growth of Lebanon and ensuring the relative stability of the financial sector as a

whole. The accomplishments of Lebanon's financial industry are continuously appearing on international news and events. In fact, the banking industry beats the odds since Lebanese banks are still budding strongly compared to other countries. Unfortunately, in the security aspect all this good news turns into bad news because financial success acts as a magnet for criminals. When businesses are growing and thriving, criminals' attention will be raised and the best method to attain their goal is simply through cyber threats. This is a problem felt by all banks. With the draft law having been stuck for years in the legislative pipeline, banks have found some practical fixes by relying on global standards and regulations. They have been applying standards accepted by Banque du Liban; Lebanon's central bank, but the need for a legal framework was essential due to the high percentage of threats. The delay in implementing a law dealing with electronic transaction issues discouraged global third party online payment processors from penetrating the Lebanese market.

Moreover, cyber defence planning was not much of a priority for the Lebanese government. The country did not have legislation to protect digital rights, lacked legal penalties to deter criminal cyber-attacks, and had only patchwork solutions in place for cyber defence.

For example, in 2012, a National Cyber Security committee was formed by the Presidency of the Council of Ministers (PCM). It issued decision number 32 dated 25/7/2012 to release a national and common strategy for the protection of the Lebanese governmental websites. The committee was formed of members from the PCM, Office of the Minister of State for Administrative Reform (OMSAR), the Ministry of Interior and Municipality (MOIM), the Ministry of Economy and Trade (MOET), the Ministry of Defence (MOD), the Ministry of Telecom (MOT), and the Central Bank of Lebanon (BDL). After numerous consultations, OMSAR was

delegated to work on and organize a minimum set of security policy guides that obey international security standards. Accordingly, OMSAR organized a “National Cyber Security Policy Guidelines” document to be applied in all Lebanese public agencies but all was considered ink on paper without a governing law (OMSAR, 2012).

2.3.2 State of Cybercrime Legislation

After most countries adopted legislations to regulate technology and electronic transactions; particularly the use of "personal information data", Lebanon’s turn had come to go on board of this journey and that’s where Ecomleb started.

The Ecomleb project was born early in 2002; when the Ministry of Economy and Trade recognized the importance of e-commerce as a tool that can help Lebanese firms take advantage of the global market. The project aimed to develop a complete legal framework for e-commerce by drafting a comprehensive regulatory framework that included all aspects of internet interaction and trading. As a result, 200 articles were proposed under nine titles. Funding was secured through a € 1.7 Million grant from the European Commission. The first draft of the law bill on communication and electronic transactions was prepared by French experts Prof. Pierre Catala and Professor Valerie Cedalian in May of 2005. In addition to these, key stakeholders as the Central Bank, the General Security Forces, prominent judges, and prominent lawyers helped (Ministry of Economy and Trade, 2011).

The fate of this project was similar to most of the Lebanese bills that were amended to distort. In August of 2010, the Advisory Committee of the Lebanese Parliament, headed by member of parliament (MP) Ghinwa Jalloul, submitted a revised version of the Ecomleb bill. The new draft was expanded to include all themes related to e-

transaction and personal data such as e-payment, e-banking, e-signature, consumer protection, privacy, copyright, and cyber-crime. However, it generated negative reactions from civil society organizations and legal centres for it allowed performing operations that would greatly infringe privacy rights (Makhlouf, 2011). Since then, the draft has been in the hand of the joint parliamentary committee for revision, but it was difficult back then to predict a date of enactment especially in the light of the political turmoil in the country.

It is worth mentioning that Lebanon has signed several bilateral agreements that aimed on strengthening cooperation in the field of cybercrime, cyber security, and transnational organized crimes with countries such as the Arab countries and France. Lebanon also signed the United Nations Convention against Transnational Organized Crime on the 18th of December 2001 and ratified it on the 5th of October 2005. On the other hand, Lebanon neither signed the Budapest Convention nor the Arab Convention on Combatting Information Technology Offences although they are considered international conventions against Cybercrime (Council of Europe, 20 February 2018).

2.3.3 Cyber-Crime Level in Lebanon

Cybercrime in Lebanon more than doubled in the recent years as hackers find new ways to enter into bank accounts and illicitly transfer money into their own pockets. The number of cases of such actions touched; according to the Special Investigation Commission (SIC), 134 in 2016 when it was 84 in 2015. The costs of these operations amounted respectively to 12.6 million dollars and 12 million dollars in the two years.

The SIC received in 2016 a total of 470 cases; 107 were from foreign sources and 363 from native sources. Out of which, 161 cases were furthered to the General prosecutor where it was decided to restrict accounts and lift banking secrecy in 42 cases; 37 from local sources and 5 from foreign sources. It also enclosed risk based onsite compliance examinations at 22 banks, 14 financial institutions, 22 insurance companies and other entities, in addition to handling 514 spontaneous disclosures. The cases were distributed among embezzlement of private funds (32.8%), forgery (14.8%), terrorism or terrorist financing (10.8%), fraud (4.2%), trade of narcotics (3.0%), corruption (2.8%), tax evasion (2.1%), human trafficking & insider trading & smuggling (0.7% for each), kidnapping and organized crimes (0.5% for each), environmental crimes (0.2%) and not specified cases (26.2%). The geographical distribution was as follows: Beirut (60.4%), Mount Lebanon (23.5%), South Lebanon (7.3%), Bekaa (5.4%) and North Lebanon (3.4%) (Association of Banks in Lebanon Annual Report, 2016).

Consequently, the Lebanese banking sector adopted wise and defensive effective measures. These include the expansion of anti-virus protection programs, resolutions to protect internet access sites, and the activation of the latest Microsoft protection software. Moreover, it organized conferences and seminars to raise awareness on how to combat cybercrime and avoid piracy in the financial and nonfinancial sectors. In addition to these, a guide under the name of “Fighting Financial Cybercrime in Lebanon” was issued by the association of banks in Lebanon in 2016 proposing strategies to prevent cybercriminal acts through emails ensuring the safe implementation of electronic operations (Association of Banks in Lebanon Annual Report, 2016).

As troubling as all this may sound, there is more. Companies and civil infrastructures in the region alongside banks have emerged as targets in cyber warfare. Often, there is very little journalistic reporting or public debate in Lebanon and other Middle East countries about who is collecting our data and which countries our governments have decided to share it with.

Cyber-attacks targeting sensitive systems are already frequent in Lebanon. Lebanon is a heavily targeted country mostly for the reason that people like to meddle in Lebanese affairs as said by co-director of the Cyber Policy Initiative at Carnegie Tim Maurer. U.S, Russia, and Western intelligence agencies who keep an eye on geopolitics are few of those involved. In 2012, Kaspersky Lab released a report on a virus named Gauss which had infected approximately 2500 computers of financial institutions in the Middle East. The largest numbers of computers affected were Lebanese accounting for 1660. Malicious attacks targeting the systems of Saudi Aramco, world's biggest oil company, wiped out 35000 computers in a matter of hours in August 2017. Attacks aiming at stealing information rather than money face the risk of dire consequences since clients rely heavily on the institutions' ability to grant them anonymity (Marsi, 2018).

Speaking at a recent panel organized by the Samir Kassir Foundation, Mohamad Najem; internet policy expert, gave an example on how the Lebanese government is regularly violating state privacy laws when it comes to information sharing. In reaction of a case concerning a missing person, it handed over data from every cell phone in the city and surrounding suburbs without having an approval from the Prime Minister (Battah, 2015).

2.3.4 Lebanon's Capabilities to Face Attacks

There are a few channels and authorities that are taking a role in identifying and tracing cybercrimes such as the Internal Security Forces, Cybercrime and Intellectual Property Office, and the Telecommunications Regulatory Authority.

The Anti-Cybercrime and Intellectual Property Rights Bureau was established by the Internal Security Forces in 2006 to strengthen online security and fight cybercrime in Lebanon. In addition to proving controversial due to the lack of specific modern laws concerning online rights and internet crimes, the agency's way of work in dealing with cases against activists, bloggers and journalists, made many free speech organizations uneasy (The Daily Star Lebanon, 7 December 2016).

Infrastructure and funding are both essential necessities to effectively counter cybercrime and attain cyber security. The need for cooperation between stakeholders within the private and public sector was a message conveyed by Riad Salameh; Banque Du Liban Governor.

Dr. Joe Hage, CEO of Universant Technology (a company that offers IT and cyber security solutions) added that most companies start taking cyber-security seriously only after they are attacked. Thus, what is necessary is more awareness and better infrastructure to adequately combat cyber criminals. Bank Audi's information security and business continuity professional Salomon Frangieh reported that no one is safe. Companies are either hacked or will be hacked; specifically in a country like Lebanon where it takes companies an almost of 200 days to notice a breach within its system (El-Amine, 2016).

