

**REGIME BUILDING IN CYBERCRIME:  
COMPARISON BETWEEN CYBERCRIME  
AND  
ANTI-MONEY LAUNDERING POLICIES**



**BiRKAN UZUN**

**MAY 2016**



**REGIME BUILDING IN CYBERCRIME:  
COMPARISON BETWEEN CYBERCRIME  
AND  
ANTI-MONEY LAUNDERING POLICIES**


**A THESIS SUBMITTED TO  
THE GRADUATE SCHOOL OF SOCIAL SCIENCES  
OF  
IZMIR UNIVERSITY OF ECONOMICS**

**BY**


**BIRKAN UZUN**

**MAY 2016**


Approval of the Graduate School of Social Sciences

  
Assoc. Prof. Dr. Ö. Osman Demirbaş  
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science

  
Prof. Dr. Filiz Başkan Canyaş  
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science

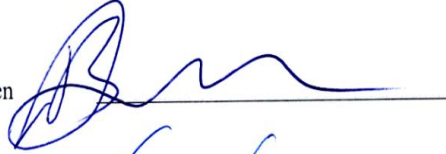
  
Assoc. Prof. Dr. Balkan DEVLEN  
Supervisor

Examining Committee Members

Assoc. Prof. Dr. Çiğdem Kentmen Çin



Assoc. Prof. Dr. Balkan Devlen



Assoc. Prof. Dr. Ali Şevket Ovalı



# ABSTRACT

## REGIME BUILDING IN CYBERCRIME: COMPARISON BETWEEN CYBERCRIME AND ANTI-MONEY LAUNDERING POLICIES

Uzun, Birkan

Political Science and International Relations

Supervisor: Assoc. Prof. Balkan Devlen

May 2016

*Within the last few decades networks and Internet have been part of our daily life with the spread among individuals. This state has increased the crimes towards individuals, companies and governmental structures. The Internet has no borders between states. The increase in crimes and borderless structure of global network require a comprehensive cooperation to investigate cybercrimes effectively, collect evidences, and prevent lawless havens where criminals shelter. Although, Council of Europe's Convention on Cybercrime has been adopted in 2001, 82 countries have signed one or more of the regional or international binding or non-binding initiatives on cybercrime. Another international crime policy area, Anti-Money laundering, has been diffused in the same years*

*drastically in global level. The aim of this work is trying to understand what the shortcomings of international cybercrime treaties are, precisely Convention on Cybercrime. While trying to figure out the shortcomings, a comparison between cybercrime policy and anti-money laundering policy has been found reasonable as international cooperation is inevitable in both areas and as the emergence of the need and diffusion occurred approximately in the same years.*

**Keywords:** Cybercrime, Cyber security, Anti-Money Laundering, Regime Building



## ÖZET

### SİBER SUÇLARDA REJİM OLUŞTURMA: SİBER SUÇLAR VE KARAPARA AKLAMA POLİTİKALARI ARASINDA KARŞILAŞTIRMA

Uzun, Birkan

Siyaset Bilimi ve Uluslararası İlişkiler

Tez Yöneticisi: Doç. Dr. Balkan Devlen

Mayıs 2016

*Son yıllarda ağlar ve internet bireyler arasında yaygınlaşması ile günlük hayatımızın bir parçası haline geldi. Bu durum kişilere, şirketlere ve devlet organlarına karşı işlenen suçların artmasına sebep oldu. İnternetin devletler arasında sınırları yoktur. Suçlardaki artış ve küresel ağın sınırsız yapısı, siber suçları etkin şekilde araştırılması, delillerin toplanması suçluların sığınabileceği kanunların erişmediği limanların engellenmesi bakımından geniş bir işbirliğini gerektirir. Avrupa Konseyi Siber Suçlar Sözleşmesi 2001 yılında kabul edilmesine rağmen, 82 ülke bölgesel ya da uluslararası bağlayıcı veya bağlayıcı olmayan siber suçlar sözleşmesini imzaladı ya da yürürlüğe koydu. Bir başka uluslararası suç politikası alanı olan Kara Para Aklama politikası ise aynı yıllarda sert bir biçimde küresel olarak genişledi. Bu çalışmanın amacı uluslararası siber suçlar sözleşmelerinin, tam olarak Siber Suçlar Sözleşmesinin*

*noksanlıklarını anlamaktır. Bu noksanlıkları ortaya çıkarmaya çalışırken siber suçlar politikası ile kara para aklama politikalarının karşılaştırılmasının her iki alandaki uluslararası işbirliğinin kaçınılmaz olması ve ihtiyaç ile genişleme sürecinin yaklaşık olarak aynı zamanda ortaya çıkmış olması sebebiyle yerinde olduğu değerlendirilmiştir.*

**Anahtar Kelimeler:** *Siber Suç, Siber Güvenlik, Karapara Aklama, Rejim Oluşturma*





## ABBREVIATIONS

AML	: Anti-Money Laundering
AML/CFT	: Anti-Money Laundering / Counter Financing of Terrorism
APEC	: Asia Pacific Economic Cooperation
CDD	: Customer Due Diligence
CDPC	: European Committee on Crime Problems
CICTE	: Inter-American Committee against Terrorism
CITEL	: Inter-American Telecommunication Commission
CoE	: Council of Europe
EU	: European Union
GCC	: The Gulf Cooperation Council
G8	: The Group of Eight
ICCP	: Information, Computer and Communications Policy
ICT	: Information and Communications Technology
IMPACT	: International Multilateral Partnership against Cyber-Threats
ISPs	: Internet Service Providers
ITU	: The International Telecommunication Union
MLATs	: Mutual Legal Assistance Treaties
NCCT	: Non-Cooperative Countries and Territories
OAS	: Organization of American States
OECD	: Organisation for Economic Co-operation and Development
REMJA Americas	: Ministers of Justice or Ministers or Attorneys General of the Americas

- TFEU : Treaty on the Functioning of the European Union
- UN : United Nations
- UNTOC : United Nations Convention against Transnational Organized  
Crime
- WSIS : World Summit on the Information Society



## INDEX

ABSTRACT .....	iii
ÖZET .....	v
ABBREVIATIONS .....	vii
INDEX .....	ix
INTRODUCTION.....	1
CHAPTER 1.....	6
WHY INTERNATIONAL COOPERATION IS NEEDED? .....	6
1.1. The Reasons to Look for a Cooperation.....	6
1.1.1. Distance between suspect and victim.....	6
1.1.2. The Ground of the Evidences.....	7
1.1.3. Sole Method to Identify Suspect .....	8
1.1.4. Vulnerability of the Evidences .....	8
1.1.5. A New Phenomenon.....	9
1.1.6. Safe Havens.....	9
1.2. Scope of Cooperation .....	9
CHAPTER2.....	11
BUILDING A REGIME .....	11
2.1. Mechanisms of Diffusion .....	14
2.1.1. Coercion and Blacklisting .....	14
2.1.2. Mimicry or Social Acceptance.....	15
2.1.3. Competition and Risk Ratings.....	17
2.2. Hegemony and Diffusion .....	18
2.3. Summary of the Progress .....	18
CHAPTER 3.....	20
ANTI-MONEY LAUNDERING .....	20
3.1. Anti-Money Laundering Initiatives.....	22
3.1.1. The European ML Conventions and Directives.....	22
3.1.2. Interpol .....	23
3.1.3. The Egmont Group of Financial Intelligence Units (FIUs) .....	23
3.1.4. The Wolfsberg Group.....	23

3.1.5.	The UN Convention against Transnational Organized Crime (Palermo Convention).....	24
3.1.6.	The United Nations Convention against Corruption (UNCAC) .....	24
3.1.7.	OECD .....	24
3.1.8.	ASEAN’s AML initiative.....	25
3.1.9.	FATF .....	25
3.2.	The FATF 40 Recommendations .....	26
CHAPTER 4.....		31
CYBERCRIME INITIATIVES .....		31
4.1. International Developments on Cybercrime: .....		31
4.1.1.	G8.....	31
4.1.2.	United Nations.....	32
4.1.3.	International Telecommunication Union .....	35
4.2. Regional Developments on Cybercrime .....		36
4.2.1.	European Union.....	36
4.2.2.	Organization for Economic Co-operation and Development (OECD).....	41
4.2.3.	Asia Pacific Economic Cooperation .....	42
4.2.4.	Commonwealth .....	43
4.2.5.	African Union.....	44
4.2.6.	Arab League and Gulf Cooperation Council.....	46
4.2.7.	Organization of American States .....	47
4.2.8.	Council of Europe .....	50
4.3. Why Did So Many Initiatives Emerge? .....		50
CHAPTER 5.....		52
CONVENTION ON CYBERCRIME.....		52
5.1. Features of the Convention .....		54
5.1.1.	Difficulties in Fighting against Cybercrime.....	54
5.1.2.	Fundamental Principles of Judicial Cooperation .....	57
5.1.3.	Procedures of Judicial Cooperation.....	57
5.2. Critiques .....		58
5.2.1.	Harmonization .....	58
5.2.2.	Jurisdiction Related Issues .....	59
5.2.3.	Comprehensiveness .....	60

5.2.4.	Burden on ISPs.....	63
5.2.5.	Human Rights.....	64
5.3.	Evaluation of Convention.....	65
5.4.	Proposals .....	66
5.4.1.	Amendment on Convention on Cybercrime.....	66
5.4.2.	Russia’s Proposal on International Cyber Arms Control.....	67
5.4.3.	Cybercrime Model Code .....	68
5.4.4.	Russia’s Proposal on Code of Conduct.....	69
CHAPTER 6.....		70
WHY IS SUCCESS OF CYBERCRIME DIFFUSION LIMITED? .....		70
6.1.	Organized Crime .....	70
6.2.	Burden on Private Institutions.....	71
6.3.	Terrorism.....	72
6.4.	Limited/Regional Contribution .....	72
6.5.	Anxiety of Sovereignty .....	73
6.6.	Reservation.....	73
6.7.	Amendment Process.....	74
6.8.	Sanctions .....	74
CHAPTER 7.....		76
RECOMMENDATION FOR A COMPREHENSIVE CONVENTION .....		76
CHAPTER 8.....		78
CONCLUSION .....		78
BIBLIOGRAPHY .....		81

## INTRODUCTION

Within the last few decades networks and Internet have been part of our daily life with the spread among individuals. This virtual world is ambiguous, intriguing, and impressive for most of us. Further than being in our life, by the Smartphone technology, it has entered into our pockets. Although it has many benefits to carry this network in our pockets, it contains many threats from uninvited and anonymous intruders. Many of these intruders may be from different countries, from a very distant place on earth. They may steal other's individual documents, academic studies, private photos, and credit card numbers or use your computer as a proxy to attack another computer. When the attacker is very far from a victim's location and also beyond his/her country's borders, how can the victim's country official agencies redress his/her grievances?

Information technology has in one way or the other invaded almost every aspect of human activities (CoE, 2001b, ¶ 1). Internet is a network which millions of computers are connected to with one another. Any computer which is connected to this network might attain information by connecting to a server which is available for any user without a boundary restriction. In this way, any person may reach any information available for the public within few seconds thanks to the screen in front of him/her. Although this simplicity has deeply entered into our daily life, it contains some hazards. The network that you are connected to might make the data on your computer available for others. Thus, on contrary to your will, your data might be available to the public by a person who is thousands kilometres away.

The development and interconnection of information and communications technologies (ICTs) like Internet, email, satellite television and mobile phones are spreading in the world at an impressive speed (Eriksson & Giacomello, 2006, p. 221). Today, the Internet has countless communication channels which allow their legitimate users to log in and spread their messages to the audiences. However, the Internet is designed to maximize the simplicity of the communication, not security of the communication (Eriksson & Giacomello, 2006, p. 225).

In 2011, more than one third of the total world population, at least 2.3 billion people had access to the Internet. It is estimated that by 2017 mobile broadband

number will be approaching 70 per cent of the world population. By 2020, the number of network devices will be six times bigger than the number of the people (UNODC, 2013, p. xvii).

By the increase in the number of Internet users day by day, Cyber crimes are increasing as well. The Internet can be used for other reasons which are inconsistent with the objectives of peace and security, thus may affect the integrity of critical systems (G8, 2011). Computers, laptops, tablets and cell phones make the Internet available for us everywhere. By the software products such as social networks, location services, people check in where they are and inform their friends what they do, what they like etc. Their preferences, social lives, political tendencies, expectations are seen by others. On the other hand, people send messages to each other by instant messaging programmes or e-mails. Furthermore, people can check their banks details and make remittances by online banking systems. We watch our house or office by IP cameras from a distant place. We save our private data in virtual storages. All these developments in daily life make us vulnerable from attacks of anonymous assailants.

When you understand the increase of cybercrime, it is not easy to provide cross-nationally comparative statistics on cybercrime because of the difficulties of defining and identifying cybercrime. However, law enforcement correspondences at global level indicate that both individual offenders and organized criminal groups exploit new opportunities for profit and personal gain (UNODC, 2013, p. 6).

Information revolution makes security an increasingly important concern in all sectors of society (Eriksson & Giacomello, 2006, p. 222). G8 countries state in Deauville Declaration that *“As we adopt more innovative Internet-based services, we face challenges in promoting interoperability and convergence among our public policies on issues such as the protection of personal data, net neutrality, transborder data flow, ICT security, and intellectual property (G8, 2011).”*

Furthermore, cyber-threats have originated in both the private and public sphere, among military as well as civilian actors. In the business community and within the police, cyber-crime has become a prominent threat image. In North America,

Europe, Russia China and other parts of the world, governments are establishing new units and employing personnel for monitoring, analyzing and countering risks and threats of the global network society (Eriksson & Giacomello, 2006, p. 225).

The common view is that as societies and governments are becoming more reliable about information technology, they are also becoming more vulnerable to all sorts of cyber-threats (Eriksson & Giacomello, 2006, p. 226).

The main problem of cybercrime is the ambiguity on which country has the jurisdiction over cyberspace (August, 2002, p. 531). The main challenges of cybercrime are states' inability in identifying assailants, collecting evidences, conducting investigations and harmonizing domestic laws. Transnational access to the information also makes the servers vulnerable to the attacks. But global networking prevents states' authority to investigate and judge. On the other hand, vulnerability of the evidences makes it very difficult to obtain necessary evidences before they are abolished. Moreover, it has been realized that harmonization of the domestic laws are very crucial in terms of providing international cooperation.<sup>1</sup> So, it is important to create a rule which works smoothly across local, national, international boundaries (August, 2002, p. 532).

At last, some of the international organizations and states commenced on working together on dealing with this issue. After several improvements in the international environment, the 2001 Convention on Cybercrime has been signed by the Council of Europe countries with a few other contributors. But, until now Cybercrime Convention and other cybercrime related initiatives have implemented very little.

Cybercrime Convention and other related initiatives state that Cybercrime challenges can only be sorted out by global cooperation. This is because it is a new phenomenon; the states are so stranger to the phenomenon, the technical problems

---

<sup>1</sup> One of the most devastating cyberattacks occurred in 2000, by a virus which is called "love bug". It is estimated that the virus affected over forty-five million users in more than twenty countries. Estimated damage was between 2 billion and 10 billion dollars. The attackers have been identified in Phillipines, but the charges have dropped as the act is not enacted as a crime in Phillipines penal code. Furthermore, the suspects were not be able to extradited because of the requirement of "dual criminality." (Available at: <http://www.marccgoodman.net/2002/09/08/oxford-international-journal-of-law-and-information-technology/>, accessed on May 2, 2016)



in collecting evidences and jurisdictional difficulties. Traditional criminal investigation methods are not sufficient for cybercrime.

Although a comprehensive cybercrime regime is tremendously needed, the development has been slow and limited. Thus, consistent with the aim of the thesis, it is found reasonable to compare anti-money laundering policy, where international cooperation means implemented rather quickly.

To understand the reason why the cyber crime regime has deficiencies I will be elaborating on the main structures of anti-money laundering policy and cyber crime policy. 40 Recommendations of FATF and Council of Europe's Convention on Cybercrime, which are the most prominent initiatives of both realms, will be discussed. The Anti-Money laundering policy has been selected as a case study as it is thought that AML Policy and Cybercrime Policy have similar features. First of all, their emergence and implementation periods meet approximately same years. And secondly, international cooperation is extremely needed in terms of conducting efficient investigations.

The purpose of this study is to understand why the cyber crime policy is lacking the comprehensive cooperation while another international cooperation, anti-money laundering policy, has the widest cooperation globally.

J.C. Sharman states that international regimes of anti-money laundering policy among developing countries implemented by power-based mechanisms (Sharman, 2008, p. 635). Consistent with Sharman's proposal, the cybercrime policy will be elaborated whether a coercive mechanism is needed for the diffusion of the policy.

In the first part of the thesis, it will be discussed why international cooperation is needed. In the second part, Sharman's theoretical framework in the diffusion mechanisms of AML regime will be explained. In the third part, past and recent developments will be mentioned and the main body of AML regime, the Forty Recommendations, will be explained. In the fourth section past and recent developments conducted by regional and international organizations will be elaborated on regarding the cybercrime policies. Council of Europe's Convention on Cybercrime which is the most important initiative of the Cybercrime policy shall be discussed separately in terms of features and critiques forwarded to the

Convention in the fifth part. In the sixth part the differences of both policies will be discussed. In the seventh chapter, the proposals of the writer for a comprehensive cybercrime regime will be revealed. Finally in the eighth chapter the conclusion of the thesis will be discussed.



# CHAPTER 1

## WHY INTERNATIONAL COOPERATION IS NEEDED?

### 1.1. The Reasons to Look for a Cooperation

#### 1.1.1. Distance between suspect and victim

When a person connects to the Internet, he/she connects to a single network where billions of devices are connected. Internet is a realm where there are no borders, no security checks, no identification cards or numbers. Thus, while the suspect is in a particular country in the world, the person who is the victim of cyber crime can be from any other country of the world. The first reason why international cooperation is needed is the distance between suspect and the victim.

The state has authority of jurisdiction within its territory. The competent authorities of a sovereign state apply its laws on its own territory.<sup>2</sup> For traditional crimes, when the suspect is outside of the territory of the state conducting the investigation/prosecution, the state applies for extradition according to bilateral/multilateral agreements to other country where the suspect resides. Multilateral agreements are signed between parties according to mutual relations, geographical distances or being members of same international organization. But when the issue is cyber crime the state is likely to be in cooperation with another state where there is no direct engagement.

Usually, it is difficult to identify the suspect from another country. First of all, the party which is conducting the investigation has to search evidences on the victim's computer and the victim's service provider<sup>3</sup> and if possible to the content provider<sup>4</sup>. The victim's computer and the victim's service providers are easy to

---

<sup>2</sup> According to territorial principle, states have exclusive authority to deal with criminal issues arising within their territories; this principle has modified to permit officials from one state to act within... Available at: <http://global.britannica.com/topic/territorial-principle> , accessed on March 6, 2016.

<sup>3</sup> An Internet Service Provider (ISP) is a company that provides accession to the Internet, usually for a fee. The most common ways to connect to an ISP are by using a phone line (dial-up) or broadband connection (cable or DSL). Available at: <http://windows.microsoft.com/en-us/windows/what-is-internet-service-provider#1TC=windows-7> , accessed on March 3, 2016

<sup>4</sup> Content provider is an organization or individual that creates information, educational or entertainment content for the Internet, CD-ROMs or other software-based products. Available at:

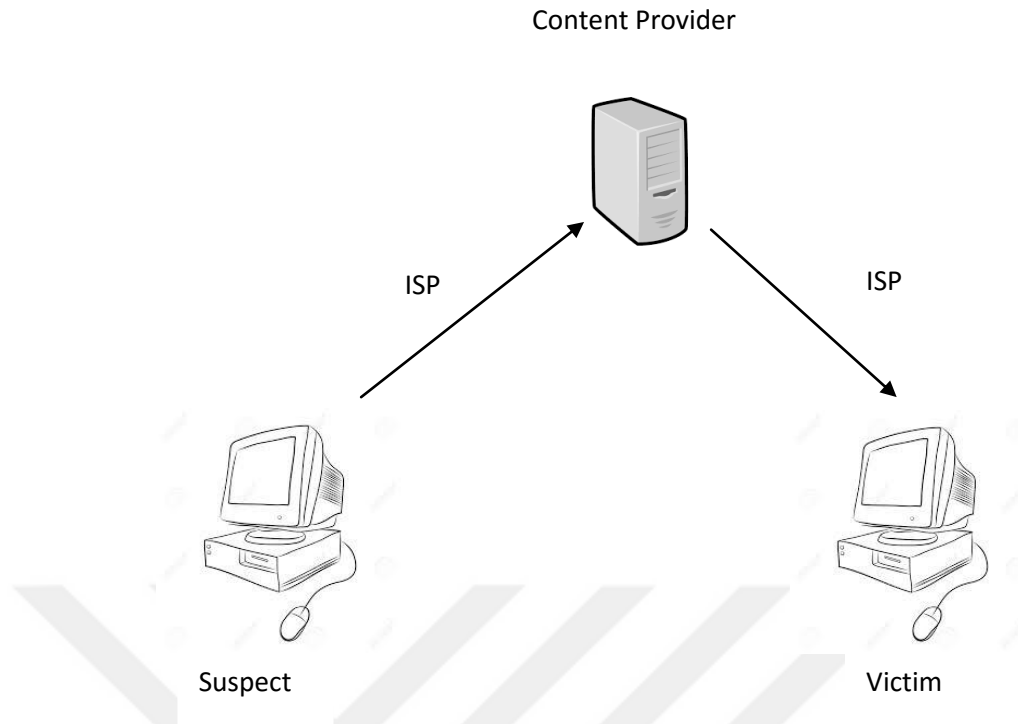
access as they are usually in the same country. Thus, the investigators try to pick necessary information from the computer of the victim or demand them from the service provider. If everything goes according to plan, the investigators will find the traffic data of the suspect. But traffic data information, which consists of digits, will not provide the identification of the suspect. This information shall be useful only if the requested country provides identification of the suspect to the requesting party. Close cooperation between countries is very crucial in terms of identification of a suspect who is outside the country and demanding compensation for the loss.

