TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technology

Department of Software Science

TUT Centre for Digital Forensics and Cyber Security

Zaghum Wahab Awan 132115IVCMM

ANALYTICAL COMPREHENSIVE APPROACH TO CYBER LAUNDERING AND ITS SOLUTIONS

Master's Thesis

ITC70LT

Supervisors: Tiia Sõmer, MSc

Researcher

Tallinn university of Technology

Declaration

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been acknowledged in this thesis. This thesis has not been presented for any degree or diploma at any other university.

Author: Zaghum Wahab Awan

Signature: …..........................

Date: …..........................

Abstract

It would not be wrong to say Internet is one of the most important inventions at preset time and it has dramatically changed our life. In simple words internet is kind of luxury in our life. Government, financial institutions, hospitals and transports are dependent on cyberspace for their daily operations. With all these advantages of internet there are associated disadvantages as well and cybercrime is one of them. Due to unique features of internet the cyber criminals are more organized and internet provides them platform to conceal their ill derived proceedings which are referred to as cyber laundering.

Economy plays very important role in the strength of any country and financial institutions act as the pillar in the economy of any country. Financial institution have direct link with the cyber laundering. The main focus of this thesis is about the different aspects of cyber laundering. The thesis highlights the role of internet, how it revolutionized the concept of money laundering and finds the link between cyber laundering and cybercrime.

The possible outcome for this thesis is to clear understanding of cyber laundering, its impacts on various businesses and international efforts for the prevention of cyber laundering. It will also give detail analysis of different strategies and possible recommendations.

Keywords

Cyber laundering, Internet, Smurf, Transactions, Money laundering, Electronic money

Cybercrime, Anonymity, Terrorism, Cyberspace, Attacks, Infrastructure

Annotatsioon

Internet on kaasaja olulisemaid leiutisi ja on toonud endaga kaasa suuri muudatusi meie elustiilis. Ühelt poolt on internet meie elu lihtsamaks teinud. Valitsus, pangad, haiglad ja transport on oma igapäevatöös sõltuvad küberruumist. Teiselt poolt kaasnevad interneti poolt pakutavate hüvedega ka ohud, näiteks küberkuritegevus. Internetiavarused võimaldavad küberkurjategijatel oma tegevust paremini organiseerida ja hõlpsamini varjata. Küberkuritegevuse hulka kuulub nii rahapesu kui ka sellele eelnev küberkelmus.

Tugev majandus on tugeva riigi alustala ning rahaasutused mängivad riigi majanduses olulist rolli. Finantsasutustel on otsene seos rahapesuga ja sellele eelneva küberkuritegevusega. Käesolev töö keskendub erinevatele küberkuritegudele ja küberruumis kasutuses olevatele rahapesuskeemidele. Interneti tulekuga kaasnenud küberrevolutsioon on mõjutanud ka rahapesukuritegusid ning küberkelmused on nendega otseselt seotud.

Käesolev töö annab ülevaate rahapesust küberruumis ja selle mõjudest erinevatele ettevõtetele. Rahapesu tõkestamiseks ja küberturbe tagamiseks on vajalikud rahvusvahelised abinõud. Töö analüüsib erinevaid rahapesu tõkestamise strateegiaid ja pakub võimalikke lahendusi.

Märksõnad: küberkuritegevus, internet, smurf, rahatehing, rahapesu, elektrooniline maksevahend, anonüümsus, terrorism, küberruum, rünnak, taristu.

Acknowledgement

I am greatly thankful for my supervisor Mrs Tiia Somer for her guidance, support and for her timely feedback related to my thesis work. I am also thankful for my all professors and lecturers I consulted during my Master study in Tallinn University of Technology.

Zaghum Wahab Awan

List of Abbreviations

IMF	International Monetary funds
DEA	Drug Enforcement Administration
NDIC	National Drug Intelligence Centre
EMONEY/CASH	Electronic Money/Cash
CHIPS	computer based Fed wire and Clearing House Interbank Payments Systems in terms of dollars exchanged
ECB	European Central Bank
NAB	National Accountability Bureau of Pakistan.
Interpol	International Police Organisation.
ISAC	Information Sharing and Analysis Centre.
CoE	Council of Europe
SIM	Subscriber identity module
SWIFT	Society for Worldwide Interbank Financial Telecommunication
AML/ML/CL	Anti Money Laundering / Money Laundering/Cyber Laundering
TCP	Transmission Control Protocol.
CSP	Cyber payment Security Protocol
GIS	Global Information System
ICT	Information and Communication Technology
IMF	International Mutual funds
FATF	Financial Action Task Force
MLD	Money Laundering Detection
NAB	National Accountability Bureau

Table of Contents

List of Figures

1 Introductions

The ICT (Information and Communication Technology) advancements have great impact on the modern society in numerous areas which includes communication, commerce, education and so on. These advancements indeed have brought incredible benefits but in mean time also create the opportunities and motivations for the criminals to conduct organized crimes in the cyberspace. Cyberspace has also made online crimes highly profitable. The Modern ICT provides effectiveness and efficiency that create the opportunity for the money launderers to utilize the cyberspace for more beneficial gains. In fact due to efficiency and effectiveness it could be easily predicted that soon the electronic transactions will replace almost all other business transactions. Advancement in the field of information and communication technology also make it hard to identify the money laundering modus as it help to conceal the origin of money .[1]

Money laundering (ML) for illicit funds has been taking place more than decades and indeed is not a new phenomenon. It has forced national governments, international organisations, regulators and private sectors to undertake strong steps to tackle the movements of illicit funds to legal sectors .[2]

The money launderers from cyberspace can derive huge benefits like low risk, great transactional speeds and better anonymity. The money laundering conduct using the medium of cyberspace is called as Cyber laundering .[2]

The structure of global information networks (GIS) and the way they operate raises number of unique challenges and vulnerabilities that imposes the risk of cyber laundering. It increases the chances for the criminals to exploit the worldwide communications and information networks. Simply by keeping themselves undetected initiates the money laundering activities due to their anonymity, ease of use, speedy transactions and without being physically present on site have the ability to operate in different jurisdictions .[2]

1.1 Catalysts involved in the Cyber laundering Dilemma

To understand the full concept of cyber laundering it is crucial to understand how it evolved [3]. After the invention of internet the Cyber laundering Phenomenon was triggered more rapidly. Some of the internet unique features and traits that forms the blueprint on the bases of which cyber laundering thrives are further discussed below. [3]

Modern computer are designed in such a way that make them capable to process large data at the blink of eye due to extraordinary processing speed of the computer central processing device(CPU). CPU data processing speed is measured in Gigahertz. Other factors that determine speeds are computer's graphic card and random Access Memory (RAM). Later refers to depository which stored the current files. Fast processing speeds of RAM provide guarantee for easy access to one’s file and while on the other hand the graphic card is the hardware that processes graphics.[3]

The fast graphic card is very crucial for computer to process in per second more graphs or display images or frames. The computer speed is further complemented by fast internet services. It is easy to grab the idea that cyber laundering is directly linked with all these basic features of technology, because with the absence of all these features there wouldn’t be any existence of the notion of cyber laundering. Internet is another catalyst for the cyber laundering dilemma which acts as virtual playground for cyber laundering. Generally originated from the several United States government projects in the late 1960s. Nowadays internet plays central role in cyber laundering because of its ubiquitous nature and presence. [3]

Many countries such as France, Finland, Greece, Estonia and Spain entitled the access of internet as a part of individual basic fundamental rights .[3]

In early 1990s mainly in United Kingdom and United States the internet was popular only among households and businesses and this popularity was due to increase awareness about the internet's never-ending capacity and practical functionalities. That’s why we can say that Cyber laundering phenomena is borne out of the internet globalization. The notion of anonymity is another catalyst in the cyber laundering dilemma. Anonymity issues always have been a subject of contention .[3]

The issue of anonymity initially was regarded as one's fundamental right of free speech, freedom of self expression and privacy etc. The anonymity factor is very visible on internet as any individual on internet can conduct activities without disclosing their true identities and by hiding his exact traceable locations. By using this anonymity features of internet, the criminals over internet can spin a perfect web of transaction thus by simply wiping out all traces of the original act. This is what essentially cyber laundering is all about .[3]

1.2 Problem statement

Cyber laundering is currently one of the hottest issues worldwide. It is kind of plague not only for the highly developed countries economies but also for third world countries where corruption is widespread. Cyber laundering is not only damaging the legitimate economies and businesses but also is the source to promote other cybercrimes e.g. Cyber terrorism financing etc. After the invention of internet it is acting like a breeding ground for the cybercriminals. By utilizing certain unique features of internet the cybercriminals are much safer in the cyberspace as never before from the reach of law enforcement agencies. The main motive of this paper is to unleash the various aspects of cyber laundering.

1) Why cyber laundering is organized cybercrime?

2) How the invention of internet changes the concept of traditional money laundering into cyber laundering?

3) What modern techniques adopted by cyber launderers for the cyber laundering?

4) What is the role of International organizations to curb the cyber laundering evil?

5) How cyber laundering can be source of financing for the cyber terrorism?

6) Which businesses are vulnerable due to cyber laundering?

7) What are the precautionary measures to prevent the cyber laundering

1.3 Aim & Objectives

Aim & Objective for this thesis are as follows.

- To demonstrate a critical analytical view of Cyber Laundering and analyze the difference between money laundering and cyber laundering.

- To demonstrate the techniques used by cyber launderers for cyber laundering with the help of hypothesis.

- To demonstrate the analytical view of cyber terrorism and cyber payment systems.

- To demonstrate the analytical view on different international strategies to prevent cyber laundering.

- To demonstrate the strength and weakness of real time Tallinn based start-up with the possibility of exploitation for cyber laundering and cyber terrorism.

- To demonstrate the case study of “Bangladesh Bank cyber-heist” to highlight the links between cybercrime and cyber laundering.

1.4 Methodology

This research is done by adopting programmatic approach. This is based in most of cases by using secondary online data and primary data was also in consideration. For the accomplishment of this research many online journals, online books, articles, newspapers was consulted.

1.5 Thesis Outline

Thesis outline is as follows.

Chapter-1 is based on the introduction with the brief outline about the research and problem statement. Chapter-2 discuss about the cybercrime from the cyber laundering perspective and about the classification of different cybercrime. Chapter-3 overlooks the traditional form of money laundering and its traditional techniques to convert illicit funds into white money. Chapter-4 is focus on E-money or Electronic money which is back bone for the execution of cyber laundering in cyberspace.Chapter-5 is based on the cyber laundering which discuss that how internet revolutionized the traditional money laundering for its execution in cyberspace.Chapter-6 is on different models for the cyber payment systems, Chapter-7 describes different international organizational efforts to tackle the evil of cyber laundering.Chapter-8 is based on critical analysis of Tallinn base start-up from the cyber laundering prospective and cyber terrorism.Chapter-9 is case study on Bangladesh Bank cyber-heist which shows how cybercrime is link with cyber laundering.

2 Cyber Crime from the cyber laundering perspective

There is rapid increase of Cyber attack reflecting high level of sophistication both in complexity and intensity with new emerging vulnerabilities and threats. Detica states that "*Cyber criminal networks include international criminal organisations, intelligence agencies, individuals and small criminal groups, and legitimate organisations*" .[4]

The operational platform for the cyber criminals are typically loosely organised networks consists of relatively independent parts with the capability of quick assembly and/or dispersion. Those business units which impersonate as legitimate industries for the provision of specialist services including the marketing, development and sales of attack tools (provide services to plan and execute attacks in cyberspace) and to assist the laundering of stolen or illicit assets in cyberspace are also included in modern cyber crime activities .[4]

2.1 Cybercrime: "The Cyber Root" of Cyber laundering

Cyber laundering can be stated as the offspring of two very distinct and indigenous forms of criminality-money laundering and cybercrime. To understand Cyberlaundering it also becomes important to explore briefly the concept of cyber crime. Furthermore in order to trace the roots of cyber laundering to cybercrime have to put the concept of cyber laundering in its appropriate frame .[5]

The term "Cybercrime" is often surrounded by linguistic confusion. Different terms such as computer based crime, computer crime and computer abuses are all synonyms of the same things .[5]

Cyber crime can defined as criminal acts that are carried out in cyberspace by using electronic communications networks and information systems. Cyber crime has no boundaries and can be classified as follows . [6]

- Internet related crimes such as attacks against information systems or phishing (fake bank site to steal passwords to access the victim's bank account).

- Forgery and online fraud, frauds on large scale can be committed online by using instruments such as identity theft, malicious code and spam and phishing.

- Improper or illegal contents online including incitement to racial hatred, child sexual abuse material, incitement to terrorist acts and glorification of violence, racism and xenophobia and terrorism .[6]

Many other authors have taken a different approach to define cybercrime. Majid Yar elaborate the definition of cybercrime by distinguishes between computer-assisted crime on one side and computer focused crime on other. The former entails crimes that exist before the advent of internet, but after the internet has taken a new appearance making such crimes to wear a new look. [5]

This includes fraud, theft, pornography, hate speech, sexual harassment and money laundering. Cyberlaundering is also found within this sphere. The computer focused crimes as identified by Majid Yar encompasses crimes that emerged with the internet advent and which was not possible without the internet. Examples here are website defacement, Phishing and hacking and viral attacks. [5]

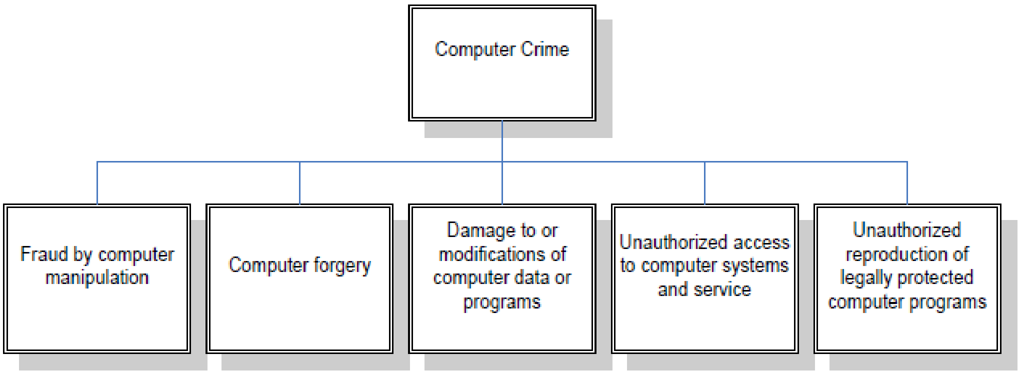
2.2 Classification of cyber crime

The specific crimes that are encompassed by the terms computer crime or cybercrime have a considerable difference. Cybercrimes are classified by the Foreign Affairs and International Trade of Canada into two categories. [7]

1) Computers and Networks are being used for committing the crimes (e.g. hacking and viruses).

2) Computer involvement to facilitate the traditional crime (e.g. online fraud and child pornography) .[7]

The UN manual published in 1999 related to the prevention and control of computer-related crime as shown in figure 2.1.[7]

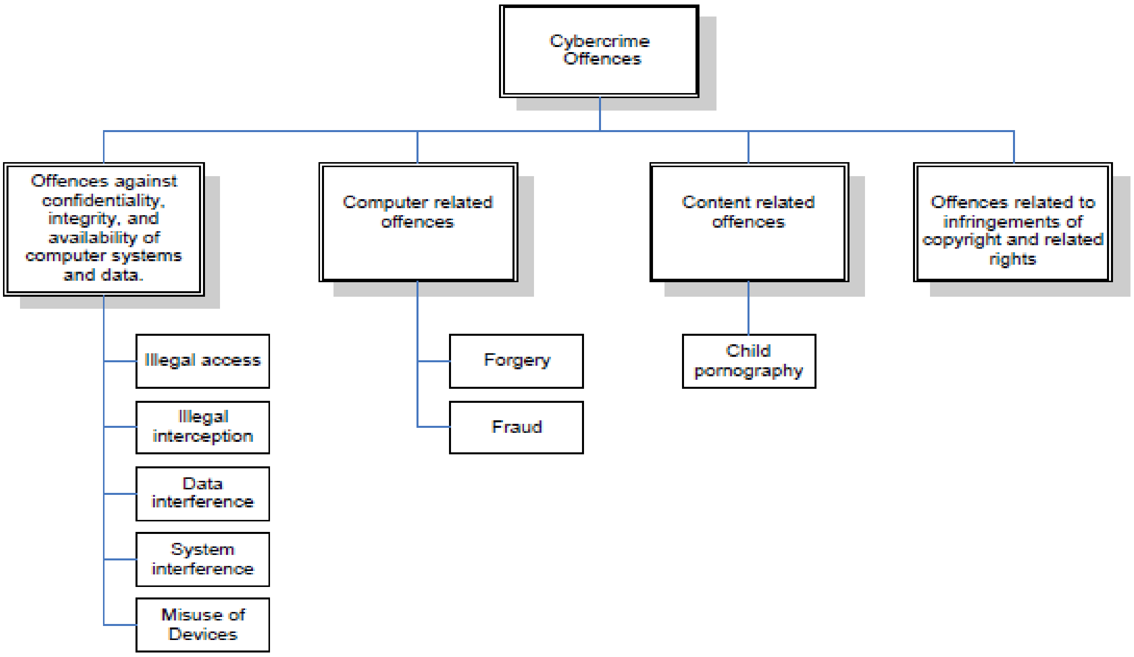


Computer Crime
Fraud by computer manipulation
Computer forgery
Damage to or modifications of computer data or programs
Unauthorized access to computer systems and service
Unauthorized reproduction of legally protected computer programs

Figure 2.1 According to United Nation common type of computer crime .[7]

The crime against computer systems and data are part of United Nation manual, it also focus on some crimes that facilitated by the use of computer such as forgery and fraud. However other types of offenses such as money laundering, identity theft and storing illegal contents that are facilitated or committed by a computer or computer systems doesn't address by the manual[7].