It's evident that the Lebanese government is alert of the high need to step up its cyber security efforts and meet or even exceed the abilities of modern

cybercriminals. To get there, it will be essential to advance the collaboration between private-public sectors, instruct professionals and ethical hackers, and assign more funds to where they are needed.

On the other hand; and according to a new study done by Lookout Security and the Electronic Frontier Foundation, there was a series of spyware movements operating out of a government building in Lebanon. “Dark Caracal”, is connected to outbreaks on thousands of victims in more than 21 different countries targeting individuals through spear phishing then using malware transplants to quietly draw off data from their phones. That data include passwords, phone registers, and conversations enough to build an inclusive picture of where a person has been and who they’ve communicated with. The malware itself isn’t particularly refined but the effect is still destructive for anyone compromised. The earliest data presented a sequence of connections to a network called “Bld3F6”. When traced to a physical location, it led to a building in downtown Beirut directed by Lebanon’s General Directorate of General Security; the country’s chief intelligence agency (Brandom, 2018).

Having good offensive skills does not necessarily mean having a good defense. It is easy to commit a crime but the hard part is trying to get away with it. It requires a different skillset with a larger financial investment. This raises questions about Lebanon’s ability to protect itself from attacks.

Chapter Three
Methodology

Cyber law is the part of the overall legal system that deals with the internet, cyberspace, and their respective legal issues. It covers a fairly broad area encompassing several subtopics including freedom of expression, access to and usage of the internet, and online privacy.

In Lebanon, these areas fall under the Electronic Transactions and Personal Data Act which was stuck in the parliament drawer since 2012. Many factors were a cause of this delay (see figure 5). In this section, we study these factors and take into consideration how much they affected the law implementation using the qualitative method to support our findings. This chapter covers the methodology used to conduct our research.

3.1 Research Design

Qualitative research is a type of exploratory research. It seeks to comprehend a given research topic from the perspective of the local citizens it involves. It is used to gain an understanding of underlying reasons, opinions, and motivations. It consists of an investigation that seeks answer to a question, gathers evidence, produces results that were not determined before, and collects outcomes that are relevant outside the current boundaries of the study. It is an essential method for the researcher to be able to better understand the research subject.

To study the topic “Cyber law in Lebanon: Reasons That Burdened its Enactment and the Effect on Electronic Financial Transactions” we will have to collect

information, opinions, discuss real life situations with experts in the study subject, and shed light on the factors that affected the law enactment and caused its delay. The purpose is to test which of the below factors had an influence and contributed to the delay in law enactment.

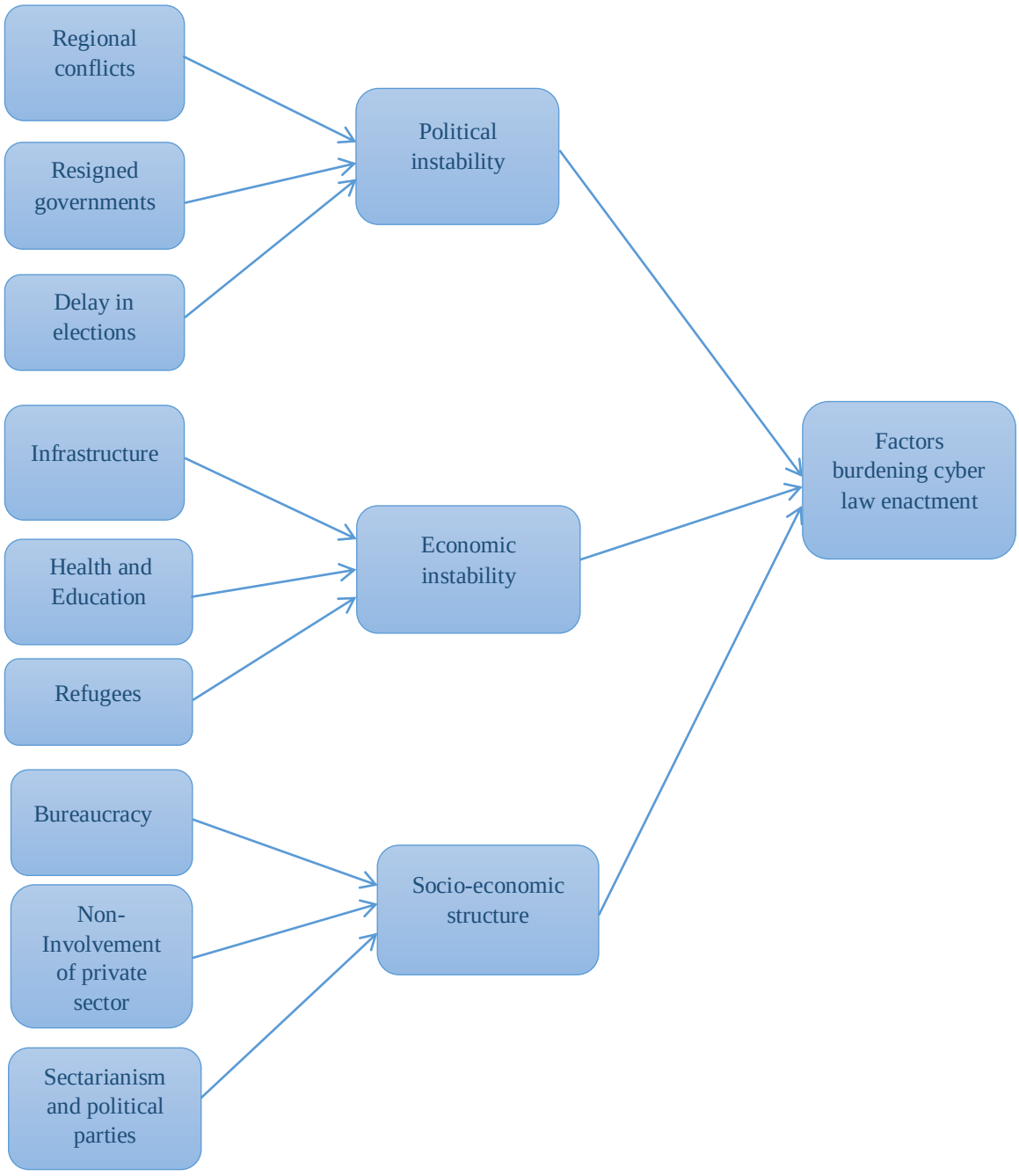

Figure 5: Module of the factors burdening cyber-law enactment in Lebanon

Conducting in-depth interviews is one of the most common qualitative research methods. It is a personal interview that is carried out with one respondent at a time. This is purely a conversational method and allows the researcher the opportunity to get details in depth from the respondent. In-depth interviews are ideal for assembling data on individuals' personal histories, views, and practices; particularly when delicate topics are being explored. The use of open-ended questions gives participants the opportunity to respond in their own words rather than forcing them to reply with a more fixed response. Open-ended questions have the capacity to arouse responses that are: evocative and culturally striking, unanticipated by the researcher, rich and explanatory in nature.

A questionnaire (with open-ended questions) about EFTs and the factors that effected the delay of law was targeted to a selected sample of employees in Lebanese banks (experts in the field of security and financial sector) to identify the level of risk banks face daily due to cyber threats and the damage they face in the absence of a governing law. Interviews were made with them based on those questions. It was also necessary to test the level of awareness the Lebanese society have with respect to cybercrime in their daily transactions.

Interviews based on the above questionnaire were also communicated with Lebanese lawyers to identify the gap in the Lebanese courts and to clarify how cybercrimes are ruled out with the absence of a cyber-law.

3.2 Method

For achieving the purpose of this research, one-on-one interviews were conducted with a diverse range of people with respect to expertise. Lawyers, bank IT & security experts, and a professor of experience were among the people needed to be interviewed. The advising doctors assigned two participants from the head security department of two Lebanese banks, a professor of experience, and three lawyers to participate in this research. A branch manager in one of the Lebanese banks was also a participant. The advising doctors also provided the names, contact numbers, and the emails of the interviewees to schedule a meeting. After contacting the above mentioned in person, the researcher was informed with a respective date to schedule an interview with each respective person.

The interview questions that were asked to the two heads of security department and the branch manager revolved around testing whether the factors mentioned (political instability (delay in elections / resigned governments / regional conflicts), economic instability (health and education / refugees / infrastructure), socio-economic structure (sectarianism and political parties / non-involvement of private sector / bureaucracy)) had an influence on delaying the law enactment, how financial institutions handle security breaches, whether Lebanese people are aware of the dangers of cyber threats and crimes, and do financial institutions disclose security breaches to the respective sources (see appendix A).