### **1.1.2. The Ground of the Evidences**

Second reason for cooperation is the ground where the investigators find the evidences. As we mentioned the victim's computer and the victim's service provider may be found within the range of the jurisdiction of the state. Moreover, if the content provider is also in the same country, the evidences may be compiled and provided by the company. But if the content provider and suspect are in another country, law enforcement authorities cannot retrieve the necessary information by their traditional judicial power. This information may be a traffic data which is temporarily sheltered by internet service provider (ISP) or content provider. In case of mutual cooperation, this information can be retrieved from these companies or else fail to get this information. Finally, the last chance to find the evidence is by obtaining the proof through digital forensics which is applied on the suspect's computer. But traditional regulations do not let the state conduct criminal investigations by searching a suspect's computer. Harmonization of cybercrime laws is very essential and crucial in terms of global evidence collection (UNODC, 2013, p. 56).

---

<http://www.pcmag.com/encyclopedia/term/40275/content-provider> , accessed on March 3, 2016.



### **1.1.3. Sole Method to Identify Suspect**

Usually, aforementioned ways of collecting evidences are the key ways to identify the suspect. When the crime is committed through Internet, there are no available fingerprints, DNA samples, witnesses, or camera recordings. So, traditional investigation methods fail to conduct an effective investigation. Lack of close cooperation between the states creates a gap which is an attractive realm for criminals to commit their crimes easily without leaving a trace to be followed by investigators.

### **1.1.4. Vulnerability of the Evidences**

The only data which is necessary for criminal investigation may be vulnerable. Firstly, necessary information may be overwritten because of the limited storage of the computers, content providers' servers or ISPs' servers. Secondly, anytime physical or digital malfunctioning and destruction is possible. Thus, it is very crucial to keep and retrieve traffic data as long as possible. However, traditional judicial cooperation methods are very cumbersome. Before fulfilling necessary procedures, this data is likely to be lost. Accordingly, extraordinary method of

judicial cooperation is of utmost importance in terms of cyber crime investigations.

#### **1.1.5. A New Phenomenon**

Cyber crime is a very new phenomenon for many of the developing countries. Significant amount of the states or the users of the Internet are not aware of the threat they are facing. The Lack of judicial cooperation between states, procedural and substantial law procedures, insufficient physical and digital conditions of content providers or service providers render a vast ground for the suspects. Some countries did not adopt cyber crimes or still in the eve of adopting their domestic laws. Some developed countries have sufficient experience about cyber crimes. Consequently, developing countries need to learn from developed countries' experiences.

#### **1.1.6. Safe Havens**

As we have discussed above, a close cooperation is needed globally to fight against cyber crimes. As long as there are countries which do not adopt cyber crimes in their domestic laws and be in close cooperation with others, there will not be a comprehensive struggling against cyber crime. Because those people who aim to commit cyber crime shall have a shelter as safe havens. As a consequence, abolishing safe havens is very crucial to deter criminals and fight against those crimes.

### **1.2. Scope of Cooperation**

The complicated structure of cybercrimes push states to look for new methods of cooperation which differs from traditional methods. First of all, substantive criminal law should be redefined for cybercrime. Some of the countries did not describe the new types of crimes similarly. And some other did not describe at all. A common criminalization is needed to promote international cooperation. Similar criminalization of the acts committed through Internet is important as well.

Secondly, procedural law should be defined. When these discussions started law enforcement authorities and judicial authorities did not have the ability to take necessary actions for criminal investigations. These actions are about expedited

preservation of stored computer data, real time collection of traffic data, interception of content data, collecting digital evidences by search, and seizure certain digital devices. So, for conducting an efficient criminal investigation and procedure, it is crucially important to frame procedural law.

Thirdly, extra-territorial dimension make international cooperation inevitable in terms of collecting evidences, extradition, thus, conducting an efficient investigation and proceed. For traditional crimes, usually countries need close cooperation with the states which is adjacent to its borders. But, cybercrime is rather different from traditional crimes. It may require cooperation with a very far state. Eventually, it is important to create a binding international initiative and correspondingly harmonizing domestic laws for providing international cooperation.

Finally, it is very important to take immediate actions because of the vulnerability of the digital evidences. Traditional judicial cooperation has long and cumbersome procedures. Before completing these procedures, evidence that is needed may be lost. Accordingly, a contact chain should be created which will be competent to take necessary actions before the evidences get lost within his country and will be in touch with other cooperative states for investigative purposes.

All these reasons forced states and international organizations to search for a comprehensive initiation to provide necessary cooperation. Simultaneously, in the middle 1990s regional and international organizations started discussing the proper ways of fighting cybercrimes.

Before proceeding to Cybercrime Policy, diffusion of Anti-Money Laundering regime will be discussed as a case study in the next section.

## CHAPTER 2

### BUILDING A REGIME

One of the most prominent definitions of regime has been made by Krasner. By Krasner, international regime has been described as:

*“sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors’ expectations converge in a given area of international relations. Principles are beliefs of fact, causation, and rectitude. Norms are standards of behaviour defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action. Decision-making procedures are prevailing practices for making and implementing collective choice (Krasner, 1982, p. 186)”*.

However, Haas contends that regimes are not simply static summaries of rules and norms: they may also serve as important means for international learning which creates similar state policies. In his work he demonstrates that Mediterranean Action Plan, a regime for marine pollution control in the Mediterranean Sea, the regime played a key role in the balance of power within Mediterranean governments by empowering a group of experts who then led the development of state policies in compliance with the regime (Haas, 1989, p. 379).

Thus, a regime is expected to create specific norms and rules which is necessary for international common goals. As a result of creation a regime, similar actions to the same situations are expected from all parties.

When it comes to one of our focal work, Le Nguyen states that Anti-Money Laundering (AML) regime has diffused under pressure from other states rather than on a voluntary basis (Le Nguyen, 2014, p. 197). Until 1990s, it was mainly developed states’ concern to fight against money laundering. It became those developed states’ aim to spread AML policies to the whole world to prevent safe havens where criminals would go. Finally, by announcement of a blacklist FATF applied pressure for change to those countries where there are no such laws.



Nearly at the same time, some other regional bodies<sup>5</sup> have been created to spread AML policies to all part of the world by '*seminar diplomacy*' (Sharman, 2008, p. 641).

Before 1986, there was no single country adopting money laundering as a crime. By 2008<sup>6</sup>, over 170 states have criminalized money laundering and set up institutions to fight against it. This change represents an example of '*sameness amid diversity*'. Sharman claims that although there are some other mechanisms explaining why these states are tending to opt for the same policies although they have nothing in common, four mechanisms are accepted as most common mechanisms: *learning or lesson drawing, coercion, mimicry or emulation, and competition effects*. It is stated that rational or boundedly rational learning has played little or no role. In addition to direct coercion, mimicry and competition effects have also been important in policy transfer (Sharman, 2008, pp. 635-6).

Coercion as blacklisting has been FATF's deliberate use of power to impose AML policies. Mimicry, as second mechanism, states have seen AML policies should be adopted in line with changing social expectations among transnational networks of regulators which defined these regulations as something all progressive that should be fulfilled by modern states. Competition effects have revealed as private firms which constructed abstract proxies for AML risk, coincidentally creating material penalties for those states which failed to adopt AML policies (Sharman, 2008, p. 636).

In his article Sharman conducts a small-N cross regional study by focusing on three small developing countries: Barbados in Caribbean, Mauritius in the Indian Ocean, and Vanuatu in the Pacific. These countries are few of the states which

---

<sup>5</sup> FATF, APG, CFATF, EAG, ESAAMLG, GAFILAT, GIABA, MENAFATF, GABAC and MONEYVAL are the organizations working on anti-money laundering. Available at: <http://www.fatf-gafi.org/countries/> , accessed February 7, 2016

<sup>6</sup> See *Ibid*, Most of the countries contribute anti-money laundering initiatives. The total number of the states contributing to those initiatives is 219 while some of them are members of more than one initiative. Two states are accepted as high-risk and non co-operative states (Democratic People's Republic of Korea and Iran). Available at: <http://www.fatf-gafi.org/countries/#high-risk> . Eleven states are indicated as "Jurisdictions with strategic deficiencies" (Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, Lao PDR, Myanmar, Papua New Guinea, Syria, Uganda, Vanuatu and Yemen). Available at: <http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-february-2016.html> accessed March 9, 2016)

adopted earlier within developing countries. Note worthily, none of these countries has been classified as posing high money-laundering risk neither by FATF nor US government (Sharman, 2008, pp. 638-9).

It is difficult to evaluate the success of laundering policies either before or after AML policies are adopted. OECD members have applied very few convictions and confiscations of dirty money. However, the United States have applied many convictions. FATF has assumed that the number of the convictions and asset confiscations are the indicators of appropriate measures of effectiveness (Sharman, 2008, p. 642).

AML policies are expensive policies while the benefits are elusive (Le Nguyen, 2014, p. 197). A study in the United States stated that: *“Little systematic evidence has been advanced that... extension of AML regime, with the costs they impose on legitimate businesses and their customers, will do more than marginally inconvenience those who need to launder the proceeds of their crimes”* (Reuter & Truman, 2004, p. 7; J.C.Sharman, 2008, p. 642). Expanding dynamism of due diligence and Know Your Customer requirements are significant burdens on firms and subsequently customers. Eventually, expansion of AML policy is not a candidate for policy diffusion by rational learning or lesson drawing (Sharman, 2008, p. 642).

Money laundering model suggests common criminal legislation which allows freezing and confiscation of criminal funds, instituting due diligence and Know Your Customer requirements for financial institutions, establishing suspicious transactions reporting system for banks and firms, creating Financial Intelligence Units and allowing financial intelligence for sharing obtained information with foreign law enforcement and regulatory agencies (Sharman, 2008, p. 642).

According to results obtained from Sharman’s study, it is ambiguous if new measures enforced in those three countries are effective to prevent money laundering. Legislative provisions for confiscating and criminal assets which are primary indicators of effectiveness for FATF have not been applied at all (Sharman, 2008, p. 642).

Weyland claims that states will adopt ineffective policies to legitimate themselves internationally only when measures are cheap, or at least costs are shared and thus politically low-profile. But this is quite different what experienced in AML policy. Although the cost of those policies is high and politically annoying especially for developing countries it has been expanded (Sharman, 2008, p. 643).

## **2.1. Mechanisms of Diffusion**

Sharman states that power is explained in three forms from a constructive perspective: by a centralized power-coercion, de-centralized manner within social peer groups-mimicry or markets-competition. Author claims that although they work in combination, coercion comes before mimicry and competition logically and temporally (Sharman, 2008, p. 643)

### **2.1.1. Coercion and Blacklisting**

The most important coercive power of FATF is blacklisting of Non-Cooperative Countries and Territories which is drawn up in June 2000. FATF had already started compiling a list from 1998 and losing its patience. The US was concerned financial secrecy and crime while European states were concerned with tax losses of jurisdictions with ambiguous financial sectors. FATF seemed to lack of coercive power as it has no formal legal existence or cannot make international law. Re-invention was needed to be able to apply trade sanctions. Funds were needed to apply and monitor sanctions on member states. But the organization was never able to extend or withhold loans. Furthermore, none of the members were in favour of these sanctions. As a result of discussions, publicly branding those countries which are non-compliant was found consistent with existing procedures (Sharman, 2008, p. 644).

In 2001, 23 jurisdictions of 47 assessed countries were placed in blacklist until they legislate and implement AML policies. Although blacklisting did not have any formal legal sanctions, it is recommended that financial institutions should be more vigilant on transactions going to, and from those jurisdictions (Sharman, 2008, p. 644).

Barbados, Mauritius, and Vanuatu were not listed within 23 jurisdictions. But policy-makers and financial services believed that being listed would be dangerous. It seemed as a demonstration effect such as *'heads on sticks'*. With FATF blacklist, not only listed countries but also other countries were warned to amend their policies consistent with AML policies. As a result of blacklisting many countries raced to adopt those policies. Those states which were blacklisted agreed that they suffered a lot being blacklisted. Many large international banks cut off their links with others in those tainted jurisdictions. Others which did not want to cut their links had to compensate the costs of scrutiny. Moreover, the tourist sector has also been affected badly by foreign hotel-developers who were worried about their ability to use international financial networks (Sharman, 2008, p. 645).

It is difficult to link material decline to the effects of blacklisting. Nonetheless, according to many government officials being blacklisted caused the damage in those countries. As a result, those countries tried to adopt the policies as soon as possible. Blacklisting was seen as *'a gun to the head.'* Countries were ready to do what is required to avoid the wrath of the FATF; otherwise it was believed that their international finance sector would be destroyed (Sharman, 2008, p. 645).

Blacklisting had two powers. Like public trials or executions of hundreds years ago, the affects were not only on targets but also on the audiences (Sharman, 2008, p. 645).

### **2.1.2. Mimicry or Social Acceptance**

In mimicry or social acceptance the policy-makers copy the organizational forms of selected leaders when the situation is complex and uncertain. The purpose is to share common values of modern international society whether the policies are suited for the local conditions and for the solutions of the problems. The governments adopted these policies and funded them although these policies were not critically important. They just fund them to show what is approved. The expenditure of the government is mostly a symbol. Similarly establishing a Financial Intelligence Unit does not contain a meaning of attacking on money laundering, but to share what is done by peers and they are in line with shared

values. Both governmental and non-governmental international organizations play a leading role in distributing these shared values (Sharman, 2008, p. 646).

Sharman's view explains mimicry as centred on power. Contrary to what is believed, mimicry does not reveal by endeavour to reduce uncertainty in complex environment or to receive public praise and enhanced self-esteem, but by fear of losing social acceptance. Similarly Weyland states that: Governments dread the stigma of backwardness and therefore willingly adopt those policy innovations, regardless of functional needs (Weyland, 2005, p. 270).

The Author claims that scholars understate the power based character of mimicry and also the proposition that, at least for developing countries policy diffusion by mimicry occurs in a coercive process. (Sharman, 2008, p. 647). Once they initiate to adopt policies they engage in assessments, meetings, conferences and exchanges conducted with a large number of international organizations. They carry out regular assessments and peer reviews in terms of basic standards and see if they are met or not. National regulators refrain from being qualified as derelict in their duties, backwards, or substandard by their peers. Reputation among one's peer is a very strong tool of professional socialization especially in the profession of governance (Sharman, 2008, p. 648).

Behaviours are intentional but not wilful. They fulfil the obligations and try to determine the imperatives of holding position. Action comes from a conception of necessity, rather than preference (March & Olsen, 1989, pp. 160-61; J.C.Sharman, 2008, p. 648).

Conversely, Jon Elster stated that it is not possible to reduce the effects of common perceptions of appropriate behaviour to avoidance from social sanctions. Applying social sanctions is costly. While there is sanction to be applied, if it fails to apply to inappropriate behaviour then it becomes vulnerable of infinite regress (Elster, 1989, p. 120; J.C.Sharman, 2008, p. 649).

In this regard, mimicry and coercion are linked in the process. For the occurrence of socialization, parties must be in regular touch with a community sharing and defined by certain values and practices. Mimicry itself poses a problem: if a country does not have AML institutions then why would engage with those

international organizations? Mimicry logically and temporally comes after blacklisting as blacklisted countries did not have any benefit from establishing AML institutions before they were in the list. Similarly, the NCCT (Non-Cooperative Countries and Territories) list provided impetus for developing countries to follow developed countries as adopting AML policies became a marker of international respectability (Sharman, 2008, p. 649).

### **2.1.3. Competition and Risk Ratings**

In this policy diffusion method, politics' choices become interdependent rather than independent choices reflecting domestic circumstances. This method has a simple logic. If country "A" decreases corporate tax rates, country "B" becomes under pressure to do so, otherwise capital will be flying to country "A" (Sharman, 2008, p. 649). Same situation is effective for ML policy. If a state is not cooperative in terms of ML policy, it is assumed as risky and out of the team. This situation makes the state non-investable (Sharman, 2008, p. 650).

McNamara states that *'governments choose to delegate not because of narrow functional benefits but rather because delegation has important legitimizing and symbolic properties.'* What McNamara stated is about monetary policy to independent central banks. Sharman states that it is also consistent with ML policy (Sharman, 2008, p. 650)

Furthermore, adopting ML policies impress foreign firms not only by the reduction of policy risk or fitting with local circumstances, but also as it is an indication about the country within the fold (Sharman, 2008, p. 650).

There is no evidence in terms of the presence of AML policies decrease the risk of money laundering in developing countries or acts as an indicator of such risk. In this sense, for developing countries or firms adopting AML policies seems unnecessary (Sharman, 2008, p. 651).

On the other hand the author claims that, similar to mimicry, competition is a form of diffusion and it has a problem of origins: for competitive dynamic to diffuse AML policy, certain number of countries must have already adopted AML standards. So if some few countries have adopted this policy, there may be little

competition between such states. Eventually it is claimed that by blacklisting the FATF not only had been successful in 23 targeted countries but also reinforced itself by largely unintended process of socialization and competition which now made AML policy a near-universal standard (Sharman, 2008, p. 651).

## **2.2. Hegemony and Diffusion**

Some scholars of International Relations state that homogenization of economic policy is driven by hard or soft power of United States (Ikenberry & Kupchan, 1990, p. 283; Lake, 1993, p. 476; J.C.Sharman, 2008, p. 652). Similarly, the United States played a more prominent role than any other state both in establishing FATF and blacklisting strategy (Sharman, 2008, p. 652).

Most of the scholars would agree that the United States has more influence than any other state in most aspects of international policy-making and enforcement. In this tradition, hegemony provides public goods either benevolently or coercively. But it must be noted that there is very little evidence of AML policy constitutes public good. The situation is the same for whether the US or any other country benefit from AML standards (Sharman, 2008, p. 652).

## **2.3. Summary of the Progress**

As a result AML policy has been diffused within developing world through the direct and indirect effects of power despite significant and politically high-profile costs. Three mechanisms have been propellant: coercive (blacklisting), mimicry and competition.

Coercion provided a negative status which was widely linked with material costs. Unlike blacklisting, mimicry operated in a decentralized and indirect manner. By mimicry, AML policies have become norms. The officers felt the need to respond to those expectations. Competition effects produced mediated material pressures with international AML standards. Developing states instrumentally adopted so-called useful but ineffective policy to minimize material costs (Sharman, 2008, p. 653).

Sharman alleges that diffusion in various disciplines should be more sensitive to the direct and indirect effects of coercion and it should be possible to advance

power-based explanations that are outside the rationalist and materialist frame (Sharman, 2008, p. 653).

Before proceeding to Cybercrime Policy, diffusion of Anti-Money Laundering regime will be discussed as a case study in the next section.





## CHAPTER 3

### ANTI-MONEY LAUNDERING

Money laundering is defined as “*the process that disguises illegal profits without compromising the criminals who wish to benefit from the proceeds*” (Nelson, 2007, p. 725; J.C.Sharman, 2008, p. 639). In this context, money laundering is a serious problem not only for banking circuits but also for national economies as a whole (Popa, 2012, p. 575). Money laundering has been assumed as one of the transnational organized crime. For this reason, state agencies dealing with the issue have to adopt new agencies and methods to follow up the operators engaged in international money laundering to prevent and apply sanctions on such crimes (Popa, 2012, p. 576). In this context, between national agencies of different countries new ways of cooperation refers to legal institutions of extradition, rogatory letters, enforcement of the final sentences issued by other states, seizure and confiscation proceeds for crimes committed abroad in the area of crime investigation and financial, banking and property crimes (Popa, 2012, p. 575).