Convention on cybercrime, the Council of Europe (CoE) classifies cyber crime or computer crime into four categories as described in figure 2.2



Cybercrime Offences
Offences against confidentiality, integrity, and availability of computer systems and data.
Computer related offences
Content related offences
Offences related to infringements of copyright and related rights
Illegal access
Illegal interception
Data interference
System interference
Misuse of Devices
Forgery
Fraud
Child pornography

Figure 2.2 cybercrime classifications by Council of Europe [7]

Some of the crime categorized by the Council of Europe doesn't address certain kind of crimes which are committed or facilitated by using the computer such as money laundering and identity theft .[7]

In 2001 conference on High-Tech Crime, the G8 government/Industry Conference participants discussed the requirement to categorise high-tech crime according to the type of threat not the type of crime. The motive behind was to avoid the issues raised by the variations in criminal law across jurisdictions. In return it varying local definitions of computer crime or high tech [7] as can be seen in figure 2.3.

They examined and found the Council of Europe classification to address all computer assisted threats is not comprehensive. The threats divided into two major categories by conference workshop which as follows.

1) Attacks on computer infrastructure:"*operations to disrupt, deny, degrade, or destroy information resident in computer and computer networks or the computers and network themselves*".[7]

2) Threats assisted by computer: "*malicious activities.... which are facilitated by computer .The use of computer as a tool in the offense or threats* ".[7]

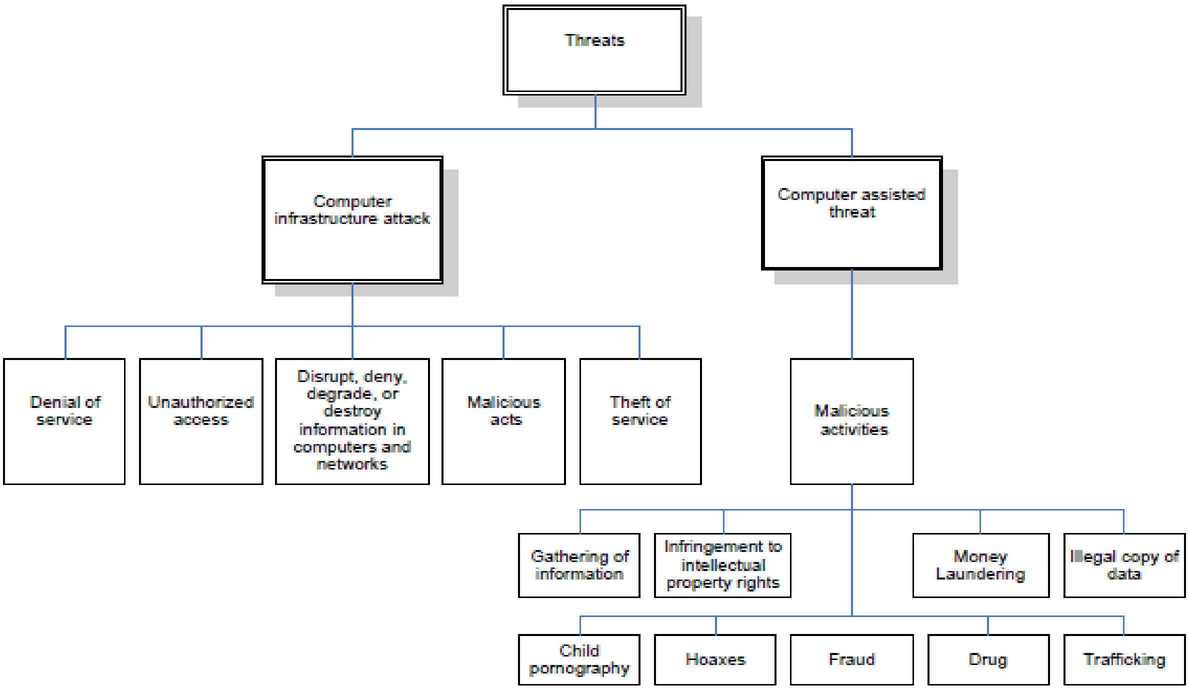


Figure 2.3 Threats categorized by G 8. [7]

Some very interesting points are observed by G8. Firstly "Attacks on computer infrastructures" which cover all crimes by criminal activities related to computer or computer networks. This category of threats is widely accepted which covers all type of attacks on computers and computer networks. Secondly the category "Threats assisted by computer" in which computer or computer systems facilitate threats. They also consider Money laundering as threats (Cybercrime). [7]

2.3 Revenue generation for Cyber criminals

A lot have been discussed about the cost of cybercrime or typically focuses on the negative economic impacts to the victims based on the calculation of overall cost of loss or a breach. It is very important to know how much profit specific cyber criminal entities are making or for the specific cyber crime type the actual profit is sparse. The cost of loss due to cyber attacks to an individual or organisation does not directly equal to the amount of tangible profit the cyber-criminal derives. [4]

In 2012 Khoo Boon Hui the president of Interpol states that "*US banks reportedly lost US $890 million to conventional robbers during 2011, they lost $12 billion to cyber criminals that same year".* Which clearly shows that criminal from digit economy can yield greater revenue comparatively some other traditional criminal methods .[4]

Stone-Gross et-al (2011) published two researches about the revenue generation from two cyber-criminal activities which includes the sale of fake Anti-Virus software and running of Botnet. Their research results relate to botnet services states that : *"We estimate the Cutwail gang's profit for providing spam services at roughly $1.7 million to $4.2 million (contingent on whether bulk discounts were provided to customers)"*. Based on their other research from three fake Anti-Virus vendors they analysed the back end information, the resulting output on their investigation finding that *"These three fake Anti-Virus businesses had earned a combined revenue of more than $130 million dollars"[4].*

Karami et al. (2013) conducted a study to calculate the revenue that criminals could generate by adopting Black-hat Search engine optimisation (SEO) techniques which directs the customer to fake websites of counterfeit luxury goods websites and herbal supplements. On the basis of this research it was revealed that over a two years time period estimated USD 6 million was paid to over 119 criminals. Due to two reasons it is useful to build a picture of profitability based on the analysis of this work [4].

1) By adopting Black Hat techniques to direct traffic and advertising to a website requires minimal infrastructure. This could be facilitated from third party hosted services (To generate spam and to boost the SEO ranking, the criminals lease and utilise established botnet). In addition to this by code scripting a significant portion of it could be automated with limited human interaction.

2) Counterfeit goods website should be with some infrastructure with the capacity of some level of supply chain as well with the information of actual cost of products and shipping information. In addition to that some resources and efforts require to keep alive the website online. On the basis of research it can be logically concluded, once the criminals had covered overheads, with the ability to pay out nearly USD 6 million in "cooperative marketing funds" across just under 60000 orders post sales, successful to made ample profit [4].

Kapersky (2014) provides the insight profitability of certain cyber-crimes and make a comparison of costs of malware or cyber-criminal service leasing in respect to amount generated by cyber criminals per 100 successful attacks. Based on research the most profitable type of cyber-crime is utilising banking Trojans with the approximate cost to purchase USD 3,000 yielding per 100 victims an average of USD 72,200[4].

This shows how cyber crimes are gaining grounds to generate high revenue for cyber criminals. After the invention of internet, money laundering has been transferred into entirely new form with the global reach and sophisticated techniques to execute on cyberspace in the entirely new form as cyber laundering. Cyber laundering is one of cybercrime which help the criminals to generate revenue, clean the illicit funds and help to initiate other cybercrime such as cyber terrorism (financing by using cyber laundering). The main focus of this paper is all about cyber laundering and its execution in cyber space.

3 Overview of Money laundering

The main focus of this paper is on cyber laundering but as we know that cyber laundering is subset of money laundering. So first we have to understand the concept of money laundering which as follows. With the purpose to have financial gain through illegal activities a lot of economics crimes are committed which includes from murder, drugs, arms trafficking to financial frauds etc. Such crimes at the cost of others can make many people wealthy. The consequences of such actions create social ills and cause the diversion of money from the legitimate business activities. To utilize the benefits of illicit money, the criminals must have to first clean the money by establishing the legal source of funds as it is earned from the legitimate business activities. Such process is known as money laundering. [8]

Tom Dely who was the 24th major leader for the United State House of Representative in October 2005 was forced to resign because of money laundering allegations. . In 2003 Late Pakistani prime minster Benazzir Bhutto was convicted for money laundering through Swiss bank account. [9]

In present days, in office current Pakistani Prime Minister Nawaz Sharif there are strong allegations of money laundering and offshore companies from opposition political parties and his case is in High court of Pakistan .[10]

In 1996 Franklin an expert and an economist of Harvard university was found quality in money laundering case for Santacriz Londono(Columbian drug lord) for the $32 million. From 1930 money laundering has been considered as organized crime and still it is plague for the current financial market. According to the International Monetary Fund every year around 5 % of the world's gross domestic product which make sum of roughly $600 billion of money is laundered . As economy is getting more into a digital economy which allow the money launderers to find new and easier ways to utilize the banking rules and regulations for their benefits. [9]

3.1 Money Laundering

It is assumed that Mafia group in united states of America originated term of money laundering for the substantial amounts of money derived from unlawful businesses e.g. prostitution, extortion, gambling and Bootleg liquor. To legitimate their illicitly gained money they utilised Laundromats as a mechanism to white their illegal money. The money laundering as a technique for legitimising the proceed of crime is consider to be triggered by Al Capone Laundromats. [11]

The term “Money laundering” is an old crime but it is rather new for the law enforcement agencies for its integration and the general understanding of this term. Interpol(2011) defines the term money laundering as *"money laundering involves an attempt to disguise or conceal the identity of proceeds obtained illegally in order to make them appear as if they have been obtained from legal sources*".[11]

International Monetary Fund (IMF) also accepts this definition. Which argues that *“money laundering is a process by which the illicit source of assets obtained or generated by criminal activity is concealed to obscure the link between funds and the original criminal activity”*(IMF 2011)[11]. Similarly to Interpol’s definition the term money laundering defines by Odeh (2010) “*money laundering as the process of accumulating the incomes of crime into the legitimate path of financial commerce by camouflaging its source and making illegitimate funds appear authentic*”. [11]

3.2 Stages of Money laundering

The traditional Money laundering is complex process which is usually achieved in the traditional scheme of the three stages. [12]

The illegal money or profit is placed on first stage (placement), which facilitates the physical infiltration of cash (derived from illicit source), into the financial systems. This cash is then converted into book money (primary and secondary deposit) this is followed finally by a layering process (illegal fund's stacking). These sophisticated actions are taken to hide the source of the illicit money by developing complex financing transactions between different states and piling up several layers of dealings. Parking and reintegration of this illegal money which shows no link with illicit sources and later converted into outwardly assets make up the third stage by investments in an industrial enterprises, business and tourism projects.[13]

Three stages involved in money laundering are placement, layering and integration as shown in figure 3.

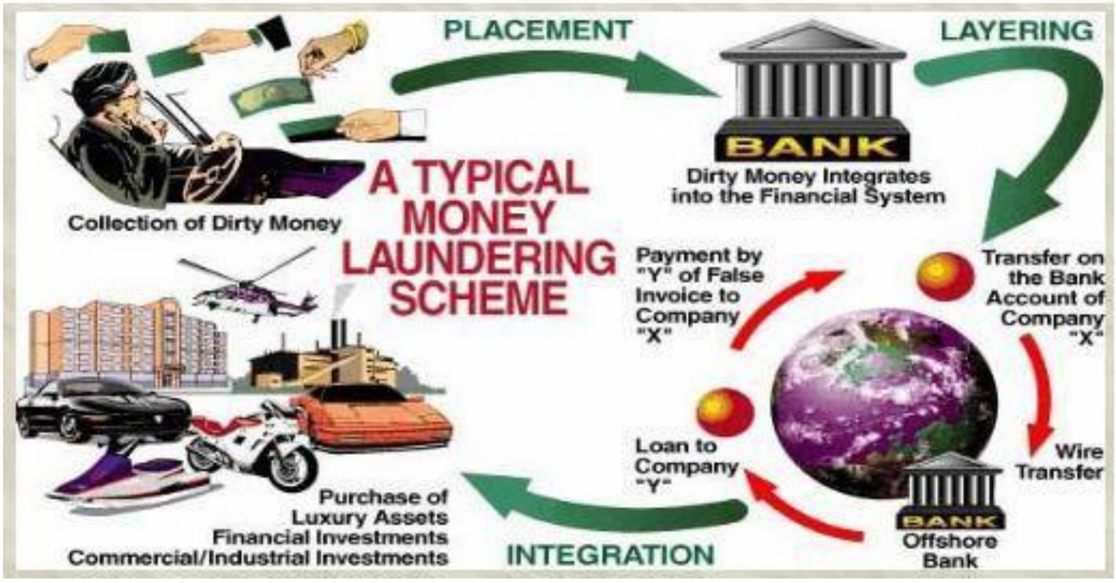

PLACEMENT
LAYERING
BANK
Dirty Money Integrates into the Financial System
Collection of Dirty Money
A TYPICAL MONEY LAUNDERING SCHEME
Payment by "Y" of False Invoice to Company "X"
Transfer on the Bank Account of Company "X"
Wire Transfer
Loan to Company "Y"
BANK
Offshore Bank
Purchase of Luxury Assets
Financial Investments
Commercial/Industrial Investments
INTEGRATION

Figure 3. Stages of money Laundering [14]

3.2.1 Placement

In money laundering "placement" is the first stage where the money gained from criminal activities is entered into the financial system. For money launderers, this is very critical stage as it allows them to hide their dirty money with the clean funds to create an aura of legitimacy .[15]

Example of placement include

- Deposit into bank account by using ATMs, tellers or night deposits
- changing the currency by other financial tools such as banker’s drafts, cashier’s checks or other negotiable instruments
- Small currency notes exchange for large notes/bills
- Shipping or smuggling cash outside from the country. [15]

3.2.2 Layering

- In the money laundering process the second stage is layering where money launderer made efforts to hide the origin of illicit money source by using multiple financial transactions layers.[15] Example of layering include
- Transfer of funds to different offshore or onshore bank accounts
- Complex financial transactions are being created.
- Borrowing and loans on the basis of both non-financial and financial assets
- Letters of credits, financial instruments and Bank Guarantees etc.
- By Investments and investment schemes
- Insurance products. [15]

3.2.3 Integration

The third stage in the money laundering process is integration .Which involves the process of successfully cleaning the illicit funds that become visible legally originated funds in financial systems and accessible for the direct investment, expenditure or saving **. [16]**

- Debit and Credit cards
- Consultants
- Sales and purchase of assets
- Business recycling
- Export and Import transactions .[16]

3.3 Traditional Money Laundering Techniques to avoid criminal Persecutions:

In this section, author describes what techniques money launderers should adopt to convert their illicit money into white money to avoid the criminal prosecutions. It will help us to understand how cyber space changed the traditional way of Money laundering into Cyber laundering. Which author describes in upcoming chapters in more details.