In addition to the above conducted interviews, three lawyers were contacted in the area of Beirut to discuss and better understand how cybercrimes were being ruled out, the difficulties faced while applying or binding a cybercrime case to a Lebanese law, in addition to testing the above mentioned factors and their effect on delaying

the law enactment. The researcher selected this sample because it best fits the purpose of this study and because the number of lawyers who are selected to this topic is limited (see appendix B).

The researcher had to wait for weeks to be able to conduct these interviews and to actually find an available time slot with the lawyers and heads of security department. It should be noted that the information collected through those interviews will only be used for scientific research and will not be disclosed to public media. The researcher has chosen to do the interviews with security experts; precisely from Lebanese banks, for that each Lebanese registered bank have to have a cyber-security division running under its name to handle cyber-attacks and to protect the bank from any cybercrime per to the obligations of the Central Bank of Lebanon. The below tables summarize the interviewee numbers along with their position and the interview duration.

Table 1: Interview conducted with heads of security department and branch manager

Interviewee number	**Interviewee position**	**Interview duration**
Security expert 1	Head of Information Security Department at Federal Bank of Lebanon	One hour
Security expert 2	Head of Security Department at Bank of Beirut	One hour

Expert 3	Branch Manager at BankMed	Thirty minutes

Table 2: Interview conducted with an expert (professor of experience at LAU)

Interviewee number	**Interviewee position**	**Interview duration**
Professor 1	Professor of experience at LAU	Twenty minutes

Table 3: Interview conducted with Lebanese lawyers

Interviewee number	**Interviewee position**	**Interview duration**
Lawyer 1	Lebanese lawyer	Ten minutes
Lawyer 2	Lebanese lawyer	Forty minutes
Lawyer 3	Lebanese lawyer	One hour

3.3 Data Collection Procedures

A copy of the interview questions was sent to the interviewee to be checked and approved. It gave the interviewee enough time to prepare any document that might come in handy. Before the interview started, the researcher explained the purpose of the research and the reason behind the interview and assured the interviewee that all personal information will remain confidential and that interview answers will only be used for scientific purposes and will not be distributed to public media.

3.4 Instruments for Data Collection

3.4.1 Interview with Heads of Security Department and Professor of Experience

The interview was composed of ten open/ended questions with approximately three questions having one sub question about the interviewee's perception of the capability of institutions to face cyber-attacks as well as facilitating public-private partnership and plans for raising cyber awareness. The interview questions were developed specifically for this research by the researcher. Before the interview questions were sent to the heads of security department, they were reviewed and modified by the advising doctor that holds a PhD in information systems security. In addition to exploring the current implemented framework for combating cybercrime and the factors delaying the law enactment, the interview has shed light on the importance of passing a cyber-law in Lebanon.

While conducting the interview, the interviewee was asked for more clarifications on few points. The conducted interviews took about one hour. The interview was held face to face in the bank branch that each of those persons work in. The interviews were half phone recorded; after the approval of the interviewee, and half hand written in the form of notes. Recordings were zipped and compressed securely (password protected), and were stored on the researchers personal computer for reference.

3.4.2 Interviews with Lebanese Lawyers

Interviews with Lebanese lawyers consisted of ten open/ended questions having two questions with two sub questions about the interviewee's perception of the reasons behind the difficulties faced when binding a cybercrime case to the Lebanese law and

the rate of cybercrime cases in the past years. This instrument have confirmed the gap found in the Lebanese law for handling such cases and have focused on the importance of legislating a cyber-law.

Conducted interviews took a time range between ten minutes to one hour. Interviews were also phone recorded; after the approval of the lawyers, with one written in the form of notes. Recordings were stored on the researcher's personal computer for later references (password protected).

3.5 Data Analysis

After the researcher conducted interviews with two heads of security department, one professor of experience, one branch manager, and three lawyers; all seven interviews were transcribed. Then, the researcher analysed the interview responses using open-coding which is known for highlighting the headings and the categories of all transcribed data (Burnard, 1991). Open-coding was conducted by reading the transcribed interviews and highlighting headings, titles, terminologies, statements, and major concepts.

Once the above exercise was done, the researcher counted the frequency and repetition of similar concepts identified within each question of all seven interviews conducted.

Chapter Four
Results

The results in this chapter are divided into three parts. The first part of the results is based on the data collected from the interview conducted with a professor of experience regarding the fundamentals of financial transactions ecosystem. The second part consists of the results obtained from the interviews with heads of security department and branch manager on how financial institutions tackle cyber-attacks, the level of cyber awareness found in the Lebanese community, and how those two affected the passing of law. The third part of the results revolved around the data collected from the interviews with lawyers discussing cybercrimes and the way they are handled in the absence of a governing law in addition to the factors that delayed putting the law in action.

With that being stated, the below tables define the fundamentals of any regulation, the procedures undertaken by the heads of security departments to report cybercrimes, the flaws in the current implemented system, and the factors that have direct effect on successful cyber law implementation. Moreover, few tables contain data obtained from a fellow researcher's paper (Shehab, 2018) having conducted interviews with five judges and an Internal Security Forces (I.S.F) member on a similar matter.

4.1 Professor of Experience's Perception on Cyber Law Obstacles:

For the purpose of this exploratory research, the researcher conducted an interview with a professor of experience at LAU. The interview was semi-structured and lasted for twenty minutes. The interview was composed of ten direct questions. The professor's response to the interview questions was analyzed using the open-coding strategy which was described in the methodology chapter.

The analysis of the interview with the professor showed four different points. The points mentioned are recorded in Table 4 along with the frequencies.

Table 4:

Fundamentals of financial transactions ecosystem (whether digital or not)

Reasons	Frequency
Political stability	1
Economic stability	1
Socio-economic structure	1
Reg-Tech (regulation technology)	1
Total	4

N=1 professor

The table above clearly shows that if we want to enact a regulation regarding technology, the above three factors should be fulfilled being all related in the same chain.

The model below is a suggested model that highlights the rudiments of any regulation; in our case cyber-law. It can be used in future research.

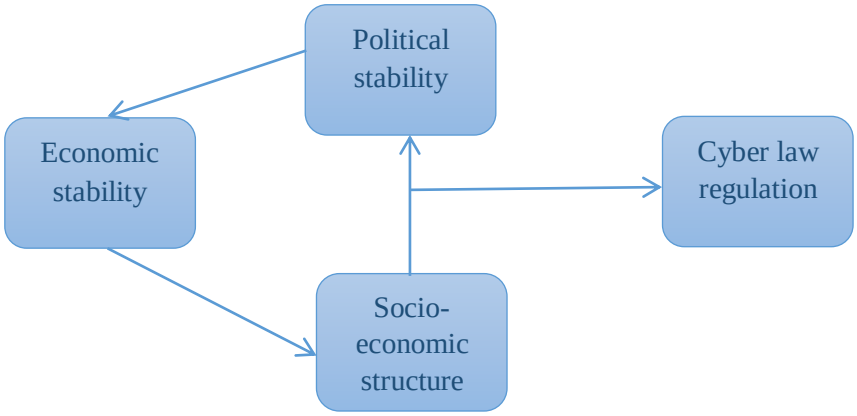

Figure 6: The fundamental factors of cyber law regulation

When asked "why did Lebanon fail to pass a cyber-law all this time", the professor clearly stated that the key reason that burdened the law enactment rotates around Lebanon being established on a sectarian charter (ميثاق) where people aren't defined as Lebanese but as this and that. We live in a divided country with a lack of trust between different parties. As for "security attacks and if companies are ready to face them", he said that there is nothing known as emergency planning. One doesn't hear or see any attempt to work on this aspect. Companies are afraid to "disclose any information regarding security breaches" fearing reputational loss; aside from the Central Bank of Lebanon since they are obliged to do so by the law. As a country, way simpler problems aroused (water, pollution of all types, electricity, etc…) with us failing to find a radical solution for so when it comes to security matters we're doomed.

On discussing the "advantages of passing this law and the people's level of awareness", he expressed that it will allow people to have a sense of stability and peace of mind especially that problems encasing from this matter is related to everyone's money. Such an issue needs a high level of awareness that is found

among educated and business people. The new generation is starting to come upon this gen as the job market is requiring experts in this field.

Ultimately, Lebanon is in need of a plan for cyber security so that when the law is passed we face no struggles in implanting it on the ground. We must also start attempts to develop software rather than only working in installing them.