Although money laundering term is relatively new, it was applied in medieval Europe. In 1970s, US government and law-makers admitted that drug traffickers use financial institutions to launder the money obtained from drugs. Thus, the first step has taken to prevent money laundering by Bank Secrecy Act, in 1970. As law enforcement agencies needed more power to prevent, detect and prosecute launderers. Money Control Act was adopted in 1986. US authorities realized that money laundering regime must include both criminalization of money laundering and deprivation of illicit profits. Furthermore, it was believed that a strong cooperation is needed between the states affected by illegal drug activities. The US also prompted development of a kind of law models in other countries through soft power. One early initiative about money laundering is Statement on Preventing Criminal Use of the Banking System for the Purpose of Money Laundering by Basel Committee on Banking Regulation in 1988. It encouraged banks to know their customers to prevent suspicious transactions and be in cooperation with law enforcement agencies (Le Nguyen, 2014, pp. 198-200).

Money laundering has taken its place as a term in United Nations Convention against illicit Traffic of the Narcotics and Psychotropic Substances<sup>7</sup> in December 19, 1988. The Convention defined the legal term for money laundering for the first time (Popa, 2012, p. 577) and stressed the importance of legal instrument on money laundering and increasing international co-operation. It is the first binding international legal instrument which obliges parties to criminalize money laundering the proceeds of drug related crimes and to adopt confiscation measures (UN, 1988; Le Nguyen, 2014, p. 201). Insufficiency of criminal system and necessity to regulate private financial intermediaries were underlined. Banks and financial institutions are required to apply due diligence or '*Know Your Customer*' rules which means verifying identity of the customers by passports, driver's licence etc. Moreover, they have been obliged to inform suspicious transactions to special units which were set up especially for financial intelligence. This application has expanded from banks to other financial companies (Sharman, 2008, p. 640). Thus, the regulations have been a burden for private institutions in terms of money laundering regulations. The Convention reflects the regulations which are already in US law. It has been cornerstone of AML regime and significant influence on other initiatives (Le Nguyen, 2014, p. 201).

A legal response to money laundering was firstly initiated by the United States and other leader countries to prevent drug treat and abolish threats to financial systems. Nevertheless, since the 1990s, international organizations and institutions, such as the FATF and the UN, have taken leadership in order to develop AML regime. Institutions have adopted each others' ideas and provisions (Le Nguyen, 2014, p. 206).

Western dominance of these organizations is obvious and undeniable. The AML regime has evolved rapidly with the expectation which will serve as a mean for: suppressing predicate crimes, particularly organized crime; protecting the integrity and supporting the good governance of financial systems; combating corruption; and countering the financing of terrorism (Le Nguyen, 2014, p. 206).

---

<sup>7</sup> United Nations Convention against Illicit Traffic of the Narcotics and Psychotropic Substances, Available at: [https://www.unodc.org/pdf/convention\\_1988\\_en.pdf](https://www.unodc.org/pdf/convention_1988_en.pdf) , accessed January 27, 2016

Active cooperation is needed between national banks and commercial banks and unification of databases by the appearance of unique international database in order to monitor effectively all financial and banking operations, especially those which are suspected as may be involved in recycling funds. International cooperation and effective action against tax havens are very crucial (Popa, 2012, p. 576).

The FATF is the most prominent organization in anti-money laundering diffusion. Although there are some other organizations and initiatives both international and regional, it has been the most effective one. It is the primary actor which provides diffusion of anti-money laundering policies.

### **3.1. Anti-Money Laundering Initiatives**

#### **3.1.1. The European ML Conventions and Directives**

Council of Europe and European Union are other important organizations actively contributing to AML policies (Le Nguyen, 2014, p. 202). On November 8, 1990 at Strasbourg, European countries adopted the Convention on Laundering, Search and Seizure and Confiscation of the Crime Product (Popa, 2012, p. 577).<sup>8</sup> In 1991, the Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering which is a key instrument has been adopted by European Council.<sup>9</sup> The most salient side of the directive was that money laundering was no longer associated with drug related crimes. Furthermore, it also introduced a mandatory reporting obligation for the financial and credit institutions including suspicious transactions (Mitsilegas & Gilmore, 2007, p. 120). This development has been received by FATF recommendations in 1996. Subsequently, further developments of FATF have been received by European Money Laundering Directives in 2001, 2005, 2008. (Le Nguyen, 2014, p. 202).

---

<sup>8</sup> Convention on Laundering, Search and Seizure and Confiscation of the Crime Product (Available at: <https://e-justice.europa.eu/fileDownload.do?id=d13b8312-5905-40ed-8731-16681d997320>, accessed January 31, 2016)

<sup>9</sup> The Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering (Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN> , accessed on February 19, 2016)

### **3.1.2. Interpol**

Interpol has adopted several resolutions which call Member States to cooperate in AML. Some of them were about dealing firmly and effectively with the system of illegal transactions in 1991, money laundering legislation, money laundering investigation and international police cooperation, and money laundering statistics in 1997. An examination conducted in Asia by Interpol has been one of the main references for law enforcement agencies to respond to money laundering activities committed in the region (Le Nguyen, 2014, p. 203).

### **3.1.3. The Egmont Group of Financial Intelligence Units (FIUs)**

To fight against money laundering Financial Intelligence Units are also important in terms of rapid exchange of information between financial institutions, law enforcement agencies and jurisdictions for the purposes of investigation and prosecution. They must be competent to systematically analyze and cross-check information with other sources (Thony, 1996, p. 264). A group of FIUs held a meeting in 1995, at Egmont Arenberg Palace in Brussels and established the Egmont Group to facilitate international cooperation (Le Nguyen, 2014, p. 204).

FIU has been defined by the Group as: *a central national agency responsible for receiving (and, as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information: (1) concerning suspected proceeds of crime and potential financing of terrorism, or (2) required by national legislation or regulation, in order to counter money laundering and terrorism financing* (Le Nguyen, 2014, p. 204).

Member FIUs meet regularly to enhance mutual co-operation in the exchange of information, training, suppression of terrorist financing and sharing of expertise in terms of AML (Le Nguyen, 2014, p. 204).

### **3.1.4. The Wolfsberg Group**

The group is an association of eleven global private banks which was established in 2000. The key function of the group is to work on global AML guidelines for private banking. The Principles of the group has been published in October 2000 and revised twice in May 2002 and June 2012. It provides the main principles on

due diligence requirement for the clients of private banks and beneficiaries of financial transactions (Le Nguyen, 2014, p. 204) <sup>10</sup>.

### **3.1.5. The UN Convention against Transnational Organized Crime (Palermo Convention)<sup>11</sup>**

The Convention is an attempt to address transnational organized crime including money laundering globally. Criminalizing activities of criminal groups, criminal proceeds of these activities, counter-measures of money laundering and measures to confiscation and seizure of proceeds both in national and international level are included in Convention. It provides legal tools to provide power to confiscate criminal assets and crack down on money laundering globally (Le Nguyen, 2014, p. 205; UN, 2004).

### **3.1.6. The United Nations Convention against Corruption (UNCAC)<sup>12</sup>**

Another complementary convention to AML regime in several dimensions is UNCAC. The Convention is the first international binding treaty which provides anti-corruption measures at international level. The link between corruption and money laundering is acknowledged in the Convention. The UNCAC requires other international AML standards, such as criminalization (UN, 2003, ¶ 23), freezing, seizure and confiscation of the proceeds obtained from crime (UN, 2003, ¶ 31). Complying with the standards of UNCAC is consistent with AML policies as well (Le Nguyen, 2014, p. 205).

### **3.1.7. OECD**

Tax related crimes and money laundering are the concern of the OECD. In order to improve cooperation between tax and AML authorities and to strengthen existing AML counter-measures, OECD's Committee on Fiscal Affairs established a dialogue with the affiliation of the FATF. New recommendations were adopted by

---

<sup>10</sup> Wolfsberg Private Banking Principles May 2012, Available at: <http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Private-Banking-Principles-May-2012.pdf> , accessed on February 19, 2016

<sup>11</sup> United Nations Convention against Transnational Organized Crime, available at: <http://www.un-documents.net/uncatoc.htm> , accessed on February 19, 2016.

<sup>12</sup> United Nations Convention Against Corruption, available at: [https://www.unodc.org/documents/brussels/UN\\_Convention\\_Against\\_Corruption.pdf](https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf) , accessed on February 22, 2016

the OECD to facilitate cooperation between tax and other law enforcement authorities to fight against serious crimes including money laundering (Le Nguyen, 2014, p. 205).

### **3.1.8. ASEAN's AML initiative<sup>13</sup>**

Since 1996-97 Association of Southeast Asian Nations (ASEAN) has been vigilant to the expansion of money laundering crimes in the region (Pushpanathan, 1999). Transnational crimes such as terrorism, money laundering, arms smuggling and piracy have been assumed as a great threat for states' security and stability of the region. ASEAN Member States signed the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters in 2004, which was an important step for cooperation in response to transnational crime. ASEAN has called Member States for widest cooperation in order to provide a peaceful and prosperous ASEAN community in 2015 (ASEAN, 2009, p. 5). Eight types of transnational crime have been prioritized in October 2011 at the ASEAN Ministerial Meeting on Transnational Crime (AMMTC): terrorism, drug trafficking, money laundering, sea piracy, trafficking in persons, international economic crime, arms smuggling, cyber crime and it has been underlined that money laundering was the backbone of the most of transnational crimes (ASEAN, 2011; Le Nguyen, 2014, p.206).

### **3.1.9. The FATF**

One of the international organizations, FATF, has taken the lead in defining and spreading international standards (Sharman, 2008, p. 640). Financial Action Task Force on Money Laundering (FATF) was established by G-7 summit in 1990 in Paris (FATF, n.d.). Its purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing (Nelson, 2007, p. 733). They released 40 recommendations in 1990 (Sharman, 2008, p. 640). FATF recommendations are not legally binding. However, the Forty Recommendations are described as "*the crown-jewel of soft law.*" Its effectiveness stems from its penalties which mean severe trade sanctions to uncooperative

---

<sup>13</sup> ASEAN is an organization which is established on 8<sup>th</sup> August 1967. It was founded by 5 states and reached to 10 member states. Available at: <http://www.asean.org/asean/about-asean/history/> , <http://www.asean.org/asean/asean-member-states/> , accessed on February 22, 2016.

countries (Nelson, 2007, p. 733). In October 2001 financing of terrorism has been added by nine special recommendations. Forty plus IX recommendations have been the most comprehensive approach and provided an important framework for both national and international AML/CFT (Counter Financing of Terrorism) regime (Le Nguyen, 2014, p. 202).

The general idea of the recommendations was to collect more information on financial transactions of firms and individuals and use this to find, freeze and confiscate criminals' money. With the rise of cross-border crime and legitimate international finance and trade, money laundering has been argued in an increasingly global character. More than any other issue, international drug trade has triggered money laundering policy agenda as a problem which should be coordinated by international response. After September 2001 money laundering has been an umbrella term for a wide range of financial crimes (Sharman, 2008, p. 640).

Money laundering policy was diffused by regional organizations. It is not expected all states to join to FATF. The states which joined to any organization which conduct anti-money laundering policy equivalent to FATF assumed as one of the partners.

### **3.2. The FATF 40 Recommendations**

The FATF recommendations call upon all countries to take necessary actions to amend their domestic laws consistent with FATF recommendations and implement them. The Recommendations consist of measures which national systems should have within their criminal justice and regulatory systems, preventive measures which should be taken by financial institutions and certain other businesses, and international cooperation (FATF, 2003, p. 2).

The Forty Recommendations were drawn up in 1990 to prevent misuse of financial systems by persons laundering drug money. In 1996 it was revised for the first time and updated several times. In 1996 the Recommendations have been endorsed by more than 130 countries and became international money laundering standard. In 2001 complementary measures expanded by Eight Special Recommendations on Terrorist Financing. The FATF Forty Recommendations and Eight Special

Recommendations have been recognised by World Bank and International Money Fund as international standards to fight against money laundering and the financing of terrorism (FATF, 2003, p. 2).

By the Recommendations it is expected that to take the necessary actions to implement Vienna Convention and to ratify it. Financial institutions' secrecy laws should not prevent the implementation of the recommendations (FATF, 1990, ¶ 2; FATF, 2003, ¶ 4&36). By an effective cooperation, mutual legal assistance and cooperation are expected in investigations, prosecutions and extradition in money laundering cases (FATF, 1990, ¶ 1-3).

Criminalization of drug money laundering is expected from parties by Forty Recommendations of 1990 (FATF, 1990, ¶ 4). Countries should adopt their domestic laws to enable their competent authorities to confiscate property laundered, proceeds, instrumentalities used or intended to use in money laundering offence. These measures should include:

- a) Identify, trace, and evaluate property which is subject to confiscation,
- b) Carry out provisional measures such as freezing and seizing to prevent any dealing, transfer or disposal of such property and,
- c) Take any appropriate investigative measures.

In addition to confiscation and criminal sanctions, some other measures should be considered such as monetary and civil penalties (FATF, 1990, ¶ 8)

The Forty Recommendations states that the recommendations between 12 and 29 should be applied not only to the banks but also to other non-bank financial institutions (FATF, 1990, ¶ 9). Similarly, the Recommendations of 2003 advice that in addition to financial institutions, some other non-financial businesses and professions such as casinos; real estate agents; dealers in precious metals and stones; lawyers, notaries, other independent legal professionals and accountants; and trust and company service providers should take certain precautions (FATF, 2003, ¶ 9).

It provides a responsibility to financial institutions that they should undertake customer due diligence (CDD) measures which includes identifying customers by



using reliable documents (FATF, 1990, ¶ 12). Furthermore, these identifications and transactions both national and international should be recorded for at least five years. These documents should be available for the investigations and prosecutions of the competent authorities (FATF, 1990, ¶ 13-14).

Financial institutions should pay special attention to unusual large money transactions. These suspicious transactions should be reported to the competent authorities as soon as possible (FATF, 1990, ¶ 15). The institutions should develop special programs against money laundering (FATF, 1990, ¶ 20).

Financial institutions should pay special attention to business relations and transactions from the countries which are not sufficiently applying recommendations (FATF, 1990, ¶ 21)

Countries should encourage the development of modern and secure techniques of money management (FATF, 1990, ¶ 25). The competent authorities of the states should ensure the effective implementation of the Recommendations (FATF, 1990, ¶ 27).

National administrations should consider about recording international flow of money. This information should be available to IMF and BIS to facilitate international studies (FATF, 1990, ¶ 30). International authorities such as Interpol and Customs Cooperation should be given responsibility to gather and disseminate information about the latest developments in money laundering (FATF, 1990, ¶ 31).

Countries should encourage signing international agreements such as the draft Convention of the Council of Europe on Confiscation of the Proceeds from Offences (FATF, 1990, ¶ 35).

Countries should create and facilitate procedures which make mutual assistance in criminal matters available. Competent authorities should be appointed for the requests on expeditious action coming from other countries (FATF, 1990, ¶ 37-8)

Special consideration should be given to the cases subject to prosecution in more than one state. The same consideration should be given to the coordination of seizure and confiscation of the proceeds (FATF, 1990, ¶ 39).

Finally, each country should recognise money laundering as extraditable. Extradition procedures in terms of money laundering should be simplified (FATF, 1990, ¶ 40).

In October 2001 Eight Special Recommendations regarding financing of terrorism has been published.<sup>14</sup> It was a quick response to the terrorist attack in September 9, 2011 (Nelson, 2007, p. 734).

By the Eight Special Recommendations immediate ratification and implementation of 1999 United Nations International Convention for the Suppression of the Financing of Terrorism is expected. Moreover, necessary adoptions on the criminalization of the financing of terrorism, terrorist acts, terrorist organisation and freezing and confiscation of terrorist assets should be completed (FATF, 2008, p. 2).

A national method of reporting suspected funds for terrorism, terrorist acts or terrorist organisations should be established. Financial and non-bank financial institutions which provide transmission of money or value should be subjected to the Recommendations. Effective and prompt criminal investigations and prosecutions on suspected terrorist financing should be ensured. CDD should be completed by all financial institutions and enhanced security measures should be adapted to the customers who do not provide originator information (FATF, 2008, pp. 2-3).

Between 2000 and 2001 FATF assessed 47 countries and announced 23 jurisdictions as not meeting the standards of FATF until they implement AML policies. Although the list did not impose any legal sanctions it recommended that financial institutions should impose high level of scrutiny on the transactions going to, from or through a blacklisted country (Sharman, 2008, p. 644).

Although blacklisting does not impose any formal sanctions, it only recommended being more vigilant on transactions going to or from a blacklisted jurisdictions.

---

<sup>14</sup> Eight Special Recommendations on Terrorist Financing is available at: <http://www.un.org/en/sc/ctc/docs/bestpractices/fatf/9specialrec/fatf-9specialrec.pdf> , accessed on March 27, 2016.

Many states started to amend their domestic laws according to FATF Recommendations (Sharman, 2008, p. 644).



## CHAPTER 4

### CYBERCRIME INITIATIVES

By the increase in awareness of cyber threats, international organizations and states have started to look for the further precautions and procedural arrangements. So far, many initiatives have been implemented by both international organizations and NGOs.

#### 4.1. International Developments on Cybercrime:

In this chapter International developments on cybercrime will be discussed. G8, United Nations and International Telecommunication Union are the organizations dealing with the issue at international level.

##### 4.1.1. G8<sup>15</sup>

It should be underlined that the most substantive international treaty, Convention on Cybercrime has widely benefited from G8 experience and decisions (CoE, 2001b, ¶ 137, 298). In 1995, a summit was held in Canada Senior Experts Group on Organized Crime has been created. The Group has prepared “Recommendations on International Organized Crime Report” in April. The Report states that: The states should review and adopt their domestic laws according to modern technologic abuses to define high tech crimes as punishable (Turhan, 2006, p. 76).

In 1997, G8 countries established a committee dealing with high-tech crimes. During their meeting Justice and Home Affairs Ministers adopted ten principles and Ten-Point Action Plan to fight against high-tech crimes (UN, 2005; Gercke, 2012, p.114). These were mainly including those principles:

- There must be no safe havens for those who abuse information technologies.

---

<sup>15</sup> The Group of Eight (G8) countries consist of 8 countries: USA, Russian Federation, Canada, France, Germany, Japan, Italy, and United Kingdom. (Available at: <http://www.cfr.org/international-organizations-and-alliances/group-eight-g8-industrialized-nations/p10647>, accessed January 2, 2016)

- Investigation and prosecution of international high-tech crimes must be coordinated among all concerned states, regardless of where harm has occurred.
- Law-enforcement personnel must be trained and equipped to address high-tech crimes (Gercke, 2012, p. 114).

In subsequent years, G8 states declared their concern on combating against child pornography, traceability of transactions and transborder access to stored data, preventing lawless heavens, data retention or preservation obligations, the need for the creation of global capacities in the fight against criminal uses of the Internet, necessity of improving effective counter-measures (G8, 2006), criminalize the misuse of the Internet by terrorist groups, blocking of child pornography websites and disseminating blacklists by international organizations (G8, 2009), and strengthening 24/7 points of contact.<sup>16</sup>

The Leaders of the Group Eight declared their concern on cybercrime as a growing threat (G8, 2010, p. 12). In 2011, they also underlined their interest on Internet usage, illicit use of Internet for other purposes, increasing awareness of public, protection of children from sexual exploitation and protection of personal data (G8, 2011).

#### **4.1.2. United Nations**

The United Nations has undertaken a few important approaches about challenge of cybercrime. While the response was limited to general guidelines, the organization has dealt more intensively with the challenges and legal responses in the recent times (Gercke, 2012, pp. 114-115).

The United Nations Convention on the Rights of the Child, adopted in 1989, contains several instruments aiming to protect children. The Convention does not define child pornography, nor does it provide provisions on the criminalization of the distribution of online child pornography. Nevertheless, Article 34 invites

---

<sup>16</sup> 24/7 points of contact idea has been picked up by some other international organizations. One example is Convention on Cybercrime, Article 35; See Gercke Marco, Understanding Cybercrime: Phenomena, Challenges, and Legal Response, ITU, September 2012, p. 114, 115

Member States to protect children from exploitative use in pornographic performances (UN, 1989).