3.3.1 Purchasing of Goods: -

In this method of money laundering the money launderers with their illicit money buy the products with the high retails value and sell them to justify the source of their income. Reuter & Truman states that "Fine *art and other valuable items such as rare stamps are attractive for laundering purposes because false certificates of sale can be produced, or phony reproductions of masterpieces purchased*" .[17]

3.3.2 Cash Smuggling

The process of cash smuggling means physically taking money from one country and move into other country. Normally money is transferred into such countries which have less or no control over laundering. This motive is to remain undetected for moving such large amount of money and to hide the sources from where the money acquired from. [17]

EU Commission on 21 December 2016 purposed to extend the already existing controls any cash equivalent or excess than 10,000 Euros leaving or entering in European Union are subject to declaration .[18]

If you are caught with undeclared money over a certain amount on your person or hide within the cargo, then you will be prosecuted. It is not essential you will be prosecuted for money laundering offences because it cannot be proved by simply moving money across the borders. Money would still be confiscated in such type of scenario without any possibility to return to the carrier. It is commonly said that criminal organisations have gone as far as to purchase export or shipping business so they can conceal money inside the Cargo and even inside the goods themselves. The other method for transferring money abroad is by using the postal services. Reuter and Truman states that *"US customs officials spend most of their resources inspecting people and cargo coming into the United States, so it is relatively easy to ship currency to another country"* .[17]

3.3.3 Gambling: Casino, Lotteries and Horse Racing

-Casino In Casino dirty money can be utilized for gambling and winning in return would be seen as the product of a win rather than a criminal activity. Robinson states that "*At least in principle, all you have to do is stroll into a casino, buy $1,000worth of chips, play for a few hours, cash out and tell your bank manager that you won the $50,000 and now you want to deposit. Of course, you might have to substantiate such a boast".*[17]

But in this process, there are chances of financial losses because all bets placed may not be successful. However, such moves could be the cost of getting that illicit money converted into white cash which can be use freely without any criminal detection .Launder money (Dirty money) in casino can be used in this way as well by buying casino Chips by pretending that those chips would be played on the casino table. These chips however could be hold back and then later can be converted into cash. This cash could be taken in the form of cheque, or a deposit into the bank account. Such dirty money will be look like winning prize paid by the casino. But nowadays casinos are quite wise to identify and detect laundering related activities. If some person plays in casino with large sum of money, his activities could be taken as doubtful and should be requested to fill out the form as explanation about the source of money. If casino is not satisfied from the fill up form details they can deny to do gambling by using this money. [17]

-Lotteries The launderers will trace down the winning lottery ticket holder and buy it more than slightly it worth. The winner will get more money than that he won and this deal create legal grounds for the origin of bad money derived from Laundering. The launderers will become liable to pay Tax on this money. But again, this small cost is nothing in front of gain by legitimizing the black money. [17]

-**Horse Racing**: This is again same like lottery as mentioned above. The winning ticket is purchased at higher price than the real winning price its worth of and later the launderer cashes in the winning ticket. According to Reuter and Truman (2004) this process appeal the genuine winner more as it helps them to avoid from tax liability. [17]

3.3.4 Insurance policies

In this Laundering method, the launderers buy insurance policies simply to legitimize dirty money. In this process, Money launderers pay for the insurance policy directly all in one transaction instead of “payment plan” where policies can be purchase on a monthly or yearly basis. A vast majority of money invested is returned to the policy holder at the time of cancellation of policy. Cancellation after 14 days may be subject to the cancellation fee. In return the bulk being received with it source of origin as a token of legitimization of dirty money but may be with some cancellation fee as loss. [17]

3.3.5 Securities

In this method, the launderers buy the security with their dirty money and simply they can further sell them on or they can invest on low priced shares. Later they can influence the markets to sell the securities on higher prices to create a legitimate source for the money origin. Mathers states that "*Manipulating the price of securities is very attractive to criminals because there is so much potential profit*". [17]

3.3.6 Hawala

Hawala is kind of local money transfer system which is based on the mutual trust between the parties to the agreement. In Hawala the money is made available internationally without moving it or leaving the transactional record. In this Money transfer system three people involved. The client who wanted to send money abroad, the hawaldar is a person for providing the services of remittance and the hawala agent in the destination country who offer the services of delivery[19]. Hawala system is in practical use in most of Middle Eastern and South Asian societies and it is not strange for other societies. For instance, in China it is known as 'Fe chi' en, in Cameroon it is commonly known as cooperative. Hawala system can be linked to the most popular money transfer system such as western Union .[19]

Author personally used Hawala system while working in London, UK. Which in Pakistani/Indian language called as “Hundi” and it was cheapest way to send money abroad. According to author’s personal experience it has very easy procedure to send money without any transactional record or any strong identification for personal information. Just simply have to tell your name and the name of receiver in Pakistan. The receiver in Pakistan which was in most of cases was author’s brother can collect the money by showing his Pakistani ID card. According to author knowledge their source of income depends upon the currency conversion rates from UK pounds into Pakistani Rupees (UK Pounds: As author used this method in UK). Which usually slightly lower than the local banking currency conversion rates. In author’s view this medium can be best used for money laundering purposes without any currency transactional record and without particle information of sender and hard for the government to crack down as they used non banking channels.

3.3.7 Shell companies

The purpose of Shell Company is to facilitate the layering of illegal funds. In most cases, they are offshore based with the bank account to aid the layering of the funds. They are used as an acting platform for the business transactions without any significant assets and less operations capabilities [19]. They are not illegal in themselves they may have legitimate business purposes. A classic example of shell corporations with money laundering involves the real estate market. The real state can be bought from the illicit money and later can then be resold with an insignificant sum to the owner of Shell Corporation [19]. This purchased real state later resold to a third party with the value it was originally bought for. But now-a-day's trend is changing after the invention of internet as it is getting easy for shell companies to set up on the internet as it takes only few clicks of the mouse .[19]

3.4 Wire Transfer: - A Process of Shifting from Hard Cash Systems.

With the technology advancement Between 1970s and 1980s, wire transfers originated by banking institutions which sought the luxury and convenience of sifting funds without physically cash handle. On the customer request the transfer of electronic funds from his bank account to a beneficiary bank account which is in most of cases another bank is referred as wire transfer.[20]

Due to the electronic nature of transferred funds only the actual value of the funds is transferred. Wire transfers in the past were affected by cable and nowadays banks can do it electronically. The famous techniques for the electronically transferring of funds are possible through electronic funds messaging service called as "Society for Worldwide Interbank Financial Telecommunication" (SWIFT)[20]. Primarily the SWIFT is used to process significantly high transactions for example in the USA it processes credit payment up to $2million and in South Africa is about R5 million. It is also used to debit transfer in the US up to $100000 and in South Africa up to R500000.[20]

3.4.1 The problems with wire transfers

Money launderers utilize the loophole in the SWIFT messaging system for their own benefits. Banks are generally insisting to fill out certain mandatory fields on the form with the basic information of the requesting person such as the account number, name and address of requesting person and details of beneficiary. Here lies the problem if the mandatory fields are not populated the wire transfer will be rejected. [20]

The mandatory fields should be filled in with any type of character; the wire transfer would be successful. This action benefits the money laundering by providing the false information. In many instances the incomplete or poorly verification of data which is in process, thereby maddening the law enforcement agencies work. The situation become more deteriorating by the fact that many countries still not have reached the acceptable standard of compliance in terms of recommendations 10 (record keeping) and 11 (unusual transactions) of 40 recommendations of the FATF (Financial action task force).[20]

3.4.2 A Bridge between cyber laundering and Wire transfer

In each individual country, the available mechanisms to regulate the illicitly financial dealings are ultimately decisive. The FATF because of this reason was established in 1989. Various countries inherent several distinct problems and challenges which are stumbling blocks in the creation of a comprehensive and tough anti-money laundering regime. The strong privacy rights in most of democratic countries benefits the money launderers to utilize to circumvent the reporting and information requirements stipulated by numerous AML laws [20]. Wire transfer in this respect bears a great resemblance to cyber laundering because they have same challenges. The only difference is that cyber laundering is causing much greater damage than the wire transfers. The rapid growth of technology and the internet in most underdeveloped countries, the money launderers who was using wire transfer as a medium now upgraded to the channel of cyber laundering .[20]

In next chapter before moving to Cyber laundering we will review about the E-money or E-currency as trends are changing economy is getting more digital. E –money is replacing the traditional paper money due to use of e-commerce business Credit/Debits cards, PayPal payments.

4 Electronic Money and possibilities of E-Cyber laundering: -

The sole purpose of this chapter is to understand E-Money as cyber laundering execution in cyberspace and future payments systems depends upon E-money. The involvement of electronic money in money laundering process is called cyber laundering which concerns the transfer of illicit funds by using internet tools and stored value cards into legitimate funds [23]. Birch and McEvoy states that "*By its decentralized, distributive nature, electronic money has the same potential for transforming economic structure as personal computers did for overhauling management and communications structure*".[21]

With the emergence of new financial system allows the economic value to be represented digitally by electronic patterns. It is possible to exchange the electronic money or e-money over the internet or by the use of smart cards. [21]

4.1 Electronic Money

E-money, unlike stored value cards, can be exchanged immediately by simple online transactions between two online parties without the need of any external help. The ultimate goal of the E-money to have same functions just like paper money without any associated risks, cost handling, inconvenience, administrative issues and protection like conventional currency .[21]

With the technological advancement and continue developing phase in real life many threats is also evolving for and by E-money as it is introduced as the latest method of exchange value[21].

But governments should be ready to tackle all threats associated with E-money by novel way. In United States 90% of all transactions done by computer based Fed wire and Clearing House Interbank Payments Systems in terms of dollars exchanged (CHIPS). These payments systems are mainly used by large financial institutions .[21]

E-money is not similar like the deposit or printed money. The payment limitations are restricted to the sum which is stored in the electronic device. The electronic money has the following specific characteristics.

1) In contrary to other payment instruments, E-money has less transactional cost. Because it can be transacted electronically (Data) without any physical involvement as it happens in printed money .[22]

2) Higher fixed cost for modern IT systems comparatively with other payment instruments. As it involved gradually renewing and upgrading of IT systems with the latest technological innovations .[22]

3) E-money itself has no value if it is not used for transactional purposes. Contrary to E-money the other payments instruments can be used as a banking deposit .[22]

4) E-money is less transparent, while the other payment instruments for example credit card contains the name and verification number of card holders [22].

5) Circulation currencies can be substituted by E-money but still it has very low influence .[22]

6) Strong cryptography for E money ensures the privacy and prevents the fraud .[21]

The transaction process for E-money is different than the other payment instruments, regarding the E-money specific characteristics as can be seen in figure 4.[22]

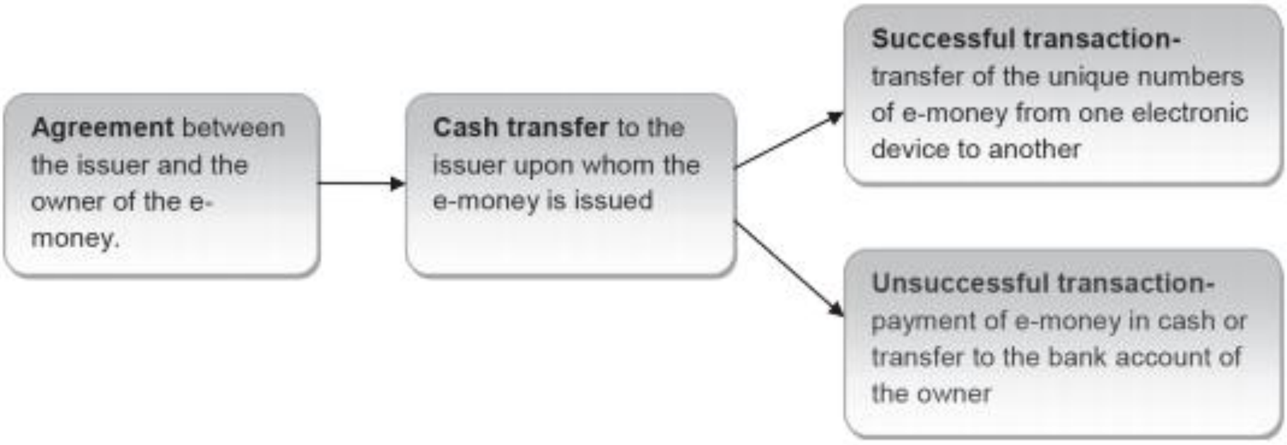

Agreement between the issuer and the owner of the e-money.
Cash transfer to the issuer upon whom the e-money is issued
Successful transaction- transfer of the unique numbers of e-money from one electronic device to another
Unsuccessful transaction- payment of e-money in cash or transfer to the bank account of the owner

Figure (4) Process of transaction with E-Money.[22]

The numbers of transactions are higher in developed world, with the largest contribution in the globalization of the financial system. Nowaday even for small payments E-money is often used either in the virtual world or among retailers .[22]

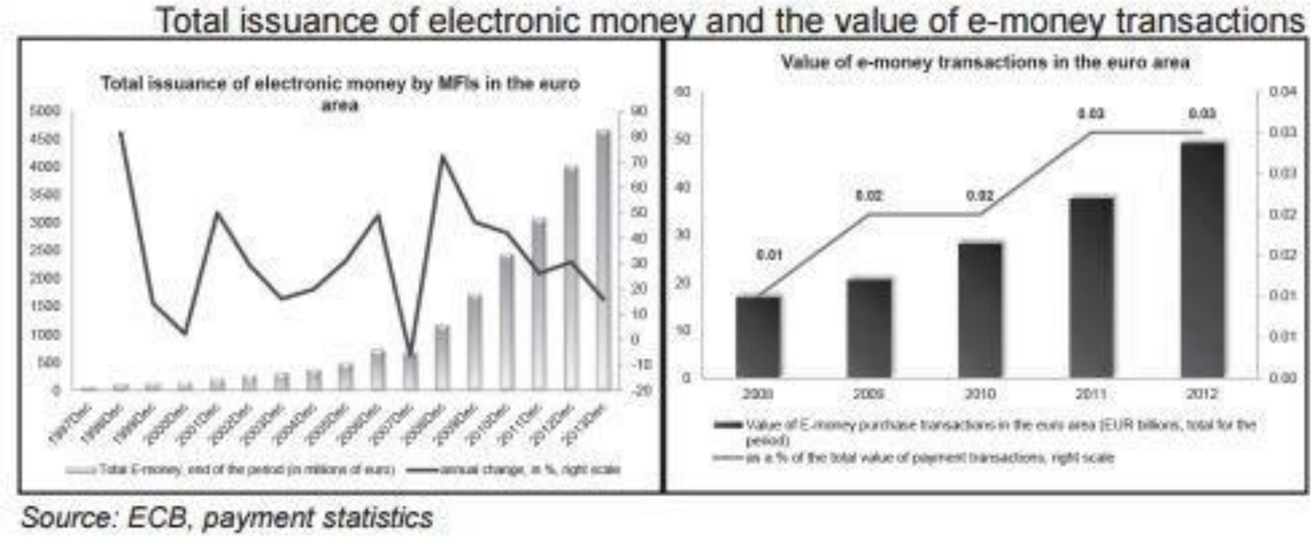
4.2 E-money usage in European countries: -

In modern banking systems E-money is becoming very important part. The factors that Influence the development of E-money has global characters (Internet, new technological advancement related to information communication) and all others depend upon in one country developing conditions. On national level the factors are: Country development level (influencing the buying power and living standard of people), the capability of nations to adopt technological innovations, the regulatory systems, market development, the potential of integration in the financial markets and global economic .[22]

Hence it is realistic to assume that E-money transactions first have been registered in the developed countries such as European Union and in other countries of European region (less developed). Electronic banking is still in its early phase and it is not yet accepted by the people and institutions .[22]

-E-Money in European countries.

According to ECB statistical data the card based E-Money started in 1998.From 2008-2011 E-Money had the highest increase of circulation as can be seen from chart below .[22]


Total issuance of electronic money and the value of e-money transactions

Source: ECB, payment statistics

Figure 4.1 E-Money transaction chat.[22].