4.2 Security Experts' Perception on What Burdened Cyber Law Enactment

In order to understand what flaws the implementation of a cyber-law, the researcher performed two interviews with heads of security department in Lebanese banks and one with a branch manager. The interviews were semi-structured and lasted in a time range between thirty minutes to one hour per interview. The interview was composed of ten questions; three questions had a maximum of two sub questions related to the topic. The responses to the interview questions were then analyzed using the open-coding strategy which is described in the methodology chapter.

4.2.1 Factors Speeding Cyber Law Implementation (Cyber Plan)

The analysis of the experts' statements showed four different responses that are related to the factors that fasten the implementation of a cyber-law. The responses are shown in Table 5 along with their frequencies.

Table 5

Factors fastening the implementation of a cyber-la*w*

Reasons	Frequency
Awareness	3
Education	3
E-trust	3
E-learning	3
Total	12

N=3 experts

Upon questioning "what delays the implementation of cyber law in Lebanon", the experts said that for the law to be passed a certain level of awareness must be present. The process to achieve such a thing isn't easy. It should start through educating children at schools and continue through courses at university. People; as well as politicians, often lack the technical knowledge to deal with anything electronic and that's why it is important to build what is known as e-learning and with it comes e-trust. When the above factors are grouped together, the process of implementation will be more sound and successful.

Figure 7 shown below is a suggested model derived from the analyzed discussion done with the experts on the factors that have a direct effect on the successful implementation of a cyber-law and are considered a part of the future cyber plan.

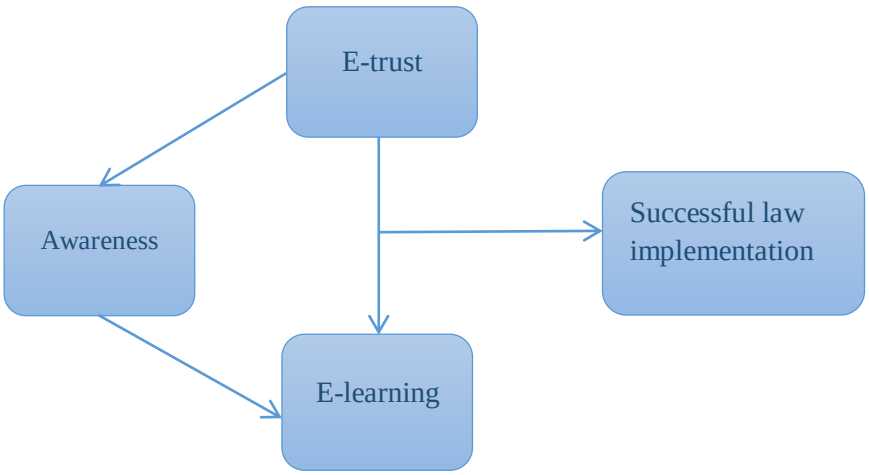

Figure 7: Factors leading to successful cyber law implementation

4.2.2 Plans on Spreading Cyber Awareness

When doing an interview with an I.S.F member, Shehab (2018) obtained answers on how the office connects with people to spread awareness.

Table 6 data show three different points on the means applied by I.S.F office to communicate with people and help spread awareness as a part of the "role of government in setting guidelines and future plans to cyber security awareness" which was one of the interview questions. The points mentioned are recorded in the below table along with their frequencies.

Table 6

Communication with people and awareness campaigns (Shehab, 2018)

Reasons	Frequency
Communication through Public Relation division	1
Approval from PR division	1
Regular awareness sessions	1
Total	3

N=1 I.S.F member

The process starts by contacting the Public Relations Division and informing them with the need of spreading news regarding security events or crimes. Once approved, the I.S.F office has the right to go to the media and spread the news. If the approval is denied, they have no authority to use the media as a channel to spread the news.

It should be noted that regular awareness sessions are performed through universities, schools, TV channels (LBC, MTV, and others), and social media (twitter, facebook…).

4.2.3 Reporting a Fraud Case through the Bank and Means of Investigation

When experts were asked about "how fraud cases are reported and the means of investigation", various results were presented. Responses analyzed are shown below. Figure 8, shows the steps undertaken to report a case of fraud and the phases the customer needs to go through in order to preserve his right. The steps differ depending on where the fraud occurred; whether internal (native country) or external (foreign country).

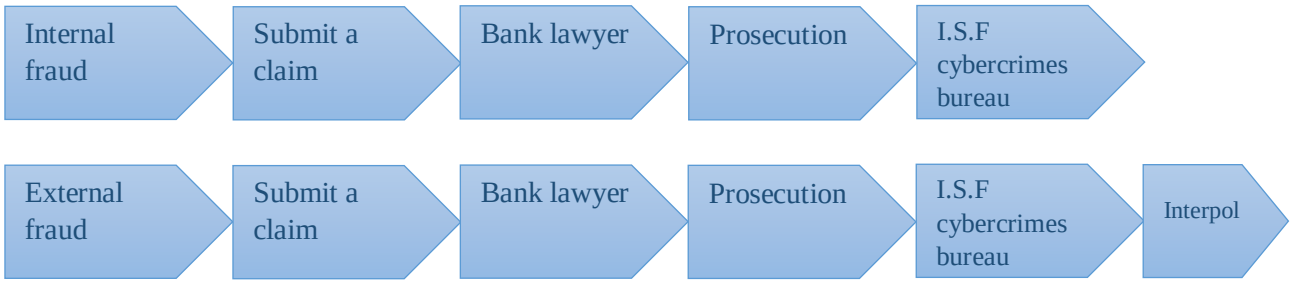

Figure 8: The reporting process of internal and external fraud

Experts stated that the first and most important step in both procedures is to submit a claim to the bank's branch. Since any transactional deduction is reported through a short message service (SMS) or by the bank's mobile application, the customer should be able to notice any ambiguous activities running on his account. Bank employees can also suspect such activities when huge amounts are withdrawn or transferred from an account; especially if they know the holder and the type of his activity. It is worth mentioning that a transaction can't happen before personally contacting the issuer through the phone.

After submitting the claim, the bank's lawyer takes matters into his own hands and files for a case where it goes to prosecution and later on is transferred to the I.S.F cybercrimes bureau being the reference to deal with such cases. The before mentioned procedures are followed when the fraud happens to be internal; however, if the fraud is external one more step is added. When the case becomes in the hand of I.S.F cybercrimes bureau, they must contact the Interpol and coordinate with them to follow up with the case outside the country.

Tables 7 and 8 show the grounds followed by the I.S.F office and the judges to start an investigation. The crime reported must have the occurrence of cybercrime as the

main reason behind the investigation. When failing to obtain those, both are unable to conduct an investigation.

Table 7

Reasons for Cybercrime Office to Start Investigations (shehab, 2018*)*

Reasons	Frequency
Judge's approval and instructions	1
Victim reporting the case	1
Total	2

N=1 I.S.F member

Table 8

Reasons to start a cybercrime investigation (shehab, 2018)

Reasons	Frequency	Percentage %
Victim reported an incident	5	55.5
No actions unless cybercrime is reported	4	44.4
Total	9	100

N=5 judges

4.3 Lawyers' Perception on the Factors that Burdened Cyber Law Enactment

To determine the exact factors that had a direct effect on the delay of law enactment, whether the number of cybercrimes has increased, and the gaps found in the legal system; interviews with three lawyers were conducted by the researcher. The

interviews were semi-structured and were done in a time range that varied between ten minutes to one hour. The interviews were composed of ten questions; three questions had a maximum of two sub questions related to the topic. The responses to the interview questions were then analyzed using the open-coding strategy that's mentioned in the methodology chapter.

4.3.1 Factors Delaying Cyber Law Enactment

The analysis of the lawyers' statements with respect to the main factors delaying cyber law enactment was combined with those of the experts. The results were demonstrated in table 9 below along with their frequencies.

Table 9

Main factors delaying cyber law enactment

Reasons	Frequency	Percentage %
Political instability	7	33.3
Economic instability	7	33.3
Socio-economic structure	7	33.3
Total	21	100

N=7 3 lawyers, 1 professor, 3 experts

The seven participants were asked "do political instability, economic instability, and socio-economic structure have direct effect on the delay of cyber law enactment"? The answers given by all of them were positively unanimous to the factors above.

In addition, six participants were asked about the "sub factors; associated with the above main factors, and the influence they hold on the process of law enactment". Their answers were analyzed and the results were demonstrated in tables 10, 11, and 12 with the respective frequencies and percentages of each sub factor.