The UN General Assembly adopted a resolution dealing with computer-crime legislation in 1990 (UN, 1990). In 1994, it published a manual on the prevention and control of computer-related crime (UN, 2000).

UN committees discussed and took initiatives on engagement of children in real or simulated explicit sexual activities or any representation of the sexual parts of a child, distribution of those materials through Internet (UN, 2000). In a workshop held in 2000, categories of the crime, transnational investigation and legal response to the phenomenon were discussed and the conclusion report involved that criminalization is required; legislation needs to include procedural instruments, international cooperation is crucial and public-private partnership should be strengthened (UN, 2000b; Gercke, 2012, p. 116).

In the same year, the UN General Assembly adopted a resolution on combating the misuse of information technologies by criminal purposes. This resolution includes a number of similarities with the G8's Ten-Point Action Plan from 1997. According to Action Plan, states should ensure that their laws prevent safe heavens for those who misuse information technologies by criminal purposes. There must be coordination between all concerned states in the investigation and prosecution of international cases. Moreover, Law enforcement personnel should be trained and equipped properly to address the criminal misuse (UN, 2001; Gercke, 2012, p. 117).

In subsequent years, UN bodies discussed about development of domestic legislations to eliminate safe heavens for criminal misuse of technologies, consolidating law-enforcement capacities, enhancing the security of data and computer systems, training law enforcement authorities, building mutual assistance procedures and increasing public awareness on cybercrime (UN, 2001; Gercke, 2012, p. 117).

By the meeting in 2005, it was stated that existing cooperation to prevent, investigate and prosecute high-technology and computer-related crime, including

by developing partnership with the private sector is welcomed by UN (UN, 2005; Gercke, 2012, p. 118).

During the discussions of twelfth UN Congress on Crime Prevention and Criminal Justice held in 2010, calls were raised by Parties and academia for a comprehensive international convention on cybercrime. The discussions mainly focused on two main issues: how harmonization of legal standards can be achieved and how can developing countries be supported. Another intensive debate has been on the issue of whether Convention on Cybercrime should be supported. Eventually, Member States decided not to suggest ratifying the Convention, but to strengthen the UN's role. As a significant result Member States invited Commission on Crime Prevention and Criminal Justice to conduct an open-ended intergovernmental expert group to conduct a comprehensive study on the problem of cybercrime (UN, 2010; Gercke, 2012, p. 118).

First meeting of intergovernmental expert group held in January 2011. The group included representatives of Member States, intergovernmental and international organizations, specialized agencies, private sector and academia. A number of members underline the usefulness of existing international legal instruments, including the United Nations Convention against Transnational Organized Crime (UNTOC) and the Council of Europe Convention on Cybercrime, and the desirability of elaborating a global legal instrument to address the problem of cybercrime. Parties were agreed that the decision on whether a global instrument should be developed or not will be given after the study is completed (Gercke, 2012, p. 120).

The Draft version of Comprehensive Study on Cybercrime has been published in February 2013. The study is quite expanded and reveals the state of cybercrime; challenges of investigations, prosecutions, international cooperation, perpetrators' profile, public-private sector and academia relation etc (UNODC, 2013).

Moreover, the study contains results from 69 Member States. It includes reviews from 500 publicly available documents and information submitted by more than 40 states and 16 academic institutions. The study indicates that the reach of regional instruments such as Convention on Cybercrime is limited. In April 2013 the

Commission on Crime Prevention and Criminal Justice discussed the results of study. The Commission calls upon the member states to review the results and invites expert group to continue the study. Although, the calls submitted for a global harmonization, the Commission did not take action in this regard (Gercke, 2014, p. 129).

#### **4.1.3. International Telecommunication Union<sup>17</sup>**

ITU was the leading agency of the World Summit on the Information Society (WSIS) which took place in two phases in Switzerland (2003) and in Tunisia (2005). Governments, policy-makers and experts from around the world shared ideas and experiences about the development of a global information society, including the development of compatible standards and laws (Gercke, 2012, p. 121).

The Geneva Plan of Action underlines the importance of measures to be taken in the fight against cybercrime (ITU, 2003). Nevertheless, second phase of WSIS in 2005 refers to UN resolutions, Council of Europe's Convention on Cybercrime, and invites governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime (ITU, 2005).

ITU was nominated as the sole facilitator for building confidence and security in the use of information and communication technology which addressed in Action Line C5, as an outcome of WSIS. ITU announced the launch of the *ITU Global Cyber security Agenda* at the second Facilitation Meeting for WSIS Action Line C5 in 2007. The Global Cyber security Agenda includes the elaboration of strategies for the development of model cybercrime legislation (Gercke, 2012, p. 122).

The ITU Secretary-General created a high-level expert group bringing together representatives from Member States, industry and scientific field in order to analyse and develop measures and strategies with regard to the seven goals of

---

<sup>17</sup> The International Telecommunication Union (ITU) is a specialized agency within the United Nations which plays a leading role in the standardization and development of telecommunications and cyber security issues.



Global Cyber security Agenda. By the report published as “Global Strategic Report” in 2008, in addition to an overview of different regional and international approaches in fighting cybercrime, an overview of criminal law provisions, procedural instruments, regulations governing the responsibility of Internet service providers and safeguards to protect fundamental rights of Internet users were provided (Gercke, 2012, p. 122).

Furthermore, ITU conducted some capacity building activities, in terms of assisting Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyber threats. These measures consist of development of national strategies, legislation and enforcement, organizational structures, among other areas. ITU has developed cyber security/CIIP tools to assist Member States in raising national awareness, conducting national cyber security self-assessments, revising legislation and expanding watch, warning and incident-response capabilities. Two of them are *Understanding Cybercrime: A Guide for Developing Countries, the ITU National Cyber security/CIIP Self-Assessment Tool and the ITU Botnet Mitigation Toolkit* (Gercke, 2012, p. 122). Lastly, ITU has published its renewed work *Understanding Cybercrime: Phenomena, Challenges and Legal Response* in November 2014.

## **4.2.Regional Developments on Cybercrime**

In this section regional developments on cybercrime will be elaborated. These organizations are European Union, Organization for Economic Co-operation and Development, Asia Pacific Economic Co-operation, Commonwealth, African Union, Arab League and Gulf Cooperation Council, Organization of American States and Council of Europe.

### **4.2.1. European Union<sup>18</sup>**

European Union is another important organization dealing with cybercrime issues. Within the last few decades the European Union (EU) has developed several legal

---

<sup>18</sup> EU is a unique economic and political regional partnership between 28 Member States. Available at: [http://europa.eu/about-eu/basic-information/about/index\\_en.htm](http://europa.eu/about-eu/basic-information/about/index_en.htm) , [http://europa.eu/about-eu/countries/member-countries/index\\_en.htm](http://europa.eu/about-eu/countries/member-countries/index_en.htm) , accessed January 8, 2016

instruments addressing aspects of cybercrime. While those instruments are only binding for the Member States, some other states are using the EU standards as a reference point in their national and regional discussions on harmonization of legislation (Gercke, 2012, p. 128).

In 1996, the EU had already addressed the risks related to the Internet in a communication dealing with illegal and harmful content on the Internet (EU, 1996). It highlighted the importance of combating illegal online content between Member States. An action plan was adopted by European Parliament and the Council on promoting safer use of the Internet and combating illegal and harmful content on global Networks. The action plan was not focusing on criminalization but rather on self-regulation (EU, 1999a; Gercke, 2012, p. 129).

In 1999, the EU launched an initiative “*eEUROPE-An Information Society for all*” (EU, 1999b). In 2001, the European Commission (EC) published a Communication titled “*Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*”. In 2001, the European Commission (EC) published a communication which analyses and addresses the need for effective action to deal with threats to the integrity, availability and dependability of information systems and networks (EU, 2001b).

Having been participated in both G8 and CoE discussions, the Commission admits complexity and difficulty of procedural law issues. But, EC states that effective co-operation within the EU to combat Cybercrime is an essential element of safer Information Society and the establishment of an Area of Freedom, Security and Justice. In the Communication aspect, it is stated that the Commission will continue to play a leading role between Member States by contributing to international discussions such as Council of Europe and G8 (EU, 2001b).

In addition to the communication on computer-related crime, the EC published a communication on “*Network and Information Security*” which elaborates the problems of network security and drafted a strategic outline for action in 2001 (EU, 2001a; Gercke, 2012, p. 130)

Both communications emphasized the need for approximation of substantive criminal law within the European Union. Harmonization of substantive criminal law against cybercrime has taken its place in all initiatives at the EU level (Gercke, 2012, p. 130).

The EU adopted a directive in 2000 on Electronic Commerce about liability of Internet service providers for acts committed by third parties. Directive highlights on the importance of harmonization of criminal law in e-commerce but also indicates that there is no intention towards it (EU, 2000; Gercke, 2012, p. 130).

In 2000, the Council published a Decision on child pornography. It was a follow up to the 1996 communication on illegal and harmful content on the Internet (EU, 1999a; Gercke, 2012, p. 130).

First EU legal framework addressing aspects of cybercrime was adopted in 2001. It contains obligations on harmonizing criminal law legislation with regards to specific aspects of computer related fraud and the production of instruments such as computer programs (EU, 2001c; Gercke, 2012, p. 131)

European Commission presented a proposal for a framework decision on attacks against information systems in 2001 (EU, 2005a). It was modified and adopted in 2005. It addresses the Convention on Cybercrime and concentrates on harmonization of substantive criminal law provisions which are designed to protect infrastructure elements (Gercke, 2012, p. 131).

The Council adopted Data Retention Directive in 2005 (EU, 2005b). The Directive contains an obligatory provision for Internet Service Providers (ISPs) to store traffic data which is necessary for the identification of offenders in cyberspace (EU, 2005b, ¶ 1.1). The proposal received many critiques on differences between legal and technical standards of data protection, its obstacles and necessity of financial investments for ISPs (Gercke, 2012, p. 131). Finally, Directive on data retention <sup>19</sup> has been ratified.<sup>20</sup>

---

<sup>19</sup> Directive 2006/24/EC of The European Parliament and of The Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. (Available at: <http://eur->

In 2007, the EC published a communication towards a general policy on cybercrime. The communication gives significant importance to the Council of Europe's Convention on Cybercrime as an international instrument in the fight against cybercrime. Additionally, the communication points out the issues which will be focused in future activities (EU, 2007; Gercke, 2012, p. 130).

In 2007 the EU discussed an amendment on the Framework decision on combating terrorism as it was not criminalizing the dissemination of terrorist expertise through Internet (EU, 2008). With the amendment EU aimed to close the gap and bring the EU closer to the Council of Europe's Convention on the Prevention of Terrorism (Gercke, 2012, p. 132).

Directive on combating the sexual abuse and sexual exploitation of children and child pornography, which was adopted in 2011 was the first cybercrime-related draft legal framework presented after the ratification of the Treaty of Lisbon. The Directive recommends the criminalization of obtaining access to child pornography by means of information and communication technology. The Explanatory Report to the Convention on the Protection of Children recommends that the provision should be applicable where the offender only views pornographic content without downloading (CoE, 2007, ¶ 140). In addition to the criminalization of child pornography, the initiation draft contained a provision which obliges Member States to implement blocking websites. But eventually, it was left to Member States as none of the technical concepts has proven to be effective and because of the risk of over-blocking (EU, 2011; Gercke, 2012, p. 132).

In September 2010, the European Union presented a proposal for a Directive on attacks against information systems to amend Council Framework Decision on attacks against information systems of 2005. The aim was to update and

---

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF](http://lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF) accessed January 14, 2016)

<sup>20</sup> The Directive has been ruled as invalid by the Court of Justice of the European Union decision on 8th April 2014, as Directive 2006/24 does not provide sufficient safeguards to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. Case Number: C-293-12 and C-594-12, paragraph 54. (Available at: <http://curia.europa.eu/juris/document/document.jsf?sessionId=9ea7d0f130d594eab14e946d4bd490b39e18680666bc.e34KaxiLc3eQc40LaxqMbN4Oc3yLe0?text=&docid=150642&pageIndex=0&dclang=en&mode=req&dir=&occ=first&part=1&cid=671505> , accessed January 14, 2016)

strengthened the legal framework to fight cybercrime in the European Union by responding to new methods of committing crimes. In addition to the criminalization of illegal access, illegal system interference and illegal data interference which are already introduced by the 2005 Framework Decision, draft Directive of 2010 contains two additional offences: illegal interception and tools used for committing offences (EU, 2010). Both of these provisions are largely consistent with the corresponding provisions of the Convention on Cybercrime (Gercke, 2012, p. 134).<sup>21</sup>

Until 2009 EU's mandate about criminal law was a little limited and contested. After Lisbon Treaty function of European Union has changed significantly. Articles from 82 to 86 of the Treaty on the Functioning of the European Union (TFEU) provide a responsibility to the EU on harmonizing criminal law legislation by the mandate (substantive criminal law and procedural law). Most relevant one with regard to cybercrime is Article 83. The article authorizes the EU to establish minimum rules regarding criminal offences and sanctions concerning serious crimes with a cross border dimension. Computer crime is one of the crimes mentioned in Article 83 particularly. Article 2 enables the EU to adopt legally binding acts and limit Member States' competence to the extent that EU has not exercised its competence. Stockholm Programme, which is adopted in 2009 as subsequent to Hague Programme, focuses on EU work in the area of justice and home affairs for a five years period. It underlines EU's intention to make use of the mandate by referring areas of crime mentioned in TFEU Article 83, and gives priority to the crimes of child pornography and computer crime (EU, 2010, p. ¶ 3.3.1; Gercke, 2012, pp. 128-9).

The European Union expressed its perspective consistent with Convention on Cybercrime (EU, 1999) and it also called its members to support the Convention (EU, 1999, ¶ 1). When the Convention was approved EU did not have a mandate to adopt a similar legal framework. Although, this state has changed after Lisbon Treaty, EU has not decided a change in its position so far. Furthermore, EU stated

---

<sup>21</sup> Draft has been approved on 12 August 2013. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013L0040&from=EN> , accessed January 06, 2016.

that the Convention should become the legal framework of reference for fighting against cybercrime at the global level. However, this does not mean that the EU will not come up with another proposal on cybercrime. The EU has two major advantages: Firstly, the EU directive has to be implemented within a short time contrary to CoE's signature and ratification process. (Gercke, 2012, p. 135). Secondly, the EU has a practice of constantly updating its instruments, whereas the Convention has not been updated in the last 13 years (Gercke, 2014, p. 146)<sup>22</sup>.

#### **4.2.2. Organization for Economic Co-operation and Development (OECD)<sup>23</sup>**

In 1983, a study on the possibility of international harmonization of criminal law to address the problem of computer crime has been initiated by the OECD. In 1985, the report was published which elaborated conventional legislation and its proposals for the fight against cybercrime. By the report, a recommendation conveyed including a list of which minimum offences should be considered criminalizing by the states, such as computer-related fraud, computer-related forgery, the alteration of computer programs and data, and the interception of the communications. In 1990, an expert group was created by the Information, Computer and Communications Policy (ICCP) Committee to develop guidelines for information security. Expert Group prepared a draft in 1992 which concerns the issues of sanctions and then it was adopted by the Council. The guidelines state that there is a growing international agreement on the core of computer-related offences which should be covered by national penal laws. Accordingly, national legislation should be reviewed periodically to ensure that it meets the dangers arising from the misuse of information systems. The guideline reviewed in 1997 (Gercke, 2012, pp. 135-6).

In 2002, "*OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*" which is also an update to the previous guideline was adopted as a recommendation by a second Expert Group. The guidelines contain nine complementary principles on: awareness, responsibility,

---

<sup>22</sup> Still there is no amendment by March 2016.

<sup>23</sup> OECD is a regional organisation of which the primary mission is to promote policies that will improve the economic and social well-being of people around the world. 34 States are member of the organisation. Available at: <http://www.oecd.org/about/>, <http://www.oecd.org/about/membersandpartners/>, accessed January 8, 2016.

response, ethics, democracy, risk assessment, Security design and implementation, security management and reassessment (OECD, 2002).

An OECD report was published in 2005, which analyzed the impact of spam on developing countries (OECD, 2005). The report indicates that spam is much more serious issue in developing countries than developed countries such as the OECD Member states. In 2007 OECD published a report on the legislative treatment of “cyber terror” in the domestic law of the individual states, after receiving a request from Secretary General of the United Nations to produce a comparative outline of domestic legislative solutions regarding the use of Internet for terrorist purposes (Gercke, 2012, p. 136).

In 2008, OECD published a Scoping Paper on online identity theft (OECD, 2008). The paper highlights that most of the OECD countries do not address the issue of the question whether ID theft should be criminalized as a standalone offence (Gercke, 2012, p. 136).

In 2009 another report was published by OECD about malicious software. Although report addresses the aspects of criminalization, the focus is on the scope of malware and its economic impact (Gercke, 2012, p. 136).

#### **4.2.3. Asia Pacific Economic Cooperation<sup>24</sup>**

The Asia-Pacific Economic Cooperation (APEC) has identified cybercrime as an important field of activity. In 2002, a Statement on Fighting Terrorism and Promoting Growth to enact comprehensive laws relating to cybercrime and develop national cybercrime investigating capabilities has been released by APEC leaders. They were dedicated to enact a comprehensive set of laws on cyber security and cybercrime which are consistent with international legal instruments such as UN Resolution 55/63 and CoE’s Convention on Cybercrime. The leaders of APEC have called for closer cooperation among the officials involved in the

---

<sup>24</sup> APEC is the premier Asia-Pacific economic forum of which the primary goal is to support sustainable economic growth and prosperity in the Asia-Pacific region with 21 Member States. Available at: <http://www.apec.org/About-Us/About-APEC/Mission-Statement.aspx> , <http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx> , accessed January 8, 2016

fight against cybercrime.<sup>25</sup> Furthermore, they decided to identify national cybercrime units, international high technology assistance points of contact and establishing institutions which exchange threat and vulnerability assessment. Additionally, APEC has closely studied the national cybercrime legislation in various countries. However, the APEC has not adopted a legal framework on cybercrime until now but referred to international standards such as Budapest Convention on Cybercrime (Gercke, 2012, p. 137).

The organization has held various conferences to call for closer cooperation among officials who are involved in cybercrime investigations. In 2005, a conference was organized on Cybercrime Legislation. The objectives of the conference were to develop legal frameworks and promote cyber security, assist law-enforcement authorities and promote cooperation between cybercrime investigators across the region (Gercke, 2012, p. 137).

The APEC Telecommunications and Information Working Group<sup>26</sup> has actively participated in APEC's works to improve cyber security. In 2002, APEC Cyber security Strategy has been adopted by the Group. The report expresses its support on international instruments such as UN Resolution 55/63 and CoE Convention on Cybercrime (CCDCOE, 2002).

#### **4.2.4. Commonwealth<sup>27</sup>**

Commonwealth is one of the organizations dealing with cybercrime issues. The activities of Commonwealth particularly concentrate on harmonization of legislation. Law Ministers of the Commonwealth decided to establish an expert group to develop a framework for combating cybercrime on the basis of the

---

<sup>25</sup> Statement on Fighting Terrorism and Promoting Growth, Los Cabos, 26 October 2002. (Available at: [http://www.apec.org/Meeting-Papers/Leaders-Declarations/2002/2002\\_aelm/statement\\_on\\_fighting.aspx](http://www.apec.org/Meeting-Papers/Leaders-Declarations/2002/2002_aelm/statement_on_fighting.aspx) , accessed January 16,2016)

<sup>26</sup> The APEC Telecommunications and Information Working Group (TEL) aims to advance the development of information and communication technology (ICTs) infrastructure and services as well as to promote cooperation, information sharing and the development of effective ICT policies and regulations within the Asia-Pacific region. It also aims to enhance social and economic development through the effective use of ICTs as well as to promote a secure and trusted ICT environment. (Available at : <http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.aspx> , accessed January 16, 2016)

<sup>27</sup> Commonwealth is a voluntary association of 53 independent states. The organization provides guidance on policy making, technical assistance and advisory services to the member countries. Available at: <http://thecommonwealth.org/about-us> , accessed January 7, 2016.



Convention of Cybercrime, in 2002. Later in 2002, the draft Model Law on Computer and Computer Related Crime was presented (Gercke, 2012, p. 137). Until very recently the Model Law was largely neglected. Even recent calls by the Commonwealth Heads of Government and the Commonwealth Cybercrime initiative do not put Model Law to the centre of their strategy. Model Law is unavailable by a cursory search on Internet. Unfortunately the model had little impact upon both Commonwealth countries and other states (COE, 2014, p. 6).

