T.C.
ATILIM UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF INTERNATIONAL RELATIONS
INTERNATIONAL RELATIONS MASTER PROGRAMME

A NEOLIBERAL ANALYSIS OF INTERNATIONAL COOPERATION WITH MULTINATIONAL SERVICE PROVIDERS: THE ROLE AND EFFECT OF THE COUNCIL OF EUROPE'S CONVENTION ON CYBERCRIME ON FIGHTING AGAINST TRANSBORDER CRIMES

Master's Thesis

Fatma Akın Akıllı

Ankara-2021

T.C.
ATILIM UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF INTERNATIONAL RELATIONS
INTERNATIONAL RELATIONS MASTER PROGRAMME

A NEOLIBERAL ANALYSIS OF INTERNATIONAL COOPERATION WITH MULTINATIONAL SERVICE PROVIDERS: THE ROLE AND EFFECT OF THE COUNCIL OF EUROPE'S CONVENTION ON CYBERCRIME ON FIGHTING AGAINST TRANSBORDER CRIMES

Master's Thesis

Fatma Akın Akıllı

Supervisor
Asst. Prof. Dr. Nilgün Eliküçük Yıldırım

Ankara-2021

ACCEPTANCE AND APPROVAL

This is to certify that this thesis titled “A Neoliberal Analysis of International Cooperation with Multinational Service Providers: The Role and Effect of the Council of Europe’s Convention on Cybercrime on Fighting Against Transborder Crimes” and prepared by Fatma AKIN AKILLI meets with the commitee’s approval unanimously/by a majority vote as Master’s Thesis in the field of International Relations following the successful defense of the thesis conducted on 14/07/2021.

Assoc. Prof. Dr. Gözde YILMAZ (Chair)

Asst. Prof. Dr. Nilgün ELİKÜÇÜK YILDIRIM (Supervisor)

Assoc. Prof. Dr. Ali İbrahim AKKUTAY (Member)

Prof. Dr. Dilaver TENGİLİMOĞLU (Director)

ETHICS DECLARATION

I hereby declare that:

- I prepared this thesis in accordance with Atılım University Graduate School of Social Sciences Thesis Writing Directive,
- I prepared this thesis within the framework of academic and ethics rules,
- I presented all information, documents, evaluations and findings in accordance with scientific ethical and moral principles,
- I cited all sources to which I made reference in my thesis,
- The work of art in this thesis is original, I hereby acknowledge all possible loss of rights in case of a contrary circumstance. (in case of any circumstance contradicting with my declaration)

Fatma AKIN AKILLI

ÖZ

Akın Akıllı, Fatma. Neoliberal perspektifte çok uluslu servis sağlayıcıları ile uluslararası ortaklaşa çalışmanın değerlendirilmesi, Avrupa Konseyi Siber Suç Konvansiyonu'nun sınır aşan suçlarla mücadelede rolü ve etkisi. Yüksek Lisans Tezi, Ankara 2021.

Avrupa Konseyi tarafından çok sayıda ülke ve uzman grubunun katkılarıyla hazırlanan ve 2021 yılı itibari ile uluslararası alanda 20. yılını tamamlamakta olan, Siber Suç Konvansiyonu ya da bir diğer deyiş ile Sanal Ortamda İşlenen Suçlar Sözleşmesi hazırlandığı yıldan bu yana uluslararası arenada bilişim suçlarına odaklanmış en çok paydaşa sahip olan anlaşmadır. Bunun yanı sıra paydaşlardan oluşan Uzmanlar Grubu'nun zamanla değişen suç trendlerine yönelik çalışmaları ile her zaman diliminde yaşayan bir anlaşma olarak varlığını devam ettirmektedir.

Bilişim suçlarının bir diğer deyişle siber suçların tarihi internetin ortaya çıkmasına dayanmaktadır. İnternetin sanal ortamının kullanıcılara sağladığı avantajlar suçlular tarafından kötüye kullanılmakta ayrıca anonim olmanın sağladığı gizlenebilecek olma yanılgısı siber suçların yıkımının artmasına neden olmaktadır. Çok uluslu servis sağlayıcılarının kullanıcılarına sunduğu neredeyse maliyetsiz olan sınırsız ve anında iletişim/etkileşim şahısların anonim olabilme avantajı ile birleştiğinde bu platformlarda suçların artmasına neden olmaktadır.

Suçun önlenmesinde, suç ve suçlu ile mücadele edilmesinde ve ortaya çıkan suçların arkasındaki anonim aktörlerin belirlenmesinde dijital kanıtların önemi artmakta ve bu durum ülkeleri birbirine bağımlı hale getirmektedir. Servis sağlayıcılar tarafından güvenli bir platforma sahip olmak önem kazanırken, ülkeler için bu durum vatandaşlarının korunabilmesi, ulusal güvenliğin sağlanabilmesi ve suçtan kaynaklanan ekonomik kayıpların önlenmesi önem kazanmaktadır. Ayrıca elektronik delillerin toplanması gerekliliği bu şirketler ile uzman polis birimleri arasında uluslararası çalışmayı gerekli kılarken, aynı zamanda uluslararası arenada yaşanan politik gerilimler soruşturmaların aksatılmasına ve hatta bazı durumlarda

davaların kapatılmasına neden olmaktır. Bu kapsamda çok sayıda paydaşın dahil olduğu uluslararası anlaşmaların önemi her geçen gün artmaktadır.

Anahtar Kelimeler: Siber suç, siber güvenlik, çok uluslu servis sağlayıcı, Avrupa Konseyi, Sanal Ortamda İşlenen Suçlar Sözleşmesi

ABSTRACT

Akın Akıllı, Fatma. A neoliberal analysis of international cooperation with multinational service providers, the role and effect of the Council of Europe's Convention on Cybercrime on fighting against trans-border crimes. Master Thesis, Ankara 2021.

Convention on Cybercrime which has completely focused on fighting against cybercrimes with more parties compared to the other international initiatives has been prepared with the special contributions of several countries and expert groups and it is also going to celebrate its 20th anniversary in 2021. In addition to that, with the changing crime trends works of the Experts Group, which consists of representatives of stakeholders, it maintains its existence as an agreement that lives in periods.

The history of internet crimes in other words cybercrimes dates back to the invention of the internet. The advantages of the virtual environment of the internet such as being able to anonym or can reaching out to any part of the world without any extra endeavor, have been misused by criminals. In addition, the delusion of criminals, like staying anonymous causes raising devastating effects of cybercrimes. Almost free unlimited and instant communication/interaction offered by multinational service providers to their users, combined with the anonymity advantage of individuals, leads to an increase in crimes on these platforms.

The importance of digital evidence to prevent crime before it happens or finding the real actors after the crime occurred increases and this situation makes the countries dependent on each other. While for service providers, having a secure platform becomes important, for states, protecting their citizens, ensuring national security and preventing economic loss caused by online crimes become important. Also on the one hand, while the need of collecting electronic evidence obliges these companies and expert police units to work harmoniously, on the other hand, the political problems in the international arena cause a serious slowdown of

investigations. Even in some instances, these problems cause rescission of the cases. In this context, the importance of international agreements concluded by a wide range of parties becomes important each passing day.

Keywords: Cybercrime, cybersecurity, multinational service provider, the Council of Europe, Convention on Cybercrime,

01000001 01101101 01101111 01110010
00100000 01110000 01100001 01110100
01110010 01101001 11000011 10100110
00100000 01101110 01101111 01110011
01110100 01110010 01100001 00100000
01101100 01100101 01111000

"**Amor patriæ nostra lex**"

ACKNOWLEDGEMENT

This research is not only my output but also includes suggestions, labor and patience of my dearest Supervisor, namely Asst. Prof. Dr. Nilgün ELİKÜÇÜK YILDIRIM. At the same time, during this journey, I had many perfect fellow travelers. Firstly, I have to extend my sincere thanks to my parents and siblings for their guidance and unique support in every moment of my life.

Additionally, I would never complete this thesis without the support of my other half Hakan AKILLI. He always trusted and encouraged me. Also, I would like to thank my all colleagues, especially my Inspector İbrahim ÖZDEMİR since he always sheds light on my way and teaches me whatever he knows. I also would like to thank my Advisor Nusret KASAP from Amasya University in which I completed my Bachelor's Degree. Whenever I needed him, he had been there.

I would like to thank my dear friends Aybüke BAY, Cenk BİRGE and Menifer KIZILKAYA for their precious friendship and motivation during my study.

TABLE OF CONTENTS

ABBREVIATIONS

BEC : Business Email Compromise
CEG : Cloud Evidence Group
CoE : Council of Europe
DCC : Department of Cybercrime
ECPA : Electronic Communication Privacy Act
GCI : Global Cybersecurity Index
ICTs : Information and Communication Technologies
ISP : Internet Service Provider
ITU : Information and Telecommunication Union
MA : Mutual Assistance
MLAT : Mutual Legal Assistance Treaty
MSP : Multinational Service Provider
OSINT : Open Source Intelligent
SCA : Stored Communications Act
SPoC : Single Point of Contact
TC-Y : Cybercrime Convention Committee
TCC : Turkish Criminal Code
TNP : Turkish National Police
USG : User Generated Content

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

This thesis aims to present a neoliberal analysis of the Council of Europe's Convention on Cybercrime and cybersecurity works of the Convention with special attention paid to its impacts on states. The main goal of this study is to perform an analysis of the role of the Convention's capacity-building works on the parties. This thesis focuses on especially the questions of: Why do states depend on each other in the virtual world? Why states, public-private entities and non-governmental organizations are eager to support the other's work? It will try to find answers to those questions through neoliberalism that concentrates on international cooperation and assumes it as the necessity of the modern global world.

Especially during the past decade, multinational service providers and their effects on societies have become on the agenda of international relations all around the world. For internet users, especially for those who are using Twitter, Facebook or Microsoft services, these tools play an important role as a main communication channel to criticize the illegal or improper actions of any state, to make propaganda or protest anything that causes disturbance on the public. Along with all their effects, criminals use Information and Communication Technologies (Hereinafter referred to as ICTs) to commit crimes too. They violate laws, damage infrastructures, share improper content(s) including harsh language, hate speech, call for terrorist action, cheat people, exploit vulnerable groups of any society, sell drugs illicit and dangerous materials, even they use the technologies for human or juvenile trafficking.

The global and national level numbers show that cybercrimes are getting serious each passing day on multinational service providers and to prevent these cases and to prosecute the criminals, capacity building works are very important. This situation raises a question mark, and the question has been answered by the

neoliberals through cooperation. Like Keohane and Nye put it[1], why states generally cooperate with each other and why they should be against possible threats.

In light of this information, this thesis is going to analyze the relation and cooperation among states' organizations (judicial authorities, law enforcement authorities, etc.) and multinational service providers. The questions addressed in the context of the research for this thesis are as follows: What is the interest of states when they became a party to international agreements? How does the Convention on Cybercrime support countries on capacity building works and legislation? How stakeholders can benefit from the Convention while they are fighting against cybercrimes?

This thesis will present the answers to all of these questions through qualitative methods and quantitative data. Neoliberal narratives and the analytical richness of the theory constitute qualitative methods in this thesis. The quantitative method is used principally for numerical data referring to the number of investigations, crimes, and victims of cybercrimes along with statistic values of the works of multinational service providers. In this study, primary sources are composed of companies, countries, and organizations' works and their interpretations regarding provisional, procedural law, and mutual cooperation on cybercrimes. Besides, the main aim of this thesis is to evaluate international cooperation within the context of the Convention on Cybercrime from the neoliberal perspective by focusing mostly on the crimes that occurred and committed on or via information and communication technologies.

In the first chapter, there will be an introduction part to discuss the need for cooperation for countries from a neoliberal perspective, for depth analysis of multinational relations among the member states. The second chapter will analyze and explain the emergence of the internet, will work on its far-reaching process along with the rising popularity of social media and with the history of cybercrimes. The first part will discuss the cooperation idea in terms of neoliberalism as one of the IR

[1] Keohane, R. O., & Nye, J. S. (1987). Power and Interdependence revisited. *International organization*, *41*(4), pp.725-753.

theories. The neoliberal theory is chosen here because the tenets of neoliberalism emphasize the ideas are related to mutual assistance, globalization, governance without a government system that has already shaped cooperation politics among 65 countries with the Convention on Cybercrime.

The third chapter will analyze the cooperation works of several international organizations mentioned and welcomed by the Council of Europe's Convention on Cybercrime. Those are also the leading organizations that especially paid attention to cybercrime and currently working on cybercrime issues by discussing the latest trends, innovations, crime detection technologies, capacity-building needs and recommended laws on those issues. It seems that using the organization's works and experiences by the Council of Europe, produced the most comprehensive legal structure on the cybercrime issue.

As claimed by Axelrod and Keohane, if a prisoner gets in touch with the other to prevent punishment with the advantages of communication, the possibility of cooperation is going to increase too, or maybe obvious.[2] When we consider states as prisoners and the crimes as punishment, it seems that with communication, negotiation, mutual assistance states can refrain from punishment, and this is the exact aim of the Convention on Cybercrime. In the third chapter, the argument of Axelrod will be discussed by mentioning several international cooperation initiatives.

The fourth chapter of this thesis is going to highlight the most criticized outcomes of the Convention and criticize the inadequate capacity-building work of the Convention by focusing on the problems among private sectors such as Twitter, Google and Yahoo! and some particular countries. While the problematic relations are investigated, the statistics of the top ten information requested countries will be used. Within the fifth chapter of this thesis, the fifth one will examine the benefits of the Convention with case examples of multinational cooperation.

[2] Axelrod, R., & Keohane, R. O. (1985). Achieving cooperation under anarchy: Strategies and institutions. *World politics*, *38*(1), pp.226-254.

Finally, in the conclusion part of this thesis, some recommendations to solve the current problems between ICTs and countries along with the recommendations to raise the efficiency of the Convention will be found.

CHAPTER 1

OVERVIEW

It is possible to discuss on many international wars in world history. WW1 and WW2, which had a devastating effect on many states, resulted from the search for power and the struggle for interest in the international arena, as well as economic problems. The struggle of the ideas of liberalism and communism between the USA and the USSR has changed the dimensions of war to technology wars. During the technology war, the Internet emerged with the purpose of securing information and providing sufficient intelligence. When the Internet, which emerged as a result of this revolution from the wars of ideologies to the wars of technologies, has become accessible to the public this made the dimension of the war much more extensive.

Today, individuals have been included in the international arena alongside the organizations and this turns the struggle from ordinary war to total war. This situation caused war-induced destruction. Computers have become weapons and hackers have caused billions of Dollars lost with these weapons and a large number of data of the states have been stolen by the white collars.[3]

Foreign fighters and terrorists organized attacks by using the free environment of the internet. Since the military technologies reduce military costs, small states have benefitted from the advantages of that. Therefore, the reducing costs with new technologies turned the large states into a sensitive position to this issue.[4]

---

[3] Barnett, C. (2000). The measurement of white-collar crime using uniform crime reporting (UCR) data. *US Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division*.

[4] Keohane, R. O., & Nye, J. S. (1987). Power and Interdependence revisited. *International organization, 41*(4), pp.725-753.

Although it has some side effects such as pollution of information and the possibility of misuses like extremism or terrorism; Information and Communication Technologies are indispensable tools for our daily life. While communication technologies are crossing borders, they also bring complex and transcontinental crimes with them. In this context, the need for international cooperation and collaboration has emerged to fight against these borderless and limitless crimes. The first example of collaboration on cybercrimes in the international arena is the "Convention on Cybercrime" (Also called as Budapest Convention.). It has been planned in an international context and provides a basic framework where governments and organizations can gather to fight against the crimes committed on the internet in the national, regional, and international arena.

The following questions will be guiding this chapter: Why did the international community need to cooperate in the virtual realm? What can be the effects and the side effects of international cooperation on human rights? What kind of difficulties and differences force the states to seek collective responsibilities to fight against cybercrimes and lastly does international cooperation work or not?

Being able to answer these comprehensive and open-ended questions, this study is to be applied to neoliberalism to understand states and information communications companies that are together with multinational and cross-border joint work to fight against cybercrimes.

1.1. Neoliberalism and Main Debates on Plurality of Actors in IR

Classical liberalism is derived from the works of many important philosophers such as Immanuel Kant and John Locke. However, the liberal theory became popular in the field of economic politics in the 18th and 19th centuries, supported by the work of Adam Smith and David Ricardo.