In European countries by comparing with other instruments of payment system, we can draw a very clear picture. For example, the transaction by debit/credit card account is around 40% for the total payments of transactions in comparisons with the E-Money transactions which are very low as can be seen in figure 4.2. In Euro area, the E-Money total share number of transactions of the payment system was only 2.33% which was slightly better than previous years e.g. 1.35% in 2008 and 1.70% in 2010. According to European central bank statistical data for each European country, the highest number of E-money transaction was registered in 2008.[22]

This highest ratio of transaction was mostly due to transactions in Luxembourg. PayPal which is the most powerful electronic company also moved it’s headquarter into Luxembourg from the Great Britain in 2007. PayPal became accessible on internet pages from anywhere after gaining new licence. Before it was only possible through the internet pages in Great Britain [22]. The highest number of E-Money transitions according to analysis was registered in the Germany, Czech Republic, Luxembourg, Italy, Holland and Belgium. But still the transactions conducted methods were different .[22]

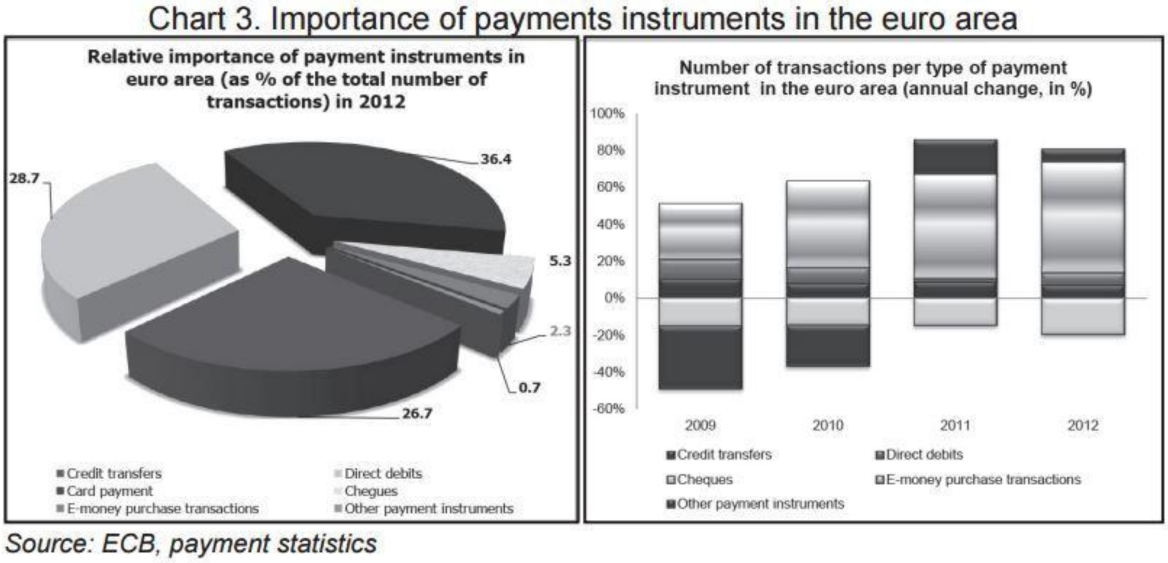


Chart 3. Importance of payments instruments in the euro area

Relative importance of payment instruments in euro area (as % of the total number of transactions) in 2012

Number of transactions per type of payment instrument in the euro area (annual change, in %)

Source: ECB, payment statistics

Figure 4.2 Payment instrument in Euro Area. [22]

4.3 E-Money features which attracts the cyber launderers

E-money system very attractive for money launderers [21] due to two factors: un-traceability and mobility.

-Un-traceability

The adoption of E-money systems will involve less face-to-face financial transactions. E-money feature of anonymity will make much more difficult "Knowing your customer". In

E-Money system there is possibility for the two parties to deal with each other directly for the financial based transactions without any help of a regulated financial institution. Thus, therefore wouldn’t be any possibility of traditional audit trail. [21]

-Mobility

E-Money hypothetically could be receiving and send from anywhere in the world. Thus, we can say that E-money system can transfer funds over network instantaneously without any subject to jurisdictional restrictions. [21]

The main purpose of this chapter is to understand the E-Money which is soul of digital economy and E banking systems and how it is revolutionizing the money launderings techniques in cyberspace.

5 Cyber laundering

Cyber laundering can be defined as a system in which the mechanism of internet is used to hide the illicit funds derived from illegal activities in order to make such funds less suspicious and less traceable to law enforcement agencies .[20]

Nick Kochan states that “Cyber laundering as the potential for easy and convenient laundering through e-auctions, online casinos, and telemarketing is all too real to ignore. The lack of a paper trail and government control makes this channel a tempting one for the goons to abuse, as they do”.[24]

Countries like Canada and USA have advance level of check and balance but still numbers of countries are lack in infrastructure to monitor and control the cyber laundering and legislations to apprehend the criminals are still weak .[24]

5.1 Stages of process of Cyber laundering

Three stages are involved in the cyber laundering process in contrast with its super set that is money laundering. These three stages are placement, layering and integrity. Which are explained below. [24]

5.1.1 Placement

Placement is the stage where cyber laundering benefits from the anonymity of transactions on cyberspace and e-cash [25]**.** As transaction, will take place on cyberspace without any face to face interaction and physical contact. This let them undetected and helps to avoid from the strict reporting requirements as imposed by traditional financial institutions. [25]

5.1.2 Layering

It is the stage where the advantages of internet and its unique features make it truly distinguish from traditional layering [25]. Internet provides opportunity to the launderer to easily locate the online institute such as gambling sites that let them to register for active account without any documentary identification and physical verification. In such circumstances, for law enforcement agencies it becomes harder to locate such account that are operated by cyber launderers[25]. Furthermore cyberspace provides opportunity to cyber launderer to transfer funds any part of the world by simple online click. It is particularly difficult to track down online bank transfers if it is executed by the use of hidden IPs etc. Deeper infiltration of "Dirty money" into the international banking system, make it more difficult to identify the origin. [25]

5.1.3 Integrations

Cyber laundering makes easy the integration process. For instance, a launderer could set up online gambling website and transfer all illicit funds and mix it with the legally originated funds from the site [25]. For investigation authorities to track the audit trail of profit will appear as legitimate funds. Other method for the integration are purchasing online with the help of the offshore banks issued debit cards, offshore companies provided fake loans or can utilize traditional integration methods of buying online the high value assets such as real estate .[25]

5.2 The key factors of cyberspace which attracts the Cyber launderers

Following are the key factors which attracts the cyber launderers are as follows: -

5.2.1 No face to face contacts

No Face to face contacts is called as depersonalize of financial operations. To access available online financial services we connects the bank server by using only our Computer (software included). In this whole process of placing order (making request) and execution of this order will take place automatically without the involvement of a human factor. So, we can visit the bank on cyberspace by simply pretending someone else each time because bank or financial institution server only checks log in ID (Unique ID numbers) and the selected password not the customer true identity .[26]

After matching the password and login ID with the data which already stored in server's memory grant us the bank services online. In the result, it would be hard to detect and block transactions which deemed related to cyber laundering activities and also prevent other potential source of reporting to the Employees from financial institution .[26]

5.2.2 Speed of Transactions.

Contrary to old fashioned transactions in money laundering process, the new payment technologies allow the funds to transfer more rapidly on far distances as can be seen from the figure 5.1 and further will be discussed in next chapters too. It also makes more difficult for the state investigation agencies to track down such transactions[26]. Few of them are instant e.g. within one financial institutions. It makes easy for launderers to move funds online more swiftly within in country or any part of the world. In simple words, it makes possible for illicit money to be hide easily and difficult to trace. [26]

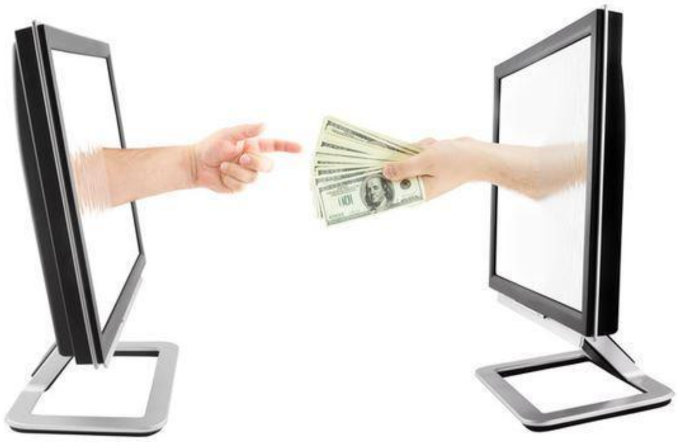


Figure 5. Speed transactions using new payments technologies .[27]

5.2.3 Anonymity

By utilizing the unique internet feature of anonymity anyone can hide himself among other millions internet users. It is easy to be pretended someone else over internet (cyberspace) since it is hard to recognize from our true identity. But it seems that it would not long lasting as there are certain legal obligations related with the internet service providers to keep record of all log files for certain time limits[26]. That’s shows which computer at what time is connected with the internet. These moves are being taken to prevent the cyber related crimes. Such actions make easy for the law enforcement to trace some particular person’s activities in cyberspace. Of course, still there are some ways to circumvent them or keep the status of anonymity. These includes by spoofing IP (internet protocol), wireless fidelity technology which allow to abuse the internet services for public called as "hot spot”, or by using the unprotected routers to connect to internet, and by using the prepaid phones as a modem for internet connections (which help to hide the identity). Also by using the encryption technology (usually available on internet) and many proxy servers that hinder the law enforcement efforts to apprehend the cyber criminals. [26]

5.3 Vulnerable businesses and Techniques for cyber laundering.

Following techniques are adopted by cyber launderers to make their illicit funds legitimate and their actions make vulnerable following business as mentioned below.

5.3.1 Internet Banking.

Internet banking revolutionized the old banking system and makes us enable to transfer a large sum of money by single click without involvement of any person to person interaction. Gosling states that "*But with the growth of electronic commerce, in which transactions can be conducted without the involvement of banks, the potential for cyber laundering is much greater*" . [17]

One of the drawbacks in the internet banking is that cyber launderers or likeminded offenders can set up account with little personal information, which helps to protect their identity and make new one. By transferring small amount of money into that account, the cyber launderers thus avoid the suspicion from the banking authorities and therefore they don’t question about the origin of money. Once the money is entered within that account then the cyber launderers can transfer money out into offshore accounts or to somewhere else which is out of control of authorities involved and this is quick and easy process. Funds can be transferred at single click of a mouse and launderers transfer this money into those areas where there is no strict regulation regime for laundering money. Kochan states that "*Internet banking is plagued by sloppy security*" . [17]

A hypothetical scenario in which cyber launderer Operates using online banking.

[(Note: The hypothetical scenario is created by author based on the idea derived from the paper with reference [20])]. Mr Imam is living in Pakistan with fraudulent background. He is running fake orphan donation website online (www.donateorphan.pk) among several other illegal activities which includes smuggling, narcotics and illegal weapons business etc. He also holds one online special bank account with AL-Habib bank Islamabad in Pakistan under the name “help orphans” to support his orphan organization. Due to government strong crackdown on illicit derived money and taxable money Mr Imran wanted to legalize his illicit money by mixing into legal derived funds to make them legal. Mr Bilal **(smurf[1])** on other hand is man with expert level skills for internet but unemployed with financial constraints and looking for job. Mr Imran approaches Mr Bilal to help him and in return take cash in hand. Both entered in a deal. Mr Imran then deposits some portion of illicit funds in his saving account in Pak-Bank (Placement). With the rest of funds Mr Imran top up several smartcards 2 and gift cards at different times. He give several of them to Mr Bilal (smurf) with the instructions to visit his orphan house and to make deposit in “help orphan” bank account with different identities as well as in his personal account at strategic interval (Layering). Mr Bilal performed all these actions by using online banking system of Pak-Bank. Note:-The work of smurf can be performed by Mr Bilal himself and as well can be performed by others acting as smurf.

5.3.2 Digital Cash/Electronic Cash (E-Cash)

Other than Credit/Debit cards there are many other online payment services available on the internet known as Digital cash or sometimes electronic cash. The launderers can use the facility of internet payment system by feeding money into these accounts and convert them into E-Cash. The amount is deposited into small amount to avoid the suspicion from bank authorities’. Once the amount is entered in the digital systems, the launderers can transfer anywhere effortlessly including overseas into jurisdictions with less strict anti-money laundering laws. This E-cash system is very well suited to money launderers because of anonymity it provides to those who use it. Denning& Baugh states that "*Some methods allow users to make transactions with complete anonymity; others allow traceability under exigent circumstances, for example, a court order*".[17]

[1] Smurf is the famous method adopted by the Money launderer to launder cash in the placement stage. In this techniques many individuals (the “smurf") involves ,who exchange the illicit funds into highly liquid items which includes bank drafts travellers cheques or deposited directly into saving accounts .Such instruments then handover to the launderers who then begins the layering stages. For example in less than two weeks ten smurfs could place $1 million into financial institutions [32].

[2] Appearance wise smart card looks same like a credit card. The owner of smart card can top up with electronic money from any bank, vending machines, Automated Teller Machines, Personal computer or through a specially equipped telephone. Once smart card is loaded with the e-cash/money it can be used for purchasing over the internet or through other communication devices [20].

5.3.2 Online Gambling

After the emergence of online gambling and online casinos cyberspace turned an ideal place to set up cyber laundering scam that wouldn’t now easily possible in real world casino due to the implementation of new tough regulations. Lilley states that "*These sites seek to replicate the experience of playing in a real casino – and just like the real world they aim to take as much money off you as possible.*[17]

For criminals the internet provides an environment where they can make fake identities to protect themselves and their money. It is very hard to monitor all criminal activities on internet in result a lot of internet crimes will go undetected. The launderers in similar way of physical casino can do gambling online thanks to the internet. Simply by log in on casinos online portal and deposit money into casino account. After depositing money into account, they place some non-risky and low value bets and then request their money back. The return of money into their bank account will legitimise the source of origin. [17]

Coates states that “*According to research, criminals can deposit money under a false name and wager an amount before withdrawing it from their account, or open a remote gambling account to store funds until they can be transferred into a legitimate account, pretending that they are winnings*”. [17]

Another issue with the online casino they not necessary stationed within the jurisdiction and laws of the relevant country in which they are being used (Providing online services). Therefore, country has less control over online casinos and therefore cannot monitor and trace the transactions. For example, in USA laws related to gambling and anti-money laundering are strict. But people can log in and play where the gaming rules and regulations are completely different than USA. NCIS states that “*The more important issue, however, is the development of offshore gaming sites – the on-line gambling business can base itself in the country with the lowest barriers to entry and weakest controls*” [17].

5.3.3 Online Auctions

Online Auctions are generally used for the selling and buying of different goods. Kochan states that "*Online auction houses such as eBay attract consumers and launderers because they are accessible and inexpensive*". [17]

The launderers can manipulate the websites like E-Bay by buying items of significantly high values. Later they can put up again for sale on an auction site and employ two falsify bidders for bidding wars. In result of this the items are usually sold on higher value so the launderers lost nothing financially and if authorities questioned about the money originated from, the launderers can claim it come from the sales of items online. It Cost very less to the launderers for setting up the account but can legitimised the dirty money. [17]

A hypothetical scenario in which cyber launderer use online auction website.

[(Note: The hypothetical scenario is created by author based on the idea derived from the paper with reference [20])].

Mr Anwar is weapon dealer from Kazakhstan. Other than smuggling of weapons he also do small business of selling and buying on auction websites(www.Gooddeal.com) to keep his legal business activities alive to avoid the law enforcement agencies scrutiny. He wanted to legalize his illicit funds which he derived from weapon smuggling.

On same website he interacted with Mr Lee who is Singaporean citizen and is smurf. Both entered into deal that Mr Lee buys a diamond necklace (Which could be real or fake as verification is sent by the buyer to online auction team which just provide platform for online auction) from an online bidding on the website www.GoodDeal.com.

Mr Akram Purchase's smart cards which he top up with the proceeds of his illegal earnings. He emails to Mr Lee the encryption of smart card which he decrypts and extracts the value in the smart card. Mr Akram at the decided time put the diamond necklace on the auction website for the bid. Mr Lee Bid highest for the diamond necklaces and in return sold to him. My Lee then deposit the money into the account of "GoodDeal" auction website. “GoodDeal” administrative authorities after necessary verification pay the money to Mr Akram which will provide him the ground to create source of income to legitimate his illicit funds. Note:-Mr Akram may use multiple smurfs.

5.4 Cyber Laundering techniques to support Terrorism

Cyberspace is used by the terrorist for money laundering to finance terrorist related activities. Arabinda Acharya (2009) states that “*cyber-laundering is about using the Internet and electronic cash to turn illegally obtained money into untraceable funds*”.[28]

E-cash is effective tools to launder money for the terrorist related activities. Al Qaeda famous leaders such as OSAMA bin Laden and Ayman al-Zawahiri used internet as a medium to post their radical ideologies to attract fellow terrorist in form of appeal for financial support. [28]

They used websites as medium for their hate speeches and financial motivations .The head of terrorist groups acknowledge the importance of cyberspace for the execution of money laundering. Terrorist network around the globe encourage all fellow radical jihadist and terrorism supporter to provide the material support for the growth of jihad. Osama bin Laden the founder and leader of Al Qaeda leader appealed in his messages from all Muslims as stated by Acharya to help "their brothers in Iraq with money and men"[28].

Many jihadist leader consider the financial contribution (by radical Muslims and terrorism supporter) as equal as the physical involvement in jihads operations. Many calls already have been for donations on internet. For example the terrorist group in Pakistan used the website as a medium to argues that as stated by Acharya "Allah gives an opportunity to take part in the struggle for Muslim rights – jihad". Acharya further states that "No doubt due to anti-West widespread politics such appeals for jihad donations can be assessed as extremely influential"[28].

The following factors on cyberspace such as anonymity, accessibility and ease of use, permits terrorist organization to avoid the dangers of conducting financial transaction through traditional channels. We can take Al Qaeda as an example to check how much terrorist organizations are successful in raising funds [29].