Table 10

Sub factors affecting political instability

Reasons	Frequency	Percentage %
Regional conflicts	4	25
Resigned governments	6	37.5
Delay in elections	6	37.5
Total	16	100

N=6 3 lawyers, 3 experts

Table 11

Sub factors affecting economic instability

Reasons	Frequency	Percentage %
Infrastructure	5	62.5
Health and Education	0	0
Refugees	3	37.5
Total	8	100

N=6 3 lawyers, 3 experts

Table 12

Sub factors affecting socio-economic structure

Reasons	Frequency	Percentage %
Bureaucracy	6	37.5
Non-involvement of private sector	4	25
Political parties and sectarianism	6	37.5
Total	16	100

N=6 3 lawyers, 3 experts

4.3.2 Additional Factors Delaying Cyber Law Enactment

In addition to the above mentioned factors, the researcher adapted further results from another researcher's paper with a similar subject. The outcomes are shown in the table below.

Table 13

Reasons for the absence of cyber law and digital forensic procedures (Shehab, 2018)

Reasons	Frequency	Percentage %
Not a priority to politicians	3	25
Draft conflicts	3	25
Not aware of cybercrime impact on society	2	16.6
Lack of awareness for people and politicians	2	16.6
Political issues	2	16.6
Total	12	100

N=5 judges

The results presented in table 13 above were adopted from Shehab's paper (2018) based on an interview done with five judges with respect to the reasons behind the absence of cyber law and digital forensic procedures.

Judges believe that the main reason was due to political issues and conflicts. Lebanese people and politicians are now aware of cybercrime's impact on society. The Lebanese parliament was not being very productive about this issue. The politicians were fighting over the validity of cyber laws upon drafting and which law should be chosen. Consequently, this led to the dismissal of the voting and the non-implementation of a cyber-law. One other reason that was delaying the implementation of a cyber-security law was the fact that it was not considered a priority yet.

4.3.3 Cybercrime Rate in the Past Years

To determine the rate of cybercrimes in Lebanon and whether courts have noticed an increase in such crimes in the past years, the researcher asked the participants about their view on this matter and adopted further outcomes. The results are shown in tables 14 and 15.

Table 14

Cybercrime rate in the past years

Reasons	Frequency	Percentage %
Increase in the number of cybercrime	7	100
Total	7	100

N=7 3 experts, 3 lawyers, 1 professor

Table 15

Number of cybercrime within the past 5 years (Shehab, 2018)

Reasons	Frequency	Percentage %
Increase in the number of cybercrime	5	100
Total	5	100

N=5 judges

As noticed above, all participants agreed that cybercrime rates have increased in the past years. Numbers have definitely doubled and even tripled.

4.3.4 Difficulties Faced Binding Cybercrime Cases with Lebanese Laws

To determine the reasons behind the difficulties faced while dealing with a cybercrime case and the gap found in the Lebanese legal system; whether in law or courts, the researcher adapted interviews done with five judges on a similar matter. The questions asked revolved around the gap in the Lebanese law when dealing with such cases and the difficulties judges face when binding such crimes to the Lebanese law that has no specific regulations to this subject.

Table 16 below shows the results with their percentages and frequencies. The main reason behind this gap was that such law wasn't yet implemented in Lebanon. Furthermore, Lebanese lawyers and judges do no study this material as a core requirement through their educational cycle and consequently don't get the proper training that allows them to handle such cases.

Table 16

Reasons leading to the gap between judges and I.S.F (Shehab, 2018)

Reasons	Frequency	Percentage %
Lack of knowledge about cybercrime	4	30.76
Absence of cyber law or digital forensic procedures	3	23.07
Lack of technical skills	3	23.07
Subject not given as core requirement in universities	1	7.69
Lack of training opportunities	1	8.33
Not aware about the importance of the subject	1	8.33
Total	13	100

N=6 5 judges, 1 I.S.F member

Chapter Five
Discussion and Conclusion

The purpose of this study is to explore the reasons that burdened cyber law enactment in Lebanon. It also aims to explore how were cases handled in the absence of a governing law, how was this affecting electronic financial transactions and cyber-crime cases in Lebanon, and how this was distressing the Lebanese financial institutions.

To achieve all that, a total of seven interviews were conducted with Lebanese lawyers, a professor of experience, and security experts in Lebanese banks. Using results from the collected and analyzed data, these questions will be answered and discussed in this chapter. Limitations, implications, and conclusion are also presented in this chapter.

5.1 Main Factors Burdening Cyber Law Enactment

The responses to the interview questions with the Lebanese lawyers, heads of security department, and professor of experience about the extent by which political instability, economic instability, and socio-economic structure burdened the process of law enactment revealed the high contribution all these have on complicating the progression instead of facilitating it. Therefore, the below sections will highlight these factors and talk about each one in details.

5.1.1 The Effect of Political Instability on the Law

Taking into consideration the effect political instability has on law enactment; three sub-factors were tested and taken into consideration to validate this analysis. Regional conflicts, delayed elections, and resigned governments are all part of the reasons contributing to political instability which in turn affects law enactment. In this paragraph we will discuss each sub-factor briefly.

It is worth mentioning that when starting this research, the Lebanese elections weren't held yet. After nine years and following several false starts over the past five years, Lebanon finally held a parliamentary election on May 2018 but the results have not brought change to the country's political status quo. The same old political elites continued to dominate Lebanon's political scene winning the vast majority of seats aided by an electoral law that works in their favor as it disregards the results of any electoral list that did not achieve a minimum threshold of votes.

It doesn't stop here. With elections being held and over with, a new problem aroused which is the formation of a new government. Since May 6th 2018, politicians have failed to agree on the members of cabinet leading Lebanon to enter its nine month with ministerial vacancy. There was a deadlock over the issue of the Sunni lawmakers from outside the Future Movement. Efforts to form a cabinet were derailed when Prime Minister designate Saad Hariri refused to comply with the demands of the March 8 MPs on including a group of "independent" Sunni lawmakers in the Cabinet.

In addition to the governmental problem, the impact of the Syrian crisis on Lebanon has been immense. The situation in neighboring Syria has exacerbated Lebanon's political instability, and led to a political standstill. Cross-border movements of

fighters have been reported during the past years and the level of violence increased. Lebanon needs to politically stabilize its rocky relations with Syria while complying with Beirut's declared policy of dissociation from regional conflicts; particularly Syria's seven-year-old war.

To overcome all these, new government ought to maintain unity to confront political, security, and economic challenges. The key lies in the ability of the political establishments to preserve minimal cohesion while confronting a turbulent and polarized region. Hence, political stability is a requirement to enable the Lebanese army and security agencies to confront any attempt to destabilize the country and corrupt its peace.

5.1.2 The Effect of Economic Instability on the Law

The second challenge that faces Lebanon is the government's ability to slow down the growing public debt maintaining economic stability while meeting the infrastructure's high demands. Moreover, the matter of refugees is creating an additional problem that is straining Lebanon's economy and burdening it even more. All will be discussed in this section.

Lebanon has the third highest debt-to-GDP (Gross Domestic Product) ratio in the world, at about 150 percent. Our investment spending does not exceed 8 percent; compared to 92 percent expenditure, which is between salaries, wages, debt service, and power deficit. The World Bank estimates Lebanon's national debt to stand at 155 percent of gross domestic product by the end of 2018, with an increase in the fiscal deficit to 8.3 percent due to a rise in current spending (Dakroub, 2018).

Moody's Investors Service changed Lebanon's outlook from stable to negative but maintained its long-term rating at B3, which indicates high credit risk. The report implies an increase in risk to the government's liquidity position and financial stability as a result of domestic and geopolitical risks surrounding the country (Dakroub, 2018).

In addition to that, the government failed to resolve the chronic problem of garbage collection and to provide basic public services such as running water, electricity, and fast internet. The country's infrastructure specifically roads, sewage system, water, and garbage collection has further deteriorated. Electricite du Liban (Lebanon's national electric company) is costing the government around $2 billion in annual subsidies. Above all that, the rising levels of unemployment, especially among graduates, is becoming a serious problem the government can no longer neglect (Dakroub, 2018).

Moreover, Lebanon is hosting 1.5 million Syrian refugees; about 30 percent of Lebanon's population, which constitutes the highest rate in the world. Lebanon cannot bear this number for it puts its future at risk making it impossible to tackle urgent challenges and delivering basic services to the Lebanese population. Politicians are sharply divided over the method adopted to return Syrian refugees to their home country. While some refuse to hold direct talks with Syrian authorities; recommending that the United Nations mediate, others believe that direct talks are needed between Damascus and Beirut to coordinate the returns (The Daily Star Lebanon, 13 December 2018).

All these factors were draining the government's budget that was already burdened. Implementing cyber-law procedures is very costly for that digital evidences are not like regular ones and require a lot of money to be analyzed and processed. Getting

the help of foreign experts as well as training the security and judiciary forces is not something that can be done with little fees.