It is hard to gain a historical perspective on neoliberalism because it is mostly associated with globalization and recurring financial crises. In the interwar years

during the Great Depression neoliberalism emerged from debates among liberals. Differently from liberals, neoliberals accept new forms of intervention, social provision and harnessing state power to maintain market order. With some new recommendations, they left from laissez-faire doctrine. The development process of this idea is divided into three terms. The first phase of neoliberalism lasted from 1920s and 1950s at that time neoliberalism reformulated liberalism to address the concerns of the 1930s.[5] The second phase, namely the modern version of neoliberalism picked with Thatcher and Reagan, lasted from 1950s until the free market ascendency of Thatcher and Regan in 1980s.[6] The third phase launched around the 1980s and affected predominantly North Atlantic and Western Europe regions.[7]

The main themes of neoliberalism can be listed as follows; neoliberals see the state as an active structure they accept mutual assistance as important.[8] Additionally, the emphasis of neoliberalism is mostly on political, republican, sociological and social issues.[9] The rising understanding of state intervention especially after 1920s caused born of neoliberalism. Several elements included in neoliberalism are also included in the content of liberalism, such as autonomy, human rights, responsibility, being private instead of belonging to the public.[10]

---

[5]Princeton University," Introduction" Retrieved from: http://assets.press.princeton.edu/chapters/i9827.pdf (Accessed on February 20, 2020). p.6/8

[6] Altvater, E. (2008). The Roots Of Neoliberalism. *Socialist Register*, pp. *44*.

[7] Princeton University Press. Retrieved from: http://assets.press.princeton.edu/chapters/i9827.pdf (Accessed on January 23, 2021)

[8] Isnarti, R. (2016). A Comparison of Neorealism, Liberalism, and Constructivism in Analyzing Cyber War. *Andalas Journal of International Studies (AJIS)*, *5*(2), pp. 155

[9] Parmar, I., Miller, L. B., & Ledwidge, M. (Eds.). (2009). *New directions in US foreign policy*. Routledge. p 48-57

[10] Kendall, G. (2003). From liberalism to neoliberalism. In *Social Change in the 21st Century 2003 Conference Refereed Proceedings* (pp. 1-14). Centre for Social Change Research, School of Humanities and Human Services QUT.

Liberal scholars focus on pluralism, interdependence and globalization.[11] Also; ideologically liberalism claims economic, political or social relations are organized best within the body of free markets. In this context for liberals, the state should watch the activities of companies but should not intervene with them. Like the economy, when it comes to social life state should not intervene in the actions of its citizens.[12]

The limited action brought human rights fore. According to liberals, people can make their own choices, and those choices are much more accurate than what others choose for them. People are their own best judges. Individuals must live within the framework of the law so that wrong choices do not cost the freedom of others. Like liberals, all neoliberal philosophers esteem human freedom and rights.[13]

The emphasis on human rights and freedoms by Liberalism and Neoliberalism has enabled the theory to find a common point of sharing with online service providers. For example, in the content published by Twitter in its own guideline on defending and respecting the rights of users as stated by it exactly that "Defending and respecting the user's voice is one of our core values at Twitter. This value is a two-layered commitment to freedom of expression and privacy."[14]

Although neoliberalism is generally discussed more in the economic field, the globalization that comes with neoliberalism has not only caused the removal of economic boundaries but also led to the globalization of knowledge and

---

[11] Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations:(IR) relevant theory?. *International political science review*, *27*(3), pp. 221

[12] Jessop, B. (2002). *Liberalism, Neoliberalism, and Urban Governance: A State-Theoretical Perspective. Antipode, 34(3), 452–472.* doi:10.1111/1467-8330.00250

[13] Freeman, M. (2015). Neoliberal Policies and Human Rights. *Dokuz Eylul Universitesi Faculty of Law Journal*, *17*, pp.141.

[14] Twitter, Defending and respecting the rights of people using our service, Retrieved from: https://help.twitter.com/en/rules-and-policies/defending-and-respecting-our-users-voice (Accessed on January 23, 2021.)

technology.[15] In a way, neoliberalism offers a transnational perspective together with the nation-states. Neoliberals leave the state in the background and add new actors to the administration. This also means new rules and new policies are included with new actors.

For example, Facebook is one of the new actors and it is so powerful that there are some allegations about Facebook's intervention in the 2016 USA election. Again, during the election of the USA in 2016, the political data company named Cambridge Analytica reached the information of 87 million users through a survey conducted on the Facebook platform.[16] The illegally captured information was used by Russia by creating fake voters profiles so that Donald Trump wins the election.[17] The case shows the extent and the effects of ICTs on both the national and international levels.

The plurality of the actors brings the institutions into the agenda. Neoliberal institutionalism does not discuss the world state, but refers to the harmonious engagement of states and non-state actors with the issues on the global agenda. The liberal perspective focuses on four key assumptions. These are as follows: firstly, states, non-state actors and transnational actors having effective roles in world politics. Multinational corporations, even humans (who are sovereignty-free) play an important role in world politics. Secondly, states are not the only actors in the international arena. Non-state actors or multinational corporations can bring absolute gain (all can win). Thirdly, according to neoliberals, economic dependence brings social, cultural and political dependence. This leads to the globalization of the world and turns states into intercontinental nongovernmental organizations. Lastly,

[15] Baysal, T. (2017). Neo-Liberalizm Tartişmalari Çerçevesinde Kamu Yönetiminin Dönüşümü: Türkiye Pratiği. *Kafkas Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *8*(15), pp. 171-195

[16] The New York Times, (April 4, 2018), Facebook says Cambridge Analytica harvested data of up to 87 million users, Retrieved from: https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html

[17] BBC News, (January 8, 2019) Facebook ad campaign helped Donald Trump win election, claims executive, Retrieved from: https://www.bbc.com/news/technology-51034641

according to liberals international politics cannot be dominated only by military security so for international relations, state and society relation is a cornerstone.[18]

The action of states can affect others either positively or negatively due to linkages such as trade, communication, commercial or transportation networks. There is an invisible dependence between them. The information revolution is also one of the factors that change the meaning of dependency as complex interdependence. The cheaper communication, the easier access to the masses, and the anonymity supplied to NGOs and even individuals become stronger.[19]

In addition, the neoliberal idea refers to the private sector more than other theories. Private companies increase their effects on several realms including ICTs. This situation leads to the weakening of the security and sovereignty of the states each passing day.[20] Private sectors inevitably create a globally complex and interdependent relationship. Besides, these organizations internationally cause a sensitive and fragile structure.

According to Nye and Keohane, the term complex interdependence is related to mutual dependencies such as money, product, or human communication. A dependency exists when there is a relationship of reciprocity between two countries or organizations.[21] In the case of anarchy, even if states have a common interest, reaching international institutions became difficult due to the discredited nature of anarchy. However, neoliberals claim that states can solve this problem through international institutions. Because these institutions decrease the possibility of cheat and increase the attraction of compliance.[22] Compared to previous decades, the world

[18] Viotti, P. R., & Kauppi, M. V. (2019). *International relations theory*. Rowman & Littlefield.

[19] Keohane, R. O., & Nye Jr, J. S. (2000). Globalization: What's new? What's not? (And so what?). *Foreign policy*, pp. 104-119.

[20] Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR) relevant theory?. *International political science review*, *27*(3), pp. 221-244.

[21] Viotti, P. R., & Kauppi, M. V. (2019). *International relations theory*. Rowman & Littlefield.

[22] Keohane, R. O. (1984). *After hegemony: Cooperation and discord in the world political economy*. Princeton university press. (p.p. 89-90)

became more crowded and complexed, multiple issues come to the agenda, and these made states non-sufficient to find effective solutions to these superabundant issues, inevitably search for the interests of the countries that brought them together.[23] As Keohane stressed, if there is no common governance, interdependence may on these superabundant issues cause conflict among international actors.[24]

Another issue that is strongly mentioned by neoliberals is globalization. According to them, for those who try to explain neoliberalism several factors are triggering and expediting globalization. One of them is that undoubtedly internet and its borderless nature. The term global governance is the result of increased mutual dependence. Governance in the classic interpretation can be defined as making rules, enforcing them and using authority while global governance refers to using global rules and involves strategic interactions among entities.[25]

Increasing factors with globalization made the world unstable also with the effects of modern technologies and inventions states had to get interested in several factors such as illegal migration, ecological problems or organized crimes etc. Since these problems concerned and interested all the actors in the international arena including NGOs, regional or local interdependence transformed into global interdependence.[26] Because there is no single authority or government in the world of the states, diplomacy and politics between and within states, coalition and cooperation regarding global issues can effectively emerge with global governance.[27] There cannot be a single power as powerful as to control other nation-states but governance on a global level can absorb and eliminates rapid changes and problems

[23] Zacher, M. W. (1990). Toward a theory of international regimes. *Journal of International Affairs*, pp. 139-157.

[24] Keohane, R. O. (2003). *Global governance and democratic accountability* pp. 130-156.

[25] Viotti, P. R., & Kauppi, M. V. (2019). *International relations theory*. Rowman & Littlefield.

[26] Rosenau, J. N., Czempiel, E. O., & Smith, S. (Eds.). (1992). *Governance without government: order and change in world politics* (Vol. 20). Cambridge University Press.

[27] Finkelstein, L. S. (1995). What is global governance?. *Global Governance: A Review of Multilateralism and International Organizations*, *1*(3), pp.367-372.

by acting as if a supra-state organization.[28] The spread of global problems necessitates collective action and cooperation because problems become unsolvable at the national level.

One of the other main assumptions on which neoliberalism built is that states need cooperation to be sufficient and strong in new issues and unfamiliar fields. This happens by providing maximum benefit through international exchanges to parties and minimizing a possible negative cost for them. The option of being an autarky is not possible in the modern world in which we currently live. It becomes impossible to talk about the existence of an independent, self-sufficient state under modern conditions.[29]

A state, which is not developed sufficiently in the field of information technologies, cannot offer it to the consumption of its citizens. When a cybercrime occurred, it is not expectable of such a state to counter it either. In this case, for such a country finding criminals and prosecuting them is not possible. Lack of law is going to cause the spreading of these crimes from one country to another at the end of the day. Namely, due to the internet used by a huge amount of people and state organizations, there is a serious need to have an international agreement about cyber issues.

Describing the cooperation as only among states is going to be wrong. It cannot be expected from a state to fight against cybercrime in today's developing and changing world and meet the needs of modern society[30] without the support of other states or private sectors. What's more the form of cooperation and dispute can only be understood within the scope of institutions. Institutions do not constrain states or other participants as presumed or this does not mean that the interests of other states

[28] Rosenau, J. N., Czempiel, E. O., & Smith, S. (Eds.). (1992). *Governance without government: order and change in world politics* (Vol. 20). Cambridge University Press.

[29] Steans, J., Pettiford, L., Diez, T., & El-Anis, I. (2013). *An introduction to international relations theory: Perspectives and themes*. Routledge.

[30] Isnarti, R. (2016). A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. *Andalas Journal of International Studies (AJIS)*, *5*(2), pp. 158-160

are ignored. Institutional arrangements provide the parties with the following information through negotiation. In addition, it allows the other party to submit complaints or contributions and prevents the expected attitude towards the rigidity of international agreements.[31]

Successful cooperation does not depend on the existence of a hegemon. Rather, it depends on the long-term benefit that the parties involved in co-operation will receive from the joint work. According to neoliberal ideology, international relations are not fundamentally anarchic. States are seen as dominant actors. However, rational and mutually beneficial international organizations can be established through cooperation.[32]

The importance of cooperation and collaboration, which is often advocated by neoliberals, is accepted by the Council of Europe which drafted the Convention on Cybercrime. The organization aims to provide states reaching maximum benefit by supplying education, training, meetings and workshops to successfully fight against cybercrime and build common legislation on those issues. Namely, the main purpose of the Convention is to strengthen joint work with other states and organizations[33] proposed by neoliberal philosophy.

Contemporary world politics needs international governance, the zone of democratic peace, and complex interdependence. For the neoliberal political agenda, international institutions are important. Robert Keohane paid attention to international organizations and institutional learning. The idea of bringing

[31] Hughes, C. W., & Lai, Y. M. (Eds.). (2011). *Security studies: a reader*. Routledge. pp. 157-162

[32] Steans, J., Pettiford, L., Diez, T., & El-Anis, I. (2013). *An introduction to international relations theory: Perspectives and themes*. Routledge.

[33] Convention on Cybercrime, (2001), Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on January 15, 2020)

international organizations back and extending their role has emerged after the Cold War.[34]

For neoliberals, the winner can be two if they find a meeting point of mind. Here according to neoliberals by controlling the fear of losing, states can find a common point and sign an agreement to guarantee their benefits.[35] When considered from this perspective, the number of states which signed and ratified the Budapest Convention looks more meaningful. (Namely, the winner's number is 65)[36]

1.2. The Need of Combating Cybercrime in the International Arena

A company named Statista published a report in 2016 including predictions about the number of internet-connected devices in 2020. The estimated amount was 6.58 billion.[37] However, another published report about the number of internet-connected devices shows that in 2020 the number of internet-connected devices will be 202 billion. Another interesting point is that the report also shows that as of 2009 internet-connected devices exceeded the number of the world population.[38] Compared to the world population, the increase in internet-connected devices shows that the users of ICTs exceed expectations and it is growing rampantly. This situation proves that counties getting closer, borders are eliminating and cooperation is being an inevitable necessity.

---

[34] Jørgensen, K. E. (2017). *International relations theory: A new introduction*. Macmillan International Higher Education.pp.184-187

[35] Keohane, R. (2011). Neoliberal institutionalism. *Security studies: A reader*. pp. 157-164.

[36] Council of Europe, Chart of signatures and ratifications of Treaty 185, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Upslst88 (Accessed on January 15, 2020)

[37] Statista, Number of network connected devices per person around the world from 2003 to 2020, Retrieved from: https://www.statista.com/statistics/678739/forecast-on-connected-devices-per-person/, (Accessed on January 17, 2021)

[38] DaCosta, F., & Henderson, B. (2013). *Rethinking the Internet of Things: a scalable approach to connecting everything* Springer Nature. pp. 42.

As a starting point, it will be beneficial to understand the background of the Convention on Cybercrime. It was opened for signature on 23.11.2001 by member and non-member countries of the Council of Europe. It entered into force on 01.07.2004 by the signatures of 5 countries at least 3 of them should be members of the Council of Europe.[39] The Convention was signed by Turkey on 10.11. 2010 and it was ratified on 22.04.2014 with the negotiations of the Turkish Grand National Assembly. It entered into force with the promulgation in the Official Gazette with the name "Sanal Ortamda İşlenen Suçlar Sözleşmesi" (Convention on Cybercrime) and with the number 6533, on 02.05.2014.[40]

The Convention interested in the crimes committed through the internet or other computer networks particularly addresses topics that are committed in a computer environment and it focuses on combating crimes of computer fraud such as copyright, child abuse, and violation of computer network security. The objectives of the regulation of the Convention are to ensure a common policy to fight against cybercrimes, to establish a common legal system and to strengthen international cooperation.[41] As stated above, considering that internet-connected devices are much more than the world population, it is seen how reasonable this pursuit is.

Since the internet is a global network and people can access data or people on different continents, in different parts of the world via the Internet, there is a need for joint work and cooperation for the proper work of the criminal justice system. As a matter of fact, that if justice cannot be supplied in a country, this causes the purpose of the state to be questioned. It is unlikely that a state in which power and

[39] Council of Europe, Details of treaty no 185, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Accessed on October 13, 2020).

[40] Açar, K.V., Avrupa konseyi budapeşte sözleşmesi kapsamında saklama talebi ve Türkiye uygulamaları çalıştayı, Retrieved from: https://www.researchgate.net/publication/336578876_Avrupa_Konseyi_Budapeste_Sozlesmesi_Kapsaminda_Saklama_Talebi_ve_Turkiye_Uygulamalari_Calistay_Raporu (Accessed on October 14, 20220)

[41] COE, Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

sovereignty are questioned inside will have an effective presence in the international arena.

Keohane and Nye define the term cyberspace as a place that exists always and everywhere. Those scholars also indicated that rules would be necessary to manage cyberspace, protect internet users from criminals and protect intellectual property rights.[42]

There is also an invisible linkage between liberalism and information technology. It would not be correct to say that all democratic states are leading in the information revolution. However, what is true is that many democratic states are the leaders of the information revolution, and they play important roles. The reason why democratic states are leaders is that these states are more prone to exchanging information due to their free structures.[43]

There is no coincidence that authoritarian regimes cannot adapt to information technologies and integration with information technologies. For example, China controls service providers, monitors users' movements on online platforms. In this case, it cannot be expected to emerge from information technologies and giant multinational service providers like Facebook, Twitter etc. in China. It would be also surprise if the service providers used in China are among the most popular service providers worldwide. As a matter of fact, the Convention on Cybercrime, which aims to support the public and private sectors in combating crime at the global level and developing technologies, has not been signed and approved by China or Russia and this can't be explained only with coincidence. The countries like China and Russia maybe try to protect their own netizens and even they maybe try to preserve their own camp. But from the neoliberal perspective in this global era choosing self-sufficiency either this or that way will result in clear isolation.