It is difficult to assume exactly that how much funds Al Qaeda raises every year. The estimated figure for 2004 is $30 million which is likely lower today. Not all funds certainly raised by AL Qaeda passed through the internet[29].

But the terrorist organization and their network of followers significantly relies on the internet and cyber laundering to distribute its wealth. We can say by adopting modern technologies the terrorist organizations are successful in maintaining their core financial stability[29].

5.5 Analytical view of cyber laundering for supporting Terrorism

In author's opinion there are several reasons which make Terrorist successful on cyberspace to acquire funds for their vicious activities.

1) Lack of coordination among the Law enforcement agencies and financial institutions to apprehend the cyber criminals (Involved in terrorist financial activities).

2) Soft punishments for financial institution who breaches the Money laundering rules and regulations. This help the network of terrorist groups to utilize these loopholes to attract the sympathizer to finance their terrorist activities either via cyber laundering or traditional laundering.

3) Lack of effective use of modern IT technologies to identify terrorist financial threats in cyberspace.

4) Lack of Government efficiency to identify and penetration ability into terrorist cyber financial network.

5) Lack of international coordination among the states to break vicious chain of cyber laundering for terrorism.

6) Deep religious radicalization of society provides stage to the terrorist organizations to attract the educated youth towards religious intolerance/terrorism. This brainwash youth can help the terrorist organizations to achieve their financial goals internationally (trigger the cyber laundering elements) by using social media, bloggers and other electronic communication channels.

7) Rival countries by using cyber laundering phenomena (Financing) can incite sectarian violence in other countries .For example in Islamic world Shia Sunni incidents.

8) Less strict rules and regulation by the government over the religious charities group and their possible international and domestic financial links .No scrutiny over their annual budgets, resources and the medium(Possible cyber laundering) they adopt to finance their activities could be link with the terrorism .

9) The limited jurisdictions power of financial institutions restricted their ability to tackle effectively the cyber laundering incidents as it is global vicious chain.

6 Cyber payment systems and its potential exploitation for money laundering

The transfer of value electronically the cyber payment systems act as an instrument. Such transfer takes place by using the cyberspace as medium or by the use of stored value smart type card. Cyber payment systems are designed to replace the cash for many retails and consumer level transactions. Cyber payment system also raises new challenges for the law enforcement agencies. These systems with the help of existence modern technology can combine the features such as current bank based wire transfer speeds and the currency anonymity together [30]. Such issues should be address as the objective for the development of such systems is to make ensure the detection and prevention against the money laundering and related unlawful transactions [30]. In simple words we can say that cyber payment systems represent the products of the intersections between the ongoing revolution in information technology and strong trends towards the market de-regulations that are taking place into the world of electronic commerce as can be seen in figure 6. [30]

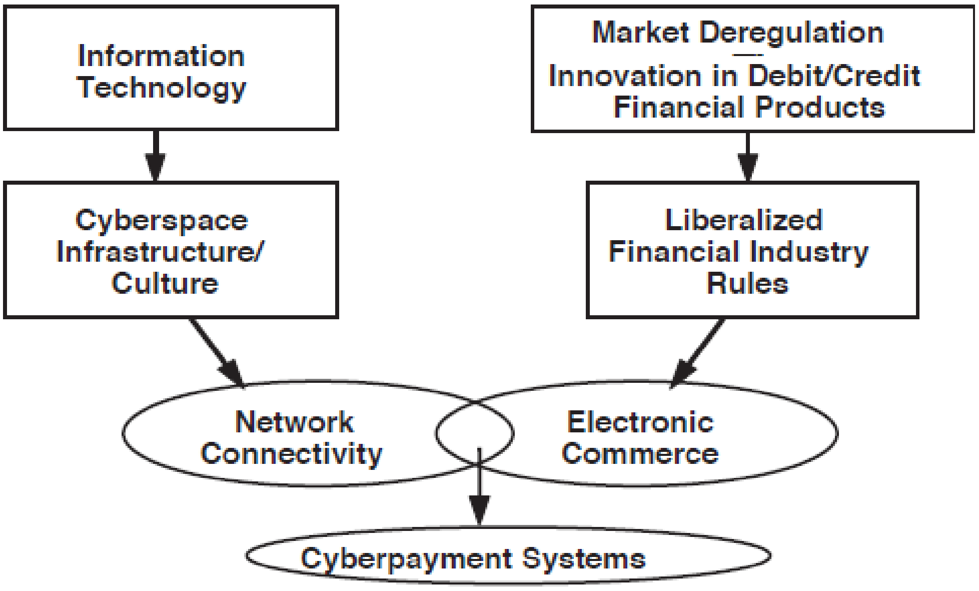

Information Technology
Market Deregulation
Innovation in Debit/Credit Financial Products
Cyberspace Infrastructure/ Culture
Liberalized Financial Industry Rules
Network Connectivity
Electronic Commerce
Cyberpayment Systems

Figure 6 Cyber payment systems and payment system dynamics. [30]

A broad range of cyber payment systems are currently under development. Two dominant standard types of systems are:-

1-Stored value smart cards

2-Internet based payment systems.[30]

6.1 Four model for Cyber Payment Systems

There are four basic examples of cyber payment systems which are stated below.

-The Merchant Issuer Model.

In this cyber payment system the issuer of smart card and good seller both are same. Example: - Tallinn/Tartu transport daily, weekly bus passes as shown in figure 6.1.[30]

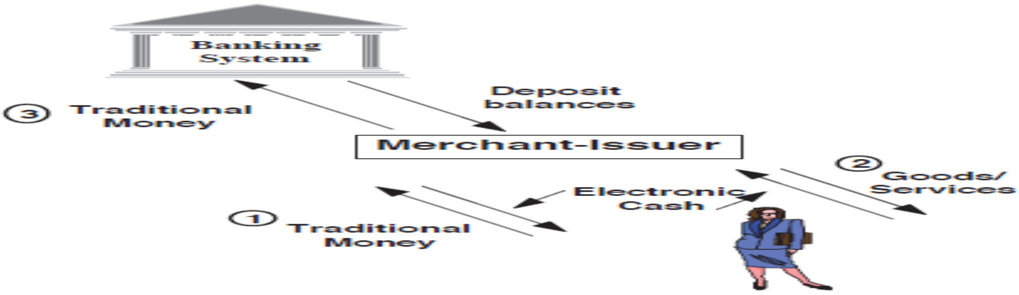


Figure 6.1 Merchant Issuer Models. [30]

-The Bank Issuer Model.

In this model the issuer of smart card and the merchant both are separate bodies and transactions are cleared by traditional financial systems. Example: - In Tallinn any debit/Credit card issued by SEB bank or Swedbank 6.2. [30]

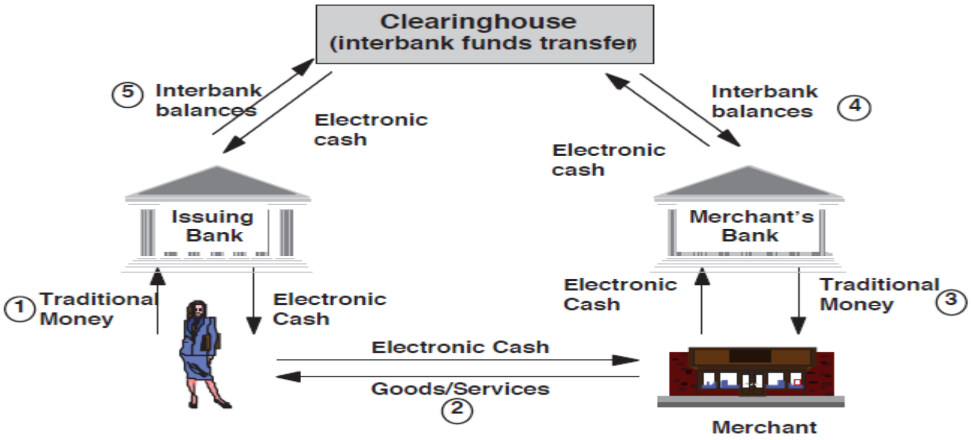


Figure 6.2 Bank Issuer model. [30]

-Non Bank Issuer Model:-

In this model the user with the help of traditional money buy the electronic cash from the issuer and can spend that e-cash only to certain merchants. Example:"Cyber Cash’s electronic coin product" as described in figure 6.3.[30]

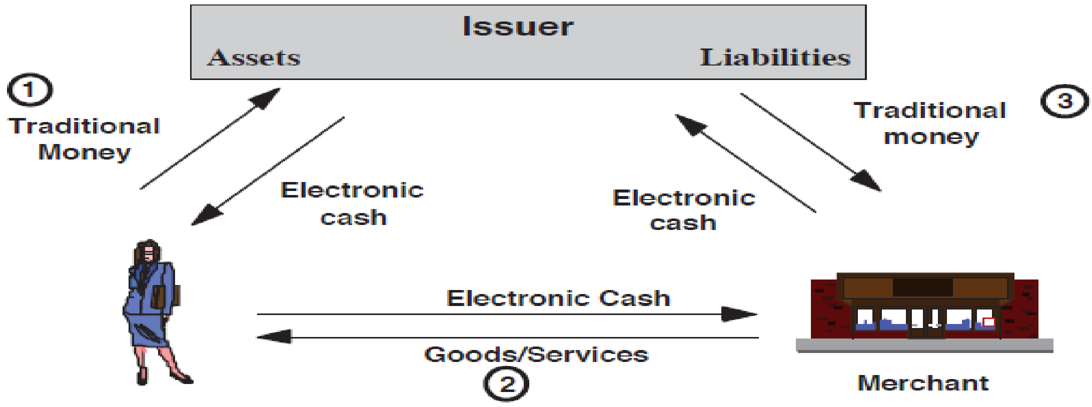


Figure 6.3 Non Bank Issuer Model.[30]

-Peer to peer model

In this model the user can transfer electronic cash among each other which is issued by bank or non bank:- Example :By the “*MONDEX stored value smart card*” peer-to-peer value transferred. [30]

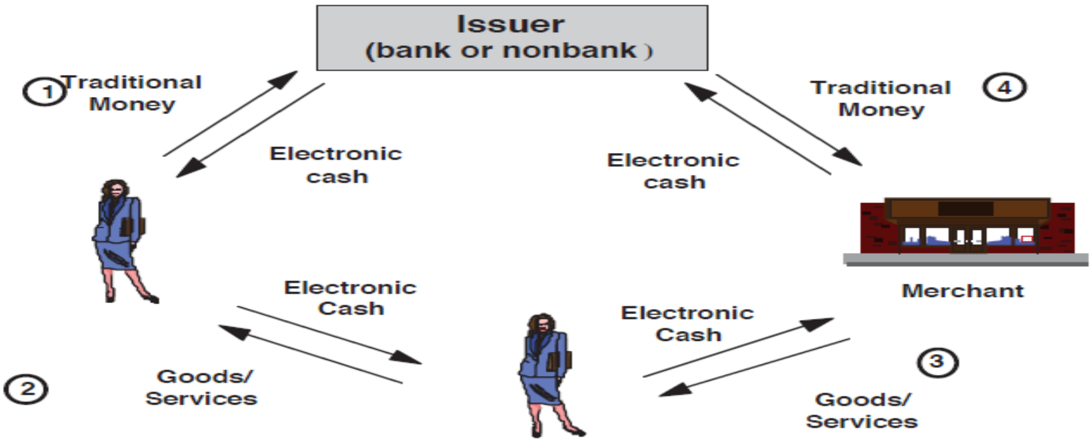


Figure 6.4 Peer to Peer model [30].

6.2 Cyber Payment Based Investigative Techniques To Identify Possible Cyber Laundering.

In cyber payment systems two emerging features create possibilities for the remote interrogation of transaction records. First: During the value transfer, generation of tags which means that the funds moved from one cyber payment instrument to another carried unique markers that reveal information regarding transactions. The second features lies in cyber payment networks on their integration with the open network standards featured within the TCP/IP internet protocol suite. The IP (Internet protocol) "tunneling"(Describe in detail below) technique make possible to segregate "value-transfers" from other internet traffic would make cyber payment enable to ensure the integrity of their links with consumers and also make easy for the government authorities to trace suspicious flows of funds linked with the drug trafficking and money laundering[30].

It is daunting challenge for the authorities to conduct any kind of surveillance of information flows over the internet due to huge volume of network traffic. Higher demanding Privacy strict policies by service users over internet involved in e-mail and electronic commerce also limit the acceptability of investigations into the contents of network messages. Keeping in view the privacy policies over internet , the law enforcement requests for the authorization of sensitive data records is difficult, but there is more possibility to make more acceptable to affected user communities if network traffic could be categorized or differentiated according to the nature of data as being transmitted. The data differentiation itself raises the questions of how unstructured network data is to be filtered and permitting for the capture of discrete types of data and for the other data for the secure transmission [30].

The difference value transfer from generalized internet traffic is potentially possible by IP Tunneling and then this value flow is subjecting to sophisticated network analysis and data mining techniques. A virtual network is created by IP Tunneling link within the Internet packet-switched network. In virtual network there are two points, initiating point and an end point. To measure the volume and nature of information flows these two points’ help to establish network audit and traffic analysis tools. In IP Tunnels the initiation and termination points are themselves IP (Internet Protocol) addresses as can be seen in figure 6.5.Because these addresses are dynamically (for customers to allocate the network connections by available addresses) allocated by many networks, available IP addresses subset would have to be set aside for value transfers alone[30].

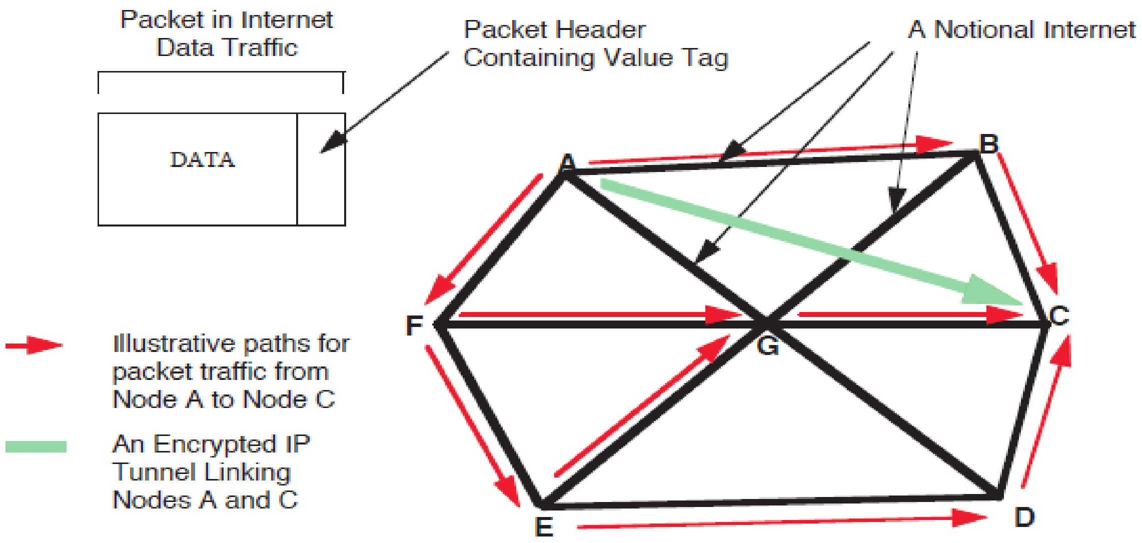

Packet in Internet Data Traffic
DATA
Packet Header Containing Value Tag
A Notional Internet
A
B
C
D
E
F
G
Illustrative paths for packet traffic from Node A to Node C
An Encrypted IP Tunnel Linking Nodes A and C

Figure 6.5 Application of IP Tunnelling Concept Applied to Cyber payment Systems [30].

The application which is designed for the cyber payment systems, a tag placed on a value transfer message would invoke a special protocol (termed as Cyber payment security protocol-CSP) with in TCP/IP that itself would create between two known IP addresses a virtual (and encrypted) link. The created IP Tunnel thus would act as the conduit within which the value transfers could be conducted. *"Servers would require maintaining logs of CSP-related network traffic using TCP/IP with the CSP functions built in .Such records would then made available by law enforcement and payment system authorities subject to judicial review"[30]*. The generation of "CSP Traffic Reports" would be the alternative to this requirement by the network operating system itself through an autonomous intelligent agent application. This application could record value by placing within servers in proximity to CSP-designated IP addresses and transfers and return the information to secure servers maintained by cyber payment oversight authorities. [30]

6.3 Positive & Negative factors related to cyber based payment

In author's opinion the following benefits (Positive) and negative factors are associated with the cyber based payments after reviewing various literatures.