5.1.3 The Effect of Socio-economic Structure on the Law

Sectarianism and bureaucracy are sub-factors that have huge effect on the Lebanese socio-economic structure forcing pressure on the governmental procedures and preventing things from going out smoothly and freely. The non-involvement of private sector is an addition to those sub-factors which all together are burdening the initiation of the law.

Lebanon's sectarian political system lies at the heart of the problem. After ten years of intermittent civil war, a political settlement known as the T'aif Agreement was finally formulated in 1989, by Lebanese statesmen, in the Saudi city of T'aif under Saudi encouragement (Krayem, 1997). To a war drained population frantic to end its prolonged misery and the horrendous destruction of its country, the T'aif Agreement certainly seemed as a great release and a necessary step towards unifying the country and rehabilitating and rebuilding its institutions (Salibi, 1988). Yet, the agreement has left behind severe socio-economic problems and a political muddle which the country remains struggling with. It failed to end political rivalry and meet the ambitions of all communal groups.

Furthermore, the Lebanese bureaucracy is constructed on the basis of sectarianism. Seats in the parliament are shared out proportionally among eighteen religious groups. Government posts and public-sector jobs are also distributed according to sects and the granting of favorable treatment by bureaucrats on the basis of political loyalty, family influence, and class (Kisirwani and Parle, 1987). These practices of

bureaucratic pathology are of great impact on conflict-prone cultures since such practices have aided in making bureaucratic performance a continuous political issue.

The formation of a new government appears to obey a similar rule. It took two and a half years for the country to elect its current president, nine years to hold parliamentary elections, and twelve years to pass a budget. Talks to form a cabinet have dragged on for over eight months until it was finally formed on January 31, 2019.

The political paralysis leads to a decrease in private sector funding. Political deadlock was negatively influencing the monetary wellbeing of the country. Growth needs stability; especially political, so that public and private sectors can build strategies to ensure prosperity; putting in practice public-private projects. Lebanon has a golden opportunity to boost its economy thanks to the $11 billion funding pledged last April by the international community at the Conference for Development and Reform with Businesses (CEDRE) (The Daily Star Lebanon, 1 February 2019). Up to 40% of the CEDRE financing is expected to come from the private sector. Lebanon committed to introduce structural and fiscal reforms to put the Lebanese economy on track and attract international private and public capital. The only way to advance is by having the government introduce the needed reforms and bring in the funding allocated in CEDRE.

Reaching a conclusion on anything requires the confessional groups to put aside their differences and work for the greater good. In a society divided along sectarian lines, this takes time.

5.2 General Laws Regulating Cybercrime Cases in the Absence of a Specific Law

In the recent years, Lebanon has seen rapid developments in the Information and Communication Technologies (ICT) and their use in various fields all in the absence of special legislation, integrated care, and governance on this sector.

The Lebanese legislator was aware of the need to control this sector through the adoption of special integrated legislations; represented by the general penal provisions, to secure the readiness of Lebanon and to enable it to play a leading role in that environment. On the other hand, the central bank of Lebanon, through its circulars, tried to protect the banking and financial sector from pirates and criminals; however, these circulars were not enough and cannot include all electronic crimes.

Lebanese courts adopted two kinds of provisions to deal with these types of cases. Traditional general provisions were adapted to resolve some of the legal problems related to this technology in addition to the provisions of some new texts; in particular the Law on the Protection of Intellectual Property Rights.

5.2.1 Examples of Articles Used on Electronic Crimes

Lebanese judiciary, despite the lack of legislation, has managed in the past years to address the situation with remarkable success through the legal texts available. However, the provisions of the Penal Code were enacted in 1943 at a time when the computer and informatics programs were not known. These provisions were still unable to grasp the various forms of cybercrime; especially the crimes of information systems and data as well as the protection of public freedoms and human rights.

Below are few examples of some articles taken from general and new provisions implemented on electronic crimes (Khamis, 2009).

- The internet has become a public network open to the community and may be considered as an automatic mean specified in article 209 Penalties.

- Article 281 of the Penal Code states that it shall be punishable by imprisonment the entry or attempted entry into a prohibited place in order to obtain objects or documents or information that must remain muffled in the interest of the State.

- The provisions of articles 282 and 283 of the Penal Code also punish by imprisonment the theft or possession of documents or information such as those mentioned in article 281. Here, the information or documents listed above may be recorded on electronic tapes or CDs used in the computer, and can therefore be considered criminal substances.

- It is also possible through the provisions of the Penal Code to punish many electronic crimes obtained through the dissemination of materials, images, or the routing of electronic messages through the internet that can weaken national sentiment or stir up racism or sectarianism in time of war or when it is expected to occur (Article 295 Penalties and what follows it).

- Electronic credit card fraud can also be penalized and used in support of articles 471 and 454 penalties.

- Article 655 of the Penal Code can be used to penalize fraudulent maneuvers obtained by electronic means.

- The law on the protection of intellectual property rights No. 75 dated 13/4/1999 considered computer programs to be protected by copyright and the offense of infringement. It stated in article 81 and what follows the procedures, restraints, and penalties applied as a deterrent to violators; providing imprisonment from one month to three years and fining in the amount between five million to fifty million Lebanese pounds, with the confiscation of tools and the obligation to pay up damages to the damaged person.

- Law No. 431/2002 concerning the regulation of the telecommunications sector services in the Lebanese territory regulated how to grant internet service licenses and imposed penalties for violating its provisions.

- Consumer Protection Act; No. 659 dated 4/2/2005, regulated some business processes conducted by professionals; remotely by the internet, and imposed penalties for certain offenses and crimes related to the subject.

At a time when there was no law concerning the Siberian world and laws still did not recognize the term "Internet", laws such as the Penal Code were applied to theft, fraud, sexual assault and other crimes. In contrast, prosecution found it difficult to characterize a number of cybercrime offenses such as entering and remaining illegally in an information system, distorting it, obstructing its operation, introducing other information and deleting it, in addition to producing, marketing, and acquiring indecent cartoons and tapes.

5.2.2 Examples of Cybercrime Cases Presented in Lebanese Courts

In 2000, the Lebanese judiciary faced an issue in which there was a serious violation of public morals through the internet where the Lebanese security authorities; in cooperation with Interpol, arrested a Lebanese person for broadcasting and publishing pornographic pictures of children via the internet. The Public Prosecution referred him to the investigating judge in Beirut, who condemned him by articles 531, 532 and 533 penalties and referred him to the criminal judge in Beirut who convicted him of supporting the aforementioned materials and sentenced him with imprisonment and a fine.

The court of criminal appeal partially reinstated the sentence as it considered the elements of the offenses set out in articles 531 and 532 not available because of the lack of a public requirement and public opinion provided in article 209 penalties and convicted him solely in support of article 533 (Khamis, 2009).

In another case, it was found that a group of people took advantage of their knowledge of the working minutes on the internet to access websites and financial information in preparation for the seizure of funds through obtaining information on credit cards for United States citizens. These people then used the cards information to transfer the accounts to imaginary people in Lebanon via the western union network. With a previous deal between the pirates and Lebanese people, the latter were returning the transferred money to the pirates for a commission.

After the required investigations under the supervision of the discriminatory public prosecution, the defendants were referred before the judge for the trial in Beirut. On 28/2/2008 the judge convicted them of theft through articles 636, 219, and 220 penal code on the grounds that they have entered the accounts of others in the United States

making conversions to seize the funds deposited in those accounts by means of internet hacking (Khamis, 2009).

In a more recent case, Rana, a Lebanese doctor (a pseudonym for the secrecy of the investigation) was blackmailed by an African man after being tricked that he was a successful American surgeon practicing her profession. Things were followed by professional conversations and were reinforced by pictures from inside the operating rooms confirming his success. Despite Rana's educational level and maturity, the culprit was able to gain her trust and capture her heart taking advantage of her emotions until the doctor entered with him in a relationship authenticated with pictures and letters. Things ended up with her losing $ 250,000 for fear of exposing what was between them.

The Internal Security Forces Cybercrime Bureau managed to arrest the perpetrator after monitoring his accounts. Unfortunately, Rana was unable to recover the money because it was transferred into abroad accounts (Maroun, Al-Jomhoriah Newspaper).

5.3 The Effect the Absence of Law had on Electronic Financial Transactions

The growing proliferation of e-transactions has led to the emergence of many negative phenomena under the heading of cybercrime and related fraud and piracy. According to the European Central Bank statistics, 70% of bank officials believe that electronic threats are increasing and 48% say a potential attack on their institution could hit the organization's electronic system. At the international level, this topic has been the subject of work of several international organizations, including the work of Interpol's general assembly at its 86th session in September 2017.