---

[42] Keohane, R. O., & Nye Jr, J. S. (1998). Power and interdependence in the information age. *Foreign Aff.*, *77*, pp.81.

[43] Keohane, R. O., & Nye, J. S. (1987). Power and Interdependence revisited. *International organization*, *41*(4), pp.725-753.

In the following parts of this study, the emergence of the internet as information technology, the issue of complex interdependence about crimes conducted on the virtual environment, the effects and the role of multinational service provides to combat cybercrimes, the importance of harmonization of law in combating cybercrime and whether the Convention is the best existing solution to solve the current jurisdictional and democratic dilemma on cybercrimes will be discussed within the context of neoliberalism.

CHAPTER 2

THE BACKSTAGE OF THE INTERNET

Things that led to the emergence of the internet were the possibility of nuclear annihilation and the fear of communism. In reality, the internet is an unintended consequence of military competition between the United States and the Union of Soviet Socialist Republics. The United States Department of Defense launched Advanced Research Projects Agency Network **(**ARPANET) to create an alternative communication device. During the Cold War years, four computers are arranged to reach that aim and the first data was transmitted on September 2, 1969. The results of the works were expedited to the public in 1972.[44] By 1975, there were around 2.000 users but many of them were physicists, engineers or researchers at universities. While Pentagon's expectations were supplying both the secure network system and protect the state from any nuclear attack, universities' expectation was accessing free academic research sources.[45] In 1983 ARPANET was divided into two parts, the first one was Military Network (MILNET) which was used for the military and the second one was ARPANET and that one was used for non-military traffic. Because the development of the system continued, there was the need to standardize it. Therefore, National Science Foundation (NSFNET) founded 6 computer centers. This was the first time using the internet by researchers to share their ideas and their researches. However, in a short time, the number of addresses was so much that, in 1983 Paul Mockapetris created 7 Domain Name System (DNS) to compensate for the high number of addresses. Those were "com" (commercial), "edu" (educational), "gov" (government), "mil" (military), "net" (networking organizations), "org" non-commercial organizations), "int" (international organizations)[46] Additionally the

[44] Marson, S. M. (1997). A selective history of Internet technology and social work. *Computers in Human Services, 14*(2), pp.35-49

[45] Briggs, A., & Burke, P. (2009). *A social history of the media: From Gutenberg to the Internet*. Polity. pp.13-61

[46] Marson, S. M. (1997). A selective history of Internet technology and social work. *Computers in Human Services, 14*(2), pp.35-49

mark @ became routine to indicate transmission.[47] In June 1990, use of the ARPANET had been ended[48] and the internet nearly reached today's form that we currently use.

Just like the internet, cybercrimes are new too. In the literature, Robert Morris produced the first internet worm. He blocked the internet for a few hours. Although he defends himself about the event that was not intentionally conducted, he was punished for three years in prison. After this illegal action, the idea of legal control in the virtual environment gained strength. However, at the same time, the problems that emerged on the internet also contributed to its development. Technological improvements emerged especially in three areas. Those were communication, information acquisition and other things like FTP, etc. The most important was "www" within the title of information acquisition. In 1989, the first web page was published with the support of the European Laboratory for Particle Research sources combined with 18 European countries. The answer to why "www" gained popularity compared to other tools is that "www" was more user-friendly.[49]

The creator of "www" is an English engineer named Tim Berners Lee and he created it in 1989. He aimed to supply a free virtual environment that connects everything, to store all the information everywhere in which accessed by computers. About the internet, there were different approaches some of the opponents defined it as "pollute the human spirit" but the supporters believed that the internet is going to liberated and empowered individuals. Those were scientists, engineers or scholars who believed the more freedom makes the public the more powerful.[50]

---

[47] Briggs, A., & Burke, P. (2009). *A social history of the media: From Gutenberg to the Internet*. Polity. pp.61-67

[48]İstanbul Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı, (September 7, 2013)., Retrieved from: https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarih%C3%A7esi (Accessed on October 13, 2020).

[49] Marson, S. M. (1997). A selective history of Internet technology and social work. *Computers in Human Services*, *14*(2), pp.35-49

[50] Briggs, A., & Burke, P. (2009). *A social history of the media: From Gutenberg to the Internet*. Polity. pp.264

In reality, the internet is nothing more than the combination of several computer networks, telephone lines, and agreed protocols[51]. It brings together all the electronic media into one mechanic delivery system by using some basic codes[52] but with the proliferation of www, the internet has become reachable and affordable all around the world and this made it beyond the control of any country.

Additionally, when it comes to the history of the internet in Turkey the first publicly available internet works were conducted by ODTU (Middle East Technical University) and TUBITAK (Scientific and Technological Research Council of Turkey) and the first successfully planned connection was realized to the USA, to NFSNET on April 12, 1993. So the birthday of the internet is accepted as April 12th in Turkey.[53]

Although the internet came to Turkey, a couple of years later, spreading and using it draw attention. As of January 2020, the number of internet users in Turkey is 62.07 million. This number shows that 74 percent of Turkey's population uses the internet actively. As of January 2020, the number of social media users is 54 million. Namely, 64 percent of Turkey's population uses social media actively. The number of having a mobile internet connection is 77.39 million 92 percent of those people use mobile devices to reach social media.[54] (According to TUİK (Turkish Statistical Institute) the total population of Turkey on 31, December 2019 is 83.154.997[55])

---

[51] Schulzrinne, H., & Rosenberg, J. (1999). Internet telephony: Architecture and protocols–an IETF perspective. *Computer Networks*, *31*(3), pp.237-255.

[52] Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), pp.22-31.

[53] Mestçi A., (2007). Turkey's internet report in 2007, Retrieved from: http://inet-tr.org.tr/inetconf12/kitap/Bildiriler/30_24_inet07.pdf (Accessed on September 7, 2020).

[54] Simon Kemp (18 February 2020), Digital 200: Turkey, retrieved from: https://web.archive.org/web/20200612160417/https://datareportal.com/reports/digital-2020-turkey (Accessed on September 7, 2020).

[55] TUİK. . (04 February 2020). Adrese Dayalı Nüfus Kayıt Sistemi Sonuçları, 2019, Retrieved from: https://data.tuik.gov.tr/Bulten/Index?p=Adrese-Dayali-Nufus-Kayit-Sistemi-Sonuclari-2019-33705, (Accessed on November 11, 2020).

The World's average online spending time is 6 hours 43 minutes in a day. However, users in Turkey are online for 7 hours 29 minutes. This rate is more than the USA, India, or even China.[56] When the time-wasting in social media is researched, it is revealed that 2 hours 24 minutes for the World. However, Turkey's average rate is 2 hours 51 minutes.[57] This means internet users in Turkey spend more time on online platforms than the rest of the world.

2.1. Internet and Acceleration of Informational Globalization

Globalization is a process that affects and changes the international system and there are several definitions of what is globalization. Some define it as a process of resembling the peoples of the world with the emergence of global culture.[58] Others define it as a process of expressing and defining the differences between societies, communities, and identities.[59]

The root of globalization comes from the neoliberal idea. Namely, in a sense globalization is the product of neoliberalism and capitalism. Neoliberalism integrated people into markets and it gained strength with the contributions of capitalism such as race, innovation, restructuring and etc.[60]

According to Langhorne, there are three phases that shape and affect globalization. The first one was steam engines with the emergence of steam engines

---

[56] We are Social. (Jan 2020). Time per day spent using the internet. Retrieved From: https://wearesocial-net.s3.amazonaws.com/uk/wp-content/uploads/sites/2/2020/01/02-Internet-Daily-Time-%E2%80%93-DataReportal-Digital-2020-Global-Digital-Overview-Slide-43.png (Accessed on February 17, 2020)

[57] We are Social, (Jan 2020) Daily time spent using social media. Retrieved from: https://wearesocial-net.s3.amazonaws.com/uk/wp-content/uploads/sites/2/2020/01/10-Social-Media-Daily-Time-%E2%80%93-DataReportal-Digital-2020-Global-Digital-Overview-Slide-92.png (Accessed on February 17, 2020)

[58] Pieterse, J. N. (1996). Globalization and culture: Three paradigms. *Economic and political weekly*, p.1389-1393.

[59] Johnson, D. G. (2002). Globalization: what it is and who benefits. *Journal of Asian Economics*, *13*(4), pp.427-439.

[60] Castells, M. (1999). *Information technology, globalization and social development* (No. 114). Geneva: UNRISD. pp.4-7

transportation of people and goods accelerated, with railways things exceeded borders, especially via telegram communication homogenized communities. The second phase was the technology war it emerged during WW2 with the production of the German V2 rockets. With V2 rockets and satellite technology, states had more secure communication tools. The last phase was the invention of computers and that one is the creator of today's informational global system.[61]

According to Held, there are three dominant points of view about what is globalization. For him, the first one is skeptics and for them, globalization is not a new issue it is only a process that has already continued for centuries and places cultural, social, and economic issues. The second one is hyper-globalists, they do not reject the attributes of previous acts but they evaluate previous times as a pre-global era or internationalization. According to hyper-globalists, globalization is related to the down of the nation-state and erosion of power. Lastly, for transformationalists, globalization constitutes a major force and triggers social, political, and economic changes those are also the factors of reshaping modern society and world order, the nation-state is still there, but with some differences. The transformationalist idea is actually a mixed idea and has the touch of both skeptics and hyper-globalist ideas.[62]

According to Nye and Keohane, global interaction is inevitable. At the global level, substitution is divided into four parts. The first one is the substitution of information and this one includes communication, tradition, belief, and information while the second one is the substitution of war materials and properties. The third one has included the substation of money and other commercial things. Lastly, the fourth one is the substation of people. Especially the substation of information brings borderless inclusion. Again according to Nye and Keohane if there is no transnational interaction the relation of states remains highly simple as between states or between state and IGO (Figure 2.1 a). However, in the condition of

[61] Dreher, A., Gaston, N., & Martens, P. (2008). Measuring Globalisation. *Gauging its Consequences Springer, New York*.

[62] Dreher, A., Gaston, N., & Martens, P. (2008). Measuring Globalisation. *Gauging its Consequences Springer, New York*. P.16-17

transnational interaction, the relation between states becomes complex and interactive (Figure 2.1 b).[63]

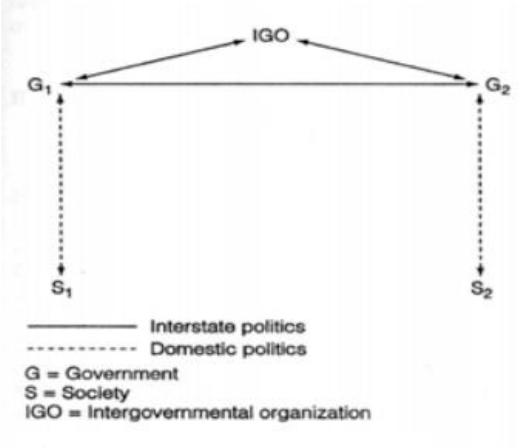

Figure 2. 1. Basic relation

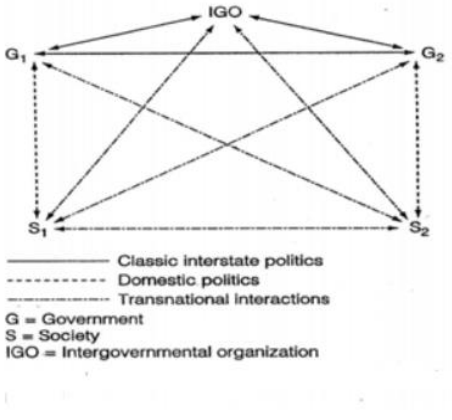

Figure 2. 2. Transnational interaction

According to Barber, several things, which are invading our daily life like business, trade, banking, etc, depend on communication technologies.[64] Today even science depends on it. For example, a shared tweet by Samuel Hunnington as "clash of cultures will lead to all future problems"[65] answered by Benjamin Barber "unfortunately, different cultures will always create controversy between two worlds"[66] and after his tweet, Hans Kung joined the discussion and shared his idea about this dispute "It doesn't matter who you are or where you come from. People can work together we are all humans".[67] Overall, this dispute was realized on Twitter

[63] Nye, J. S., & Keohane, R. O. (1971). Transnational relations and world politics: An introduction. *International organization*, *25*(3), p.24-26

[64] The Atlantic. Barber R. B. Retrieved From: https://www.theatlantic.com/magazine/archive/1992/03/jihad-vs-mcworld/303882/ (Accessed on November 5, 2020)

[65] Twitter, @samuelhunningt1, (February 18, 2020) Retrieved from: https://mobile.twitter.com/samuelhunningt1/status/1229670935273377793 (Accessed on November 5, 2020).

[66] Twitter, @benjami2533977, (February 18, 2020 responded to @samuelhunningt1) Retrieved from: https://mobile.twitter.com/benjami25333977/status/1229671592181063681 (Accessed on November 5, 2020)

[67] Twitter, @SchimelfenigX, (February 18, 2020 responded to @samuelhunningt1 and @benjami2533977) https://mobile.twitter.com/SchimelfenigX/status/1229672055227940864 (Accessed on November 5, 2020)

and it shows the reality that a combination of the internet and social media reached such a degree that it is important even spreading of ideas.

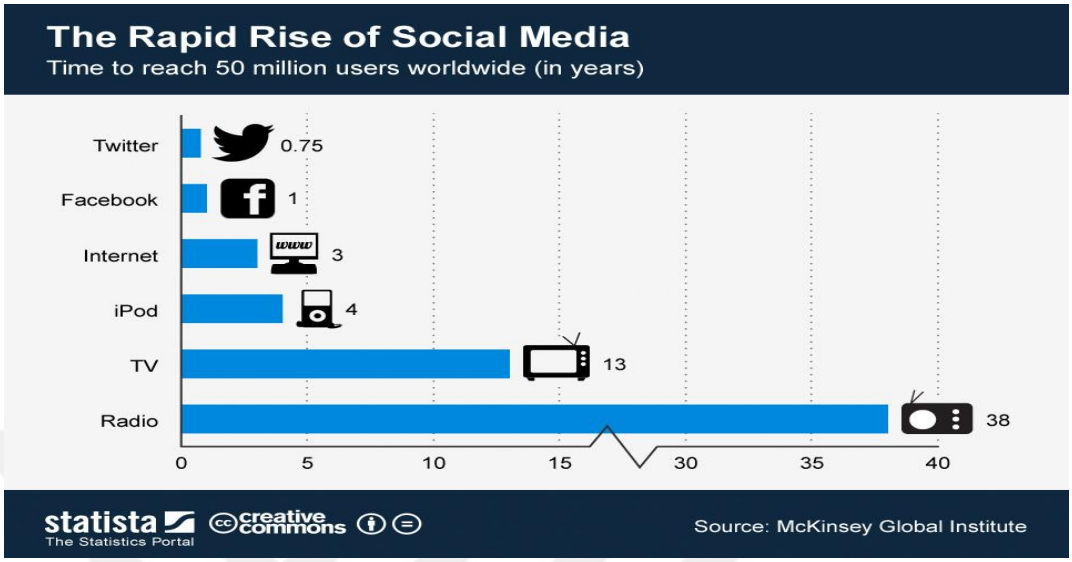

Figure 2. 3. The rapid rise of social media

The figure shows that the popular communication tools reached 50 million users in how many years. For radio, reaching 50 million users took 38 years, for TV the duration was 13 years. Respectively for iPod, the process was 4 years, for www 3 years and for Facebook 1 year. When it comes to Twitter the spending time to reach 50 million users took only 0,75 years.[68] This figure shows us that as mentioned ICTs are increasingly becoming one of the parts of our lives faster than all the previous tools.

2.2. The Emergence of Social Media

"Communication networks are the patterns of contact that are created by the flow of messages among communicators through time and space"[69] After www emerged in 1991, within the context of Web 1, hypertext which was produced by

[68] Statista, Richter. F., (August 2, 2012), The rapid rise of social media, https://www.statista.com/chart/521/the-rapid-rise-of-social-media/ (Accessed on September 01, 2020).

[69] Monge, Peter and Contractor, Noshir (2003) Theories of Communication Networks. Oxford: Oxford University Press.