-Positive Factors

1) Ease in running the business operations.
2) Low cost transactions boost the economic activities.
3) Provide multiple methods of payment.
4) Value transfer in E-money minimizes the burden of carrying huge traditional money.
5) Easy to make payments behind the jurisdiction limits. For example paying by SEB/Swedbank issued credit/Debit cards in another region like Asia.
6) It provides the direct transactions facility between two parties without involving the third party
7) It increases the trust among the business communities
8) Financial security against the theft (Bank cards or other smart card). In case of lost or misuse can be cancel or block by Phone/Email.
9) Providing tremendous Boost to E-commerce businesses across the globe. The present real life examples are E-Bay, Amazon and Alibaba (Aliexpress) and many more online retailers.
10) Cyber payment system provides inter-connection among different financial entities which help to maintain the financial momentum.

It also helps the owner of cyber payment products to maintain the record of each financial transaction (Debit/credit card bank statement) and it provides freedom to have control over it.

-Negative Factors

1. Possibility of identity theft (Cyber payments products) related to bank/ financial institutions customers.
2. Cyber launderers can exploit the cyber payment system for cyber laundering by adopting various techniques such as hacking, using fake ids and so on.

3. Expensive to keep up-to-date (With latest related technologies) and maintain the large infrastructure of Cyber payment systems.

4. Due to privacy concern the banks are reluctant to give the information of their customers to law enforcement agencies which could be dangerous for the society.

5. Millions of transactions done every day it is hard to monitor or investigate each of them unless found any particular very suspicious transaction.

6. Possibility of Misuse of cyber payments products such as Debit/credits cards by criminals for online payments from steal information gathered from numerous online websites or from other sources for example by hacking. Such incidents are very common in western world.

7. No restrictions that only owner of Debit/Credit (Cyber payment products) card can take out or deposit cash in ATM or paying online. This initiates the criminals to take advantage for their financial gain.

In next chapter we will discuss what the different institutions are doing to prevent the cyber laundering.

7 Organizational role in efforts to prevent the cyber laundering

In this chapter we will over look what different institutions are doing to prevent the cyber laundering and how they are combating with the techniques used by cyber launderer for the electronically launder funds. The exploitation of electronic banking vulnerabilities by Cyber launderers can be confronted by developing an encryption key recovery program. All the public keys in this programme used by the electronic banks will be shared as per the regulations that will be set by the federal government and to view the decrypted transactions required the private key by the programme that will be designed by the joint efforts of professional of encryption and information security equipment vendors.[24]

The digital signature should be required by each transaction that should hold the user identification, the amount of transactions including the location of teller machine where it was used and with the date/time stamp. To tackle the technology related frauds and possibility of Cyber laundering related incidents this should be the minimum requirements to be embedded in the smart cards and the teller machines daily reporting.[24]

To set up a pattern of similar transactions into one or more account the Neural Computing and Artificial intelligence such as PRISM®Money Laundering Detection(MLD) can be used to form a universal group number (UGN) of that smart card which are used in one or number of the teller machine to transfer funds. The IP-Address should be used to locate the place where the creation of the electronic banking account taking place in case of same transaction over the internet. In any investigation related to cyber laundering this would be helpful for the law enforcement. [24]

The regulation of Domain Naming System is one of the serious issues to implement any such solution to fight against the cyber laundering. The ISP providers in return of high value packages provide the facility of hidden websites address .An audit is required to investigate any discrepancies from the ISPs. [24]

7.1 Current AML measures and Cyber Laundering:-

The preventive measures related to AML can be quickly summarized as follows. We will discuss two provisions one is reporting and other is record keeping. "*The Bank secrecy act is the model legislation for all financial institutions requires reporting all transactions above the value of $10,000".*[20]

It is also required for a period up to 5 years the financial institutions to maintain records of all transactions after such transaction have been concluded. To assist the law enforcement authorities for investigations and prosecutions for cyber related crimes most of telecommunication services and internet service providers are required to monitor and maintain the user data for a period up to one year .[20]

The requirements such as reporting and recording are suitable for certain kind of tangible or physical transactions but they are not ultimate solutions to the problem of cyberlaundering. These measures are nothing in front of cyberlaundering dilemma. Following are the main reasons behind these facts. Firstly for the online transactions by virtue of its nature one should not be physically present at the relevant place or site where such transactions conducted. This reveals the issue of anonymity. [20]

While the problem here is not this either certain ISPs including some online financial institutions meets the requirement of reporting and recording but the issues are related with the information provided by the customers or users is viable or true which are stored by ISP's. It is also problematic to enforce the "Know Your Customer (KYC) principle directly due to this reason. Secondly due to rapid advancement in terms of speed at which internet operates make it highly unlikely to leave trails behind (especially for hackers) which are evident in certain online transactions. Due to the intangible nature of internet it makes the internet users enable to avoid certain steps and process which normally required. To monitor the transactions closely by the law enforcement agencies become difficult in result. Other things one should remember over internet million of transactions are conducted in per second which is technically difficult with respect to maintaining and closely scrutinizing each transaction .[20]

Cyberspace is also constantly exposed to different threats of viruses and malware with the destructive capabilities. These viruses and malware mostly are designed to steal data and hide or conceal data to make inaccessible for others. Certain viruses are so capable they even shut down the websites completely.[20]

In presence of all these dangers that is due to the nature and numerous features of the internet, it is extremely difficult for the effective implementation of the reporting and recordkeeping requirements as preventive solutions to cyber laundering. [20]

7.2 Efforts by Anti-Money Laundering Agencies

To fight against the evil of money laundering several enforcement measures in respect to the general AML regime have been put in place by certain agencies and institutions. General AML regime measures are not capable to specifically deal with the issue of cyber laundering as it has not been really put into perspective. Many government and financial organizations have adopted some measures which are initial move towards fighting cyber laundering. In this section we will discuss about these government agencies and financial organizations and how they are tackling with the emerging challenges related to cyber laundering. [20]

7.2.1 Federal bureau of investigation:-

FBI set up nine goals according to its "National Money Laundering Strategy 2007" to counter the money laundering related issues; these goals are as follow .[24]

National Money Laundering strategy 2007 states that these goals are *" Continue to safeguard The Banking System, Enhance Financial Transparency In Money Services Business, Stem The Flow Of Illicit Bulk Cash Out Of The united Sates, Attack Trade-Based Money Laundering At Home And Abroad, Promote Transparency In The Ownership Of Legal Entities, Examine Anti-Money Laundering Regulatory Oversight And Enforcement At Casinos, Implement And Enforce Anti-Money Laundering Regulations For The Insurance Industry, Support Anti-Money Laundering Capacity Building And Enforcement Effort and Improve How We Measure Our Progress*".[33]

FBI is determined to tackle the issues in relations to cyber laundering by developing active co-operations with other countries to achieve global solutions to cybercrimes. In respect to Money Laundering they have identified depository institution, banks and traditional casinos are actively assisting. In USA the gaming industry is on rise driven by native Indian tribes. The cybercrime investigation department of FBI is actively involved to root out the national and transnational organized criminal enterprises who are involved in cybercrime. [24]

7.2.2 National Accountability Bureau

In February 2002 **National Accountability Bureau of Pakistan (NAB)** [3]launched a project to eradicate the corruption which is considered one of the biggest problems in Pakistan. They also highlighted the issues which are root case to achieve a corruption free society. The criminals can easily exploit the weakness of corruption by giving heavy bribes to the government official for neglecting or to keep blind eyes from reporting and to take action on any incident related to the money laundering. In Pakistan it is easy to hide the illicit money due to complex stages of the process of money laundering and lack of effective monitoring control over financial institutions and government officials. Criminals are adopting modern technologies for their cause and law enforcement agencies are lacking to adopt and to use the modern technologies may be due to low financial budget .The private sector is also not well prepared to address this phenomena which shows a huge chaos to monitor and control Cyber laundering[24].

According to US State Department International Narcotics Control Strategy Report Pakistan loses $10 bn on annual bases from the trade based money laundering only. [34]

Money changer are not following any rules and regulations as they are free to use the alternate banking remittances. One of them we have discussed in previous chapter with the name Hawala system and it is commonly used for foreign remittances. To achieve high remittances and foreign exchange government is dealing with these money changers but neglecting them in relation to money laundering. [24]

The government is in the process of formulating an Anti Money laundering law and tightening regulation for money changers in collaboration with the World bank, FATF ,Asia Pacific bank and State Bank Federal investigation Agency. In the near past there was sharp rise in the cybercrime and to counter the cyber crime related threats it is essential there must be an organization to track, monitor and apprehend all such criminals. According to the law of Pakistan electronic crime ordinance 2007-2008 the Federal Investigation Agency department name "National response centre for cyber crime (NR3C)" is dealing with all

[3] National Accountability Bureau is anti-corruption public organization and it headquarter is situated in Islamabad with four provincial capitals in Pakistan. It operated under the National Accountability Ordnance 1999 Pakistan with the tasks to eradicate the corruption by creating the awareness, prevention and enforcement .[35]

matters related to cyber crime. It is also responsible for the training to different organizations regarding cyber threats which could affect their information resources. [24]

7.2.3 The Drug Enforcement Administration.

The United States Government established the Drug Enforcement Administration to control the sale and distribution of illegal drugs in the US.[20]

On global scale the trade related to illicit drug has been a steadily growing business. Alone in US according to the studies conducted on illegal drugs showed that about $65 billion are being spent on illegal drugs. [20]

On such basis DEA as the key prosecutorial agency for drug related crimes in the country has been very active in the enforcement of money laundering laws in the USA. New York City in previous studies identified by DEA as one the main financial hubs in the US where the threat of cyber laundering operations relating to the proceeds of illegal drugs is at dangerous level. As economy is getting more digitalized that we have discussed in previous chapters and in result traditional form of money is constantly being replaced by E-money. [20]

Nowaday's hard cash is hardly used to pay for drugs. One of the key focus areas for DEA is the e-payment systems as most of payments are now done online. To have a firm control over this phenomenon a special unit called the National Drug Intelligence Centre (NDIC) which is managed by DEA with the task to uncover such practice. A scenario has been examined by DEA where law enforcement officer seized a drug dealer with certain smart card or prepaid cards in his or her possession .[20]

The question arises here in this regard that whether the seizure of the pre-paid cards consequently hinders the business of the suspect in interrogation. This wouldn't be issue for hard cash derived from crime is seized by the law enforcement bodies. The NDIC arm of DEA examined this and outcome result for the first investigation shows that stopping electronic payments by seizing pre-paid cards is futile. [20]

The reason behind is that this pre-paid cards can be accessed by both the cardholder and other third parties who usually in link to the card. Thus the prepaid card might be in the possession of law enforcement officer but funds can still transferred from that card either by the interrogated criminal once released on bail or third party who is not in need to physically in the presence. The only possible remedy for this nature of problem would be a legislative one. In USA the Nevada is the only state with a possible solution to the problem. The new law called SB-82 was enacted in the Nevada which came into the effect from 1ST July 2009.This law empower the law enforcement officer to investigate the suspicious pre-paid card transactions and fraud cases that occur each year.[20]

Thus the relevant authority with the warrant can freeze funds up to 10 days on the prepaid card. Such moves prevent the criminals as well third parties from removing or transferring the funds from that pre paid card within that period. The SB-82 law in certain instances allows authorities to seize funds on a pre-paid loaded card without a warrant. In the end as a whole credit goes to DEA for inspiring this legislative initiative. [20]

7.2.4 The Financial Action Task Force

In 1989's G-7 summit in Paris the financial Action Task Force which is an inter-government agency was established to fight against the money laundering and it plays a policy making role.[20]

Initially to combat the money laundering and terrorist financing the FATF sets international standards. [20]

According to the recommendation of FATF in its 15th recommendations ("*International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation*") it highlighted the danger of cyber laundering. [20]

To tackle the threats related to the money laundering it cautions the financial institutions to pay special attention that could may be arise from the new and developing technologies which might favour anonymity. [19]

It also warns about the latest technologies that could be used in money laundering schemes and addresses those risks that associated with no-face-to-face business transactions conducted in the cyberspace .[19]

FATF has tried closely to follow these trends due to increasing manifestation of these threats. This resulted in its 2006 new payment method report and its 2010 Report on Money Laundering using New Payment Method. Later Report derived from several case studies conducted, identifies the laundering capabilities of new payment systems which includes the internet payment systems and prepaid cards. Some case studies highlighted the fact by using New Payment Systems how illicit funds derived either from high and low values are being laundered. The FATF explains the fact that the modern technologies certain key features have helped to promote the attractiveness of New Payment System for the money laundering purposes. Anonymity of the internet is one of these. Others are higher utility of funds and global access via automatic teller machines (ATM).But for New Payment System presently there is no uniformity across jurisdictions on the classifications and regulatory measures [19]

The FATF special Recommendations to prevent money laundering and terrorist financing has proposed that relevant law enforcement or prosecutorial body should have access to the originator information in order to aid investigations and prosecutions. [20]

This originator information would also help the intelligent units of financial institutions and their beneficiary to identify and report these suspicious transactions including their related risks. [20]

7.2.5 Serious Organized Crime Agency (SOCA)

In order to effect for a proper regulations of fraud, human trafficking, illegal drugs, gun crimes, computer crimes and money laundering the “Serious Organized Crime Agency” act as the United Kingdom's incentive. The Serious Organized Crime Agency with respect to anti-money laundering activities primarily deals with suspicious activity reports and act in accordance with the proceeds of **Computer Misuse Act** [4]and the **Crime Act** .[20]

7.2.6 The Wolfsberg Group

The Wolfsberg Group in October 2011 issued a guidance paper on the prepaid and stored value cards related risks. All these risks arise with the advent of cyber laundering and steady shift from traditional paper-based payment system to the now predominant electronic payment system.[19]

This largely monopolized by the non-bank services providers (NBSPs) as they do not require necessarily to fit into the respective frame of a financial institution that is typically regulated and controlled. [19]

[4] -The proceed of crime acts deals with the aspects of civil recovery of criminal proceeds, The Computer Misuse Act deals with computer technology laws basic violations.[20]

Often NBSPs are private entities (i.e. companies or corporations) that issue electronic payment instruments such as smart cards, stored or prepaid value cards. In case of Cyber laundering phenomena non Bank Service Providers are often badly tainted, some play more positive role by acting for financial institutions as outsourcing agents, by rendering certain specialist services to financial institutions or in their capacity acting as financial service providers and to financial institutions competitors .[19]

Although NBSPs require to be controlled, the Wolfsberg adopt a risk based approach in prescribing control measures for the use of stored value and prepaid cards[19]. This give a good optimism what should be expected in the near future. [19]

7.2.7 The Basel Committee on Banking Supervision

In case of Cyber laundering the Basel Committee on Banking Supervision addresses this issue from the angle of online banking [19]. This indicates problems for those banks without any physical existence that operate solely on internet. [19]

Client for these banks do not require same rigid verification process as terrestrial bank conduct for prospective clients. Telephone banking even not provides remedy which is now complementary to online banking. Possibility exists that an independent third party conduct such verification and identification but still doubt exist for the credibility and veracity of such third party or agency[19].