In 2014, Lebanon witnessed a remarkable increase in the cases of electronic crimes resulting from counterfeit emails. Director General of Internal Security Forces; Major General Imad Othman, said that some merchants and banks have been exposed to cyber piracy enabling criminals to hack emails and create similar ones directed to bank customers and merchant suppliers. This resulted in substantial and material losses. Statistics show that these crimes have increased in the last three years where the volume of misappropriated funds has increased. After extensive analysis and study of the patterns used, it was found that the means of direct control are very difficult. Raising awareness to their patterns and methods may be the best means of treatment. Fortunately, the number of email frauds experienced by banks declined in the past years. The number of violations decreased from 78 cases in 2016 to 32 cases in the first nine months of 2017. However, we did not see a similar decline in cases where individuals are involved as the number increased from 47 in 2016 to 90 in the first nine months of 2017 (Alnashra, 29 November 2017).

The Secretary General of the Special Investigation Unit for Combating Money Laundering at the Banque du Liban; Abdel Hafiz Mansour, said that the past years have seen an increasing prevalence in the use of the internet and a grow in the volume of transactions executed through them. The figures presented by Mansour indicate the development of cybercrime since 2011. The Commission received 84 cases in 2015 valued at $ 12 million, 137 in 2016 valued at $ 8.5 million, and a single case for $ 5000. He drew attention to the existence of cases not reported; either for the preservation of reputation, or for the impossibility of recovering such funds (Soma, 2016).

The responsibility to combat cybercrime is a national duty that requires concerted efforts of all parties involved as well as the availability of an effective emergency

body whose work is to redress these crimes and put them under control. This requires an awareness plan that starts from individuals and then the community as a whole. It calls for the development of a national strategy and cooperation between the government and the private sector for the establishment of a center that qualifies specialists able to deal with such matters.

Moreover, it is necessary to build up a legal environment for cyber legislation by updating and training judges, lawyers, specialists, and specialized legal committees in the parliament. These are the nucleus for setting the pace with technology related crimes. Judicial institutions and Arab lawyer unions can cooperate through bar associations and specialized legal houses to help in the preparation of unique issues related to information crimes and materials.

5.4 Conclusion, Recommendations, Implications, and Limitations

5.4.1 Conclusion

Cyber law is a very technical law that is considered vital because it touches almost all aspects of transactions and behaviors concerning the internet, the World Wide Web, and cyberspace. Such crimes may threaten a nation's security and financial health and that is why it is important to have such a law and the right means to be able to protect the country from any cyber evasion.

The interviewed Lebanese lawyers, security experts, and professor of experience all agreed on the importance of passing such a law and the reasons to why such a law wasn't passed yet. The results of this study have indicated the reasons that burdened the enactment of this law, and have highlighted the framework of dealing with such cases in the absence of a specific law governing it. In addition, this study has showed

how the absence of cyber law is affecting electronic financial transactions in specific and the economy of Lebanon in general. Political turmoil and sluggish economic growth are prompting questions on how long Lebanon can avoid a financial meltdown. It all comes to the new government and its ability to reform the situation by putting aside all political differences working hand in hand with all parties to what is best for the country.

5.4.2 Recommendations

On 18/10/2018, the Lebanese parliament approved; under the concept of necessary legislation, the law on electronic transactions and personal data. It was published in the Official Gazette; issue 45, having its provisions in effect three months after its publication.

It is recommended that more studies be done on the strategies, policies, and procedures used to solve cybercrimes. Going deep in cases containing digital evidence and the criteria used to deal with such evidences is and addition.

It is also recommended to test the implementation of electronic transactions and personal data law on its conformity with other laws, the success of its provisions when dealing with cyber cases, and the limitations faced while executing it.

In terms of knowledge, it is recommended to increase cyber awareness so that it reaches all Lebanese people and organizations. It is also important to increase cyber training for lawyers, judges, and I.S.F members allowing them to be able to handle different case scenarios and increasing their experience.

5.4.3 Implications and Limitations

In this study, we have highlighted the way cases are handled in the absence of a cyber-law; however, only three lawyers were interviewed due to the lack of specific knowledge in these cases. Some of the contacted lawyers have never dealt with such cases and had no idea how to handle such ones. Perhaps by the time further studies on this subject are explored, the number of lawyers dealing with cybercrime cases would have increased or the knowledge concerning such cases would have amplified.

Also due to the lack of time, the researcher wasn't able to conduct interviews with Lebanese judges for it requires prior notice and approval from the ministry of justice. The researcher couldn't afford the delay and unfortunately the outlook judges have on this matter wasn't documented.

Bibliography

Association of Banks in Lebanon, (2016), The Lebanese Banking Sector in 2016: The Annual Report. Retrieved from: http://www.abl.org.lb/Library/Files/Files/Ann%20rep%202016%20En%204.pdf

Battah, H. (2015). Who's Got Your Data, BOLD Magazine. Retrieved from: http://www.beirutreport.com/2015/07/whosgot-your-data-2.html

Brandom, R. (2018, January 18), Researchers have discovered a new kind of government spyware for hire: A Lebanese hacking campaign could be part of something much larger, The Verge. Retrieved from: https://www.theverge.com/2018/1/18/16905464/spyware-lebanon-government-research-dark-caracal-gdgs

Burnard, P. (1991). A Method of Analyzing Interview Transcripts in Qualitative Research, Nurse Education Today, 11(6), 461-466.

Council of Europe, (2018, February 20), Lebanon's Status Regarding Budapest Convention. Retrieved from: https://www.coe.int/en/web/octopus/country-wiki/ /asset_publisher/hFPA5fbKjyCJ/content/lebanon

Crede, A. (1995). Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet, Journal of Computer Mediated Communication, Vol.1, No.3.

Dakroub, H. (2018, December 28). Challenges Await Lebanon in 2019, The Daily Star Lebanon. Retrieved from: http://www.dailystar.com.lb/News/Lebanon-News/2018/Dec-28/472791-challenges-await-lebanon-in-2019.ashx

El-Amine, Y. (2016, November 29), Cyber Security Awareness Growing in Lebanon, Annahar newspaper. Retrieved from: https://en.annahar.com/article/503624-cyber-security-awareness-growing-in-lebanon

Electronic Financial Transactions Act. Retrieved from: https://www.fsc.go.kr/downManager?bbsid=BBS0085&no=106341

Felix, J., Hauck, C. (1987). System Security: A Hacker's Perspective. Interex Proceedings, Vol.1.

Glaessner, T., Kellermann, T., McNevin, V. (2002). Electronic Security: Risk Mitigation in Financial Transactions Public Policy Issues, The World Bank. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.119.8602&rep=rep1&type=pdf

Hasan, M., and Harris, E. (2009). Entrepreneurship and Innovation in E-commerce, Journal of Achievements in Materials and Manufacturing Engineering, Vol.32, Issue 1.

ITRC, (2017), Identity Theft: The Aftermath 2017, Identity Theft Resource Center. Retrieved from: https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf

Kalakota, R., Whinston, A. (1997). Electronic Commerce: A Manager's Guide, Addison-Wesley.

Karake- Shalhoub, Z., Al Qasimi, L. (2010), Cyber Law and Cyber Security in Developing and Emerging Economies, Edward Elgar Publishing Inc.

Kaspersky Lab, Online and Mobile Banking Threats. Retrieved from: https://media.kaspersky.com/en/business-security/online-and-mobile-banking-threats-kaspersky-whitepaper.pdf?icid=en-UK:ent-content

Kaspersky Security Bulletin 2015, (2015, December 15), Overall statistics for 2015. Retrieved from: https://securelist.com/kaspersky-security-bulletin-2015-overall-statistics-for-2015/73038/

Ministry of Economy and Trade, (2011, May 3), E-commerce. Retrieved from: https://www.economy.gov.lb/en/projects/e-commerce

Kisirwani, M., and Parle, W. (1987). Assessing the impact of the post-civil war period on the Lebanese bureaucracy: A view from inside, Joumal of Asian and African Studies.

Krayem, H. (1997). Conflict resolution in the Arab world: Selected essays. Retrieved from: ddc.aub.edu.lb

Leyden, J. (2007, January 16). Trojans fuel ID Theft Boom, The Register. Retrieved from: http://www.theregister.co.uk/2007/01/16/mcafee_id_theft_trends/

Makhlouf, Y. (2011, September 26). The Electronic Transactions Regulation Act: Differentiation in the Declaration of the Principle of "Respect for Privacy" and its Differentiation in its Fragmentation, Legal Agenda. Retrieved from: http://legal-agenda.com/article.php?id=31&lang=ar

Marsi, F. (2018, February 6). Dark Caracal: Lebanon in the age of cyber warfare, The Daily Star. Retrieved from: http://www.dailystar.com.lb/News/Lebanon-News/2018/Feb-06/437019-dark-caracal-lebanon-in-the-age-of-cyberwarfare.ashx

Moore, R. (2005). Cybercrime: Investigating High-Technology Computer Crime, Anderson Publishing.