Tim Barners provided to internet users a new type of communication channel. The open Diary which was created by Bruce and Susan Abelson brought together the online dairy writers. This also may be the first social media in history. In 1979, the Usenet was created by Tom Truscott and Jim Ellis via this site, users could send their posts. Being commercial websites such as Amazon and e-bay emerged in 1995. Over time, in 1999 Blogger, in 2001 Wikipedia[70] in 2003 MySpace also emerged.[71] When it comes to Facebook, it was established by Mark Zuckerberg in 2003[72] it became popular rapidly and became reachable all around the world on September 26, 2006,[73] in 2004 Flickr, in 2005 YouTube, in 2006 Twitter become popular and powerful actors on the internet.[74]

When an answer is sought for about why communication networks became so popular and how they could reach such a broad mass, especially 3 specialties of them draw attention. The first is flexibility, namely the ability to reshape and protecting the content in a different environment. Secondly, scalability is the ability to store and shrinking data with tiny damage. Last is the survivability, namely the specialty of keeping any data in a different environment or condition.[75]

Internet and multinational providers are simple. However, their impacts on communities are multidimensional. Crime, unrest, and corruption can affect a huge amount of people not only in a country but also in the world. Technology and communication are not and will not be the solution to the world's problem. However,

---

[70] Van Dijck, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford University Press.

[71] Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, *53*(1), pp.59-68.

[72] The Harvard Crimson. Kaplan A. Katherine, (November 19, 2003) https://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/ (Accessed on September 1, 2020).

[73] Wikipedia, Retrieved from: https://en.wikipedia.org/wiki/Facebook (Accessed on September 1, 2020).

[74] Van Dijck, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford University Press.

[75] Castells, M. (2013). *Communication power*. OUP Oxford. pp. 238-239

for economic and social development information and communication technologies are the sine qua non since they bring changes to countries for modernizing their product and their policy.

According to Kaplan and Haenlein, social media includes two factors, Web 2.0 and User Generated Content. (Hereinafter referred to as UGC.) Moreover, the definition of social media is as follows: it is a combination of applications based on web 2.0 and gives change to all the users produce their own UGC. There are three requirements for being a UGC. First, a published content should be accessible to people. Secondly, it should be a product of the creator's endeavor and unique to it and lastly, it should not produce by professionals.[76]

2.3. The Reconstruction of Power and Reconstructed Role of the State: From Military Power to Information Power

According to Castell via social media, power is gathering on a few global media companies' servers; this supplies more power to the companies but also causes resistance of others who remained under the shadow of that power.[77]

Power is related to having the ability to affect others for a subject's own benefit and controlling others in the direction of its own interests. Even if for MSPs this can't observe concretely when it comes to social actors the control on others can be easily observed. Power is not located in one particular social sphere or institution, but it is distributed throughout the entire realm of human action.

When it comes to the relation between globalization and the state, globalization does not eliminate the states it is only a new arena where the state and

[76] Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, *53*(1), pp.59-68.

[77] Castells, M. (2013). *Communication power*. OUP Oxford. pp. 240-243

counter power factors should work together.[78] However, global integration has reached such a level that it has led to the limitation of states. It limits the states, causes the state institutions to be reshaped and the institutions that are responsible for making decisions become dependent on other power actors.[79] Therefore, with global integration fed by the internet and social media, in the cyber realm, several things attributed to states like power, domination, authority lost their meanings to some extent.

However, the most important side of cyber power is that any power or any hegemony cannot control it. It cannot be controlled since the numbers of the actors are nearly equal to the number of internet users. In addition, because Google is a product of Silicon Valley it has to obey the law of the USA (CA region) as clearly indicated by the company on its website.[80] Fully controlling service providers is not possible for other states because the law in question might have some differences from a country to another.

In the past, the most popular propaganda devices for states were radio and television. By using these tools, states could reach massive audiences without any opponent's idea. For example, Nazis were strongly believed in media power and if Nazis led by Hitler had not used the power of radio they would have not won the election.[81] However, in time, professional media organizations have emerged and people could reach different ideas via them. Also with the emergence of human rights organizations or different kinds of media devices, both states and their citizens could learn something different from the things served to them by the authority.

[78] Ibid, pp. 243-246

[79] Weiss, L. (2005). The state-augmenting effects of globalization. *New Political Economy*, *10*(3), pp.345

[80] Google, Policies, Retrieved from: https://policies.google.com/terms/information-requests (Accessed on July 17, 2021)

[81] Adena, M., Enikolopov, R., Petrova, M., Santarosa, V., & Zhuravskaya, E. (2015). Radio and the Rise of the Nazis in Prewar Germany. *The Quarterly Journal of Economics*, *130*(4), pp.1885-1939

While the information revolution continues, the flowing of messages, images, and ideas accelerated and this triggered the advancement of information technology.[82]

To give examples of MSPs' effects on states and their policy I want to use Twitter and Facebook revolutions. When the communist party won the election in Moldova, in 2009 this caused a riot there. The spread of content in a fast way through Facebook and Twitter, supplied a perfect opportunity for the organization of the young population. After a while, young people reached Parliament. The government called the event a coup d'état and accused Romania of that.[83]

Unlike Moldova, the Iranian revolution in 2009 was well organized. Andrew Sullivan stated that the Iranian revolution would happen with Twitter. For the revolution, Twitter was a necessary tool. In 2009 when Ahmadinejad won the election, a dispute emerged between Mousavi's supporters and the state's institutions. During the dispute, the state used Facebook and Twitter for gathering information about the opposite side and used OSINT to detect them and to prevent their cooperation. In the end, the internet-social media users who support Mousavi are detected and arrested again via the internet.[84] In 2011, another social media revolution happened in Egypt. The uprising against Hosni Mubarek and his suppressing, authoritarian system with the name 18 Days Revolution resulted in the down of Mubarak. The contents shared by a user (@OcuupiedCairo "URGENT CALL Wounded desperately need medical supplies in Bab El Loq and transport to hospital DM me for details.") shows that in Egypt people used Twitter not only to

[82] Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations:(IR) relevant theory?. *International political science review*, *27*(3), pp.224

[83] The Guardian, (April, 8, 2009) Moldova forces regain control of parliament after 'Twitter revolution' Retrieved from: https://www.theguardian.com/world/2009/apr/08/moldova-protest-election-chisinau (Accessed on September 9, 2020).

[84] Morozov, E. (2009). Iran: Downside to the" Twitter revolution". *Dissent*, *56*(4), pp.10-14.

become social but also stay alive during the war they even declared against the state.[85]

In addition to all these, the information revolution also affected security understanding. Once, while having destructive guns and weapons are mostly enough for states, in today's world states try to reach more information as a modern gun. This situation caused disputes on security. Finding a universal definition about what is security is not easy but the definitions share some common points like refrain from threats and freedom to main rights such as the right to life, freedom of thought. The main reason for the disagreement about "what is security" comes from the manifoldness of point of view but definitions mostly focus on the individual, national, international, and global security. In addition, the understanding of security is mostly affected by the state's political conditions. For example, during the Cold War era the definition of security, focused on military issues and during the 1929 World Economic Crises, definitions normally focused on monetary issues.

When it comes to cybersecurity, in the literature, cybersecurity means a secure digital-virtual environment for those who using computer networks like the internet and other kinds of digital devices.[86]

As claimed, the internet and multinational service providers have important effects on security issues from state security to personal security. A published report clearly shows that the CIA collects data from the internet via computer networks. The easiest way of collecting intelligence from the internet is Open Source Intelligence shortly OSINT. It has been conducted as of the 1930s at Princeton University. In 1941, during World War II, Foreign Broadcast Intelligence Service began to use radio waves as intelligence. These means, whose pioneers work on collecting data about people and states by observing their actions. Reaching a person's information means in a roundabout way someone collecting info from

[85] Eltantawy, N., & Wiest, J. B. (2011). The Arab spring| Social media in the Egyptian revolution: reconsidering resource mobilization theory. *International journal of communication*, *5*, pp. 18.

[86] Baylis, J. (2020). *The globalization of world politics: An introduction to international relations*. Oxford university press, USA. pp. 240-245

networks about states and persons. From the United States of America to Japan someone is watching the action of a person or a state with their mouse clicks.[87]

For example, according to news published by The Guardian, the US military service was hacked by Chinese hackers, the leader of the hacking group was Su Bin and two unknown people assisted him. The leader of the hack organization, Su Bin, admitted that between the years 2008 and 2014 US military information was exported to the communist nation. The stolen data were related to the military such as aircraft and weapon systems. According to court papers, the men targeted fighter jets such as the F-22 and the F-35 as well as Boeing's C-17 military cargo aircraft program.[88]

Therefore, this example and many other examples that could have been given like this, show that the dimension of security changed with time. States should be updated regarding the era. Classic security ideas are not enough in today's modern and global world both because of the flows between states such as information, goods or even humans both because of the new type of struggle called information intelligence.

2.4. The Democratic Dilemma: From Democracy to Autocracy

When Mark Zuckerberg created “the Facebook” in February 2004, he has defined it as “an online directory that connects people through social networks at colleges”. When he was chosen as the person of the year in 2010 Facebook had 550

[87] Mercado,S.C. (2007). Sailing the sea of OSINT in the information age, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html#top. (Accessed on July 17, 2020)

[88] The Guardian, (2014). https://www.theguardian.com/technology/2014/jul/12/chinese-man-charged-with-hacking-into-us-fighter-jet-plans. (Accessed on July 27, 2020).

million users.[89] However, today the number of users of Facebook is around 2.7 billion and as a network Facebook is the largest in the world.[90]

Although social media is a new way of communication, it has devastating potential to reach the masses. Additionally, like so many things it has two different faces. When an idea can reach more users compared to others it is accepted as the true one and can suppress the other ideas even if they are wrong. This can cause to spreading of extremist, one-sided ideas and can damage or threaten democratic states.[91]

Contents produced in social media are different from classical media understanding and approach. That is not under the hegemony of a specific or single ideology. With this communication tool, people can reach like-minded people and organize meetings or protests. While this free platform enables the organized parties to reach a wider audience, it also reduces the influence of the other party. In other words, the rising sound on one side suppresses or even destroys the other side's voice. This is exactly what poses a problem for democracies. The living complex structure of social media can also cause a pro-democratic rise in democratic societies and an authoritarian rise in nondemocratic societies.

In addition to all of these, the fact that social media is a very open platform, nondemocratic countries effectively use censorship, online harassment, parsing and DDOS attacks to strengthen their own policies. This situation affects the world democracies, causes international problems, and leads to an information war. With these service providers, users can choose their own news networks far from any

[89] Lev Grossman, "Person of the Year 2010: Mark Zuckerberg," *Time*, 15 December 2010, http://content.time.com/time/specials/packages/article/0,28804,2036683_2037183_2037185,00.html (Accessed on October 7, 2020).

[90] Clement j.," Number of monthly active Facebook users worldwide as of 2nd quarter 2020", *Statista*, August 10, 2020., https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide, (Accessed on October 07, 2020).

[91] Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. *Journal of democracy*, *28*(4), pp.46-59.

propaganda, censorship or parsing. Today, just because of that service providers are also used by many users as a daily news tool.[92]

For example, social media users use online service providers to take the news at the rate of 58% in Turkey, 71% in Greece, 53% in Canada, 50% in Italy, 48% in the United States and 25% in Germany. The numbers are important because they show both the trust of the traditional news agencies and the vulnerability of the people. Numbers show vulnerability because the news published on the internet cannot serve the truth every time, cannot be objective or some creators may share fake news to create unrest.[93]

The most striking thing here is that social media, in which freedom of thought and expression is used without restrictions, is one of the most interfered elements by authoritarian and repressive regimes. The concern about internet censorship around the world stems from the enforcement of censorship by authoritarian systems to ensure the permanence of their regimes.

The effort to control the internet environment by dictatorial regimes is not just about closing accounts or blocking access to contents. Flooding is used in social media in order to spread information or an ideology or on the contrary, to prevent the spreading of information or an ideology. Flooding is benefitted from the free nature of the internet. Authoritarian regimes have a group of people to support so that they support and defend their ideologies and regimes via propaganda. Contents are published intentionally on strategic timing, bot accounts are used to spread the government's ideology. Overall, authoritarian regimes have their own online armies[94]

---

[92] Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. *Journal of democracy*, *28*(4),pp. 46-59.

[93] Watson Amy, Jun 23 2020, Share of adults who use social media as a source of news in selected countries worldwide as of February 2020, Statista, https://www.statista.com/statistics/718019/social-media-news-source/, (Accessed on October 8, 2020).

[94] Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. *Journal of democracy*, *28*(4), pp.46-59.

but for users, escaping from flooding is not difficult compared with the other media tools.

2.5. The Rise of Networks and the 4. World Created by Internet

The concept of the 3rd World and 3rd World countries are frequently used, it expresses that the countries lag behind the age in many areas.

The 4th World, on the other hand, refers to lost mass and that does not have a location, time or region. This mass, which is lost, ignored and postponed, is partially the product of globalization and information and communication technologies. Staying on the networks means increasing their chances, being separated from networks means being completely isolated.

This 4th World people and lands are lost their place in informational capitalism and became the "other". This group, which is called “the other”, is uneducated, or inadequate in networks, it is the group that loses the equality of opportunity, physically or mentally ill, too poor to meet their physical needs, unable to cope with life, dependent, living by selling their bodies, innocent criminals who are harmed by the inability of the criminal justice system or those who are stuck in the hierarchy. While the valuable segment, that is, the segment in the upper segment in inequality of opportunity, can integrate into global information and communication technologies, the worthless “other” group is pushed aside. The social exclusion increases with the increase of global capitalization. Due to cybercrimes do not happen in a local area, exceed borders, damage to several countries, organizations and even people in the world the need for cooperation advocated especially by neoliberal idea became populist knowledge.[95]

Briefly, the members of the 4th World have experienced losses in their life or they are obliged to lose something because of another person's mistakes. These losses can be caused by problems that may be encountered in daily life and can also

[95] Castells, M. (1999). *Information technology, globalization and social development* (No. 114). Geneva: UNRISD. pp.10

be caused by the cyber world, which has become a part of our daily life today. Therefore, preventing and punishing the crimes that occurred on online platforms is going to prevent also the rising number of citizens of the 4th World. On the other hand, this struggle imposes various responsibilities to both judicial the law enforcement agencies in a country and makes it necessary to work in harmony with other agencies all around the world.

As clarified above globalization is the new formation of traditional capitalism in the modern world. In time, the rise of the global flow of information and money with technology brings the need for some supranational organizations that are working in cooperation.[96] Due to cybercrimes do not happen in a local area, exceed borders, damage several countries, organizations and even people in the world the need for cooperation advocated especially by neoliberal ideas became popular.

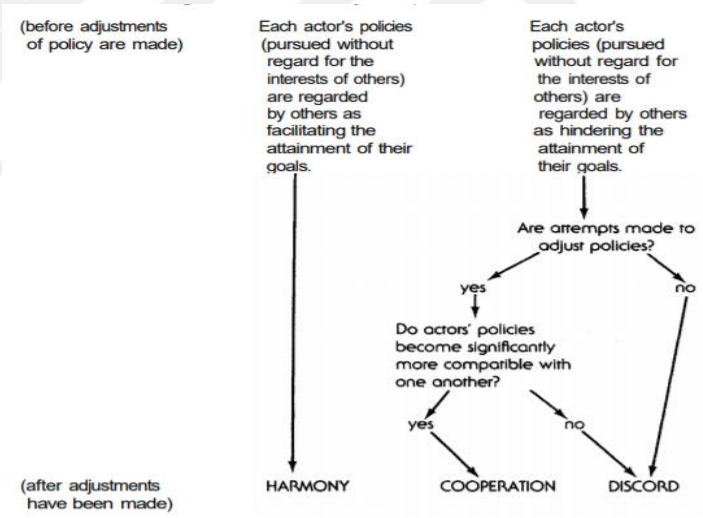

Figure 2. 4. The process of cooperation

The above mentioned figure shows how harmony, cooperation and discord emerged. According to Keohane harmony is different from cooperation. Unlike cooperation, harmony indicates a situation that states are interested in only their benefit and self-efficient to solve disputes. If one actor's policy facilitates the others,

[96] Ibid, pp. 7

where there is harmony and there is no need for adjustment. If there is harmony there is no need to cooperate. However, the definition of cooperation focuses on negotiation, actions of separate individuals or organizations, coordinated decisions, includes decisions that are planned before. When it comes to discord, it compels the actors changing of policies. In cooperation, like harmony, each actor pursues their self-interest but makes negotiations with others to benefit all parties to deal. Unlike cooperation, harmony has an apolitical structure and goes without communication. Cooperation takes place only in the situation of conflict and by mutually beneficial cooperation states and organizations try to find a shared point. The aim of international negotiation is to reduce possible costs on states.[97]

Starting from the Neoliberal cooperation idea, in the next part of this thesis, the international search for cooperation to fight against cybercrime, their contributions to the international arena and their failures or differences about building a common structure will be discussed.