In 2000, the Law Ministers and Attorney-Generals of small Commonwealth jurisdictions decided to set up an expert group to develop model legislation on digital evidence. The model law was presented in 2002 (Sofia University, 2002; Gercke, 2012, p. 137).

Moreover, the Commonwealth has organized several training activities such as Commonwealth Network of IT and Development co-organized training on cybercrime in 2007, Commonwealth Third Country Training Programme on legal framework for ICT in 2009 and 2011 (Gercke, 2012, p. 138).

In 2011 “*The Commonwealth Cybercrime Initiative*” was presented. The main objective of the initiative is to assist member states in building their institutional, human and technical capacities with respect to policy, legislation, regulation, investigation and law enforcement to enable an effective cooperation in the global combat of cybercrime (WAIGF, 2011; Gercke, 2012, p. 137).

#### **4.2.5. African Union<sup>28</sup>**

In the extra-ordinary conference, held in 2009, African Union Communication and Information Technologies Ministers addressed various topics about the increasing use of ICT in the African countries. Eventually, it was decided that a legal framework should be developed by African Union Commission with UN Economic Commission for Africa on issues such as electronic transactions, cyber security and data protection (AU, 2009; Gercke, 2012, p. 138). In 2011, Draft African Union Convention on the Establishment of a Credible Legal Framework

---

<sup>28</sup> Regional Organization with 54 Member States, established to facilitate cooperation between African states in certain areas. Available at: <http://www.au.int/en/>, accessed January 8, 2016

for Cyber Security in Africa was presented.<sup>29</sup> The draft was not only including cyber crime but also data protection and electronic transactions (AU, 2012; Gercke, 2012, p. 138)

Gercke states that, if there was no other international instrument, Draft African Union Convention cannot be used as a comprehensive framework. Articles 21 and 25 express explanations which are difficult to apply. Article 21 states that each member states should adopt such measures to foster exchange of information and sharing of quick expeditious and reciprocal data by Member States' organizations and similar organizations of other Member States with responsibility to cause the law to be applied in the territory on bilateral or multilateral basis. Secondly, article 25 states that, each member state shall adopt necessary measures to participate in regional and international cooperation in cyber security. A large number of international governmental bodies and organizations have established model frameworks for international cooperation which Member States may adopt as a guide. These rules seems to be difficult in terms of international cooperation (Gercke, 2012, p. 139).

One new concept which was introduced by the draft is the introduction of an obligation of businesses to submit their products fro vulnerability testing (Gercke, 2012, p. 139).<sup>30</sup>

Moreover, the criminalization of an illegal use of computer data is going beyond the standards defined by most of other regional instruments (Gercke, 2012, p. 140).

Furthermore, the Draft contains provisions which are not included in other regional frameworks. By those provisions it is intended to amend domestic provisions to ensure applicability to the involvement of computer systems and

---

<sup>29</sup> 2011 version of the Draft could not be retrieved in Internet. 2012 version of the Draft is available at: [http://au.int/en/sites/default/files/AU%20Convention%20EN.%20%283-9-2012%29%20clean\\_0.pdf](http://au.int/en/sites/default/files/AU%20Convention%20EN.%20%283-9-2012%29%20clean_0.pdf) , Accessed on January 16, 2016

<sup>30</sup> The proposal has taken its place in the Convention as follows: (Article 29/1):

“State Parties further undertake to:

g) Adopt regulations compelling vendors of information and communication technology products to have vulnerability and safety guarantee assessments carried out on their products by independent experts and researchers, and disclose any vulnerability detected and the solutions recommended to correct them to consumers.”

data. This requires countries to establish an aggravation of penalty if traditional crimes are committed by using information and communication technology, the criminalization of violation of property by offences such as theft, abuse of trust or blackmail involving computer data; update provisions that include dissemination facilities to ensure that the use of means of digital electronic communication is covered and ensure that provisions which protect secrecy in the interest of national security (Gercke, 2012, p. 141; AU, 2012, ¶ III-24). Those provisions have been adopted in the provisions 30/1/a, b, c, d of the Convention (AU, 2014).

African Union Convention on Cyber Security and Personal Data Protection has been adopted by the African Union in June 2014. The Convention includes electronic commerce, procedural law, measures to be taken at national level, international cooperation, trainings, public-private partnership, protection of critical infrastructure and personal data protection provisions. (AU, 2014).

#### **4.2.6. Arab League<sup>31</sup> and Gulf Cooperation Council<sup>32</sup>**

Some countries from Arabic region have already taken some national measures and adopted approaches to fight against cybercrime or are in the process of drafting legislation. United Arab Emirates submitted model legislation, Guiding Law to Fight IT Crime, to Arab League for harmonizing legislation in the region. In 2003, the law was adopted by Arab Interior Ministers Council and the Arab Justice Ministers Council (POGAR, 2007). In 2015, background report of Joint Defence Council of Arab League it is stated that a focus should be given to prevent extremism in Arab countries (NCUSAR, 2015).

In 2007, the Gulf Cooperation Council (GCC) recommended that GCC countries to seek a joint approach which takes into consideration international standards (Gercke, 2012, p. 141).

An Information Communications Technology Regional Workshop for Cyber security and Critical Infrastructure Protection and Cyber Security Forensics

---

<sup>31</sup> Regional organization with 22 Member States to strengthen ties among the member states, coordinate their policies, and promote their common interests. Available at: [http://www.nationsonline.org/oneworld/arab\\_league.htm](http://www.nationsonline.org/oneworld/arab_league.htm) , accessed January 8, 2016

<sup>32</sup> Regional Organization with 6 countries for coordination, cooperation and integration of Member States. Available at: <http://www.gcc-sg.org/eng/indexfc7a.html?action=Sec-Show&ID=1> , accessed January 8, 2016

Workshop was held in Doha in February 2008. The Workshop underlined the importance of reviewing domestic cyber crime legislation to address threats in cyberspace and develop proper tools to fight against cyber attacks. The issue was also discussed in the 15<sup>th</sup> GCC e-government and e-Services forum which was held in Dubai 23-27 May 2009 (Masadeh, 2010, p. 38). By March 2015 none of the countries from GCC joined to an international treaty on cybercrime. Between six GCC countries Qatar and Oman have developed technical, organizational and legal measures to address cybercrime. The others are still working on these measures but they are lack of capacity to address cyber crime issues (Alazab & Chon, 2015)

#### **4.2.7. Organization of American States<sup>33</sup>**

The Organization of American States (OAS) has actively been involved in the issue of cybercrime within the region. The organization held a number of meetings within the mandate and scope of REMJA<sup>34</sup>, the Ministers of Justice or Ministers or Attorneys General of the Americas (Gercke, 2012, p. 141).

In 1999, establishment of an intergovernmental expert group on cybercrime was recommended by REMJA. Its mandate was to identify criminal activity which targets computers and information, which uses computers as a tool of committing a crime; a diagnosis of national legislation, policies and practices of such activity; identifying national and international bodies and identify mechanisms of cooperation within the inter-American system to fight against cybercrime (Gercke, 2012, p. 141) .

So far, REMJA has held ten meetings (OAS, 2015). At the third meeting, in 2000, the Ministers of Justice or Attorneys General of the Americas discussed on cybercrime and agreed on some recommendations. These recommendations were included to support consideration of the recommendations which were made by the Group of Governmental Experts and to ask them to continue to support on the

---

<sup>33</sup> Regional Organization bringing 35 states of America and constitutes the main political, juridical and social governmental forum in the Hemisphere. Available at: [http://www.oas.org/en/about/who\\_we\\_are.asp](http://www.oas.org/en/about/who_we_are.asp) , accessed January 8, 2016

<sup>34</sup> The REMJA process is the premier policy and technical forum at the hemispheric level on matters related to justice and international legal cooperation, (available at: <http://www.oas.org/en/sla/dlc/remja/> , accessed January 8, 2016)

preparation of the strategy (OAS, 2000, ¶ 1.9). Furthermore, it was recommended that members should review their own mechanisms to facilitate broad and efficient cooperation between member states, development of technical and legal capacity to join the 24/7 Network established by G8 to assist cybercrime investigations (OAS, 2000, ¶ 1.3-1.5). Member states were asked to evaluate the principles of Council of Europe's Convention on Cybercrime and consider the possibility of acceding to the Convention. United States and Canada signed the Convention in 2001 and some others were invited to accede. Finally, OAS Member States were recommended to review the Convention and if appropriate update the structure and work of domestic bodies which are in charge of enforcing laws to adapt to the shifting nature of cybercrime, including the relationship between agencies that fight against cybercrime and those that provide traditional police or mutual legal assistance (Gercke, 2012, pp. 141-2).

In the fourth meeting of Ministers of Justice Ministers or Attorneys General of Americas in 2002 recommended to follow up on implementation of the recommendations prepared by the group of experts and considering preparation of pertinent inter-American legal instruments and model legislation in terms of cooperation in combating cybercrime, considering standards relating to privacy, the protection of information, procedural aspects, and crime prevention (OAS, 2002; Gercke, 2012, p. 142).

Sixth meeting of Ministers of Justice came out with a call to continue to strengthen cooperation with the Council of Europe to facilitate OAS Member States to apply the principles of the Convention on Cybercrime and amending their domestic laws consistent with the Convention. Similarly, efforts should continue to increase cooperation with other international organizations and agencies working on cybercrime issues such as UN, G8, EU, Commonwealth, APEC, OECD and Interpol. Furthermore, Member States were invited to establish new specialized bodies to investigate cybercrime, identify authorities who will serve as points of contact and expedite the exchange of information and obtaining evidence. Additionally, the cooperation between government authorities, Internet service providers and other private-sector enterprises should be fostered (OAS, 2006; Gercke, 2012, p. 142).

The recommendations were renewed at the seventh meeting in 2008. It is recommended to continue to the efforts of strengthen exchange of information and cooperation with other international organizations. The secretariats of the Inter-American Committee against Terrorism (CICTE) and the Inter-American Telecommunication Commission (CITEL) and Working Group on Cybercrime were requested to resume developing perpetual coordination and cooperation actions to ensure the implementation of the Comprehensive Inter-American Cyber security Strategy adopted through OAS General Assembly Resolution in 2004 (OAS, 2008; Gercke, 2012, p. 142).

In 2010, REMJA addressed the issue of cybercrime at their eighth meeting. They discussed importance of cooperation and strengthening states' capacity to develop legislation and procedural measures related to cybercrime and electronic evidence. It was additionally highlighted that the exchange of information and cooperation with other international organizations and agencies such as Council of Europe, the UN, the EU, OECD, G8, APEC, the Commonwealth and Interpol, thus OAS Member States can take the advantage of permanent cooperation with those entities (OAS, 2010; Gercke, 2012, p. 142).

In the ninth meeting of Working Group on Cybercrime Report which was held in 6-7 February 2012, states that the Parties were agreed to highlight the importance of specific cybercrime units and they should be established as soon as possible (OAS, 2012a, p. 1). Furthermore, member states were invited to examine their legal system and adopt their domestic laws in terms of procedural law, electronic evidence and criminal trials (Gercke, 2014, p. 153). Organization recommends to the states to assess the usefulness of applying principles of Council of Europe's Convention on Cybercrime bearing in mind the recommendations adopted by REMJA Working Group on Cybercrime and by REMJA (OAS, 2012b, p. 8).

The last meeting of REMJA has been held in 2015 and parallel expectations have been declared in line with previous meeting (OAS, 2015)

#### **4.2.8. Council of Europe<sup>35</sup>**

Council of Europe is one of the organizations playing active role in addressing challenges of cybercrime. At a conference dealing with aspects of economic crimes, Council of Europe highlighted the international nature of computer related crimes in 1976 and since then computer crimes have been on its agenda. In 1985, CoE appointed an Expert Committee to discuss legal aspects of the crimes. In 1989, the European Committee on Crime Problems adopted the “*Expert Report on Computer-Related Crime*” which analysis substantive criminal law provisions necessary to fight against new forms of electronic crimes, including computer fraud and forgery (UNCTAD, 2005, p. 233; Gercke, 2012, p. 123). The Committee of Ministers adopted a recommendation in particular highlighting the international nature of computer crime. By the recommendation it is advised that when Member States reviewing or initiating new legislation, the guidelines for the national legislatures should be taken into account and any developments in their legislation, judicial practice and experiences in respect of computer-related crime should be reported to the Secretary General of the Council of Europe during 1993 (COE, 1989).

In 1995, another recommendation which deals with the problems arising from transnational computer crimes has been adopted by Committee of Ministers. The recommendation had an appendix which was included guidelines for reviewing their internal legislation and practice (COE, 1995; Gercke, 2012, p. 124).

Efforts of Council of Europe’s have been resulted by Convention on Cybercrime. The Convention will be discussed in the part 5 separately.

#### **4.3. Why Did So Many Initiatives Emerge?**

Gercke states that there are two main reasons for growing number of regional and national approaches. The first reason is legislative speed. He states that Commonwealth or Council of Europe cannot force their Member States to use their instruments. Therefore harmonization process is often considered to be slow compared to national and regional approaches. However, the European Union has

---

<sup>35</sup> Council of Europe is a regional organization with 47 Member States, founded in 1949. (Available at: <http://www.coe.int/en/web/about-us/our-member-states> , accessed January 17,2016)

means to force Member States to implement framework decisions and directives and this is the reason why a number of European Union countries which signed the Convention on Cybercrime have not yet ratified it. Furthermore, these countries have implemented the 2005 EU Council Framework Decision on attacks against information systems (Gercke, 2014, p. 157).

The second reason is national and regional differences. Some of the offences are criminalized in certain countries in a region. Religious offences can be stated between them. Although in terms of international harmonization of criminal provisions related to offences against religious symbols unlikely to be promulgated, a national approach can be maintained (Gercke, 2014, p. 157)

Although there are so many initiatives working on increasing the cooperation on cybercrime, there is no fully comprehensive one. This is another reason why both regional and international organizations keep on working on the issue. Once a convention which is admissible to majority of the states is prepared, there will not be a need to work on the issue.



## CHAPTER 5

### CONVENTION ON CYBERCRIME

Convention on cybercrime represents the most substantive, and broadly subscribed, multilateral agreement on cybercrime in existence today. It offers a comprehensive approach to harmonize national legislation between Parties to address cybercrime. On the other hand, it presents a framework for international cooperation which did not exist before, except on bilateral or *ad hoc* basis (Vatis, 2010, p. 219).

The origins of the Convention date back to November 1996. European Committee on Crime Problems (CDPC) recommended that the COE to set up an experts committee on cybercrime (CoE, 2001b, p. ¶ 7). CDPC recognized that cyber-space offences, which are committed through internet, are in conflict with territoriality of national law enforcement authorities (Vatis, 2010, p. 208). Accordingly, CoE Committee of Ministers established the “*the Committee of Experts on crime in Cyber-space*” in February 1997 (CoE, 2001b, ¶ 12). The new committee was responsible for the following subjects and to draft a binding legal instrument addressing them as far as possible:

*cyber-space offences, in particular those committed through the use of telecommunication networks, e.g. the Internet, such as illegal money transactions, offering illegal services, violation of copyright, as well as those which violate human dignity and the protection of minors;*

*other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation such as definitions, sanctions and responsibility of the actors in cyber-space, including Internet service providers;*

*the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment, e.g. interception of telecommunications and electronic surveillance of information networks, e.g. via the Internet, search and seizure in information-processing systems (including Internet sites), rendering illegal material inaccessible and requiring service providers to comply with special obligations, taking into account the problems*

*caused by particular measures of information security, e.g. encryption;*

*the question of jurisdiction in relation to information technology offences, e.g. to determine the place where the offence was committed (locus delicti) and which law should accordingly apply, including the problem of ne bis idem in the case of multiple jurisdictions and the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts;*

*questions of international co-operation in the investigation of cyber-space offences, in close co-operation with the Committee of Experts on the Operation of European Conventions in the Penal Field (PC-OC) (CoE, 2001b, p. ¶ 11).*

The Committee discussed and drafted the text over the four years. Final draft was approved by CDPC in June 2001. It was adopted by COE's Committee of Ministers on 8<sup>th</sup> November 2001. On November 23, 2001 in Budapest, it was submitted for signature by CoE Member States and observers; Canada, Japan, South Africa and the United States (Vatis, 2010, p. 209).<sup>36</sup> Since that date, 44 member states, 4 non-member states have signed the convention and it has entered into force in 40 member states, 8 non-member states.<sup>37</sup>

On November 7, 2002 Committee of Ministers adopted the Additional Protocol to the Convention on Cybercrime.<sup>38</sup> By the protocol Member States is required ratifying to pass laws criminalizing “*acts of racist or xenophobic nature committed through computer networks.*” By the provision, dissemination of racist or xenophobic materials, making racist or xenophobic threats or insults and the denial of the Holocaust and other genocides are included as a crime. Moreover, nations should ratify their laws to extend to investigative capabilities and procedures created pursuant to the main Convention (Vatis, 2010, p. 210). So far,

---

<sup>36</sup> Convention on Cybercrime is available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>, accessed January 18, 2016

<sup>37</sup> Available at: <http://www.coe.int/tr/web/conventions/full-list/-/conventions/treaty/185/signatures>, accessed November 26, 2015.

<sup>38</sup> Additional Protocol to the Convention on Cybercrime is available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f>, accessed January 18, 2016

36 member states and 2 non-member states signed additional protocol and 24 member states ratified the protocol.<sup>39</sup>

Convention contains the chapters below:

In the first chapter of the Convention “Definitions” are explained by article one. In the second chapter, measures that are taken at the national level are represented. Under second chapter by section one Substantive criminal law is elaborated from article 2 to 13. In the second section Procedural Law has been explained with provision 14 through 21. In the third section Jurisdiction procedures have been explained by provision 22. In chapter 3, international cooperation is defined. In chapter 4 final provisions are explained (CoE, 2001a).

The Convention has mainly three aspects:

- 1) Providing opportunity to harmonize domestic laws by defining substantive criminal law,
- 2) Providing opportunity to harmonize jurisdiction rules by defining common authorities in terms of cybercrime investigations,
- 3) And, by defining both traditional and contemporary cooperation procedures applicable to cybercrimes, providing opportunity to parties for applying these procedures (Csonka, 2006, p. 483; Weber, 2003, p. 426; Önok, 2013, p. 1242).

## **5.1.Features of the Convention**

### **5.1.1. Difficulties in Fighting against Cybercrime**

Cybercrime legislation’s problem is lack of geographically based jurisdictional boundaries. Professor James Boyle states that *“If the king’s writ reaches only as far as the king’s sword, then much of the content on Internet might be presume to be free from the regulation of any particular sovereign.”* Without sanctions it is impossible to regulate criminal behaviour. By Convention on Cybercrime it is sought to extend the ambit of the king’s sword through cooperation (Weber, 2003, p. 425).

---

<sup>39</sup> Available at: [http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p\\_auth=guOFJszD](http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=guOFJszD), accessed November 26, 2015.

It is a new phenomenon in comparison with the traditional criminal incidents. Thus, it is not easily possible to create rules to identify cybercrimes. And this is an obstacle to prepare crime maps which indicates how the sources shall be spent in fighting against cyber crimes (Brenner, 2004, p. 17). Although we still have limited data about the rate of the crime, it is obvious that the rate is increasing rapidly (Önok, 2013, p. 1231).

As it is a new type of crime, many members of the criminal justice system are not familiar with the crime (Moitra, 2005, p. 446). Relatively police is improving its skills in terms of fighting against crime. But prosecutors and judges do not have sufficient information about the crime yet. The shortcomings need to be abolished by the trainings and their knowledge should be kept up to date (Calderoni, 2010, p. 341; Önok, 2013, p. 1232).

Definitions of cybercrimes are usually blurred (Moitra, 2005, p. 446). This situation makes it difficult to improve judicial co-operation between parties. From this point of view it is very important to maintain synchronization of laws. When traditional crime definitions are applied to cybercrimes it is not always possible to punish offenders without updating domestic laws (Urbas, 2006, p. 99). Even if the laws are rectified, it needs to be updated time to time because of the fluctuating features of the cybercrimes (Gercke, 2009, p. 410).

Typical feature of cybercrimes is the distance between victim and suspect. Usually, the cyber offence is related to many states (Gercke, 2011, p. 133). These two features of cybercrimes make international solidarity inevitable (Gercke, 2011, p. 173). Then, the question of "*where the crime is committed*" reveals. It is usually a sovereignty issue as more than one country is involved in the offence. The typical rule of international law is that, a state has the judicial authority within its own territory (Csonka, 2006, p. 477). According to conventional rules of international law, a party cannot conduct an investigation on another's territory (August, 2002, p. 561). So, cybercrime features and international criminal law differ from each other and cybercrime necessitates international co-operation. The solidarity comes with the consistency between the laws of the related states (Csonka, 2006, p. 477; Keyser, 2003, p. 326).