Nehmzow, C. (1997). The Internet Will Shake Banking Medieval Foundations, Journal of Internet Banking and Commerce, Vol.2, No.2.

OMSAR, (2012), Lebanese National Cyber Security Policy Guidelines, Office of the Minister of State for Administrative Reform. Retrieved from: http://www.omsar.gov.lb/Cultures/en-US/ResourcesSupport/SupportAdministration/Pages/NationalCyberSecurityPolicyGuidelines.aspx

Ooi, S. (1999). Surge in E-commerce Transactions, SME IT Guide.

Paget, F. (2007). Identity theft, McAfee Avert Labs.

PWC, (2018), Pulling Fraud Out of the Shadows: Global Economic Crime and Fraud Survey 2018. Retrieved from: https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf

Salibi, K. (1988). A House of Many Mansions: The History of Lebanon Reconsidered, B Tauris and Co Ltd. London, Vol. 52, Issue 2.

Seitz, J., Stickel, E. (1998). Internet Banking: An Overview, Journal of Internet Banking and Commerce, Vol.3, No.1.

Shehab, M. (2018). Legislation of Cyber Law and Digital Forensic in Lebanon, Lebanese American University.

Sterling, B. (1993). The Hacker Crackdown: Law and Disorder on the Electronic Frontier, The University of Adelaide Library. Retrieved from: https://ebooks.adelaide.edu.au/s/sterling/bruce/hacker/complete.html

The Daily Star Lebanon, (2016, December 7), Facts on Anti Cybercrime and Intellectual Property Rights Bureau. Retrieved from:

http://www.dailystar.com.lb/News/Lebanon-News/2016/Dec-07/384401-facts-on-anti-cybercrime-and-intellectual-property-rights-bureau.ashx

The Daily Star Lebanon, (2018, December 13), Refugees are "victims and not criminals": Bou Assi. Retrieved from, http://www.dailystar.com.lb/News/Lebanon-News/2018/Dec-13/471709-refugees-are-victims-not-criminals-bou-assi.ashx

The Daily Star Lebanon, (2019, February 1), Moody's: New government faces challenges to implement reforms. Retrieved from, http://www.dailystar.com.lb/Business/Local/2019/Feb-01/475619-moodys-new-govt-faces-challenges-to-implement.ashx

Trautman, L.J. and Altenbaumer-Price, K. (2010, December 17). The Board's Responsibility for Information Technology Governance, John Marshall Journal of Computer & Information Law, Vol. 29.

Trautman, L.J., Triche, J., and Wetherbe, J. (2013, October 28). Corporate Information Technology Governance under Fire, Journal of Strategic and International Studies, Vol. VIII, No. 3 Available at SSRN: https://ssrn.com/abstract=2346583.

Turban, E., King, D., McKay, J., Marshall, P., Lee, J., and Viehland, D. (2008). Electronic commerce 2008: A managerial perspective (5th edition), Upper Saddle River, NJ: Pearson Prentice Hall.

Westerlind, J. M. (2000). The Magna Carta Meets the Twenty-First Century: Personal Jurisdiction and the Internet, Journal of Civil Rights and Economic Development: Vol. 15, Issue 2, Article 5. Retrieved from: https://scholarship.law.stjohns.edu/jcred/vol15/iss2/5.

Whitley, E.A., Hosein, I.R., Angell, I.O., Davies, S. (2007). Reflections on the Academic Policy Analysis Process and the UK Identity Cards Scheme, The Information Society, Vol.23, Issue1. Retrieved from:

https://pdfs.semanticscholar.org/8b99/71dcffdf01b158ff5c42bfcd22de1d9efdbe.pdf

Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., and Deng, H. (2011, July 13). A Survey of Cyber-Crimes, Wiley Online Library.

النشرة.(٢٠١٧ ،٢٩ تشرين الثاني). التقرير اليومي 2017/11/29: منصور خلال مؤتمر "مكافحة الجريمة الإلكترونية": الوسيلة الأفضل لمكافحة هذه الجرائم هي الوقاية.

https://www.eliktisad.com/news/show/320418/%D8%A7%D9%84%D8%AA%D9%82%D8%B1%D9%8A%D8%B1%D8%A7%D9%84%D9%8A%D9%88%D9%85%D9%8A-29112017:%D9%85%D9%86%D8%B5%D9%88%D8%B1%D8%AE%D9%84%D8%A7%D9%84%D9%85%D8%A4%D8%AA%D9%85%D8%B1%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%A7

خميس، ف. (2009). جرائم المعلوماتية في ضوء القانون اللبناني والاجتهاد.

https://www.unescwa.org/sites/www.unescwa.org/files/events/files/event_detail_id_2040_d11a.pdf

صوما، ب. (30،2016 ت2). «ملتقى الجرائم الإلكترونية»: للوقاية بغياب القانون، جريدة السفير. http://assafir.com/Article/518863

مارون، س. هكذا تعمل عصابات الإنترنت... ولبنان «في مهب الريح»، جريدة الجمهورية.

http://www.aljoumhouria.com/pages/view/143215

مخلوف،ي. (2011، 26 أيلول). مشروع قانون تنظيم المعاملات الالكترونية: التمايز في اعلان مبدأ "احترام الخصوصية" والتمايز في نسفه، المفكرة القانونية.

http://legalagenda.com/article.php?id=31&lang=ar

Appendix A: Interview with Lebanese Lawyers

1- What are the factors that limit or burden the enactment of a law governing EFTs?

2- How much do the following (political instability, socio-economic structure[1], and economic instability) affect EFTs in general and the cyber-law enactment in specific?

3- Do you think that the regional conflicts, resigned governments and delayed elections affected political instability which in turn affected the enactment of a cyber-law?

4- Did the following factors (infrastructure, health/education, refugees) have any direct link to the delay in law enactment being an economic priority?

5- Have the political parties/sectarianism[2], non-involvement of private sector, and bureaucracy[3] helped in delaying the process of law enactment in terms of the socio-economic structure?

6- In case of a dispute, how is it settled? What law is enacted?

7- Have you ever worked out on a case that required digital investigation and digital evidence?

   a- Clarify any difficulties faced while applying/binding a cybercrime case to a Lebanese law?

   b- What suggestions would you recommend to overcome the difficulties that Lebanese judges face while working with cybercrimes and their investigations?

[1] Is the social science that studies how economic activity affects and is shaped by social processes. Societies are divided into three groups: social, cultural and economic. In general it analyzes how societies progress, stagnate, or regress

[2] Excessive attachment to a particular sect or party, especially in religion

[3] A system of government in which most of the important decisions are taken by state officials rather than by elected representatives

8- Within the past years, did you notice any change in the number of cybercrime cases?

   a- What do you think is the reason behind this change (whether they increased or decreased)?

   b- Do you think the implementation of a cyber-law would limit the number of cyber-criminal cases?

9- A draft was given to the Lebanese Parliament in order to enforce cyber-security. Do you believe that the law draft is now outdated and needs to be modified?

10- Meanwhile, can we modify and apply general legal principles (rules of tort, property, or criminal law) to online interactions until a cyber-law is born?

Appendix B: Interview with Experts in the Field

1- What are the factors that limit or burden the enactment of a law governing EFTs?

2- How much do the following (political instability, socio-economic structure, and economic instability) affect EFT in general and the cyber law enactment in specific?

3- Do you think that the regional conflicts, resigned governments and delayed elections affected political instability which in turn affected the enactment of a cyber-law?

4- Did the following factors (infrastructure, health/education, refugees) have any direct link to the delay in law enactment being an economic priority?

5- Did the political parties/sectarianism, involvement of private sector, and bureaucracy help in delaying the process of law enactment in terms of the socio-economic structure?

6- In case of an attack, how is the situation handled? Are the companies ready to defense such an attack?

7- Do you think that Lebanese people are aware of cyber security and cyber-attacks? Are there any future plans to spread cyber security awareness?

8- What are the main advantages of passing or enacting such a law?

9- Are financial service providers given proper incentives to fully share timely and accurate information with law enforcement on security breaches? What actions might be taken to facilitate public -private cooperation to remedy the situation?

10- What role should the government play in setting out policies, standards, and guidelines for e-security?