[97] Keohane, R. O. (2005). *After hegemony: Cooperation and discord in the world political economy*. Princeton university press. P. 49-52

CHAPTER 3

CYBERCRIME, CYBERSECURITY AND COOPERATION INITIATIVES ON THE INTERNATIONAL LEVEL

3.1. Cybercrime and Cybersecurity

Threats of cybercrime occurred with the invention of the internet. Xingan Li divides the history of cybercrime into four stages those are respectively "germination" (1940-1960), "rapid development" (1970-1990), "broad expansion" (the 1990s), and "routinization" (2020s).[98] In the first stage, the first prosecuted financial cybercrime in history emerged and it was regarding alteration of bank accounts and the prosecution process of it took eight years. (From 1958 to 1966) After the process, it was revealed that an employee used a company's computer to embezzle money from long terms accounts.[99] This time range shows us that without a comprehensive legal structure, the criminal justice system cannot work or even if it works, the process takes a remarkable time of JAs.

Malicious software like Trojan horses, viruses, worms and logic bombs came into the agenda in the 1980s during the second phase. In the third stage, the number of personal computer users raised when the spreading of www added the process the number of crimes raised enormously and in that phase crimes begin to be a serious international problem. At the last stage comparing to the previous sections, a critical decrease was observed in the prosecuting process. The effective factors for this decrease were the Convention on Cybercrime and raising awareness after the 9/11 attacks.[100]

---

[98] Li, J. X. (2017). Cybercrime and legal countermeasures: A historical analysis. *International Journal of Criminal Justice Sciences*, *12*(2), pp.196-207.

[99] Parker, D. B., Abt Associates, & SRI International. (1989). *Computer crime: Criminal justice resource manual*. US Department of Justice, National Institute of Justice, Office of Justice Programs.pp.2

[100] Li, J. X. (2017). Cybercrime and legal countermeasures: A historical analysis. *International Journal of Criminal Justice Sciences*, *12*(2), pp.196-207.

In the literature, cybercrime is generally defined as using internet, internet-connected devices in order to enact criminal behavior.[101] Mostly, the basic definition of cybercrime indicates any violation of law by using internet-connected devices. Online crimes are generally called cybercrime because suspects use peculiar advantages of cyberspace. These types of crimes generally include both computers and the internet and those are also direct results of technology and would not exist without it.[102]

The UN divides cybercrime into three categories respectively as cyber-dependent crime, cyber-enabled crime and online child exploitation. The first one namely the cyber-dependent one includes ICT infrastructure and the typical examples are generally malware, ransomware, DDOS attacks. The second can happen offline and can be run by ICT. Examples of these kinds of crimes can be theft, fraud, online money laundering (those generally happen via cryptocurrencies) and the last one is abusing an underage person can be called sextortion, grooming, sexual extortion, cyber sexual bullying and sexual harassment also.[103] Compared to the UN, the European Union's cybercrime definition includes much more factors. Like the UN, the EU divides cybercrime into three categories as crimes specific to the internet, online fraud and forgery, and illegal online content.[104] Especially by using the third one agency can broaden their investigation capacities.

Gordon and Ford divide cybercrimes into two categories as Type 1 and Type 2. The first one includes mostly technology like viruses, worms and keystroke logging facilitated by crimeware programs. Secondly, Type 2, most general examples

[101] Koziarski, J., & Lee, J. R. (2020). Connecting evidence-based policing and cybercrime. *Policing: An International Journal*.pp.199

[102] Furnell, S. (2002). *Cybercrime: Vandalizing the information society* London: Addison-Wesley.

[103] UN, Cybercrime, Retrieved from: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html (Accessed on February 18, 2021.)

[104] EU, Cybercrime, Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en (Accessed on February 18, 2021)

of these crimes are cyberstalking, extortion, complex corporate espionage, planning or carrying out terrorist activities online, romance scam, digital voyeurism etc.[105]

We can use two crimes examples from Israel to make Type 1 and Type 2 more clear. The first one is business email compromise (Hereinafter referred to as BEC.). During April and May 2019, three different European countries launched an investigation about BEC crime and the pieces of evidence showed that the sources of the IP addresses are from Israel. Moreover, investigations revealed that there were several persons who aiding and abetting the crime. The problem was solved with the advantages of 24/7 point of contact by cooperation.[106] This example was one of the best examples of Type 1 crime because suspects need high technical ability to exploit systems.

The second type of cybercrime was regarding the threat. In September 2019, suspects shared several contents on different web pages including threats against Israel's Prime Minister. Investigations revealed that the source of IP comes from the USA and belongs to a person who is originally from Israel and illegally residing in the USA. The suspect was detected again by using the advantage of 24/7 point of contact and was deported from the USA and was arrested in the airport by Israeli police. [107]

Those examples can be raised definitely but shortly if a criminal used the advantages of computer technology and absolutely internet and if he violated law here, we can claim that it is a cybercrime.

---

[105] Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), pp.13-20.

[106] Council of Europe, (July 13, 2020), The Budapest Convention on Cybercrime: benefits and impact in practice https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed on March 7, 2021) pp.106

[107] Council of Europe, (July 13, 2020), The Budapest Convention on Cybercrime: benefits and impact in practice https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed on March 7, 2021) pp. 20-21

Cybersecurity covers the security of hardware, software and network security and the term has several usages like "Computer Security", "IT Security" or "Information Security". Compared to the others, cybersecurity became more popular after President Barack Obama used it.[108] During his press release, he informed the audience about the benefits and threats of the internet by using his victimization as an example regarding illegally accessing the data processing system, preventing the functioning of a system and deletion, alteration or corrupting of data along with interference to election etc.[109]

In literature, there is no consensus about what exactly cybersecurity is or not.[110] Some researchers like Kemmerer[111] and Lewis[112] focus mostly on defensive methods. However, Cybersecurity contains much more from the defense. It cannot only contain defensive or protective methods claimed by Kissel[113] and in order to supply cybersecurity states need much more. For example, unlike the experts mentioned, the Information and Telecommunication Union (Hereinafter referred to as ITU.) which is a specialized agency of the United Nations indicates much more needs to supply cybersecurity.

According to ITU "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the

---

[108] Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cybersecurity. *Journal of Digital Forensics, Security and Law*, *12*(2), pp. 53-74.

[109] YouTube, The Obama White House, (May, 29, 2009). President Obama on Cybersecurity, Retrieved from: https://www.youtube.com/watch?v=wjfzyj4eyQM&ab_channel=TheObamaWhiteHouse (Accessed on March 10, 2021).

[110] Baylon, C. (2014). Challenges at the intersection of cybersecurity and space security. *International Security*. pp. 10-15

[111] Kemmerer, R. A. (2003). *Cybersecurity. 25th International Conference on Software Engineering, 2003. Proceedings.* pp.3

[112] Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. *Center for Strategic and International Studies*. pp.1

[113] Kissel, R. (Ed.). (2011). *Glossary of key information security terms*. Diane Publishing. pp. 57

cyber environment and organization and user's assets. The general security objectives comprise; Availability, Integrity and Confidentiality".[114]

According to the ENISA (The European Union Agency for Cybersecurity), information and network security are the subsets of cybersecurity. Again, according to ENISA cybersecurity should cover the following: "Availability, reliability, safety, confidentiality, integrity, maintainability, robustness, survivability, resilience, accountability, authenticity and non-repudiation.[115] Although there is no consensus about what is cybersecurity when the definitions of experts and professional organizations are investigated it is obvious that all of them especially indicates a secure virtual environment.

Although there are several definitions about what is cybercrime or what is cybersecurity, focusing on the Council of Europe's definition is going to be more proper because of the main argument of this thesis. In the reports published on the organization's web page the term cybercrime is divided into two parts as narrow definition and broad definition. In the narrow sense, it includes any offense targeting computer data or computer systems but in the broad sense, it indicates any crimes involving computer systems[116] and the definition accepted by the United Nations on 10-17 April 2000 defines the term as the Council of Europe did.[117]

---

[114] ITU, (April 18, 2008) Retrieved from: https://www.itu.int/rec/T-REC-X.1205-200804-I (Accessed on February 18, 2021).

[115] ENISA, (September 2017). ENISA overview of cybersecurity and related terminology, Retrieved from: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology. (Accessed on February 18, 2021).

[116]Seger. A. (2012) "Cybercrime Strategies". Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e1 (Accessed on November 1, 2020).

[117] UN. (April 10-17, 2000). "Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders" Retrieved from: https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf (Accessed on November 1, 2020)

In this context all the crimes related to data interference, system interference, illegally obtaining and giving data, preventing the functioning of a system and deletion, alteration or corrupting of data, misuse of devices and the crimes such as child exploitation, sexual harassment, threatening, blackmailing, xenophobia, racism, extremism, drug trafficking, money laundering, terrorism etc. accepted as cybercrimes when any suspects used computer-related technology to violate terms, rules or laws. In short, the dimension of cybercrime is directly related to, what suspects could do with their computers.

Because these kinds of crimes increased all around the world the cybersecurity issue came along with them and the definition made by the Council of Europe on cybersecurity indicates national and technological issues. It indicates national security because the offenders may target critical infrastructures of any state also indicates technological security because to guarantee permanence, integrity and confidentiality on virtual networks.[118]

However, what does cybersecurity mean and what does not mean in the international arena? Cybersecurity in the international arena does not only mean using antivirus programs, two-factor authentication, strong passwords or things like that. Unlike them in the international arena, cybersecurity means supplying cooperation among participants. When it comes to participants, it covers all the entities that join the process such as public-private sectors, NGOs, universities, IGOs etc.

All the participants' aims are to strengthen cybersecurity but this goal includes several necessities such as globally harmonized legislation, enhanced operational capacity, judicial training of LEA, interagency cooperation between

[118]Seger. A. (2012) "Cybercrime Strategies". Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e1 (Accessed on November 1, 2020).

LEA-JA and ICTs-LEA, cooperative work between LEAs and private sectors and finally international cooperation among states JAs.[119]

Attributing the issues (fighting against cybercrime or supplying cybersecurity) to only one agency or one organization cannot produce proper solutions to solve the problems. Besides that, any agency without collaboration cannot be enough to protect netizens. Namely, cybercrime is not the sole responsibility of a specific organization. So to prevent a possible crime before it, to find criminals in the virtual world after it happened, to compensate emerged damages, and to punishing criminals after it detected there is the need for close cooperation between parties and very importantly having common legislation will make things easier than ever before.

The reality of the need for cooperation realized before by several international organizations and now the efficiency of the organizations will be discussed in this chapter.

3.2. Cooperation against Cybercrime

Providing cooperation is easy to some extent on the international level because of the lack of authority on the international level.[120] According to Axelrod and Keohane, cooperation among parties is based on three issues. The first one is the mutuality of interest namely if the parties have a mutual benefit or if by cooperating they can diminish the possible damage, the possibility of cooperation rises too. When a dual benefit is supplied, states can cooperate except for armament because there can be only one winner in this situation cooperation on military issues often have payoff structures. The second one is the shadow of the future. Concerns about the

[119]Seger, A. (2012) "Cybercrime Strategies". Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e1 (Accessed on November 1, 2020)

[120] Jervis, R. (1978). Cooperation under the security dilemma. *World Politics: A Quarterly Journal of International Relations*, pp.167-214.

future help to promote cooperation. Some specific factors help to make the shadow of the future an effective promoter of cooperation. Those are; long time horizon, the regularity of stakes, reliability of information about the others' actions, quick feedback about changes in the other's actions.[121] When it comes to the numbers of the actors, the plurality of actors makes it difficult to satisfy and makes also cooperation more difficult.[122] Interestingly when the topic is taking action against criminals having huge amounts of shareholders will be in favor of both the public and private sectors. After all, any state or private sector does not desire to support criminals or any of them does not turn a blind eye to the violation of rules and laws if they have no profit from this situation and from the proceeds of crime.

Cooperation does occur with the civilization and modern communities are based upon it. When the issue is cooperation among the sides the first thing that comes to mind is the prisoner's dilemma, to raise benefit or to diminish the cost. If the game is played by two egoists, the result will be defection but what happens if they interact with each other? With interaction among parties, cooperation can emerge. People are more prone to think of the game as if there can be only one winner at the end of the game. However, real life is different from then and there can be several winners and cooperation can bring benefits to the sides[123] just stressed by the COE on Convention on Cybercrime.

Neoliberals also believe that interdependence in the economic dimension affects the reaction of the nation-state for the better. Interdependence rises with modernization and in the modern world; states are more prone to cooperation because the modern world raises the cost of mistakes and failures.[124]

---

[121] Axelrod, R., & Keohane, R. O. (1985). Achieving cooperation under anarchy: Strategies and institutions. *World politics*, *38*(1), pp.226-254.

[122] Axelrod, R., & Dion, D. (1988). The further evolution of cooperation. *Science*, *242*(4884), pp.1385-1390.

[123] Axelrod, R., & Hamilton, W. D. (1981). The evolution of cooperation. *science*, *211*(4489), pp.1390-1396.

[124] Drezner, D. W., & Drezner, D. W. (1999). *The sanctions paradox: Economic statecraft and international relations* (No. 65). Cambridge University Press. pp 7-9

Here the economic interdependence should not accept as only import or export. According to the report prepared by the Center for Strategies and International Studies with the partnership of McAfee, cybercrimes have serious economic impacts on the global economy. The damage of cybercrime is close to 600 billion dollars. This constitutes nearly one percent of global GDP (0,8%).[125] As indicated by Erdal ÇETİNKAYA, the head of the Turkish National Police Counter Cybercrime Department (TNP-DCC) on the 6th International Workshop on Cybercrime if the damage caused by cybercrime has constituted a country's GDP, that country would have had the 13th largest GDP in the world. According to ÇETİNKAYA, only the cost of the crimes conducted on ICTs is 3.25 billion dollars on the global level.[126]

When cybercrimes adjust to game theory as mentioned above the only solution can be cooperation. Otherwise, the results can be more devastating for the states and ICTs. If ICTs refrain from cooperation with the public sector the rising crimes turn them into the devil, in another possibility if the public sector refrains from cooperation the failure of the criminal justice system cause the questioning of the sovereignty of the states. As a result, all the subjects are bound to each other. As cybercrimes increases, concerns of the states rise because the first responsibility of a state is creating a secure environment for the people but crimes threaten the expectation. In addition, the cost of cyberattacks is several times cheaper than defending a system. Deletion, alteration or seizing of a system can take only a few seconds but fixing and compensating for the damage can cause millions of dollars.

[125] McAfee, Lewis j. (February 18). Economic impact of cybercrime no slowing down, Retrieved from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf (Accessed on November 1, 2020)

[126] Sabah, (January 31, 2020) We are online around 7,5 hours in a day, Retrieved from: https://www.sabah.com.tr/teknokulis/haberler/2020/01/31/gunde-75-saat-internetteyiz (Accessed on November 1, 2020).

3.3. Within the Scope of Convention on Cybercrime International Cooperation Efforts to Fight Against Cybercrime

In the traditional understanding, a crime covers a specific area. Therefore, there are courts in all cities. Just because of the same reason crime and punishment are generally local, regional and national. During the judgment, courts take into account the national penal code like the Turkish Penal Code. But the nature of cybercrime has some uniqueness, it has been conducted in the virtual environment, catching the suspects is not possible without high tech investigation, finding a real witness is not possible and violation of the law can be related to several articles of a country's penal code.

In a nutshell, there are many differences between traditional crimes and cybercrimes because of their transborderness and these reasons touched above force states to look for cooperation against criminals from local to an international degree.[127] Surely domestic-national endeavors are important but without international collaboration, it is obvious that the endeavors going to be not sufficient. Also, the Convention with its other protocols like "Additional Protocol on Xenophobia and Racism Committed by Means of Computer System" (ETS 189)[128], "Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data" (ETS 108)[129], "Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse" (CETS 201/Lanzarote Convention)[130] and

[127] Li, X. (2007). International actions against cybercrime: Networking legal systems in the networked crime scene. *Li, Xingan." International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene." Webology, 4* pp.3.

[128] Council of Europe, (January 28, 2003) Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680008160f (Accessed on March 10, 2021)

[129] Council of Europe, (October 01, 1985). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (Accessed on March 10, 2021)

[130] Council of Europe, (July 01, 2010). Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201 (Accessed on March 10, 2021)

"Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism" (CETS 198/ Warsaw Convention)[131] supply legal, procedural rules and recommends cooperation among parties to make the world safer. Here having several additional protocols organized and regulated by the organization facilitates the process of solving investigations and keeps the Convention alive against new types of crimes. This makes it more advantageous against other international initiatives.

Since this study is going to focus on only international cooperation from the neoliberal perspective many other important and valuable professional or national pursuit forms will not be handled due to this work focuses on the Convention on Cybercrime. The first sentences of the convention are about supporting cooperation. In the ongoing sections, we will discuss several valuable organizations which are clearly declared that Convention on Cybercrime welcomes recent developments.

Just like accepted by the COE, according to Cerezo, Lopez and Patel the forerunner international bodies that are working on cybercrime are the United Nations, the G-8 Subgroup on High-Tech Crime, the Organisation for Economic Cooperation and the Council of Europe.[132]

The United Nations is a global organization and has 193 member states to ensure peace, dignity and equality on a healthy planet.[133] So, due to its nature the United Nations (UN) interests in several issues from education, social justice to perpetual peace.