Identifying suspects of cybercrimes is rather difficult comparing to traditional crimes (Moitra, 2005, p. 446). Furthermore usually company victims refrain from applying to judicial authorities because of their commercial expectations (Picotti & Salvadori, p. 78). Even usually they are not aware of their losses (Broadhurst, 2006, p. 410).

Evidences of cybercrimes and the type of the evidences are quite different from of the traditional crimes (Grabosky, 2007, p. 213). Beside difficulty in collecting digital evidences, it is more difficult to collect evidences pursuant to procedures in a way that collected evidences will be accepted by the court (Choo, 2008, p. 286). This situation indicates the importance of digital forensics discipline. Digital forensics necessitates expertise of the personnel (Bell, 2002, p. 313). Furthermore, vulnerability of the digital evidences necessitates expedited co-operation of the parties. But traditional cooperation ways are usually late (Grabosky, 2007, p. 215) in terms of cybercrime cooperation particularly when more than two countries' cooperation is needed (Önok, 2013, p. 1235).

By cybercrime, offenders can make catastrophic damages by limited source and time (Broadhurst, 2006, p. 410), while cooperation may be expensive and take time (Önok, 2013, p. 1236).

The most important and difficult aspect in fighting against cybercrime is that, very few countries which do not make necessary amendments in their domestic law will be sufficient for the criminals looking for a safe haven to shelter (Putnam & Elliott, n.d., p. 51). Fighting against cybercrime can only be globally or would be useless (Broadhurst, 2006, p. 412; Önok, 2013, p. 1236). Criminals would go to those countries which do not define cybercrimes in their domestic law (Choo, 2008, p. 290).

### **5.1.2. Fundamental Principles of Judicial Cooperation**

The jurisdictional problem of cybercrime reveals in three ways: lack of criminal statutes, lack of procedural powers, and lack of enforceable mutual assistance provisions with foreign states (Weber, 2003, p. 426).

As mentioned above one of the main purpose of the Convention is judicial cooperation between Member States. By the Convention three general principles are provided: firstly, the widest cooperation is expected from the Parties. The obstacles of flow of data and evidence shall be decreased to the lowest (Weber, 2003, p. 433; CoE, 2001a, ¶ 23). Secondly, the co-operation shall be applied not only for cybercrimes but also for the crimes committed by computer systems and data or the collection of evidence in electronic form (CoE, 2001b, p. 243; Broadhurst, 2006, p. 421; Csonka, 2006, p. 495). Finally, the Convention is not superior to multilateral treaties or domestic laws concerning international cooperation (Gercke, 2011, p. 463). But, this feature of the Convention is criticized as it decreases the benefits of it (Weber, 2003, p. 442).

### **5.1.3. Procedures of Judicial Cooperation**

Liability of extradition is applicable to specific crimes determined in article 24, from 2 through 11 and which are punishable under the laws of both parties concerned by deprivation of liberty for a maximum period of one year or by a more severe penalty (Keyser, 2003, p. 317). The actual penalty is not important in terms of extraction but instead the maximum period that may legally be imposed for a violation of the offence (CoE, 2001b, ¶ 245).

Forementioned crimes are expected to be adopted as extraditable by Parties in all present and future extradition treaties. This does not mean that extradition must be granted. Instead, possibility of extradition for certain crimes should be available (CoE, 2001a, p. 24/2; CoE, 2001b, ¶ 247).

A Party which cannot fulfil the request according to lack of extradition treaty between Parties or the present treaty does not include defined crimes in the Convention, requested Party may fulfil the request based on the Convention, if volunteer (CoE, 2001a, p. 24/3; CoE, 2001b, ¶ 248).

Extradition procedures shall be applied according to MLATs (Mutual Legal Assistance Treaties) and domestic laws (CoE, 2001a, p. 24/5; CoE, 2001b, ¶ 250). Being signatory of the Convention does not provide an obligation to the Parties to assume it superior to the domestic laws.

“*Aut dedere aut judicare*” (extradite or prosecute) principle is ruling in paragraph 6 of the article 24 (CoE, 2001b, ¶ 251). Parties usually reject extradition of its own nationals for prosecution. If an extradition request is rejected on grounds of the offender’s nationality is from requested Party or requested Party deems that it has jurisdiction over the offence, requesting Party may demand prosecution of the offender. In this case, requested Party must submit it to its own authorities for investigation and proceedings. If there is no such a request, there is no an obligation for investigation. But the result must be notified to the requesting Party. The Convention does not provide an obligation to conduct a prosecution if there is no request from the other state and if extradition request has been rejected on the grounds other than nationality (Vatis, 2010, p. 214; CoE, 2001a, p. 24/6; CoE, 2001b, ¶ 251).

## **5.2.Critiques**

### **5.2.1. Harmonization**

Execution of Convention on Cyber Crimes seems problematic. The Convention was signed on November 23, 2001 by 27 member states and 4 non-member states. Although as the length of the duration has passed, so far, the number of the states which the process was completed by ratification or accession is 48. More interestingly, 3 countries which signed the Convention in 2001 did not ratify it (Sweden, Greece and South Africa). Russian Federation and San Marino, already member of CoE, did not sign or ratify the Convention.<sup>40</sup>

The Convention included long procedures of amendments (CoE, 2001b, ¶ 323,4,5). As it is still a new phenomenon and absence of a comprehensive international agreement yet, the Convention shall need amendments. Actually, the

---

<sup>40</sup> List of the Parties of the Convention is available at: [http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p\\_auth=CkY0jVx1](http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=CkY0jVx1) , accessed on March 25, 2016

states did not have sufficient experience about cyber threat. The United States had the widest experience on this and therefore made a great contribution to both drafting and plenary sessions, though it had an observer status (Vatis, 2010, p. 207). Through the long drafting process, drafters and the States did not agree on some of the articles. Rapidly changing nature of cybercrime would risk fixation of the law (Weber, 2003, p. 442).

The Convention's attempt to harmonize cybercrime laws is an illusory attempt. The reservations let Parties to preserve their laws and undermine harmonization. It is not obvious which Parties will need to amend their current laws for harmonization, however it fails to be universal. In this situation without a worldwide participation, cyber criminals may remain out of the Convention's reach (Weber, 2003, p. 444). The Convention also allows Parties to refuse assistance in many instances such as inconsistency with domestic laws or where a Party claims such assistance would prejudice its sovereignty, *ordre public* or essential interests. Thus, when a Party is suspected of being delinquent or responsible for an attack or tolerating, such Party would likely be refused cooperation (Vatis, 2010, p. 220).

The Convention does not offer an enforcement mechanism to seek redress (Vatis, 2010, p. 220). Moreover, neither do they offer an appealing agent when cooperation is rejected nor another superior mechanism to monitor cooperation between Parties. As a result of this state of affairs any Party which rejects cooperation shall not be subjected to any sanction, and such lack of enforcement prevents the will of the states to join to the community.

Substantively, the Convention is fairly comprehensive in addressing most of the cybercrimes and most common investigative tools. It prescribes mechanisms and procedures for international cooperation (Vatis, 2010, p. 220).

### **5.2.2. Jurisdiction Related Issues**

International cooperation on cybercrime has traditionally been the exception rather than the rule. Thus, these requirements are frequently an insurmountable barrier to the successful prosecution of cyber criminals (Weber, 2003, p. 426).



Jurisdiction regulations of the Convention are established loosely (Weber, 2003, p. 430). Article 42, gives a chance for Parties to make reservations on specific articles. These reservations may be the reason for justification of the Parties to refrain from amendment of their domestic law which will eventually make international cooperation impossible (Weber, 2003, p. 444; Moitra, 2005, p. 464).

Naturally Convention grants right of jurisdiction to the offences committed in that state's territory. This allows the states to assert jurisdiction in a computer crime involving a computer system within its territory, even if the perpetrator committed it from a distant place. Furthermore, Convention grants a state jurisdiction over a citizen of that state who commits a covered offence outside of the state's borders as long as the offence is punishable in other state or if the offence has occurred outside of the territorial jurisdiction of any state (Weber, 2003, p. 432; CoE, 2001a, p. ¶ 22; CoE, 2001b, ¶ 233).

Although the treaty rejects dual criminality as a prerequisite for mutual assistance (CoE, 2001a, ¶ 25-29; Weber, 2003, p. 434), subordination of the treaty to the existing MLATs and commitment to mutual agreements in investigations blurred the benefit of the convention (Weber, 2003, p. 442). The Convention leaves the issue to the existing multilateral agreements and aims to supplement existing multilateral or bilateral agreements (CoE, 2001a, ¶ 39). Thus, it is far from being a compulsive international agreement.

The Convention fails to solve the problem of extraterritorial jurisdictional issues even though it was the core issue which facilitated development of the treaty (Weber, 2003, p. 442).

### **5.2.3. Comprehensiveness**

Another criticism forwarded to Convention is that developing countries in continents such as Asia, Africa and Latin America were not represented in drafting process of the Convention. During the drafting process not only developing countries but also non-members Council of Europe countries were restricted in participation (Gercke, 2011, p. 202; Vatis, 2010, p. 220). The Convention was open for signature to member states of Council of Europe and to the states which have contributed in the elaboration process. Furthermore, article 37 states that the

Committee of Ministers of the Council of Europe may invite any state which is a non-member state and did not participate in elaboration process after consultation and obtain a unanimous consent of the contracting states to the Convention. Such a restriction not only prevents other states which are willing to participate to the team, but also prevents comprehensive cybercrime jurisdiction.

The Convention implies a selective cooperation between the Parties. Article 37 obviously state that the contributors of the Convention want to know the states which they will be cooperating. This was an obstacle for many states which wanted to join the community. It made the Convention more of a regional regime than an international Convention which is far from being a global regime in constructing a structure. Although it is the only international agreement from which most likely to emerge a regime in terms of cyber crime, it is far from it.

Another debating issue is cross-border access to stored computer data without mutual assistance. According to the Convention when the data is publicly available or when the state which conducted search has obtained "*lawful and voluntary consent of the person who is lawfully authority to disclose data*" (CoE, 2001a, p. 32). The drafters explicitly denied that the treaty permits remote extraterritorial searches. In their report they stated that: "*it was not yet possible to prepare a comprehensive, legally binding regime regulating the area* (CoE, 2001b, ¶ 293-4)." By the article it is implied that receiving lawful and voluntary consent of the owner of an account, for example, if law enforcement authorities receive the consent of the owner of an e-mail account while the servers of that e-mail provider is in another country, is it lawful to access that account? Is it possible to conduct a search in another country's territory without its consent or cooperation? Judicial fundamental principles assume that the state has the power and authority of its own territory.<sup>41</sup> Is it a search without consent on another state's territory where the one conducting search has no authority? So, it still seems difficult to find reconciliation on those questions.

This restrictive structure of the Convention pushes other states to join other communities. As we have mentioned above there are significant international and

---

<sup>41</sup> See *Supra* note 1

regional organizations which are dealing with cyber crime issues. One of the reasons why states join into other initiatives is because of the preference for international rather than regional initiatives. In the twelfth UN Crime Congress it obviously showed this expectation (Gercke, 2011, p. 203).

While many European Countries ratified the Convention, still there is notable number of major actors, such as Russia and China which has not signed it. Although Russia is one of the member states of the COE, it has not signed the Convention yet. Russia has been opposed to the section of provision allowing unilateral trans-border access by law enforcement agencies to computers or data with the consent of the owner, by admitting it as a violation of national sovereignty. Interestingly, some claim that Russia's real reason for not signing the Convention is refraining from obligation to assist other states in numerous cyber attacks that emanate from Russia, including which some people suspect that they are state-sponsored. Russia and China have been the source of many serious cyber attacks in the recent years which some of them considered as state-sponsored (Vatis, 2010, pp. 218-20).

One of other international instruments, United Nations Convention against Transnational Organized Crime (UNTOC) contains important instrument for judicial cooperation in criminal matters. But it did not address cyber crime issues specifically. As a result, it does not contain specific provisions in terms of expedited requests to preserve data (Gercke, 2012, p. 267). A UN initiative, United Nations Office on Drugs and Crime has recommended that *"the development of a global convention against cybercrime should be given careful and favourable consideration."* The slow progress in getting nations to sign the COE Convention, and the reluctance of non-COE states to accede to a treaty provides nothing in hand developing (Vatis, 2010, p. 218).

Additionally, the COE's Committee of Experts on Terrorism has stated that, no separate convention is necessary for the use of Internet for terrorist purposes, including terrorists' attacks on computer networks as it seems to be already covered by the Cybercrime Convention. Thus, Committee recommended urging more nations to accede to the Convention and giving further consideration on the question of responsibilities of Internet providers (Vatis, 2010, p. 219).

The International Telecommunication Union (ITU), a U.N. agency responsible for information and communication technology issues, has also questioned whether the Convention should be adopted as a global standard. By ITU General Secretary it is stated that the Convention is “*a little dusty.*” As an alternative, ITU sponsored the creation of “*ITU Toolkit for Cybercrime Legislation.*” By the draft a global participation is recommended. The toolkit serves model legislation for countries to adopt. The goal is to harmonize national legislations of the states without signing an international treaty. A cyber-warning organization, “*International Multilateral Partnership against Cyber-Threats*” (IMPACT), also suggested by ITU (Vatis, 2010, p. 219).

COE Secretary General stated that the Convention has received strong support from Asia-Pacific Economic Cooperation, The European Union, Interpol, the Organisation of American States, and other organisations and initiatives as well as the private sector (Vatis, 2010, p. 219).

A US Department of Justice official who is involved in cybercrime issues rates the impact of the convention as “very positive” although there are no statistics to compare pre-versus post-Convention rates. The official claims that the cooperation has increased radically in the recent years, particularly in the ability to require preservation of evidence until authorities fulfil the necessary obligations to provide disclosure, the authority to engage in “spontaneous” cooperation, the creation of 24/7 points-of-contact network, and the ability to engage in remote searches, though this authority is probably not used often (Vatis, 2010, p. 220).

#### **5.2.4. Burden on ISPs**

The Convention received so many critiques about the increased burdens on Internet Service Providers. This was because of compilation of mass data, requests for interception and stored traffic data. But after adoption the opposition was muted (Vatis, 2010, p. 218).

Such an obligation to store traffic data would bring heavy financial obligations to the ISPs and content providers. Because, such a responsibility requires big servers to protect data for certain period. On the other hand, intensive requests for the

traffic data may likely to increase the burden on companies. Before the Convention there was not such obligation.

In the Convention by article 16 the Parties should enable their authorities to order a person who preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days. This order can be renewed subsequently (CoE, 2001a, ¶ 16). In terms of mutual assistance it is also important to provide opportunity to Parties to submit their request for data preservation. Thus, article 29 explains that preservation effected in response to a mutual assistance request shall be for a period not less than 60 days (CoE, 2001a, ¶ 29).

The drafters of the Convention discussed if the Convention should oblige service providers to collect and retain traffic data for a certain period of time. But as there was no agreement, the Convention did not contain such an obligation (CoE, 2001b, ¶ 135).

Another approach which is diffusing recently is the obligation of data retention. Data retention implies the obligation of internet services to save traffic data for certain period of time. Usually states adopt their laws to enforce service providers to save the data up to 24 months. Data retention obligation has been adopted by European Parliament and is currently under discussion in the United States. The Convention defines data preservation rather than data retention. Thus, the Convention offers less constraining instrument in comparison to data retention (Gercke, 2014, pp. 259-60).

### **5.2.5. Human Rights**

The Convention's procedural requirements which assist law enforcement have been criticized for inadequately protecting civil liberties. By these critiques it is stated that treaty excessively focuses on procedural powers and is missing safeguards for human rights (Weber, 2003, p. 438). Although the Convention has received many objections because of the intrusion into the confidentiality of private life (Csonka, 2006, p. 390), it must be noted that the Convention does not include a strict intrusive electronic supervision system (Önok, 2013, p. 1246). The Convention simply provides and uses certain powers, but it does not require

justifying the systematic surveillance of personal communications or contacts by neither service providers nor law enforcement agencies, unless it is necessary for investigative purposes (Csonka, 2006, p. 390).

Many civil liberties group were opposed to the Convention when it was entered into force. Many thought that new investigative bodies would be emerged in adopting countries and increased law enforcement cooperation would abolish privacy of individual's rights and other rights (Vatis, 2010, p. 218).

### **5.3.Evaluation of Convention**

Weber claims that the structure of the Convention itself reflects an awareness of jurisdictional dilemma. The main purpose of the Convention is to provide a common criminal policy to protect society from cybercrime (CoE, 2001a, ¶ 4). Accomplishment of this purpose is up to the solutions to the lack of criminal statutes, the lack of procedural powers, and the lack of enforceable mutual assistance provisions that result from the jurisdictional gap in cybercrime regulation (Weber, 2003, p. 430). But it seems that until now the Convention is not able to achieve these goals. Firstly, the number of the Parties to the Convention is still limited. The effects of the Convention can only be observed in those countries. Rest of the states may still be far from adopting criminal statutes, procedural powers and mutual assistance provisions. Secondly, the number of the articles which there was not unanimous consent was not so small. Many of the articles were adopted without concrete description. Real time collection of computer data, interception of content data, jurisdictional scope, and cross-border access to stored data without mutual assistance can be stated as some of the issues in blur area. Thirdly, after 2001 there was no amendment on the articles of the Convention. 15 years later than the adoption of Convention, it seems that the Parties seem reluctant to improve it. It is hard to claim that the Convention does not need amendment. So the Convention does not reflect the experience gained during this period.

Furthermore, many of its procedural provisions are not limited to cybercrimes. It also includes any crime for which electronic form of evidence is necessary to collect. Convention obliges Parties to create laws allowing law enforcement

authorities to search and seize computers and computer data, engage in wiretapping, and to obtain real-time and stored communications data, whether or not the crime investigated is a cybercrime (Vatis, 2010, p. 208).

Council of Europe's Convention on Cybercrime has the broadest support from different international organizations. Nevertheless, the debate in the twelfth Crime Congress highlighted that after ten years of opening for signature, the impact is limited (Gercke, 2014, p. 135).

The Countries outside the Europe which ratified the Convention are Australia, Canada, Dominican Republic, Japan, Mauritius, Panama, Sri Lanka and the USA.<sup>42</sup> The impact of the Convention cannot be measured by the number of the states signed or ratified as some other countries such as Argentina, Pakistan, Philippines, Egypt, Botswana and Nigeria have used the Convention as a model and amended their laws in accordance with the Convention. Council of Europe claims that more than 100 countries have picked up the Convention as a model and used the Convention when drafting their domestic laws. However, it is not possible to confirm it (Gercke, 2014, p. 135). As a result, the Convention seems to have reflected less improvement than expected.

## **5.4.Proposals**

### **5.4.1. Amendment on Convention on Cybercrime**

It is claimed that in terms of their sovereignty interests although it seems unlikely to be accepted by the majority of the parties to the Convention, some offers have been proposed.

Firstly, the grounds for rejecting assistance might be narrowed. Allowing parties to reject assistance based on "prejudice to their sovereignty, security, *ordre public* or other essential interests" definition provides so much flexibility to reject assistance to the parties.

Secondly, a sufficient enforcement could be added to the Convention, by which a redress can be sought. A neutral arbitrator is recommended for a review to justify

---

<sup>42</sup> See *Supra* Note 26

it. It seems unlikely that nations would agree to give a neutral arbitrator possessing the power to compel them for assistance. But at least the arbiter might be given the authority to investigate whether the denial was legitimate. This may have some deterrent effect.

Thirdly, a reporting mechanism could be added to the Convention to oblige parties to inform CDPC or another certain entity about rejected assistance requests and the reasons for rejection. This information could be published. Thus it would have a deterrent effect.

Fourthly, an amendment could be added to the Convention to authorize requesting Parties whose assistance request was rejected without a legitimate, or credible reason, to engage unilaterally, cross-border investigation action, such as remotely searching computers in the requested nation on condition that “*obtaining the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system*”. This regulation would take the Convention to a place which is very far from present. However, such an amendment should be drafted very carefully to provide very specific definitions (Vatis, 2010, p. 221).