7.2.8 Financial Crimes Enforcement Network

In 1990 the Financial Crimes Enforcement Network (FinCEN) was established by the U.S Department of the treasury[24]. In 1994 to include regulatory responsibilities for administering the **Bank Secrecy Act**[5]**,** the operational capabilities of Financial Crimes Enforcement were broadened. To protect against organized crimes from the criminal, the FinCEN mission is to enhance and safeguard financial systems. [24]

For Fiscal Years 2008-2012 the strategic plan of Financial Action Task Force outlines three outcomes that to protect from money launderers exploitations, the financial systems must be resistant, deterrence and detection of money laundering and efficient management of Bank

[5] USA financial institutions requires assisting US government agencies to detect and prevent money laundering and requiring reporting any suspicious activities that might be signify link to money laundering, other criminal activities and tax evasion.[24]

Secrecy Act information .[24]

7.2.9 The World Bank

In respect to other regulatory or policy-making organizations the efforts by World Bank is probably the most radical and aggressive to regulate cyber laundering. To fight against cyber laundering World Bank is premised on the rationale that the internet is main root cause for this problem and it should be used to fight the crime .[20]

In conjunction with the international Monetary Fund (IMF) the World Bank has introduced the Financial Sector Assessment Program (FSAPs). This is geared towards blocking in the cyber payment systems certain loopholes with respect to the Non-Bank Issuer Model and Peer-to-Peer Model. Originated threats from these payment methods are identified as a result. [20]

World Bank proposes the Cyber threats analysis centre which should be created across all financial institutions and it could act like be an information sharing vehicle. In USA many financial institutions already have this facility generally called the Financial Services Information Sharing and Analysis Centre(ISAC).Generally ISAC act as an internet-based third party service provider which could provide real time information sharing ,provide alerts and notifications. Other than detecting potential cyber laundering transactions, it could detect other possible cyber related threats like phishing. [20]

World Bank another proposal relates to the 13th recommendation by the FATF which deals with the principle "Know Your Customer"(KYC). Generally this principle, financial institution is required to apply as closely as they can to online transactions with customers. In last it is suggested that electronic forensics in financial institution should be promoted on priority bases. [20]

First there must be electronic evidence for the bank examiners and law enforcement agencies with which they can work to investigate cyber laundering operations. The electronic evidence would only exist if there would be proper practice of preserving by the financial institutions. In order to preserve these evidences effectively there should be proper training in house or external for financial officers .[20]

7.2.10 International Police Organisation.

In order to fight against crime the International Police Organisation (Interpol) has a mandate to foster operational support by ensuring Co-ordinations between police from various jurisdictions .[19]

These actions by Interpol are to make sure the effective enforcement of laws and the crimes prevention. Interpol is key for the enforcement aspect of the global ACL legal regime. To fight against the cyber laundering Interpol exhibits itself with the characteristics of an adequately right resources and well equipped organisation. [19]

In the international sphere Interpol plays a key role to fight against cybercrime. For effective strategy against cybercrime it collect, analyzes, preserve and share information with all its member states. [19]

Since then Interpol has spearheaded some initiatives geared towards this purpose which includes the setting up of the National Central Reference Point Network. It acts as the designated network of investigators in national cybercrime unit with the purpose to be on the alert and to identify imminent threats and to facilitate cybercrime investigations. [19]

For IT crimes related incidents Interpol also established the Interpol working parties which are working group that continually works on developing strategies on the latest cybercrime methods .In every two years it conducts conference on cyber crimes .This conference provide the platform for the exchange of knowledge and expertise to fight against cybercrime.[19]

7.3 Analytical overview of different strategies

In this section author analysis different strategy which is designed by government and private institutions to prevent cyber laundering. In Author’s opinion based on discussed literature the technology advancement help to facilitate the cyber laundering activities by transferring funds from one place to another with greater speed and anonymity. But on other hand the strategies, policies and international cooperation to prevent the Cyber laundering phenomena are not progressing with same pace. Author identifies the strength and weakness of different strategies based on the literature discussed above.

7.3.1 Strength

The following factors are involved for strengthening the strategies which as follows.

-Collective Institutional Efforts

Number of public and private institutions such as World Bank, FBI, NAB and The Wolfsberg Group etc are acting as a shield to prevent the Cyber laundering and cyber crimes.

- Scrutiny over Alternative Remittance Methods

Other alternative remittances method such Hundi/Hawala which are commonly used in Sub continent and Arab countries. Pakistani government are in process to formulate an Anti Money laundering law to regulate money changer with the collaboration of other financial institutions such as World Bank, Financial Actions Task force, Asia Pacific Bank and State Bank Federal investigation Agency. This is good step to curb Money laundering. [24]

- Terrorism issue

Terrorism is globally recognized issue in present day's. Many countries and international organizations e.g. United Nation put hand together to eradicate the menace of terrorism. For execution of terrorism activities finance play crucial role and their global financial connections.*"Financial Action Task"* Force special recommendation to prevent money laundering and terrorist finance is very important step to fight against global terrorism and it also suggest law enforcement agencies should have access to original information despite neglecting privacy rules. [19, 20]

- Instrument for cyber laundering

FBI address the cyber laundering phenomena by enforcing federal laws to control and prevent this issues inside US. FBI identified cyber laundering instruments such as Casino, Gaming industry and Banks, which illustrate the strength to fight against Cyber laundering .[33,24]

-Reporting, Record keeping and monitoring

The Bank Secrecy Act is vital to safeguard the financial institutions like banks from cyber laundering by setting up some rules and regulations to fight against financial frauds by restricting them to report all transaction above the value of $10000 and to maintain record of all transactions up to 5 years. It is also required by telecommunication services and internet service providers to monitor and maintain the user data for period up to one year to assist the law enforcement agencies .[20,24]

-Know Your Customer (KYC) Policy

World Bank another proposal relates to the 13th recommendation by the FATF which deals with the principle "Know Your Customer"(KYC) could be milestone to prevent future Cyber laundering incident by closely monitoring online transactions by customers.[20]

7.3.2 Weakness of these strategies

Following factors are the reasons for the weakness of these strategies in author’s view.

-Jurisdiction issues

Cyber laundering is global problem and jurisdiction issue make difficult for the financial institutions to access the information and to operate across their jurisdictions restrictions.

-Enormous transactions

As economy across the globe is growing which leads the establishment of new financial institutions in all over the world with increase ratio of customers. So millions of financial transactions take place every day in cyberspace and it is hard to identify the suspicious one. Except those transactions which are traced as suspicious.

- Rules and regulation

Rules and regulations to combat Cyber laundering are not uniform in all countries. Similarly online batting and online Casinos are legal in some countries and some countries have strict rules for such online activities.

-Online banking

Due to growing competition among financial institutions for the online banking it is hard for the financial institute to implement the tight rule of “Know your Customer” to compete with other financial competitors.

8 Real time analysis of Tallinn based start-up from cyber laundering perspective and possibility to exploit for terrorism activities

In this chapter we will consider one real time start up from the perspective of cyber laundering and how it can be exploiting for Terrorism purposes. This start-up is Tallinn based provide online contactless banking Services in United Kingdom .The main purpose to select this company as it provide contactless less services bases to UK residents mainly immigrants . Author wants to demonstrate the real time example of cyber laundering by exploiting the weakness of this start up with the help of hypothesis.

8.1 Start up Background

This start up name is Monese which claims that Monese account could be open within 3 minutes by downloading App in our mobile. Both Mobile operating systems Android and IOS support the Monese App. This app provides full-fledged account interface Including bank account number and Short code (Important for UK residents for salary and bank transfer). It also provides low cost international money transfer and a visa card facility as shown in the figure 8. The Monese clients would be able to deposit and withdrawals money in multiple currencies [36]. The Monese clients can deposit cash at any shop with a pay point and can withdraw cash from ATMS globally [37]. For their operation across whole Europe they need only a single Electronic Money institution license [38]. After first month free trial period [37]. This start up set up monthly fee of £ 4.95 per account and it charges minor additional fee for currency exchange [36]. For all international transactions charges minimum £1[38]. The target audience for this startup is mainly migrants who find difficult to open account.

Figure 8 Monese Bank card [36]

This Company provide UK bank account regardless of their citizenship. This startup claimed it will revolutionize the banking for immigrants who have residency restrictions imposed by traditional high streets banks (down town bank) which is greater barrier to accessing the banking system in UK [38]. Monese Claims that for account opening process they validate our identity in real time based on the ID documents(Driving licence, National ID card or passport) snapshot and Selfie taken from our mobile. The company systems in addition to hundreds of data points make an instant decision whether they allow or not to open an account [38]. The Sign-up process will take as little as 120 seconds. Any one above 18 years old and live in the European Economic Area (EEA) can open an account regardless of citizenship or financial history and without valid UK residential addresses[37]. With the verified account can make card payments and can transfer money up to £40000 and daily cash with drawl limit is £300[37]. The start up claims since its launch 55000 people have installed the android app and £12 million was transacted last July with growth rate 30% percent each month [36].Before moving detail analysis for the Monese from the cyber laundering and terrorism perspective it is very essential to understand the United Kingdom Legal ID fraudulent market and immigrants history.

8.2 Strength & Weakness

In this section author purposed Critical analytical view (Strength & weakness) for Monese with his own suggestion based on Literature discussed above to find elements related to cyber laundering and Terrorism financing.

8.2.1 Strength

Following strength factors make Monese unique from other financial institution in UK which as follows.

-Latest Operating platform

Both operating systems such as Android and IOS are supporting Monese app [36]. Which increase the Monese strength and value as both are most commonly used operating systems and widely accessible by Smartphone users especially in UK. Where Smartphone user ratio is very high and mobile internet is accessible by maximum UK residents.

-Targeting Immigrants

Form Author Personal experiences, for all new arrivals in UK it always challenging to open Bank account without proof of address and credit history due to tough requirements by high street banks (Downtown Banks). In Author's opinion this start up could easily attract new arrivals (Immigrants) and can add more success stories in its portfolio to strengthen its position in UK competitive market.

-Easy To Open Account

Google Play (Androids) or APP store (IOS) support Monese App [37]. Anyone with the Basic knowledge of using and downloading Apps can easily open account for Monese by downloading app without following any specific Manual.

-Quick access to Account

The signup process takes only 120 Sec after providing their own Selfie and ID documents (Passport, Driving licence and ID Cards) [37, 38]. The clients do not have to wait for longer time .This speedy process of opening account via Monese App attracts larger pool of Clients .The maximum numbers of clients can try for Monese App without waiting so long for final decision and can access this App at their own ease. Instead of going into bank and fulfilling other accounts opening requirements after that waiting till for the final decision.

-Low Operational Cost Benefits

Monese monthly operational account fee for each client is £ 4.95 with additional international transaction charges £1[38,37] .In fact it is nothing by keeping in view the benefits the new arrivals (Immigrants) in UK can derive by opening account with minimum efforts. Low operational cost is a key to attract more clients which would increase the Monese credibility among clients and its future business arrivals.

-Full Bank Account Benefits

Monese strength hide in this fact it enable immigrants to enjoy the benefits of high street banks in UK may be more by providing bank account with short code and debit card with the facility of ATM to withdraw globally. The client can also deposit cash at any shop with a pay point in multiple currencies. The account holders can transfer money up to £40000 and daily cash withdrawal limits is £300(38, 37, 36)

-Tallinn Based Work Force

As Monese is Tallinn based and provides services in United Kingdom [36] .Which increase Monese financial strength by keeping business operations in Tallinn with low salaried work force and less operational cost comparatively to their counterparts in United Kingdom.

8.2.2 Weaknesses

Following weaknesses are related to Monese.

-Non UK Based Workforce

Monese sure can gain financial advantages by running business and support operations in Tallinn for UK clients [36]. But it is important for its Tallinn based employees to understand the dynamics of UK businesses, financial/online crimes and documents related frauds as author discussed in literature. Without knowing real UK business environment and Cyber frauds .It is really very easy to cheat their employees especially for cyber laundering and cyber terrorism.

-Verification Methods

As Monese claimed that within 120 Sec after providing the picture of ID documents (Passport, Driving licence or National ID) without residential address. Anyone without restrictions of Nationality but should be reside in EEA can open account [37].The main questions is how they can verify National documents for different nationalities within such small time .Let us suppose if someone is from war torn country and living in London do they have the ability to verify those documents and even they don’t need resident address for opening account. So in Author view it seems like first come and first serve.

-Immigrants are Main target group

In United Kingdom immigrations always main issue and this always in agenda for main streamline political parties .The key point is that those immigrants who opened accounts with Monese with debit card facilities and later due to some reasons left UK with active accounts .Do Monese have some solid strategy to tackle with these debit cards in circulation? How to recover them or to cancel them. This could be security risk for UK by criminals misuse for cybercrimes.

-Terrorist Financing

Terrorism is one of the major issues on international stage .United kingdom have been experienced many terrorist attacks in the past which causes the loss of life of many innocent people. Terrorism financing play very crucial role for the execution of terrorist attacks.

As Monese provide contact less bank services to its clients. It is very easy to exploit the Monese app for terrorism related activities.

A hypothetical scenario in which how this startup can be exploit for terrorism financing.

(Note in this scenario abbreviation for a person is used like xyz except London and United Kingdom as this start up provides services in United Kingdom)

Mr XY is educated person living in London since 40 years. He is owner of very well established chain of grocery stores all across of United Kingdom with high financial earnings .Since his childhood he has strong affiliation with religion. With his growing age his affiliation with religion is getting stronger which radicalized his thoughts. Mr XY decided to be physically involved in Islamic terrorism movement across globe. Because of his growing age he is not in position to be physically participating in Islamic related terrorist activities. So he decided to help Islamic terrorist organization by financing them in different Islamic countries. But his problem which medium he should adopt to finance them .If he adopt proper banking channels for fund transferring for terrorism activities has danger to be apprehended by law enforcement agencies. He has got to know about Monese app which he can exploit for terrorism financing as it provide contactless banking services on cyberspace with minor documents verifications for opening account .He has two issues here how to keep his personal ID in hide without leaving his digital evidence for law enforcement agencies. To keep his ID in hide he contacts with fraudulent person NX in London who delivered him high quality fake ID card under different names and to avoid digital evidence he download and registered Monese app by pay as go SIM (Smart SIM/ unregistered SIM card).Now he can run his account in multiple currencies and can finance his vicious cause which is terrorism with fake ID and unregistered SIM. Note: He can use multiple fake ID with different names and multiple Pay as go Sims for registration of Monese app.

-Exploitation for Cyber Laundering

Monese claimed that with the verified account can make card payments and can transfer money up to £40000 and daily cash with drawl limit is £300[37].Cyber launder could easily exploit this app .As by using this app with the help of fake Documents as author discussed above cyber launderer could have multiple accounts by using unregistered Sims (pay-as-go SIM/Smart SIM) as their documents verification systems is seems kind of complimentary. It takes only 120 sec to open account [36].

A hypothetical scenario shows how this startup can be exploiting for Cyber laundering

Note: [(Note: The hypothetical scenario is created by author based on the idea derived from the paper with reference [20])].

Mr Adam is Manchester based and run employment agency with the name (www.alljobs.uk). His most of targets groups are illegal immigrants. By giving employment to illegal immigrants he earned huge profit. As he gets more money from the companies where he mostly sent his employees and paid them very less by black mailing due to their illegal status in United Kingdom. He wanted to legalize all these illicit money gained from illegal activities (by Employing Illegal immigrants). He also has one charity website “www.charitypriorty.uk” with bank account under name "help charity". He contact with MR John who is smurf.

They both entered in deal and Mr Adam is agree to pay Mr John by cash in hand for his services. Mr Adam deposits some illicit cash into his personal account at placement level. Mr Adam transfer remaining funds into MR John account by using Monse app which he opened for this purpose by using Fake ID and unregistered SIM to avoid his real identity. Mr John already have got account under fake name by Monese app.

Mr John who is smurf by profession he visit his website and make deposit by using Monese app using different ID under different names to "help charity" and his personal account too. In this case Mr John could hire other smurf too with different ID and Monese App account with different names.

8.3 Recommendations

1) Monese should have to follow strict policy of “KYC” known your customer policy.

2) Monese policy shouldn’t be only profit driven by attracting immigrants .They should have well defined criteria for opening account.

3) For verification of documents they should take help from third party if they are not fully capable to verify documents as fake documents are very common in UK.

4) There Tallinn based employees should have refresh courses related to cybercrime in UK and latest cyber crime trends in UK financial markets (Including cyber laundering and cyber terrorism).

5) They should adopt multicultural environment .Diversity could open new horizon of knowledge and competition among their employees. Diversity would also help them to analysis cybercrime in batter way.

In next chapter author will consider one case study based on Bangladeshi Bank cyber-heist. This is the real example of which shows the connection between cybercrime and cyber laundering.

9 Case study on Bangladesh Bank cyber-heist

9.1 Introduction

This case study belongs to the loss of $ 81 million of Bangladesh bank (cyber heist). This incident highlights the complete failure of the existing IT infrastructure, IT specialists or executive personals of the Bank, and the law enforcement agencies. Surprisingly, hackers performed 35 orders transaction at SWIFT system, which is the worth of $ 951 million at weekend [39].The main purpose of this case study to understand how much strongly cybercriminals and cyber laundering are interconnected to achieve ill financial desires.

9.2 Background

Last year in February 2016, this incident (cyber heist) was happened. The criminals hacked the banking systems without leaving a single clue or evidence. Therefore, the Bangladeshi investigators at once were unable to trace the involvement of the culprits (cyber criminals) or possible bank personal from the inside/outside. Moreover, the printer found faulty and the bank officials was unable to gather the list of last transactions; Even, the CCTV cameras were found out of order at the bank branch. In addition to this, the next day bank officials could not open the SWIFT system [39], and got an error which indicates that ‘A file is missing or changes’ [39]. The Bank staff or employees could not handle the situation and escalated the issue to the Federal Reserve Bank (FRB). However Federal Reserve Bank was not working on Sunday, so the issue might be resolved next working day [39]. In short, that was the total negligence of the Bank employees and as well as FRB, they should have any appropriate monitoring system, especially for the weekends.

9.3 Alternatives (Constraints / Reasons)

In Author opinion the incident (cyber crime) is a symbol of talent, expertise, technology and timing. Criminals was very much familiar of victim banking system, they phishing account credential, and they planned heist activity while in the weekend, when Bangladesh banks are operates and US banks are closed [39].