---

[131] Council of Europe, (May 01, 2008). Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198 (Accessed on March 10, 2021)

[132] Cerezo, A. I., Lopez, J., & Patel, A. (2007, August). International cooperation to fight transnational cybercrime. In *Second international workshop on digital forensics and incident analysis (WDFIA 2007)* pp. 13-27. IEEE.

[133] United Nations, Member States, Retrieved from: https://www.un.org/en/member-states/ (Accessed November 2, 2020)

The UN has worked on cyber issues as of 1980, in 1990 General Assembly adopted "Guidelines Concerning Computerized Personal Data Files", in 2001 and in 2002 respectively resolutions 55/63[134] and 56/121[135] have been accepted by the General Assembly. The aims of these resolutions were to prevent using ICTs to violate the law. In addition, resolution 56/121 approves the Council of Europe's endeavor and indicates the Budapest Convention as a good example and defends building common legislation on cybercrime.[136] In a UN meeting definition of cybercrime was accepted just like the Council of Europe (COE) did. Also in the eleventh UN congress, the attendee countries demand to sign the Budapest Convention even if they are not member states to the COE.[137]

UN's resolution adopted by General Assembly on 22 January 2001 with the number 55/63 highlights how should states and private sectors fight against crime. As indicated in the resolution to combat cybercrime states need to know and accept the reality that cooperation and coordination at the global level are necessary, misusing of ICTs has a grave impact on all states so both UN and regional organizations should work to prevent cybercrimes.[138]

Like Neoliberalism, the UN accepts and approves that more freedom makes people more powerful.[139] Similarly, the UN defends that "free flow of information

---

[134] United Nationas (January 22, 2001) "55/63. Combating the criminal misuse of information technologies" Retrieved From: https://undocs.org/en/A/RES/55/63. (Accessed on November 02, 2020)

[135] United Nationas (January 23, 2020) "56/121. Combating the criminal misuse of information technologies" Retrieved from: https://undocs.org/en/A/RES/56/121. (Accessed on November 02, 2020)

[136] Ünver, M., Canbay, C., MİRZAOĞLU, A. G., ÇETİNKAYA, E., & Teknolojileri, B. (2009). Uluslararası Kuruluşların Siber GüvenliN Faaliyetleri. *Konulu makale*, pp. 10.

[137] United Nationas, (May 17, 2005). "Eleventh United Nations Congress on Crime Prevention and Criminal Justice" Retrieved from: https://www.unodc.org/documents/congress/Documentation/11Congress/ACONF203_18_e_V0584409.pdf (Accessed on November 02, 2020)

[138] United Nationas (January 22, 2001) "55/63. Combating the criminal misuse of information technologies" Retrieved From: https://undocs.org/en/A/RES/55/63. (Accessed on December 04, 2020).

[139] Odysseos, L. (2010). Human rights, liberal ontogenesis and freedom: producing a subject for neoliberalism?. *Millennium*, *38*(3), pp.747-772.

can promote economic and social development, education and democratic governance"[140] for supplying information flow and to make the internet arena safer, preventing of misusing computer system is important and to do that states should accept; law should be developed in order to prevent abusing of ICTs system, law enforcement should work with other states, needed information should be shared among stakeholders, law enforcement officers should be trained and the necessary equipment should be provided, CIA (confidentiality-integrity-availability) should be protected by legal systems, in some investigations, legal systems must allow protection and accessing data, MLAT (Mutual Legal Assistance Treaty) process should supply information in a timely manner, the public should be informed and kept updated about trends of crime, ICTs should closely work with LEA to prevent crimes and to detect criminals, FPR (Freedom-Privacy and Rights) should be protected and guaranteed by law.[141]

Concerns of the United Nations on Cybercrime are preliminary ones because the organization is one of the first, which handles crimes committed through the internet. However, as mentioned before the UN is a multifunctional global organization so the diversified amount of duty of the organization has Council of Europe, Octopus Interface, (September 15-17, 2004). Computer-related offenses, several legal systems of members of this large-scale organization hamper reaching an effective agreement on which all member states work together.[142]

Besides the UN, the CoE also highly benefitted from the works and experiences of G7. At the Halifax Summit in 1995, the Group of Seven accepted that to detect and prevent transnational crimes effective measures are needed. During that

[140] United Nationas (January 23, 2020) "56/121. Combating the criminal misuse of information technologies" Retrieved from: https://undocs.org/en/A/RES/56/121. (Accessed on November 02, 2020).

[141] United Nations (January 22, 2001) "55/63. Combating the criminal misuse of information technologies" Retrieved From: https://undocs.org/en/A/RES/55/63. (Accessed on November 02, 2020).

[142] Li, X. (2007). International actions against cybercrime: Networking legal systems in the networked crime scene. *Li, Xingan." International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene." Webology*, *4* pp.3.

summit, G7 countries also discussed the threats of organized crimes and decided to cooperate against criminals.[143] During the Lyon summit in 1996, G7 clearly declared that the actions of the UN will be followed and supported by G7 to supply security and peace in the virtual environment. Also in the same summit, G7 indicated ICTs have some unique advantages like offering a significant contribution to sustainable development, promoting economic growth, encouraging people to participate in democracy, supplying free media, promoting cultural and linguistic diversity.[144] During the Okinawa Summit in 2000, the organization decided to support ICTs because of its benefits such as strengthening democracy, increasing transparency/accountability in governance, promoting human rights, enhancing cultural diversity, fostering international peace/stability and it decided to create effective national and international strategies. During the G8's Conference (Russia joined the group in 1997 and the following year it was renamed as G8) decided to prevent cybercrime to support the internet's free and democratic environment and founded Digital Opportunity Task Force.[145] In Geneva Summit, the organization planned a joint work with 43 members combined with G8 countries, private and nonprofit sectors besides multilateral organizations,[146] in Heiligendamm Summit in 2007. It was mentioned that information and communication technologies can be used by terrorist organizations and experiences should be shared to prevent the use of modern technologies by these malicious organizations.[147] In the Hokkaido Summit in 2008, the stressed issues were that criminals share child abuse materials on the internet, a joint work should be done by respecting the national legal system, and there is a need to establish a 24/7 Single Point of Contact (SPOC) to supply prompt

[143] G7 Information Center. (June 17, 1995) "Halifax Summit Documents" Retrieved from: http://www.g7.utoronto.ca/summit/1995halifax/chairman.html (Accessed on November 4, 2020).

[144] G7 Information Center, (June 29, 1996) "Lyon Summit Documents" Retrieved from: http://www.g7.utoronto.ca/summit/1996lyon/chair.html. (Accessed on November 4, 2020).

[145] G7 Information Center, (July 21-23, 200) "G8 Okinawa Summit: Documents" Retrieved from: http://www.g7.utoronto.ca/summit/2000okinawa/ (Accessed on November 4, 2020).

[146] University of Toronto G8 Information Centre, (May 11, 2001) "Genoa Summit" Retrieved from: http://www.g7.utoronto.ca/summit/2001genoa/dotforce1.html (Accessed on November 5, 2020).

[147] G7 Information Center. (June 8, 2007) "Heiligendamm Summit" Retrieved From http://www.g7.utoronto.ca/summit/2007heiligendamm/g8-2007-ct.html (Accesed November 5, 2020).

action.[148] At the G8 Conference in Paris, G8 decided to connect its works for international solutions to the Council of Europe's Convention on Cybercrime and in 2004, in Washington, G8 Justice and Home Affairs Ministers issued a Communiqué and with that they decided to support COE's ignition.[149]

When all the summits are investigated it can be seen that G7/8 is highly experienced on cyber issues and also according to the organization even if ICTs support freedom, to guarantee the free flow of information states should work in a cooperative way.

When it comes to the OECD, the organization's first international efforts were initiated in 1983.[150] In 1985, a published report shared the concerns of the OECD regarding unauthorized access, damage to computer data etc. but at that time www and ICTs were not used by the public as common as today, so it remained restricted with the narrow definition of cybercrime[151] in this report the OECD handled personal privacy issues. In 1990, an expert group organized by the OECD along with public-private sectors, academicians and computer experts, after 2 years of work, in 1992 a report named "Guidelines for Security of Information Systems" was accepted. In that report, the organization specified the importance of cooperation, training of law enforcement along with judicial authorities, and jurisdictional competence.[152]

---

[148] G7 Information Center. (July 7–9, 2008). "Hokkaido Toyako Summit" Retrieved From http://www.g7.utoronto.ca/summit/2008hokkaido/index.html (Accessed on November5, 2020).

[149] Gercke, M. (2016). Understanding cybercrime: a guide for developing countries. ITU, (pp 89-91)

[150] Cerezo, A. I., Lopez, J., & Patel, A. (2007, August). International cooperation to fight transnational cybercrime. In *Second international workshop on digital forensics and incident analysis (WDFIA 2007)* pp. 13-27. IEEE.

[151] OECD, (September 23, 1980) "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" Retrieved From: http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Accessed on November 7, 2020). (Updated in 2013)

[152] OECD, (1992) "OECD Guidelines for the Security of Information Systems, 1992" Retrieved from: http://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm

In 1999, the OECD published another guideline with the name "OECD Guidelines for Consumer Protection in the Context of Electronic Commerce" to prevent e-consumers and recommended work with private companies.[153] In 2002, the OECD prepared another guideline but this time the guideline was not about e-commerce but it was about secure information and network system. In "Guidelines for the Security of Information Systems and Networks" the importance of secure network-internet society and the importance of cooperation, security policies, practices, measures and procedures were shared.[154]

After these reports, the OECD prepared uncountable works to combine collective measurement on cyber issues for example in 2005 it published a report about spam[155] and in 2007 about terrorist activities on networks[156] all of which were important examples of the OECD's endeavor about cyber issues. Again, the OECD's 2011 report tried to create a common definition of cybercrimes.[157] However, all the works of the OECD would not as effective as the COE's Convention on Cybercrime about creating common legislation among countries.

The European Union is also one of the leading organizations which aims to fight against cybercrime and its practices and experiences lead the way for the CoE's as stated and indicated in the main text of the Budapest Convention.

(Accessed November 7, 2020). (Replaced in 2002 as OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security)

[153] OECD, "OECD Guidelines for Consumer Protection in the Context of Electronic Commerce Frequently Asked Questions (FAQ)" Retrieved from: https://www.oecd.org/sti/consumer/2091663.pdf)Accessed on November 8, 2020).

[154] OECD, (July 25, 2002) "OECD Guidelines for the Security of Information Systems and Networks TOWARDS A CULTURE OF SECURITY" Retrieved from: http://www.oecd.org/digital/ieconomy/15582260.pdf (Accessed on November 8, 2020).

[155] OECD, (April 19, 2006). "Report Of The OECD Task Force On Spam: Anti-Spam Toolkit of Recommended Policies and Measures" Retrieved From: http://www.oecd.org/digital/consumer/36494147.pdf (Accessed on November 8, 2020).

[156] OECD, "National Terrorism Risk Insurance Programmes Of OECD Countries With Government Participation Main Features" Retrieved from: https://www.oecd.org/daf/fin/insurance/Terrorism-Risk-Insurance-Country-Comparison.pdf (Accessed on November 8, 2020).

[157] OECD, (January 14, 2020) "Reducing Systemic Cybersecurity Risk" Retrieved From: https://www.oecd.org/newsroom/46894657.pdf (Accessed on November 8, 2020).

In 1995, the work of the EU Data Protection Directive aimed to protect citizens from the processing of personal data. This was binding between member states and regulated the collecting and proceeding of personal data within confidentiality and security.[158] In 1996 a report named "Illegal and Harmful Content on Internet" was published and the framework of the report included crimes indicated by the CoE and the UN on the broad definition of cybercrime such as national security, protection of minors, privacy, reputation and human dignity, economic and informational security and intellectual property. With the report, the EU decided to fight illegal and harmful content on global networks.[159] In 1997 "Concerning the Processing of Personal Data and The Protection of Privacy in the Telecommunications Sector" was prepared the aim was to support the decisions of 1995[160]. In 1999, a report named "e-EUROPE An Information Society For All" was launched. The aim was to make ICTs as affordable and reachable as possible. (At homes, schools, hospitals briefly every area of human life)[161] In 2002 "Directive on Access to and Interconnection of Electronic Communications Networks and Associated Facilities"[162] was created and this was the roots of regulations in 2005 regarding submission-flowing of data and transmission-exchanging of confidential

[158] European Union, (October 24, 1995) "Directive 95/46/EC Of The European Parliament And Of The Council" Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN)Accessed on November 10, 2020).

[159] European Union, (October 16, 1996) "Illegal and harmful content on the Internet" Retrieved from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0487:FIN:en:PDF (Accessed November 10, 2020).

[160] European Union, (December 15, 1997) "Directive 97/66/EC Of The European Parliament And Of The Council Concerning The Processing Of Personal Data And The Protection Of Privacy In The Telecommunications Sector" Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=en (Accessed on November 10, 2020).

[161] European Union. (December 8, 199). "eEurope - An Information Society for All" Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24221&from=FI (Accessed on November 8, 2020).

[162]European Union. (March 7, 2002) "Directive 2002/19/EC Of The European Parliament And Of The Council On Access To, And Interconnection Of, Electronic Communications Networks And Associated Facilities (Access Directive)" Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0019&qid=1606722783130&from=EN (Accessed on November 10, 2020)

data.[163] In addition, it is worth noting that the recommendations and decisions still are in force nowadays.

After several initiatives to fight against cybercrimes and create common legislation, the European Union in 2000 has followed the Council of Europe's works although it criticized the convention on account of the fact that it supplied more opportunity to governmental agencies and alleged it may violate human rights and privacy.[164] Finally, in 2013 the European Union invited its members to be a part of the Budapest Convention. Additionally, according to the EU, the Convention should be accepted as a reference point to create international law.[165] In addition, the organization declared on its web page that it corresponds to the Council of Europe Convention on Cybercrime.[166]

3.4. Convention on Cybercrime and a Brief Comparison

In democratic countries, every investigation should be based on law. If the investigation in question, related to transnational crime this creates the need for an international system. To do that the Convention on Cybercrime supplies three basic things those are respectively substantive law, procedural law and international cooperation. Here substantive law covers the articles from 2 to 12 and criminalizes some computer offenses. Those crimes listed in the articles are defined as IT crimes and cover crimes against the confidentiality and integrity of computer data and systems. Procedural law with articles from 14 to 21, permits efficient investigations and uses electronic evidence during investigations. While substantive law defines

[163] European Union. (January 12, 2005) "Regulation (Ec) No 184/2005 Of The European Parliament And Of The Council On Community Statistics Concerning Balance Of Payments, International Trade In Services And Foreign Direct Investment" Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005R0184&qid=1605006979191&from=EN (Accessed on November 10, 2020).

[164] Janczewski, L., & Colarik, A. (Eds.). (2007). *Cyber warfare and cyber terrorism*. IGI Global.

[165] European Union. (2013). "Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace" Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52013JC0001&from=HU (Accessed on November 10, 2020)

[166] European Union. "Cybercrime" Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en (Accessed on November 10, 2020).

crime and supplies common legislation to countries procedural law defines investigation ways and lastly international cooperation namely the articles from 23 and 35 limits by safeguards and conditions to prevent abuse of the authority. It brings some necessities such as proportionality judicial supervision. Domestic legislations of all the Parties reach international standards to facilitate international cooperation through the agreement.[167]

The aims of the Convention described by the CoE as follows: 1) harmonizing both domestic criminal law and provisions regarding to cybercrimes, 2) providing domestic procedural law that is necessary for both investigation and prosecution, 3) creating faster and more effective ways for international cooperation.[168]

The first cybercrime legislation initiatives emerged in the homeland of the computer but it remained local and individual states took their responsibilities. Although the initiative resulted in failure Senate Bill introduced by Senator Abraham Ribicoff functioned as Model Act and had a strong impact on states legislation.[169] In Europe, the Council of Europe with the work named the Council of Europe Conference on Criminological Aspects of Economic Crime was the first initiative and happened in 1976.[170] After the US, Sweden was the first state which recognized special interest in personal data stored on the internet and it enacted a criminal provision for personal data protection in 1979. The OECD's work with a group of experts partly shaped computer-related crimes and the organization published its

[167] Council of Europe,(2013)., Capacity building on cybercrime, Retrieved from: https://rm.coe.int/16802fa3e6 (Accessed on November 1, 2020)

[168] Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on March 01, 2021)

[169] Taber, J. K. (1978). On Computer Crime (Senate Bill S. 240), 1 Computer LJ 517 (1978). *The John Marshall Journal of Information Technology & Privacy Law*, *1*(1),pp. 16.