#### **5.4.2. Russia’s Proposal on International Cyber Arms Control**

Alternatively a proposal about international cyber arms control has been submitted by Russia, in 1998. Russia urged United Nations to limit cyber attacks, destructive effect of cyber weapons in comparison with weapons of mass destruction. General Assembly adopted a resolution in 2000, calling Member States to consider

*existing potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field and to examine “international concepts aimed at strengthening the security of global information and telecommunications systems.*

Furthermore, Russia proposed some principles to

*refrain from damaging or influencing another State’s information resources and systems, the deliberate use of information to influence another State’s vital structures, unauthorized interference in information and telecommunications systems and information resources, as well their unlawful use, or encouraging the activities of international terrorist extremist or criminal associations,*



*organizations, groups or individual law breakers that pose a threat to the information resources and vital structures of States* (Vatis, 2010, p. 222).

In the end of 2009, Russian and American officials commenced on discussing cyber security issues including possible restrictions on the military use of cyber weapons, and agreed to begin talks in the U.N. Disarmament & International Security Committee. But until now, Russia's proposal on banning offensive use of cyber weapons seems unable to gain any traction. However, its proposal seems to be far from being an alternative to CoE's Convention on Cybercrime (Vatis, 2010, p. 223).

### **5.4.3. Cybercrime Model Code**

Weber recommends an alternative model to the Convention on Cybercrime. She claims that for the US either the Convention on Cybercrime should be ratified with specific reservations or rejected entirely. An alternative solution may be Cybercrime Code as it could be amended easily as technology develops. Moreover, the maintenance could be easier for states between their legislative schemes and the model code. On the other hand, such a solution might result such superior solutions to the jurisdiction problems diminishing cybercrime legislation (Weber, 2003, p. 444).

However, Cybercrime Code might not be a final solution for all the problems in the area. Worldwide harmonization of cybercrime legislation might be taking long time under a model code. Furthermore, while providing criminalization of offences, it needs another mechanism which ensures cooperation between states. Thus, a code is likely to be a replication of Convention on Cybercrime (Weber, 2003, p. 445).

She finally states that the true process of harmonization will begin when the Convention admits new members to the treaty on condition that they align their domestic laws consistent with hegemonic paradigm. Assertions of power by Convention member states might encourage non-member states to join to the Convention and bringing worldwide harmonization (Weber, 2003, p. 445).

#### **5.4.4. Russia's Proposal on Code of Conduct**

In 2011, another proposal was submitted to United Nations General Assembly by Russia and some other countries on creating a Code of Conduct for Information Security. Together with Russia, China, Tajikistan and Uzbekistan were the contributors of the proposal. The purpose and scope has been explained as;

*to identify the rights and responsibilities of States in information space, promote their constructive and responsible behaviours and enhance their cooperation in addressing the common threats and challenges in information space, so as to ensure that information and communications technologies, including networks, are to be solely used to benefit social and economic development and people's well-being, with the objective of maintaining international stability and security (UN, 2011).*

The proposal has been revised and renewed in 2015 by additional contribution of Kazakhstan and Kyrgyzstan. The renewed proposal includes minor changes (Rõigas, 2015)

The proposal is basically about how the states should treat. The Parties claim that they will respect each others' sovereignty and political independence. They should not use information and communications technologies and information and communications networks to interfere each others' internal affairs or in way that might destroy international peace and security. One of the most important features of the Code is that accession is open to all states.

However, the Code of Conduct is far from being an alternative to the Convention on Cybercrime as it has so many shortcomings in comparison. Thus, a global agreement is unlikely to occur. The Code may be implemented regionally or among like-minded states (Rõigas, 2015).

## CHAPTER 6

### WHY IS SUCCESS OF CYBERCRIME DIFFUSION LIMITED?

Although the need for Anti-Money Laundering regime and Cybercrime Regime revealed simultaneously, the implementation of those two policies did not proceed in the same manner. Anti-Money Laundering Regime has proceeded very far since the beginning. Many countries have been part of those organizations dealing with Anti-Money Laundering and thus have been one of the cooperative countries. Contrarily, in cybercrime regime, fewer countries have been part of the international cooperation. It can still be claimed that cybercrime regime is in the process of crawling. Anti-money laundering policy was diffused between 130 states in 1996 (FATF, 2003, p. 2), and more than 170 states in 2008 (Sharman, 2008, p. 635). While 197 states are member of one of the initiatives fighting against money laundering (FATF, tarih yok), in cyber crime policy the total number of the cooperative states reached to 82<sup>43</sup> by 2013 (UNODC, 2013, p. xix).

Both of these two regimes have international dimension. Without international cooperation, fighting against those crimes is impossible. For fighting against those crimes, all countries should be in close cooperation to prevent safe havens. Otherwise, criminals will not be subjected to criminal procedures.

#### 6.1.Organized Crime

First of all, those two crimes are similar to each other in terms of being transnational organized crime. Organized crime has been described in United Nations Convention against Transnational Organized Crime. According to Convention Transnational Organized Crime has been described as *“a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in*

---

<sup>43</sup> The number of the states which signed one or more binding instrument: The Council of Europe Convention on Cybercrime, the League of Arab States Convention on Combating Information Technology Offences, and the Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information, or the Shanghai Cooperation Organization Agreement in the Field of International Information Security.

*accordance with this Convention, in order to obtain directly or indirectly a financial or other material benefit* (UN, 2004)”. Transnational dimension of those crimes is quite obvious while the group dimension is not clear. Cybercrime may be committed individually as well. But it does not infer that the Cybercrime cannot be committed in organized way. On contrary, transnational dimension of the crime makes it more suitable for committing the crime by organized groups to make law enforcement authorities lose the track.

Similarly, one recent study indicates that upwards of 80 percent of digital crimes may entail some form of organized activity. The EUROPOL IOCTA claims that in near future the vast majority of investigations into transnational organized crime will necessitate some form of internet investigation. Furthermore, a number of the countries state an increasing involvement of organized criminal groups in cybercrime during the last five years (UNODC, 2013, p. 45). Thus, cybercrime is likely to be a reasonable mean for organized crime groups.

## **6.2. Burden on Private Institutions**

The burden which is attributed to private companies such as Internet service providers, content providers also criticised. It was claimed that obligatory data storage such as traffic data or customers’ personal registration information would necessitate large data storage devices and new systems. Furthermore, the requests from law enforcement authorities would bring another heavy burden to private companies. These burdens have been criticised as they are weight on private companies rather than law enforcement authorities.

Similarly anti-money laundering regime has also provided so many burdens on private companies such as banks, financial organizations. It can be claimed that the burden delivered by AML regime to the private companies is not less than the one by Cybercrime regime. First of all, CDD measures oblige parties to develop new technologies (FATF, 2003, ¶ 8). Secondly, the records should be maintained for at least five years by the institutions. Thirdly, the records of the identifications should be kept at least for five years (FATF, 2003, ¶ 10). Fourthly, a special attention should be paid to unusual large transactions and suspicious transactions, the details about these transactions should be submitted to the competent authorities and the

records should be available for the competent authorities and auditors (FATF, 2003, ¶ 11). Furthermore, the institutions should develop programmes against money laundering and terrorist financing such as training of the employee and ensuring the standards of the procedures and policies (FATF, 2003, ¶ 15).

In terms of obligations which have been burden for private companies were criticised for both regimes. Although these were also been heavy burdens in anti-money laundering regime, the burdens did not slow down the process of diffusion.

### **6.3.Terrorism**

One of the reasons why anti-money laundering policy diffused quickly is the impact of terrorist attacks in 9/11. The attacks improved the perception of terror threat a sudden reaction has been implemented. As a result of quick impact, the FATF revealed its blacklist in 2001 and the states joined the community relatively in a short time. The FATF aims to confiscate the money obtained from criminal activities, including terrorist activities. Although the anti-money laundering policy reflected in most of the countries, the cyber crime regime has diffused very slowly. Actually, it may be claimed that cyber crime is also related to terrorist activities. Cyber terrorism and fraud committed through Internet may be some of the activities conducted by terrorist organizations. Unfortunately, it seems that this perception is lack of persuasion for states and international organizations. If this claim was strong enough to convince the parties, they would have been taking an action to commence on the implementation of the process.

### **6.4.Limited/Regional Contribution**

Cybercrime Convention has been criticised by some of the parties as the leading Convention is adopted by a regional organization. They claim that a widespread regime can be created by a global organization such as United Nations. Some states may have prejudices against a convention which is adopted by an organization unfamiliar to them. This creates reluctance for membership. Additionally, limited contribution of small countries increases the reluctance of those countries. Sincerely, the adoption process of the Convention had very limited contribution. During this process Council of Europe countries and four additional invited states have been in the discussions.

Another confusing state is non-membership of few big actors. China and Russia, a CoE Member State, still did not sign and ratify the Convention. Although Russia has an easy joining process, the absence of a CoE Member State within the Parties creates ambiguity between non-member states and those countries remain reluctant to the Convention.

Furthermore, the Convention prevents other states' contribution. Article 37, itself prevents the accession to the Convention by recommending an invitation. Thus, a state which wishes to join to the Convention cannot accede. Unless the procedures fulfilled recommended by Article 37, any state will not be a party of the Convention.

On contrary to Cybercrime Convention, the FATF regime does not limit the contribution to the agreement. Rather it recommends and forces the states to join to the community. But the FATF regime accepts the states which join to any regional AML standard as mates. It is not expected to join to a single convention.

### **6.5. Anxiety of Sovereignty**

The possible accession to the Convention creates an anxiety to lose their national sovereignty partially. Although there are other bilateral or multilateral treaties oblige parties for certain responsibilities, a new phenomenon such as Cybercrime Convention make new candidates feel intimidated.

The most prominent problem of sovereignty is trans-border access to the stored computer data. If a party obtains *lawful and voluntary consent of the person who has the lawful authority to disclosure the data*, it can get access to a data stored in another country. In this situation the consent of the state where the data located geographically is not important. This is extremely contradictory to the conventional international law practices.

### **6.6. Reservation**

Article 42 of the Convention on Cybercrime provides opportunity to the parties to declare reservation to the certain articles. This right prevents effective harmonization and global standardized application of the Convention. On contrary

to the Cybercrime Convention, the FATF 40 Recommendations does not provide such a gap.

### **6.7. Amendment Process**

The amendment process of the Cybercrime Convention is quite complicated. Although the Convention was new, sooner time, it will need an amendment under the rapidly changing nature of the information technologies, the Convention's amendment process was adopted rather difficult (CoE, 2001a, ¶ 44). Contrarily, the FATF 40 Recommendations does not recommend a special process for amendment. Several amendments have already been completed in 1996, 2001 and 2003 (FATF, 2003, p. 1). On the other hand, there are only few countries left to coerce to join to the community.

### **6.8. Sanctions**

Cybercrime Convention recommends the widest cooperation between the parties. But it does not recommend any sanction. It is not obvious that what is offered if one of the parties does not fulfil its obligation enforced by the Convention. Neither condemnation nor compensation has been proposed. Or an *ad hoc* committee was not proposed to inspect or detect the level cooperation between the member states. It is a blur area what is the sanction to the party which does not obey its responsibility provided by the Convention.

However, the FATF 40 Recommendations has obvious sanctions. By the articles 21 and 22, measures to be taken to the countries that do not or insufficiently comply with the FATF Recommendations have been explained. It recommends that financial institutions should pay special attention to business relationship and transactions from those countries. Moreover, article 23 obliges parties on supervising institutions and ensuring effective implementation of the FATF Recommendations. Additionally, the Organization prepares annual reports to assess non-cooperative states and announce their statute on its website.<sup>44</sup>

---

<sup>44</sup> See *Supra* Note 40

The frame provided by the FATF Recommendations brings economic sanctions to the parties, non-cooperative countries and insufficiently complying countries. In this way, the sanctions are quite deterring especially for small countries.





## CHAPTER 7

### RECOMMENDATION FOR A COMPREHENSIVE CONVENTION

Under the light of all those discussions these amendments should be fulfilled to create a global cybercrime regime:

First of all, cybercrime cooperation is exceedingly needed. Fighting as a single state against this crime is not possible in terms of collecting evidences. Borderless structure of Internet makes international cooperation inevitable. Expedited preservation is important in the issue of collecting evidences as their vulnerability. 24/7 points of contact is very important piece of the policy. Instead of data protection, data retention for certain period of time should be accepted by the Convention. This obligation would be a burden for private companies. But minimum period of retention should be defined to conduct effective investigations and prosecutions.

Secondly, coercive structures should be created which will enforce countries. This may be an impartial body to investigate rejections of cooperation, financial or other sanctions or announcement of non-cooperative jurisdictions at least. Convention on Cybercrime is about to reach to its zenith by rational learning. From this point, significant progress of the policy can only be maintained by coercive mechanisms.

Thirdly, the Convention should be open to all voluntary countries. It should not be limited to certain region in the world. Contribution of developing countries would increase reliance on the Convention and it would encourage contribution. It might increase reliability to the convention and be more successful if prepared by an international organization such as United Nations. This might facilitate diffusion of the convention.

The provisions of the Convention should be as obvious as possible to abolish the anxieties. They should be discussed in details and prepared carefully to prevent disagreements. It should not be neglected that the policy area is quite technical.

Furthermore, developing countries do not know a lot about the capacities of the developed countries. Abolishing mysteries and mistrusts would accelerate development of the policy.

Cybercrime is a constantly changing area. A mechanism which is corresponding punctually to these changes should be established. The Convention should be reviewed regularly to fulfil necessary amendments in terms of new technological developments.

Scope of the data retention should be limited by the investigations. Authorization which may permit investigative components to save unlimited personal data should not be given to the authorities. By the Convention necessary guarantees should be provided in terms of fundamental rights and privacy of the individuals.

## CHAPTER 8

### CONCLUSION

As discussed above, Sharman states that anti-money laundering policy has diffused by direct coercion or alternative coercion ways such as mimicry and competition. In the light of the model drew by Sharman Cybercrime Regime seems to be lack of coerciveness.

Although the FATF Forty Recommendations uses soft language, it has diffused globally. While creating a new model by Cybercrime Convention, it has also used a soft language which provides privileges to the domestic laws and multilateral agreements. But, the reason why AML policy has globally accepted is the sanctions applied to the non-cooperative states.

The burdens delivered to the private companies, banks and financial institutions did not slow down the process of diffusion. This is mostly because of the sanctions which they may be subjected to. The heaviest burdens have been the increase in labour and financial costs of the precautions. But, the costs of the sanctions seemed much heavier than the burdens that the parties were volunteers to fulfil the responsibilities although their institution or state did not pose money laundering threat.

Furthermore, Cybercrime Regime provides parties an option of reservation for the certain articles. This option prevents global harmonization of Cybercrime legislation. However, the 40 Recommendations do not provide this option to the parties. A complete dedication is expected from the parties. Looking through this window, any state is either a member of the community or a state which poses risk in terms of money laundering. Thus, it can be claimed that AML Regime has strict framework.

Similarly, as the Convention on Cybercrime has been adopted by a regional organization, Council of Europe, it creates prejudice for non-member states whether they should join to the Convention. Furthermore, even if they want to join to the Convention, an invitation is needed according to the article explaining

*“accession to the Convention.”* The Convention itself also represents a limited cooperation.

However, a single treaty is not necessary for global cooperation. AML Regime did not oblige membership of a single treaty. There are nine different organizations which are associate members of the FATF dealing with AML issues. Membership to one of those organizations is thought sufficient to be assumed as cooperative. As discussed above, there are many regional organizations working on Cybercrime legislation. As long as these regional organizations have the minimal standards, membership may be accepted as sufficient.

It seems that 9/11 attacks in the US has speeded up the process of creating an AML Regime. If there was a perception that the Cybercrimes are used as a mean for financing terrorism, this may have also speeded up the process for Cybercrime. Recently terrorism on cyber world is a debate which is being researched. It should not be neglected that cyber attacks which the states are subjected to may be from terrorist organizations and the money obtained through cyber frauds may be going for financing terrorist organizations. Thus, cybercrime is also an important dimension to fight against financing terrorism.

During the process of creating AML Regime, these sanctions have not been applied until the announcement of the FATF Blacklist. The Blacklist has shown the determination of the Organization to fight against money laundering crimes. With those 23 states which has announced as non-cooperative jurisdictions, the other states has seen the serious results of being blacklisted.

Thanks to serious results of the sanctions by the FATF applied to non-cooperative jurisdictions the states commenced on amending their domestic laws consistent with the international expectations. Lack of coerciveness in Cybercrime Regime has made it to be crawling very behind of AML Regime.

In conclusion, a comprehensive cybercrime regime is needed to prevent safe havens in the world. The obstacles in front of diffusion of Cybercrime Regime should be abolished. It seems that Cybercrime policy diffusion without a coercive power has reached to its borders. Coercive mechanisms should be created to

maintain the diffusion and increase cooperation between states. This should be provided by the sanctions which will be applied to the non-cooperative states.



## ***BIBLIOGRAPHY***

- Alazab, M. & Chon, S., 2015. *Cyber Security in the Gulf Cooperation Council*. [Online] Available at: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2594624](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594624) [Accessed 23 March 2016].
- ASEAN, 2009. *Roadmap for an ASEAN Community*. Jakarta, ASEAN, pp. 1-128.
- ASEAN, 2011. *Joint Statement of the Eight Asean Ministerial Meeting on Transnational Crime (8th AMMTC)*. Bali, ASEAN.
- AU, 2009. *Extraordinary Conference of African Union Ministers in Charge of Communication and Information Technologies, November 2009*. [Online] Available at: <http://africainonespace.org/downloads/TheOliverTamboDeclaration.pdf> [Accessed 16 January 2016].
- AU, 2012. *Draft African Union Convention on the Establishment of A Legal Framework Conducive to Cyber Security in Africa or Draft African Union Convention on the Confidence and Security in Cyberspace, 1 September 2012*. [Online] Available at: [http://au.int/en/sites/default/files/AU%20Convention%20EN.%20%283-9-2012%29%20clean\\_0.pdf](http://au.int/en/sites/default/files/AU%20Convention%20EN.%20%283-9-2012%29%20clean_0.pdf) [Accessed 16 January 2016].
- AU, 2014. *African Union Convention on Cyber Security and Personal Data Protection, 27 June 2014*. [Online] Available at: <https://ccdcoe.org/sites/default/files/documents/AU-270614-CSCConvention.pdf> [Accessed 16 January 2016].
- August, R., 2002. International Cyber-Jurisdiction: A Comparative Analysis. *American Business Law Journal*, Vol.39, pp. 531-574.
- Bell, R., 2002. The Prosecution of Computer Crime. *Journal of Financial Crime- Vol.9 No.4*, pp. 308-325.
- Brenner, S. W., 2004. Toward a Criminal Law for Cyberspace: Product Liability and Other Issues. *Journal of Technology Law and Policy*, Vol. V, pp. 1-113.
- Broadhurst, R., 2006. Developments in the Global Law Enforcement of Cybercrime. 29 *Policing International Journal of Police Strategies and Management* 408, pp. 408-433.

Calderoni, F., 2010. The European Legal Framework on Cybercrime: Striving for an Effective Implementation. *Crime Law Soc Change (2010)* 54, pp. 339-357.

CCDCOE, 2002. *APEC Cybersecurity Strategy, 23 August 2002*. [Online]  
Available at: <https://ccdcoe.org/sites/default/files/documents/APEC-020823-CyberSecurityStrategy.pdf>  
[Accessed 16 January 2016].

Choo, K.-K. R., 2008. Organised Crime Groups in Cyberspace: A Typology. *Trends Organ Crime* 11, pp. 270-295.

COE, 1989. *Recommendation No. R (89) 9, adopted by Committee of Ministers on 13 September 1989 at 428th Meeting of the Ministers' Deputies*. [Online]  
Available at:  
<https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2>  
[Accessed 17 January 2016].

COE, 1995. *Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers' Deputies, 11 September 1995*. [Online]  
Available at:  
[http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec\(1995\)013\\_EN.asp](http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(1995)013_EN.asp)  
[Accessed 17 January 2016].

CoE, 2001a. *Council of Europe's Convention on Cybercrime, 23 November 2001*. [Online]  
Available at:  
[http://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest/7\\_conv\\_budapest\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest/7_conv_budapest_en.pdf)  
[Accessed 20 April 2016].

CoE, 2001b. *Explanatory Report to the Convention on Cybercrime, 23 November 2001*. [Online]  
Available at:  
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>  
[Accessed 20 April 2016].

CoE, 2007. *Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 25 October 2007*. [Online]  
Available at:  
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d3832>  
[Accessed 14 January 2016].

COE, 2014. *Cybercrime Model Laws, Discussion Paper Prepared for Cybercrime Convention Committee, 23 December 2014*. [Online]

Available at:

[https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021\\_model\\_law\\_study\\_v15.pdf](https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf)

[Accessed 16 January 2016].