The criminals steal credential through phishing then after whole security mechanism compromised. One of the transactions was not successful due to the hacker spell mistake, not because of solid cyber infrastructure [40].Moreover; they knew that the weakness and vulnerability of international banking system and have knowledge that how money landed (Cyber laundering) at Philippines casinos and the NGO in Sri Lanka. Since, casinos are not covered with Anti –Money Laundering Law (AMLL). Therefore, casinos are also not bound to coordinate for the investigation. The steal cash from Bangladeshi bank thus converted into chips for betting (Layering stage) and then headed to Hang Kong banks (Integration) [40].

According to the Head of Forensics Training Institute of Bangladesh, ‘‘ *Computer networks was not protected with a firewall, and had used second-hand $10 electronic switches to network computers linked to SWIFT global payment system*’’ [41]. Infects, they never had gone through with the cyber-crime situation, so they could not understand the importance of cyber security to prevent cybercrimes.

9.4 Proposed Solution

Author realized many flaws, weakness, and negligence in Bangladesh bank. Some of the flaws can be mitigated by adopting these steps as discussed below.

- Up to date cyber-infrastructure and competent IT-professional.
- Monitoring IT-operations based on 24/7.
- Filter system for the huge amount of transactions and as well as more number of transactions (higher orders) particularly on the weekends and public holidays.
- Design and Implement of the Law for casinos, NGO and bring them under the AML laws with the coordination of international community. Otherwise, the casinos might become the breeding ground for cybercrime by supporting cyber laundering.
- Strong mechanism for the employees criminal background check.
- Increase the co operation with other international banks to eliminate the factors of mistrust.
- Allocation of sufficient budget to address the network security flaws.
- Up to date anti viruses and Malwares

9.5 Case study-Recommendation

Bangladesh Government should take the initiative for the awareness of the Cybercrime .Govt need to promote the education, which could counter the cybercrime. Conduct intensive or extensive special courses or seminars not only for the IT-professionals but also for the professionals from other fields like banking, economists, teachers' doctors and so on.

9.6 Case study-Conclusion

In conclusion, Bangladesh Govt has to take serious action against the cybercrime (cyber heist). Investigate quickly and find the culprits, who are behind the incident. Otherwise, it may happen repeatedly and have to develop strong cyber infrastructure to shield against future cyber attacks.

Conclusion

On international stage at the moment cyber laundering is one well known issue. Many countries are directly and indirectly are affected by this vicious circle of Cyber laundering. Even Estonia was in news related to money laundering incidents which motivated author more to explore in deep about this issue. Since the emergence of money in the form of obsidian during the stone-age, humans have been known to be involved in illegal means for gaining wealth and property. With passage of time, methods of money laundering have evolved and with the addition of technological element in money laundering it became cyber laundering.

We are living in the era of technology and every day old technologies are being replaced by new inventions. This technology revolution has made cyber laundering (which exists in cyberspace for its execution) unstoppable and more profitable for cybercriminal. These technology advancements help the cybercriminal to be more organized and provide them safe heaven to avoid the law enforcement agencies.

Cyber laundering depends for its execution on speed of transaction, electronic money and cyber payment systems which require the medium of cyberspace. The cybercriminals utilize all these factors of cyber laundering to remain unnoticed from audit trail for the transfer of illicit funds. All these factors interlink the cyber laundering with the cybercrime.

Cyber laundering should not be only considered economic issue as it deprived many legal businesses from their rightful status and bring harm to the economy of any country but it is also social issue. Because it encourage the elements of corruption in any society which is root cause of inequality and injustice.

In this thesis author try to raise the awareness of cybercrime in the shape of cyber laundering. Author also discussed how technology has changed the traditional form of money laundering into cyber laundering . Author wanted to highlight how our future businesses mainly our banking sectors could be effected by future cyber laundering incidents.

The important findings based on this research is that:- As cyber laundering is global issue and to address this issue there are very less international co-ordinations on international stage .Financial initiations are trying to compete with each other by introducing new cyber payment instruments but seems negligible form future cyber security challenges .

Bangladesh Bank cyber-heist is one example in this regard. There is no global policy which could be acceptable for all countries related to cyber laundering. It wouldn't be wrong to say that we are living now in technology invention market. Every day new technology products come and next day replaced by more advance products for customers. Technology is advancing with rapid pace (new payment methods, new technologies for banking) but the international laws for future prevention for cyber laundering are not advancing with same pace. To combat the evil of cyber laundering and fight against cybercriminals we all have to come together on strong footing.

Recommendations

Author suggested following recommendation to tackle the cyber laundering phenomena based on research done for this thesis for future researcher and policy makers .

1- Increase the international efforts

Cyber laundering is an international issue as it is not focus particularly on one country. It prevails in one country and accomplish into another country. Number of international organizations are doing individual efforts to prevent the cyber laundering issues. Cyber laundering should get central stage on global platform such as United Nations as it is depriving many nations from their rightful economic benefits and many other cybercrimes are associated with it (Cyber terrorism). Future policies, legislations and strategies to prevent cyber laundering should be accomplished under United Nation umbrella. It is only possible with the co-ordinations of international community.

2- Know your customer policy

Technologies are rapidly advancing and new competitions are arising in all walks of life. Financial institutions are also trying to compete with other rival financial institutions to attract more customers by introducing services such as online banking, telephone banking, third party financial services (doorstep services) and so on. In fact competition is not bad as it is key for more improvement for the future services. But all these financial institutions should follow the strict policies of "know your customer". Because finance play very crucial role for the dirty cybercrime and other traditional crimes. Financial institution should not be an element for the execution of these dirty crimes. Government should have strong legislation on financial institutions to prevent future cyber laundering incidents. If any financial institution breaches these legislations there should be strong punishment to set up an example for other financial institutions. Such efforts could be milestone in the direction of cyber laundering preventions.

3- Online casino and gambling

Those countries that appeared as haven for the online casino and online gambling due to lack of government rules and regulations related to cyber laundering. Such countries should be sanctioned by the international communities. International community should force them to implement strict rules and regulation for online casino as cyber laundering is without boundaries.

4- Jurisdictions Barriers

Cyber laundering for its executions depends upon online transactions and E-money. With a single click the money can transfer anywhere in globe. But sometimes to find the money trail of those illicit funds involved in cyber laundering takes very long time and in some cases due to jurisdictions barriers it becomes impossible. To mitigate the risk of jurisdictions barriers it is essential to have international coordination and effective international AML laws which should be acceptable from all countries.

5- Digital signature on transaction

In Estonia digital signatures are very common practise for digital documents. The economies are getting more digitalized and the role of E-money has increased due to its unique features. To curb the cyber laundering phenomena such mechanism should be developed, in which each transaction should be digitally signed. This could be helpful to trace the location and the information of the requested person.

6- Up to date IT infrastructure

Financial institution regulatory body should ensure that all financial institutions have well developed and advance IT infrastructure to meet the future cyber challenges (financial cyber crimes). As in Bangladeshi bank cyber heist which author discussed in case study. The IT infrastructure was outdated which enable the hackers to steal the bank credentials. Later on the basis of that information they were successful to make illegal transactions and used the cyber laundering techniques to make the illicit money as legal money [39, 41].

7- Cyber security education for every one

Cyber security should not be considered education mainly for the IT specialist (In IT domain only). It should be available for professional and common people from different walk of life such as doctors, teachers, bankers and common people. To fight against the cyber laundering the financial institutions should organize refreshment courses for their employees to better understand the cybercrime related incidents.

References

[1] G. Lisanawati, “Electronic Funds Transfer in Money Laundering Crime : Regulation Needed in Response to Meeting of Technology and Crime in indonesia ,” vol. 3, no. 2, pp. 163–170, 2010. Available: http://academic-journals.org/ojs2/index.php/IJCSE/article/viewFile/915/51 .(Accessed:10/12/2016)

[2] T. Tropina, “Fighting money laundering in the age of online banking, virtual currencies and internet gambling,” *ERA Forum*, vol. 15, no. 1, pp. 69–84, 2014. Available: https://link.springer.com/article/10.1007/s12027-014-0335-2.(Accessed:10/12/2016)

[3] D. Cyberlaundering, “Cyberlaundering : Concept & Practice,” pp. 55–65, 2014. Available: https://link.springer.com/chapter/10.1007%2F978-3-319-06416-1_2 (Accessed: 15/12/2016)

[4] T. Sõmer *et al.*, “E-CRIME ‘ The economic impacts of cyber crime.’ Available: http://ecrime-project.eu/wp-content/uploads/2015/02/E-CRIME-Deliverable-2.3-resubmit-for-website-pt1.pdf (Accessed:19/04/2017)

[5] D. A. LESLIE, “THE LEGAL REGIME FOR ANTI-CYBERLAUNDERING,” 2012. Available: http://etd.uwc.ac.za/xmlui/handle/11394/4373 (Accessed: 19/04/2017)

[6] “Cybercrime.” [Online]. Available: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en. (Accessed:20/04/2017)

[7] A. Obaid and S. Alkaabi, “Combating Computer Crime: An International Perspective,” 2010. Available: http://eprints.qut.edu.au/43400/1/Ali_Alkaabi_Thesis.pdf(Accessed:21/04/2017)

[8] B. S. CALVIN LEE PACLEB, “INTERNATIONAL MONEY LAUNDERING: A COMPREHENSIVE REVIEW AND GENERAL THEORY OF CORRUPTION,” 2003. Available: https://ttu-ir.tdl.org/ttu-ir/bitstream/handle/2346/14128/31295018735125.pdf?sequence=1(Accessed:10/01/2017)

[9] B. D. Schwartz, “Deficiencies in regulations for anti-money laundering in a cyberlaundering age,”2009 Available: http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1636&context=etd[Accessed: 11/01/2017].

[10] “Sharifs used paper mill to whiten money, Dar told court in 2000 - - DAWN.COM.” [Online]. Available: https://www.dawn.com/news/848873. [Accessed: 12/01/2017].

[11] A. Alhassan, “Money Laundering and Terrorism Financing : Does the Saudi Arabian Financial Intelligence Unit Comply with International Standards ?,” 2011. Available:http://vuir.vu.edu.au/19945/1/Abdulaziz_Al-Hassan.pdf[Accessed: 18/01/2017].

[12] A. A. Dumitrache and G. Modiga, “NEW TRENDS AND PERSPECTIVES IN THE MONEY LAUNDERING PROCESS,” 2010. [Accessed: 22/01/2007].

[13] F. Schneider and U. Windischbauer, “Money laundering: some facts,” *Eur. J. Law Econ.*, vol. 26, no. 3, pp. 387–404, Dec. 2008. Available: https://core.ac.uk/download/pdf/6518199.pdf [Accessed: 22/01/2017].

[14] “Methods and Stages in Money Laundering.” [Online]. Available: http://people.exeter.ac.uk/watupman/undergrad/ron/methods and stages.htm. [Accessed: 30/01/2017].

[15] “What is Money Laundering? - KYCMap.” [Online]. Available: http://kycmap.com/what-is-money-laundering/. [Accessed: 31/01/2007].

[16] “Integration Techniques - International Money Laundering.” [Online]. Available: https://sites.google.com/site/intmoneylaunder/money-laundering-methods/integration-techniques[Accessed: 02/02/2017].

[17] C. V. Thomason, “How has the establishment of the Internet changed the ways in which offenders launder their dirty money?,” *Internet J. Criminol* https://www.noexperiencenecessarybook.com/8v05G/microsoft-word-thomason-internet-money-laundering-july-09.html. Available: [Accessed: 04/02/2017].

[18] “Cash controls - European Commission.” [Online]. Available: http://ec.europa.eu/taxation_customs/individuals/cash-controls_en. [Accessed: 10/02/2017].

[19] D. A. LESLIE, “THE LEGAL REGIME FOR ANTI-CYBERLAUNDERING,” 2012. Available: http://etd.uwc.ac.za/xmlui/handle/11394/4373. [Accessed: 12/02/2017].

[20] D. A. Leslie, “ANTI-CYBERLAUNDERING REGULATION AND CONTROL.” Available: http://etd.uwc.ac.za/xmlui/handle/11394/1438. [Accessed: 14/02/2017].

[21] “Money Laundering Final | Money Laundering.” [Online]. Available: https://www.scribd.com/document/136348455/Money-Laundering-Final. (Accessed: 16/02/2017].

[22] N. Popovska-Kamnar, “THE USE OF ELECTRONIC MONEY AND ITS IMPACT ON MONETARY POLICY,” *JCEBI*, vol. 1, no. 2, pp. 79–92, 2014. [Online]. Available: http://www.eccf.ukim.edu.mk/ArticleContents/JCEBI/JCEBI_2/spisanie%20Neda%20Popovska-Kamnar.pdf. (Accessed: 20/02/2017).

[23] “Chapter 2 “The Changing Typologies and Emerging Trends of Money Laundering Practices,” pp. 4–5. [Accessed: 22/02/2017].

[24] M. S. Jamali, “Cyber Laundering,” 2009. Available:

https://www.scribd.com/doc/17252189/Cyber-Laundering-Final[Accessed: 22/02/2017].

[25] L. E. C. Rossroads, “Cyber Laundering-The new internet Crimes Available:.http://thegiga.in/LinkClick.aspx?fileticket=xpxlb4qgFTw%3D&tabid=589) (Accessed:24/02/2017)

[26] W. Filipkowski, “Cyber Laundering : An Analysis of Typology and Techniques,” vol. 3, no. 1, pp. 15–27, 2008. Available: https://www.researchgate.net/publication/222099776_Cyber_Laundering_An_Analysis_of_Typology_and_Techniques (Accessed: 24/02/2017)

[27] “casino-money-transfer.jpg (700×444).” [Online]. Available: http://www.moneylaundering.it/wp-content/uploads/2012/05/casino-money-transfer.jpg. [Accessed: 28/02/2017]

[28] “Essay on Cyber Terrorism.” [Online]. Available: http://www.essay.ws/essay-on-cyber-terrorism/.[Accessed: 16/03/2017] .

[29] J. Hunt, “The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them,” *Inf. Commun. Technol. Law*, vol. 20, no. 2, pp. 133–152, Jun. 2011. Available: http://www.tandfonline.com/doi/pdf/10.1080/13600834.2011.578933?needAccess=true[Accessed: 18/03/2017]

[30] R. C. Molander, D. A. Mussington, and P. A. Wilson, “Cyberpayments and Money Laundering: Problems and Promise.” [Accessed: 18/03/2017]

[31] G. Farrugia, “Money Laundering in Cyberspace,” no. 35905, p. 23, 1999. Available: http://www.fiumalta.org/library/PDF/ml_cyberspace.pdf.[Accessed: 19/03/2017]

[32] “About Business Crime Solutions - Money Laundering: A Three-Stage Process.” [Online]. Available: https://www.moneylaundering.ca/public/law/3_stages_ML.php. [Accessed: 21/03/2017] .

[33] “2007 Natonal Money Launderng Strateg.” Available: https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf. [Accessed: 28/03/2017]

[34] “Pakistan loses $10bn a year to money laundering - Pakistan - DAWN.COM.” [Online]. Available: https://www.dawn.com/news/1318697.. [Accessed: 30/03/2017]

[35] “National Accountability Bureau.” [Online]. Available: http://www.nab.gov.pk/.[Accessed: 02/04/2017].

[36] “Monese, the UK banking app for immigrants and expats, finally lands on iOS | TechCrunch.” [Online]. Available: https://techcrunch.com/2016/07/28/monese-ios/.[Accessed: 07/04/2017] .

[37] Monese, “Instant UK account for mobile people | Monese,” *https://www.monese.com*. [Accessed: 07/04/2017]

[38] “Monese Launches In U.K. To Let Immigrants And Expats Get A Mobile Banking

Account | TechCrunch." [Online]. Available: https://techcrunch.com/2015/09/21/moneseasy-peasy/.[Accessed: 09/04/2017].

[39] "Bangladesh Bank: The Billion Dollar Breach | Institute for Defence Studies and Analyses." [Online]. Available: http://www.idsa.in/idsacomments/bangladesh-bank_the-billion-dollar-breach_msharma_230316. [Accessed: 30/04/2017].

[40] S. Sharmeen Karim, "Cyber-crime Scenario in Banking Sector of Bangladesh: An Overview 13 THE COST AND MANAGEMENT," vol. 44, no. 2, pp. 1817–5090, 2016. Available: http://www.icmab.org.bd/images/stories/journal/2016/Mar-Apr/3.Cyber-crime.pdf[Accessed: 30/04/2017].

[41] "How the New York Fed fumbled over the Bangladesh Bank cyber-heist." [Online]. Available: http://www.reuters.com/investigates/special-report/cyber-heist-federal/.[Accessed: 30/04/2017] .