[170] Council of Europe, Octopus Interface, (September 15-17, 2004). Computer related offences, Retrieved from: https://www.cybercrimelaw.net/documents/Strasbourg.pdf (Accessed on February 27, 2021).

report in 1986.[171] The Council of Europe's first Recommendation was published in 1981 on economic crimes. (R (81) 12)[172]. Then after the works of the CoE on computer-related crimes were shaped mostly with Recommendation No. R (81) 20 on the harmonization of laws relating to the requirement of written proofs, to the admissibility of reproductions of documents and recordings on computers[173], Recommendation No. R (85) 10 on letters rogatory for the interception of telecommunications[174], Recommendation No. R (87) 15 regulating the use of personal data in the police sector[175] and Recommendation No. R (89) 9 on computer-related crime[176]. The works of organization collected with Recommendation No. R. (95) 13 and the recommendation focused on lack of computer-related criminal procedural law[177]. In 1996 Committee of Experts on Crime in Cyberspace shortly CD-PC was established as a result of the works of CD-PC Convention on Cybercrime was created in 2001.[178]

Convention on Cybercrime particularly deals with 4 types of crimes respectively; violation of network security, computer-related fraud, child exploitation

[171] Council of Europe, (March 24, 1997). Implementation of recommendation No. R (89) 9 on computer related crime, Retrieved from: https://rm.coe.int/0900001680928683 (Accessed on February 27, 2021).

[172] Council of Europe, (May 14, 1993). Motion for a recommendation on economic crime, Retrieved from: https://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewHTML.asp?FileID=7197&lang=en (Accessed on February 27, 2021)

[173] Council of Europe, (December 11, 1981) Recommendation no. R (81) 20, Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804c66e0 (Accessed on February 27, 2021)

[174] Council of Europe, (June 28, 1985) Recommendation no. R (85) 10, Retrieved from: https://rm.coe.int/09000016804e6b5e (Accessed on February 27, 2021)

[175] Council of Europe, (September 17, 1987) Recommendation no. R (87) 15, Retrieved from: https://rm.coe.int/168062dfd4 (Accessed on February 27, 2021)

[176] Council of Europe, (September 13, 1989) Recommendation no. R (89) 9, Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094 (Accessed on February 27, 2021)

[177] Council of Europe, (September 11, 1995) Recommendation no. R (95) 13, Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 (Accessed on February 27, 2021)

[178] Weber, A. M. (2003). The Council of Europe's Convention on Cybercrime. *Berkeley technology law journal*, *18*(1), 425-446.

and copyright infringements.[179] As we before mentioned the history of cybercrime is as old as the internet. Prosecuting methods of these types of crimes caused conflicts when the criminals acted from different countries. The only solution was having an international agreement for countries and the aim of the Convention was supplying procedural law, reaching provisional law and ensuring international cooperation.[180]

If states have not a common procedural law on cybercrimes the result will be just the same as Onel De Guzman's case. The man was the creator of the I LOVE YOU virus, sent worms all around the world. As he said, in the beginning, his aim was only to reach out free internet. In his words, at that time, he was a master's student and he tried to show his professors that he exposed a hole in the operating system but because his professors are close-minded they didn't believe him and now history always remembers him. At that time the Philippines has no enough cybercrime legislation to prosecute him and he was punished only with a small amount fine[181] and the case shows us that the international arena needs effective cybercrime legislation with as many members as possible.

In order to understand the Convention following the deduction way will be more beneficial. The CoE divides it into four chapters respectively as 1) use of terms, 2) substantive law and procedural law, 3) international cooperation and lastly 4) final clauses.[182] Chapter 1 illuminates some difficult terms such as computer system,

[179] Council of Europe, Details of treaty, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Accessed on February 27, 2021)

[180] Weber, A. M. (2003). The Council of Europe's Convention on Cybercrime. *Berkeley technology law journal*, *18*(1), pp. 425-446

[181] The New York Times, (October 21, 2000) A Filipino linked to love bug talks about his license to hack. Retrieved from: https://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html (Accessed on February 28, 2021)

[182]Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on February 28, 2021)

computer data, service provider and traffic data because especially the terms used on the treaty.[183]

Chapter 2 is divided into 2 subcategories as procedural law (articles from 2 to 12) and provisional laws (articles from 14 to 21). The Table 3.1 shows a very short framework of the article's provisional law.

Table 3. 1. Articles of Provisional Law**.**[184]

Title 1:Offences against the confidentiality, integrity and availability of computer data and systems	
A.2	Illegal Access
A.3	Illegal Interception
A.4	Data Interference
A.5	System Interference
A.6	Misuse of Devices
Title 2: Computer related offenses	
A.7	Computer Related Forgery
A.8	Computer Related Fraud
Title 3: Content related offenses	
A.9	Offenses related to child pornography
Title 4: Copyright and related rights	
A.10	Offenses related to infringements of copyright and related rights
Title 5: Ancillary liability and sanctions	
A.11	Attempt and aiding or abetting
A.12	Corporate liability

As can be seen in the table the Convention handles 4 types of crimes respectively confidentiality, integrity and availability of computer data, computer-

[183] Council of Europe, (November 23, 2001) Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on February 28, 2021)

[184] Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on March 01, 2021)

related offenses, content-related offenses and copyright. The section also includes ancillary provisions that require the establishment of laws against the aforementioned crimes, as well as the establishment of a standard for corporate liability.

The purpose of Section 1 is to provide legislation at both national and international levels. Correspondence in domestic law can prevent spreading those crimes to another Party. Title 1 includes the core of computer-related offenses, titles 2 and 4 cover computer-related offenses and those offenses occur more than the previous. The reason why only one content related crime was indicated in the Convention is that at that time the committee did not reach a consensus on this title. While some supported indicating racist propaganda as a crime, the others were concerned to cut in freedom of expression. Also at that time child exploitation was a modus operandi for all the parties. Lastly, Title 4 copyright infringements are also on the agenda of several countries.[185]

Although the first section mostly covers IT crimes, to make it proper for future crimes experts preferred using neutral language. The reason for using the term "without right" several times in articles comes from the need to divide the actions as lawful and unlawful. Since, in some cases, classical legal defenses are applicable such as consent, self-defense etc. Additionally, for the Convention, all the violations should be conducted "intentionally". Here the two words give the right to LEA "interception" who work for national security and work for detection of an offense.[186]

Here the terms computer-related forgery and computer-related fraud are the most confused and discussed crimes. Computer-related forgery is probably the oldest type of crime and there are examples of it since the third generation of computers. Computer-related forgery is generally used to gain benefit from the nature of

[185] Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on March 02, 2021) pp 6-7

[186] Ibid, pp 8-10

computers and emerge as phantom users, rounding out banking or financial accounts. This type of crime mostly includes multi offenses. The other one namely computer-related fraud mostly conducted to profit from the victim's patrimony. Namely, the differences between the two come from the intent of the crime. Deletion, alteration and corrupting data are compromised with Article 7, if any person intentionally deletes, alters and corrupts data to benefit from victims' patrimony this crime is compromised with article 8.[187] Within the scope of the Convention's Article 10, crimes related to copyright should be conducted "willfully". In addition, Article 13 obliges all the parties to define all the articles from 2 to 12 as crimes in their inner penal codes and bans aiming, abetting to those crimes.[188]

When the articles of the Convention are investigated, it is revealed that the criminalized actions are very similar to the US Codes. For example Articles 2, 3, 4, 5, 6 are similar with 18 U.S. Code§1030 (fraud and related activity in connection with computers)[189] Articles 7, 8 regarding computer/internet misuse have been touched by US codes 15 U.S. Code§45 (computer fraud and abuse)[190], 15 U.S. Code § 1644 (credit card fraud)[191], 18 U.S. Code§1029 (fraud connected with illegal access)[192], 18 U.S. Code§1030 (fraud connected with computers)[193]. The only

[187] Council of Europe, (March 15, 2013). Computer-related forgery and computer-related fraud: the need to build and include these new criminal types in a modern penal code, Retrieved from: https://www.coe.int/en/web/octopus-old2019/blog/-/blogs/computer-related-forgery-and-computer-related-fraud-the-need-to-build-and-include-these-new-criminal-types-in-a-modern-penal-code/ (Accessed on March 01, 2021)

[188] Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on March 01, 2021) pp. 18-19

[189] Cornell Law School, Legal Information Institute, 18 U.S. Code § 1030 - Fraud and related activity in connection with computers, Retrieved from: https://www.law.cornell.edu/uscode/text/18/1030 (Accessed on March 01, 2021)

[190]Cornell Law School, Legal Information Institute, 15 U.S. Code § 45 - Unfair methods of competition unlawful; prevention by Commission, Retrieved from: https://www.law.cornell.edu/uscode/text/15/45 (Accessed on March 01, 2021)

[191] Cornell Law School, Legal Information Institute, 15 U.S. Code § 1644. Fraudulent use of credit cards; penalties Retrieved from: https://www.law.cornell.edu/uscode/text/15/1644 (Accessed on March 01, 2021)

[192] Cornell Law School , Legal Information Institute, 18 U.S. Code § 1029 - Fraud and related activity in connection with access devices, Retrieved from: https://www.law.cornell.edu/uscode/text/18/1029 (Accessed on March 01, 2021)

content-related crime defined with article 9 criminalized also in US code with the articles 18 U.S. Code§2251 (child exploitation)[194] and 18 U.S. Code§2421 (prostitution)[195]. Copyright infringements defined with article 10 also defined in the 17 U.S. Code § 506 (criminal offense)[196].

The reason for the similarity actually comes from the supports of the US because the treaty was drafted under the strong pressure of the US. From the beginning, the US either directly or indirectly joined the works of CD-PC. In addition to the US, the Convention has important similarities with Canadian and Japanese laws.[197]

When it comes to Turkish Criminal Code law no 5237 (Hereinafter referred to as TCC.), the offenses described in Title 1 partly reflected with the penal codes 243 (accessing a data processing system), 244 (preventing the functioning of a system and deletion alteration corrupting the data) and the Title 2, reflected with the penal codes 158/1-f (qualified theft by deception) and 245 (misuse of bank or credit cards). However, compared to the Convention and the US law the extent of the Turkish Criminal Code is very narrow. Content-related crimes with Title 3 are discussed in TCC with article 226 (Obscenity).[198] Title 4 regarding copyright and related rights comes up with the Law on Intellectual and Artistic Works with law no

---

[193] Cornell Law School , Legal Information Institute, 18 U.S. Code § 1030 - Fraud and related activity in connection with computers, Retrieved from: https://www.law.cornell.edu/uscode/text/18/1030 (Accessed on March 02, 2021)

[194] Cornell Law School , Legal Information Institute, 18 U.S. Code § 2251 - Sexual exploitation of children, Retrieved from: https://www.law.cornell.edu/uscode/text/18/2251 (Accessed on March 02, 2021)

[195] Cornell Law School , Legal Information Institute, 18 U.S. Code § 2421 - Transportation generally Retrieved from: https://www.law.cornell.edu/uscode/text/18/2421 (Accessed on March 02, 2021)

[196] Cornell Law School , Legal Information Institute, 17 U.S. Code § 506 - Criminal offenses, Retrieved from: https://www.law.cornell.edu/uscode/text/17/506 (Accessed on March 02, 2021)

[197] Kierkegaard, S. M. (2007). International Cybercrime Convention. In *Cyber warfare and cyber terrorism* pp. 469-476. IGI Global.

[198] Turkish National Assembly, (September 26, 2004), Turkish Criminal Code, Retrieved from: https://www.tbmm.gov.tr/kanunlar/k5237.html (Accessed on March 8, 2021)

4630 (previous version's code was 5846)[199]. Since TCC has had a very narrow structure, the need for international agreements to have a comprehensive provisional law is very clear.

Table 3. 2. Articles of Procedural Laws.

Title 1 – Common provisions	
A.14	Scope of procedural provisions
A.15	Conditions and safeguards
Title 2- Expedited preservation of stored computer data	
A.16	Expedited preservation of stored computer data
A.17	Expedited preservation and partial disclosure of traffic data
Title 3 – Production order	
A.18	Production order
Title 4 – Search and seizure of stored computer data	
A.19	Search and seizure of stored computer data
Title 5 – Real-time collection of computer data	
A.20	Real-time collection of traffic data
A.21	Interception of content data

When a crime happened or when LEA received a denunciation from a real person or any multinational service provider, in order to investigate or take precautions in the case of any imminent risk or threat they need some procedural measures taken international level. Therefore, the articles related to procedural law prepare a legal basis to investigate the crimes that have been already indicated in the section provisional law.

Procedural law both covers traditional methods and modern methods. For example, searching or seizing any data is a classical way of investigation. However, it should be kept in mind that in the modern world data is not static and flows during

[199] Turkish National Assembly, (February 21, 2001), Law of Intellectual Property Rights, Retrieved from: https://www.tbmm.gov.tr/kanunlar/k4630.html (Accessed on March 8, 2021)

communication. Therefore, as a modern way during the investigation process, LEA may need log details. As we said before stored data are vulnerable can be deleted by suspects or may be damaged due to technical problems so the need for preservation data so that it requests by JA also emerged. All the provisions in this section aim at permitting, obtaining or collecting data for the purpose of specific criminal investigations or proceedings. Generally, procedural law indicates three types of data respectively traffic data, content data and subscriber data.[200] (Case examples will be shown in the last chapter of this thesis.)

Articles 16 and 17 sets out that stored data has already been collected and retained by companies. It is also very important that the Convention uses only the term data preservation not retention since those two are very distinct terms in computer language. Preservation covers the already existing data but retention contains all the recordable data including future log details[201]. For instance, when Facebook Help Center's directions were investigated it can be seen that users can permanently delete their accounts in less than 30 days. However, in some cases, it may take up to 90 days but it seems to be deleted for the user. Moreover, copies can be preserved after 90 days in case of is any violation detected by the company.[202] However, already the Convention with Article 16 obliges companies to preserve the data for 90 days.[203] Moreover, it seems that preservation's date range is already on the agenda of the TC-Y committee in order to enhance it.[204]

---

[200] Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from:https://rm.coe.int/16800cce5b (Accessed on March 3, 2021) pp: 21

[201] Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from:https://rm.coe.int/16800cce5b (Accessed on March 3, 2021) pp: 25-26

[202] Facebook, Help Center, Retrieved from: https://www.facebook.com/help/224562897555674?helpref=faq_content (Accessed on March 4, 2021)

[203] Council of Europe, (November 23, 2001), Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on March 4, 2021)

[204] Council of Europe, Protocol Negotiations, Retrieved from: https://www.coe.int/en/web/cybercrime/t-cy-drafting-group (Accessed on March 4, 2021)

The order of collection of production evidence, in some countries, is only given by judges but also there are several counties that give the same authority to prosecutors and LEA. However, this does not mean having the authority of violating privacy for any offense in the cyber realm. For example, Articles 20 and 21 restrict the conditions of collecting traffic and content data as serious offenses to be determined by domestic law. For example, Article 17 supplies an important tool for competent authorities in order to find the creator/s of a virus or any content-related crime.[205] Also with Article 18 competent authorities can apply the assistance of service providers in order to detect the real user behind a username due to it compromised computer and subscriber data such as telephone number, website address or domain name, e-mail address, communication equipment like telephone devices, call centers or LANs etc.[206]

Here differently from the other articles, Article 19 supplies a legal basis to seizure physically stored data. However, the authority is restricted at the national level and does not address "transborder search and seizure".[207]

While Article 14 obliges the parties to adopt legislative and other measures, Article 15 ensures adequate measures to protect human rights with the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other international human rights agreements.[208]

---

[205] Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from:https://rm.coe.int/16800cce5b (Accessed on March 3, 2021) pp: 28-30

[206] Council of Europe, (March 1, 2017), T-CY Guidance Note #10 Production orders for subscriber information https://rm.coe.int/16806f943e pp: 5 (Accessed on March 4, 2021)

[207] Csonka, P. (2006). The council of europe's convention on cyber-crime and other European initiatives. *Revue internationale de droit penál*, *77*(3), 473-501.

[208] Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on March 3, 2021) pp: 28

When it comes to the US, the 18 U.S. Code§3121 (limiting to intercept communication)[209] and 18 U.S. Code§3127 (trap and trace device)[210] bring some rules on interception to communication. Procedural Law's Title 2, namely the articles 16, 17 and 18 reflected in US law with the code 18 U.S. Code§2703. According to the code with a search warrant and prosecutor order, a governmental entity can request disclosure of data until 180 days. Disclosure of data compromise name, surname, local and long-distance telephone connection records/sessions, length and type of service, telephone or instrument number and network address, payment details etc.[211] Rule 41. Search and Seizure define procedures to investigate storage materials and other types of pieces of evidence indicated in the Convention's Article 19.[212] Articles 20th and 21st of Title 5 have a similar structure with 18 U.S. Code§2518[213] (interception to electronic communications) and 18 U.S. Code§2511 (disclosure of electronic communication)[214].