Csonka, P., 2006. The Council of Europe's Convention on Cyber-Crime and Other European Initiatives. *Revue Internationale de Droit Pénal*, 2006/3. Vol. 77, pp. 473-501.

Elster, J., 1989. *Nuts and Bolts for the Social Sciences*. Cambridge: Cambridge University Press.

Eriksson, J. & Giacomello, G., 2006. The Information Revolution, Security and International Relations: (IR) Relevant Theory?. *International Political Science Review*, Vol.27(No.3), pp. 221-244.

EU, 1996. *Illegal and Harmful Content on the Internet, 16 October 1996*. [Online]

Available at: [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0487:FIN:EN:PDF)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0487:FIN:EN:PDF](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0487:FIN:EN:PDF)

[Accessed 13 January 2016].

EU, 1999a. *Adopting a Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks, 25 January 1999*. [Online]

[Online]

Available at: [http://eur-lex.europa.eu/legal-](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999D0276&from=EN)

[content/EN/TXT/PDF/?uri=CELEX:31999D0276&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999D0276&from=EN)

[Accessed 13 January 2016].

EU, 1999b. *e-Europe-An Information Society for All, 8 December 1999*. [Online]

Available at: [http://eur-lex.europa.eu/legal-](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l24221&from=EN)

[content/EN/TXT/HTML/?uri=URISERV:l24221&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l24221&from=EN)

[Accessed 14 January 2016].

EU, 1999. *Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the Draft Convention on Cyber Crime held in the Council of Europe, (1999/364/JHA), 27 May 1999*. [Online]

Available at: [http://eur-lex.europa.eu/legal-](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999F0364&from=EN)

[content/EN/TXT/PDF/?uri=CELEX:31999F0364&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999F0364&from=EN)

[Accessed 14 January 2016].

EU, 2000. *Directive on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce in the Internal Market, 8 June 2000*. [Online]

Available at: [http://eur-lex.europa.eu/legal-](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN)

[content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN)

[Accessed 14 January 2016].

EU, 2001a. *Network and Information Security: Proposal for A European Approach (COM (2001) 298 final), 6 January 2001*. [Online]



Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN>  
[Accessed 14 January 2016].

EU, 2001b. *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crimes (COM(2000) 890 final)*, 26 January 2001. [Online]  
Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0890&from=EN>  
[Accessed 13 January 2016].

EU, 2001c. *Council Framework Decision on Combating Fraud and Counterfeiting of non-cash means of Payment*, 28 May 2001. [Online]  
Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:149:0001:0004:EN:PDF>  
[Accessed 14 January 2016].

EU, 2005a. *Council Framework Decision on Attacks against Information Systems (2005/222/JHA)*, 24 February 2005. [Online]  
Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN>  
[Accessed 14 January 2016].

EU, 2005b. *Directive of the EP and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM (2005) 438 final)*, 21 September 2005. [Online]  
Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005PC0438&qid=1452808312924&from=EN>  
[Accessed 14 January 2016].

EU, 2007. *Towards a General Policy on the Fight against Cyber Crime (COM (2007) 267 final)*, 22 May 2007. [Online]  
Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF>  
[Accessed 14 January 2016].

EU, 2008. *Council Framework Decision 2008/919/JHA of 28 November 2008 Amending Framework Decision 2002/475/JHA on Combating Terrorism*, 28 November 2008. [Online]  
Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0919&from=EN>  
[Accessed 14 January 2016].

EU, 2010. *An Open and Secure Europe Serving and Protecting Citizens 2010C115/01*, 4 May 2010. [Online]  
Available at: <http://www.eurojust.europa.eu/doclibrary/EU-framework/EUframeworkgeneral/The%20Stockholm%20Programme%202010/Stockhol>

[m-Programme-2010-EN.pdf](#)

[Accessed 14 January 2016].

EU, 2010. *Proposal for a Directive of The EP and of the Council on Attacks against Information Systems and Repealing Council Framework Decision 2005/222/JHA*, 30 September 2010. [Online]

Available at: [http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF)

[Accessed 14 January 2016].

EU, 2011. *Directive 2011/92/EU of the EP and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography*, 13 December 2011. [Online]

Available at: [http://eur-lex.europa.eu/legal-](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN)

[content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN)

[Accessed 14 January 2016].

FATF, 1990. *FATF Forty Recommendations*. s.l., s.n.

FATF, 2003. *FATF 40 Recommendations, October 2003*. [Online]

Available at: <http://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf>

[Accessed 27 March 2016].

FATF, 2008. *FATF IX Special Recommendations, February 2008*. [Online]

Available at: <http://www.un.org/en/sc/ctc/docs/bestpractices/fatf/9specialrec/fatf-9specialrec.pdf>

[Accessed 27 March 2016].

FATF, n.d. *FATF-GAFI Website*. [Online]

Available at: <http://www.fatf-gafi.org/countries/>

[Accessed 9 March 2016].

FATF, n.d. *History of the FATF*. [Online]

Available at: <http://www.fatf-gafi.org/about/historyofthefatf/>

[Accessed 18 February 2016].

G8, 2006. *Press Conference on the Results of the G8 Justice and Home Affairs Ministerial*, 16 June 2006. [Online]

Available at: <http://www.g8.utoronto.ca/justice/justice2006.htm>

[Accessed 16 January 2016].

G8, 2009. *Final Declaration to the G8 Ministerial Meeting of Justice and Home Affairs*, 30 May 2009. [Online]

Available at: [http://www.g8italia2009.it/static/G8\\_Allegato/declaration1giu2009,0.pdf](http://www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf)

[Accessed 12 January 2016].

G8, 2010. *G8 Muskoka Declaration, Recovery and New Beginnings*. Muskoka, s.n.

- G8, 2011. *Deauville Declaration, 26-27 May 2011*. [Online]  
Available at: [http://ec.europa.eu/archives/commission\\_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration\\_en.pdf](http://ec.europa.eu/archives/commission_2010-2014/president/news/speeches-statements/pdf/deauville-g8-declaration_en.pdf)  
[Accessed 12 April 2016].
- Gercke, M., 2009. Europe's Legal Approaches to Cybercrime. *ERA Forum (2009) 10*, pp. 409-420.
- Gercke, M., 2011. Understanding Cybercrime: A Guide For Developing Countries. *ITU*, pp. 1-493.
- Gercke, M., 2012. *Understanding Cybercrime: Phenomena, Challenges, and Legal Response*. s.l.:ITU.
- Gercke, M., 2014. *Understanding Cybercrime: Phenomena, Challenges, and Legal Response*, s.l.: ITU.
- Grabosky, P., 2007. Requirements of Prosecution Services to Deal with Cyber Crime. *Crime Law Soc Change 47*, pp. 201-223.
- Haas, P. M., 1989. Do Regimes Matter? Epistemic Communities and Mediterranean Pollution Control. *International Organization, Vol. 43, Issue 3*, pp. 377-403.
- Ikenberry, G. & Kupchan, C. A., 1990. Socialization and Hegemonic Power. *International Organization 44 (2)*, pp. 283-315.
- ITU, 2003. *World Summit on the Information Society, Plan of Action, 12 December 2003*. [Online]  
Available at: <http://www.itu.int/net/wsis/docs/geneva/official/poa.html>  
[Accessed 13 January 2016].
- ITU, 2005. *Tunis Agenda for Information Society, 18 November 2005*. [Online]  
Available at: <http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>  
[Accessed 13 January 2016].
- J.C.Sharman, 2008. Power and Discourse in Policy Diffusion: Anti-Money Laundering in Developing States. *International Studies Quarterly 52*, pp. 635-656.
- Keyser, M., 2003. The Council of Europe Convention on Cybercrime. *12 J. Transnational Law and Policy 287*, pp. 287-326.
- Krasner, S. D., 1982. Structural Causes and Regime Consequences: Regimes as Intervening Variables. *International Organization, Vol. 36, No. 2*, pp. 185-205.
- Lake, D. A., 1993. Leadership, Hegemony, and the International Economy: Naked Emperor or Tattered Monarch with Potential?. *International Studies Quarterly 37 (4)*, pp. 459-489.
- Le Nguyen, C., 2014. The International Anti-Money Laundering Regime and Its Adoption by Vietnam. *Asian Journal of International Law 4*, pp. 197-225.

March, J. G. & Olsen, J. P., 1989. *Rediscovering Institutions: The Organizational Basis of Politics*. New York: Free Press.

Masadeh, A., 2010. *Combating Cyber Crimes-Legislative Approach-A Comparative Study*. [Online]

Available at:

<http://www.almeezan.qa/ReferenceFiles.aspx?id=54&type=doc&language=en>

[Accessed 17 January 2016].

Mitsilegas, V. & Gilmore, B., 2007. The EU Legislative Framework Against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards. *International and Comparative Law Quarterly*, Vol. 56, pp. 119-141.

Moitra, S. D., 2005. Developing Policies for Cybercrime: Some Empirical Issues. *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 13, Issue 3, pp. 435-464.

NCUSAR, 2015. *Background Guide, Model Arab League, Joint Defence Council*. [Online]

Available at: <http://ncusar.org/modelarableague/wordpress/wp-content/uploads/2012/08/Joint-Defense-Council.pdf>

[Accessed 25 March 2016].

Nelson, S., 2007. Regulating Money Laundering in the United States and Hong Kong: A Post 9-11 Comparison. *Washington University Global Studies Law Review*, Vol 6., Issue 3, pp. 723-745.

OAS, 2000. *Third Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, 3 March 2000*. [Online]

Available at: [http://www.oas.org/juridico/english/remjaIII\\_recom.pdf](http://www.oas.org/juridico/english/remjaIII_recom.pdf)

[Accessed 17 January 2016].

OAS, 2002. *Fourth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, 10 March 2002*. [Online]

Available at: [http://www.oas.org/juridico/english/remjaIV\\_final\\_report.pdf](http://www.oas.org/juridico/english/remjaIV_final_report.pdf)

[Accessed 17 January 2016].

OAS, 2006. *Sixth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, 26 April 2006*. [Online]

Available at: [http://www.oas.org/juridico/english/moj\\_vi\\_report\\_en.pdf](http://www.oas.org/juridico/english/moj_vi_report_en.pdf)

[Accessed 17 January 2016].

OAS, 2008. *Seventh Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, 30 April 2008*. [Online]

Available at: [http://www.oas.org/juridico/english/remjaVII\\_final\\_report.pdf](http://www.oas.org/juridico/english/remjaVII_final_report.pdf)

[Accessed 17 January 2016].

OAS, 2010. *Eighth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, 26 February 2010*. [Online]

Available at: [http://www.oas.org/en/sla/dlc/remja/recom\\_VIII\\_en.pdf](http://www.oas.org/en/sla/dlc/remja/recom_VIII_en.pdf)  
[Accessed 17 January 2016].

OAS, 2012a. *Seventh Meeting of the Working Group on Cybercrime*, Washington: OAS.

OAS, 2012b. *Ninth Meeting of Ministers of Justice or Other Ministers or Attorneys General of the Americas, 29 November 2012*. [Online]

Available at: [http://www.oas.org/en/sla/dlc/remja/pdf/recomm\\_IX.pdf](http://www.oas.org/en/sla/dlc/remja/pdf/recomm_IX.pdf)  
[Accessed 25 March 2016].

OAS, 2015. *Organization of American States, October 2015*. [Online]

Available at: <http://www.oas.org/en/sla/dlc/remja/meetings.asp>  
[Accessed 17 January 2016].

OAS, 2015. *Tenth Meeting of Ministers of Justice or Other Ministers or Attorneys General of the Americas, 16 October 2015*. [Online]

Available at: [http://www.oas.org/en/sla/dlc/remja/pdf/remja\\_x\\_rec\\_conc\\_en.pdf](http://www.oas.org/en/sla/dlc/remja/pdf/remja_x_rec_conc_en.pdf)  
[Accessed 25 March 2016].

OECD, 2002. *OECD Guidelines for the Security and Information Systems and Networks: Towards a Culture of Security, 25 Juny 2002*. [Online]

Available at: <http://www.oecd.org/sti/ieconomy/15582260.pdf>  
[Accessed 16 January 2016].

OECD, 2005. *Spam Issues in Developing Countries DSTI/CP/ICCP/SPAM(2005)6/FINAL, 26 May 2005*. [Online]

Available at: <http://www.oecd.org/internet/ieconomy/34935342.pdf>  
[Accessed 16 January 2016].

OECD, 2008. *Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, 18 June 2008*. [Online]

Available at: <http://www.oecd.org/internet/consumer/40644196.pdf>  
[Accessed 16 January 2016].

Önok, M., 2013. International Co-operation in the Fight against Cybercrimes in the Light of the Council of Europe Convention on Cybercrime. *Marmara Üniversitesi Hukuk Araştırmaları Dergisi*, 19(2), pp. 1229-1270.

Picotti, L. & Salvadori, I., 2008. National Legislation Implementing the Convention on Cybercrime: Comparative Analysis and Good Practices. *Discussion paper*, pp. 1-197.

POGAR, 2007. *Programme on "Strengthening the Rule of Law in the Arab States-Project on the Modernization of Public Prosecution Offices-Regional Conference Booklet on Cybercrime, 20 June 2007*. [Online]

Available at: <ftp://pogar.org/LocalUser/pogarp/ruleoflaw/cybercrime-09e.pdf>  
[Accessed 17 January 2016].

- Popa, G. D., 2012. International Cooperation in the Struggle against Trans-border Organized Crime and Money Laundering. *Contemporary Readings in Law and Social Justice, Vol. 4 (2)*, pp. 575-578.
- Pushpanathan, S., 1999. *Combating Transnational Crime in ASEAN*. New Delhi, India, ASEAN.
- Putnam, T. L. & Elliott, D. D., n.d. *International Responses to Cyber Crime*. [Online] Available at: [http://scholar.google.com.tr/scholar\\_url?url=http://media.hoover.org/sites/default/files/documents/0817999825\\_35.pdf&hl=tr&sa=X&scisig=AAGBfm381PK3-sH3dGqUMY313iZsm6EUqg&nossl=1&oi=scholar&ved=0ahUKEwjM-fuAntrKAhWCjSwKHW62DEoQgAMIGSgAMAA](http://scholar.google.com.tr/scholar_url?url=http://media.hoover.org/sites/default/files/documents/0817999825_35.pdf&hl=tr&sa=X&scisig=AAGBfm381PK3-sH3dGqUMY313iZsm6EUqg&nossl=1&oi=scholar&ved=0ahUKEwjM-fuAntrKAhWCjSwKHW62DEoQgAMIGSgAMAA) [Accessed 2 February 2016].
- Reuter, P. & Truman, E. M., 2004. *Chasing Dirty Money: The Fight Against Money Laundering*. Washington DC: Institute for International Economics.
- Rõigas, H., 2015. *An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?*, 10 February 2015. [Online] Available at: <https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html> [Accessed 30 March 2016].
- Sharman, J., 2008. Power and Discourse in Policy Diffusion: Anti-Money Laundering in Developing States. *International Studies Quarterly* 52, pp. 635-656.
- Sofia University, 2002. *Draft Model Law on Electronic Transactions, November 2002*. [Online] Available at: [http://www.law.uni-sofia.bg/Kat/T/IP/T/ET/e\\_commercelawunisofiabg/%D0%98%D0%B2%D0%B0%D0%BD%20%D0%98%D0%B2%D0%B0%D0%BD%D0%BE%D0%B2%20\(ivan\\_ivanov\\_primer@abv.bg\)/DRAFT%20MODEL%20LAW%20ON%20ELECTRONIC%20TRANSACTIONS%201.pdf](http://www.law.uni-sofia.bg/Kat/T/IP/T/ET/e_commercelawunisofiabg/%D0%98%D0%B2%D0%B0%D0%BD%20%D0%98%D0%B2%D0%B0%D0%BD%D0%BE%D0%B2%20(ivan_ivanov_primer@abv.bg)/DRAFT%20MODEL%20LAW%20ON%20ELECTRONIC%20TRANSACTIONS%201.pdf) [Accessed 2016 January 2016].
- Thony, J., 1996. Processing Financial Information in Money Laundering Matters: The Financial Intelligence Units. *European Journal of Crime, Criminal Law and Criminal Justice*, pp. 257-282.
- Turhan, O., 2006. *"Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar)"-Expertise Thesis*. s.l.:Devlet Planlama Teşkilatı Müsteşarlığı.
- UN, 1988. *United Nations Convention Against Illicit Traffic in Narcotics Drugs and Psychotropic Substances, arts. 3 (b) and (c)*. s.l., UN.
- UN, 1989. *Convention on the rights of the Child, 12 December 1989*. [Online] Available at: <http://www.un.org/documents/ga/res/44/a44r025.htm> [Accessed 12 January 2016].

UN, 1990. *Eighth United Nations Congress on the Prevention on Crime and Treatment of Offenders, 14 December 1990*. [Online]

Available at: <http://www.un.org/documents/ga/res/45/a45r121.htm>

[Accessed 12 January 2016].

UN, 2000b. *Tenth United Nations Congress on the Preention on Crime and the Treatment of Offenders, 3 February 2000*. [Online]

Available at:

[https://www.unodc.org/documents/congress//Previous\\_Congresses/10th\\_Congress\\_2000/017\\_ACONF.187.10\\_Crimes\\_Related\\_to\\_Computer\\_Networks.pdf](https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf)

[Accessed 12 Januray 2016].

UN, 2000. *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, 25 May 2000*. [Online]

Available at: <http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx>

[Accessed 12 January 2016].

UN, 2001. *Combating the Criminal Misuse of Information Technologies, 22 January 2001*.

[Online]

Available at: [https://www.itu.int/ITU-](https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf)

[D/cyb/cybersecurity/docs/UN\\_resolution\\_55\\_63.pdf](https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf)

[Accessed 12 January 2016].

UN, 2003. *United Nations Convention Against Corruption*. Vienna, UN.

UN, 2004. *United Nations Convention against Transnational Organized Crime*. New York, s.n.

UN, 2005. *Eleventh United Nations Congress on Crime Prevention and Criminal Justice, 17 May 2005*. [Online]

Available at:

[https://www.unodc.org/documents/congress//Documentation/11Congress/ACONF203\\_18\\_e\\_V0584409.pdf](https://www.unodc.org/documents/congress//Documentation/11Congress/ACONF203_18_e_V0584409.pdf)

[Accessed 14 March 2016].

UN, 2005. *Information Economy Report*. [Online]

Available at: [http://unctad.org/en/docs/sdteecb20051ch6\\_en.pdf](http://unctad.org/en/docs/sdteecb20051ch6_en.pdf)

[Accessed 12 January 2016].

UN, 2010. *Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 18 April 2010*. [Online]

Available at: [https://documents-dds-](https://documents-dds-ny.un.org/doc/UNDOC/LTD/V10/529/03/PDF/V1052903.pdf?OpenElement)

[ny.un.org/doc/UNDOC/LTD/V10/529/03/PDF/V1052903.pdf?OpenElement](https://documents-dds-ny.un.org/doc/UNDOC/LTD/V10/529/03/PDF/V1052903.pdf?OpenElement)

[Accessed 14 March 2016].

UN, 2011. *CCDCOE, 14 September 2011*. [Online]

Available at: <https://ccdcoe.org/sites/default/files/documents/UN-110912->

CodeOfConduct\_0.pdf

[Accessed 30 March 2016].

UNCTAD, 2005. *Information Economy Report, UNCTAD/SDTE/ECB/2005/1*. [Online]

Available at: [http://unctad.org/en/docs/sdteecb20051ch6\\_en.pdf](http://unctad.org/en/docs/sdteecb20051ch6_en.pdf)

[Accessed 17 January 2016].

UNODC, 2013. *Comprehensive Study on Cybercrime-Draft*. s.l., UN.

Urbas, G., 2006. Criminalising Computer Misconduct: Some Legal and Philosophical Problems. *14 Asia Pacific Law Review* 95, pp. 95-121.

Vatis, M. A., 2010. The Council of Europe Convention on Cybercrime. *National Academy of Sciences*, pp. 207-223.

WAIGF, 2011. *Commonwealth Cybercrime Initiative, October 2011*. [Online]

Available at: [http://www.waigf.org/IMG/pdf/Cybercrime\\_Initiative\\_Outline.pdf](http://www.waigf.org/IMG/pdf/Cybercrime_Initiative_Outline.pdf)

[Accessed 16 January 2016].

Weber, A. M., 2003. The Council of Europe's Convention on Cybercrime. *Berkeley Technology Law Journal*, No. 18, pp. 425-446.

Weyland, K., 2005. Theories of Policy Diffusion: Lessons from Latin American Pension Reform. *World Politics*, Vol. 57 No. 2, pp. 262-295.