When it comes to Turkish law, "Searching in computers, computer programs and logs, copy and seizure" are regulated in the Turkish Criminal Procedure Code (Hereinafter referred to as 5271.) with article 134. Also during investigations, the measures set out in articles from 135 to 138 of the section titled "Surveillance of communications through telecommunication facilities" used by cybercrime

[209] Cornell Law School , Legal Information Institute, 18 U.S. Code § 3121 - General prohibition on pen register and trap and trace device use; exception, Retrieved from: https://www.law.cornell.edu/uscode/text/18/3121 (Accessed on March 4, 2021)

[210] Cornell Law School , Legal Information Institute, 18 U.S. Code § 3127 - Definitions for chapter https://www.law.cornell.edu/uscode/text/18/3127 (Accessed on March 4, 2021)

[211] Cornell Law School , Legal Information Institute, 18 U.S. Code § 2703 - Required disclosure of customer communications or records https://www.law.cornell.edu/uscode/text/18/2703 (Accessed on March 4, 2021)

[212] Cornell Law School , Legal Information Institute, Rule 41. Search and Seizure https://www.law.cornell.edu/rules/frcrmp/rule_41 (Accessed on March 4, 2021)

[213] Cornell Law School , Legal Information Institute, 18 U.S. Code § 2518 - Procedure for interception of wire, oral, or electronic communications https://www.law.cornell.edu/uscode/text/18/2518 (Accessed on March 4, 2021)

[214] Cornell Law School , Legal Information Institute, 18 U.S. Code § 2511 - Interception and disclosure of wire, oral, or electronic communications prohibited, https://www.law.cornell.edu/uscode/text/18/2511 (Accessed on March 4, 2021)

investigators. Articles 16 and 17 are not issued in the Turkish Criminal Procedure Code. Moreover, although law 5651 (Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publications) has similarities with the Convention, unlike it 5651 indicates not procedural but administrative structure and because of that using 5651 during the determining process of a criminal investigation is not possible. Again, articles 17 and 18 partly come up with article 134 of 5271. Compared to 17 and 18, Article 134 remains very narrow but to some extent, it satisfies the requirements of the Convention. Article 135 of 5271 "Interception of Correspondence through Telecommunication" is generally used by governmental entities to encounter the articles of the Convention 20 and 21. But in reality, those articles have very different structures because while article 20 indicates all the traffic data including log details, IP/PORT details and Article 21 indicates content data such as message details on WhatsApp, Turkish Procedural Law's 135 covers only wiretapping.[215]

Table 3. 3. Articles regarding International Cooperation.

Section 1 General principles

Title 1 – General principles relating to international co-operation	
A.23	General principles relating to international co-operation
Title 2 – Principles relating to extradition	
A.24	Extradition
Title 3 – General principles relating to mutual assistance	
A.25	General principles relating to mutual assistance
A.26	Spontaneous information
Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	
A.27	Procedures pertaining to MA requests in the absence of applicable international agreements
A.28	Confidentiality and limitation on use

[215] Ozbek, M. (2015). The Impacts of European Cybercrime Convention on Turkish Criminal Law. *GSI Articletter*, *13*, 73.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures	
A.29	Expedited preservation of stored computer data
A.30	Expedited disclosure of preserved traffic data
Title 2 – Mutual assistance regarding investigative powers	
A.31	Mutual assistance regarding accessing stored computer data
A.32	Trans-border access to stored computer data with consent or where publicly available
A.33	Mutual assistance regarding the real-time collection of traffic data
A.34	Mutual assistance regarding the interception of content data
Title 3 – 24/7 Network	
A.35	24/7 Network

International cooperation is the most important part of the Convention. Before the CoE's works as mentioned, there have been several initiatives to criminalize some computer-related offenses. However, as different from the other works and initiatives, the CoE tried to build an international agreement in which parties help the others and benefit from the previous investigation. With article 25 of the Convention, all the signatories accept that they will always support the others to the widest extend. The term mutual assistance (Hereinafter referred to as MA.) is not a new phenomenon and it is already one of the used methods by countries. For example, Article 39 indicates the 1957 European Convention on Extradition (ETS No. 24)[216], 1959 European Convention on Mutual Assistance in Criminal Matters (ETS No. 30)[217] and 1978 Additional Protocol to the European Convention on

[216] Council of Europe, (December 13, 1957). European Convention on Extradition Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680064587 (Accessed on February 24, 2021)

[217] Council of Europe, (April 20, 1959). European Convention on Mutual Assistance in Criminal Matters, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016800656ce (Accessed on February 24, 2021)

Mutual Assistance in Criminal Matters (ETS No. 99)[218] to foster and empower mutual assistance.

However, Article 27 of the Convention provides a series of rules if parties have not MA agreements. In the second paragraph of the article, Convention obliges the parties to have and detect at least one authority that is responsible for receiving or sending MA. In Turkey, the Ministry of Justice deals with MA processes.[219] Cybercrimes exist at any location of the world. While www connects the entire world to each other, states also should have been connected to each other to fight against criminals. In this sense for all the countries, cooperation on the international level was a necessity.

Imagine a country (a) that is investigating a case regarding computer-related fraud. After a long-term work, the relevant authorities find that some of the suspects are located there, acting international level and gather all the money to launder in a bank located in the county (b). In this situation which one will be the most proper option? Should they close the file after arresting the suspects located in their country, should they wait for signing MLAT to detect the members of the illegal organization, or should they supply spontaneous information to warn the country (b)? In this situation, the only mindful option is to supplying spontaneous information to the country (b) and the Article 26 just aims at this.

In order to supply international cooperation to the widest extend Article 23 obliges all the parties to share the needed information rapidly. Here very importantly the Convention tries to expand sharing information not only on cybercrime but also on the crimes that may involve electronic evidence. After the criminal/s detected extradition comes to agenda. According to Article 24, extradition can be applied only to the crimes described in the provisional section and requires at least a one-year

[218] Council of Europe, (March 17, 1978). Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680077975 (Accessed on February 24, 2021)

[219] Council of Europe, (Status as of March, 2021). Reservations and Declarations for Treaty No.185 - Convention on Cybercrime Retrieved from: https://www.coe.int/en/web/conventions/recent-changes-for-treaties/-/conventions/treaty/185/declarations (Accessed on March 4, 2021)

penalty.[220] In addition, general principles relating to international cooperation are explained with case examples in the last chapter of this thesis not service providers but country base.

Articles 16 and 29 have similar structures because while Article 16 tries to preserve stored computer data at the national level, Article 29 tries to reach the same at the international level. In article 16, all the parties should supply protection and preservation of data and in Article 29 another party can request preservation of data located in a different country's territory and jurisdiction. Like Articles 16 and 29, Articles 18 and 30 have similarities. While Article 18 tries to oblige parties having authority on ICTs located in their territory and jurisdiction to disclose information, Article 30 provides this at the international level and if a state request traffic data from a country with the article requested party must provide a sufficient amount of traffic data to requesting party.[221] In the fourth chapter of this thesis, we will see that while some companies located and serving under the jurisdiction of the US obliges the treaty's conditions some refrain from obeying the conditions of the treaty just because of subjective reasons.

Unlike the others, Article 32 authorizes the LEA to have direct cross-border access to stored data. However, there are some necessities to directly reach these data. Firstly, the data should be accessible on open sources. Secondly, a real person should accept disclosing of data.[222] In addition, the Convention tries to build a community of trust among the parties by fostering international cooperation. One of the most important parts of international cooperation is undoubtedly the 24/7 Point of Conduct (Hereinafter referred to as SPoC.). This contact point will be used by all the parties in case of an emergency. With Article 35, each party has the obligation to

---

[220] Council of Europe, (November 23, 2001), Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on March 4, 2021)

[221] Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on February 3, 2021)

[222] Council of Europe, (December 3, 2014). T-CY Guidance Note 3, Retrieved from: https://rm.coe.int/16802e726a (Accessed on November 12, 2020).

create a point of contact that is available all day and night. This is also a direct line between parties and LEA. Each party has the liberty to choose their 24/7 SPoC they either may give the mission to the unit responsible for the MA process, or may give it to LEA. However, all the parties should appoint a completely specialized unit in fighting cybercrime. In addition, the 24/7 SPoC of all the countries should coordinate other components, acts in a fast way, be ready for any imminent risk of death, physical injury, a serious threat to any location of the country and should communicate with other representatives etc.[223] For Turkey 24/7 PoC is determined as Turkish National Police, Counter Cybercrime Department.[224]

Table 3. 4. Final provisions.

A.36	Signature and entry into force
A.37	Accession to the Convention
A.38	Territorial application
A.39	Effects of the Convention
A.40	Declarations
A.41	Federal clause
A.42	Reservations
A.43	Status and withdrawal of reservations
A.44	Amendments
A.45	Settlement of disputes
A.46	Consultations of the Parties
A.47	Denunciation
A.48	Notification

[223] Council of Europe, (November 23, 2001) Explanatory Report, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on November 12, 2020).p: 54-55

[224]Council of Europe, Search in database, Retrieved from: https://www.coe.int/en/web/conventions/recent-changes-for-treaties/-/conventions/treaty/185/declarations (Accessed on November 13, 2020).

3.5. The COE and the Cooperation Projects of the Organization

As specified in Convention on Cybercrime, the CoE respects the initiatives of the UN, OECD, EU, and the G8.[225] It welcomes good examples and practices of these organizations during the preparation of the convention. For example, the 24/7 point of contact first implemented by G8, the definition of cybercrime first implemented by the UN both narrow and broad extends and the organization which clarifies the concepts of cybercrime was the EU. Therefore, it should be accepted that convention is not a new idea but a product of broad experiences of several organizations and most importantly, it represents experiences of several states all around the world. The reason why it is supported by so many states is that Convention on Cybercrime offers mutual legal assistance and comprehensive countermeasures[226] so all around the world 65 states use the same law to draw a legal framework to get action against cybercrimes.[227]

In a Press Release of the CoE in 2000, with the approval of 41 member states the organization invited the EU to accede ETS 108 both to extend the European approach (like GDPR) and so that the EU guide to states which are not signed or ratified the convention yet.[228] On November 23, 2001, Convention on Cybercrime was completed and served to parties in Budapest with the ETS number 185.[229]

---

[225] Council of Europe. (November 23, 2001) "Convention on Cybercrime" Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on November 12, 2020).

[226] Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*. 29(2) : pp. 408-433.

[227] Council of Europe. "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY " Retrieved from: https://www.coe.int/en/web/cybercrime/parties-observers (Accessed on November 12, 2020).

[228] Council of Europe. (2000). "Assembly backs protocol on strengthening personal data protection" Retrieved from: https://rm.coe.int/0900001680962597 (Accessed on November 12, 2020).

[229] Council of Europe. (November 23, 2001) "Convention on Cybercrime" Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on November 12, 2020.)

Additionally, in 2003, an additional protocol was published with the name "The Protocol on Xenophobia and Racism" with ETS number 189 regarding xenophobic and racist offenses on computer systems.[230] This extended the scope of the convention on criminal matters but the additional protocol is separate from the main Convention. It means that a country that signed and ratified Convention on Cybercrime does not have to sign and ratify the additional protocol.[231] For example, Turkey signed and ratified the main Convention. When it comes to ETS 189, Turkey signed it in 2016 but it has not been ratified by Turkey yet.[232] This means that it is not required for Turkey to assist other countries during the investigations regarding racist or xenophobic crimes.

Convention on Cybercrime also respects and takes into account some international agreements on human rights such as the 1950 "The Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms", 1966 "United Nations International Covenant on Civil and Political Rights" and other applicable international human rights treaties. In the convention freedom of expression, freedom to seek and the right to hold opinions without any interference or suppression have been indicated. Convention also respects privacy and protection of personal data and affirms 1981 "The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS 108". In addition to all these, the Convention affirms the 1989 "The United Nations Convention on the Rights of the Child" and the 1999 "International Labour

[230]Council Of Europe. (January 28, 2003) "Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems" Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 (Accessed on November 13, 2020)

[231] Cerezo, A. I., Lopez, J., & Patel, A. (2007, August). International cooperation to fight transnational cybercrime. In *Second international workshop on digital forensics and incident analysis (WDFIA 2007)* (p. 13-27). IEEE.

[232] Council Of Europe. (Status as of November 30, 2020) Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=7tZMZRq7 (Accessed on November 13, 2020).

Organization Worst Forms of Child Labour Convention"[233] to protect children in the virtual environment.

Between the time range 2014 and 2019, the CoE organized more than 600 activities that involve more than 120 countries. With these capacity-building works by 2018, 94 UN members (49%) had substantive criminal law broadly in line with the Convention. In 2013, the number of countries was only 70. Moreover, by 2018 the number, which used the Convention to reform their legislation was more than 140 namely 72% UN members[234] the number has raised to 153 countries namely 79% UN members by February 2020. According to CoE's report, today 177 states (92%) are currently reforming their legislation.[235] Without the projects of CoE, which cover so many states and its works aiming to strengthen legislation, this could not be possible. Results also prove that in this globalized world, with the expansion of technology, cooperation and mutual assistance becoming the only possible solution for states to escape from being a haven for criminals.

Having a common law is not enough to reach the goals of the Convention so the Council of Europe initiated some projects to implement the goals. After countries had a common/provisional law in their inner law system the council organized several projects to supply training for both JA and LEA. This project brought together law enforcement authorities (LEA) and judicial authorities (JA) of several countries and most importantly organized multinational meetings including both public and private sectors to protect human rights in the virtual environment.

---

[233] Council of Europe. (November 23, 2001) "Convention on Cybercrime" Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on November 13, 2020).

[234] Seger, A., (February 25-27, 2019), Council of Europe, Retrieved from: https://rm.coe.int/09000016809326ac (Accessed on November 1, 2020).

[235] Council of Europe,(July 13, 2020)., The budapest convention on cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed on January 15, 2021).

The organized projects are: 1. GLACY+ 2. CyberCrime@Octopus 3. EndOCSEA@Europe 4. iPROCEEDS 1-2 5. CyberEast and CyberSouth[236]

3.5.1. The projects which are organized by the CoE

GLACY+ is a joint project and organized by the COE with the contribution of the EU. The aim of it, supporting several countries in Africa, Asia-Pacific and Latin America/Caribbean Region and covers the countries Benin, Burkina, Faso, Cabo Verde, Chile, Costa Rica, Dominican Republic, Ghana, Mauritius, Morocco, Nigeria, Paraguay, Philippines, Senegal, Sri Lanka and Tonga.[237]

At the same time, some of the countries counted upon are the parties of the African Union. The African Union is a continental organization and covers 55 member states. Promoting unity, supporting and coordinating cooperation, supplying territorial integrity, defending African citizen's rights as indicated in the Charter of the United Nations and the Universal Declaration of Human Rights.[238] But although all the endeavors by 2016 only 12 of the 54 countries had the law in their legislation system regarding cybercrime and computer forensic[239] so being a part of the international organization will be more beneficial for them.

The "African Union Convention on Cybersecurity and Personal Data Protection" starts with child exploitation but it does not limit the age range of the victim. It also covers so many things from national security to transparency of personal data processing, but it does not make a definition and does not draw a limit

[236] Council of Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/capacity-building-programmes (Accessed on November 15, 2020).

[237] Council of Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/glacyplus (Accessed on November 15, 2020).

[238] African Union. Retrieved from: https://au.int/en/overview Accessed on November 15, 2020.

[239] Council of Europe. (November 20, 2016). "Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime" Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806bf0f8 (Accessed on November 15, 2020).

of information that can be requested from online service providers.[240] For example, imagine a case regarding a death threat. An unknown suspect sent an email to a victim and threatened him with death. The first thing is going to be applying to the service provider and requesting the traffic data of the suspect. However, if the state in question does not limit the terms and doesn't share the limits on its legal system any service provider won't help to LEA about the case due to privacy concerns.

As a result, the ongoing project tries to build a common framework nourished by the experiences of many states and the experiences of LEA-JA so that the African countries effectively fight against cybercrime.

Another valuable project is EndOCSEA@Europe and the full name of the project is "End Online Child Sexual Exploitation and Abuse @ Europe" the scope of the project is limited with the illegal actions on the internet against children. It covers all 47 member states especially Albania, Bosnia and Herzegovina, Georgia, the Republic of Moldova, Montenegro, Serbia and Turkey.[241]

With that project, the aim is to prevent producing and elimination of sexual materials that contain children's improper footage on ICTs and darknets. Working in cooperation within the scope of the Lanzarote Convention and producing a system like WePROTECT Model National Response.[242] WePROTECT is one of the most important organizations serving at the global level and has too many members from private sectors like Facebook, Instagram, Zoom, TikTok and Apple (total number of companies 43) and covers 98 countries in total. Moreover, as civil society organizations and international organizations, it has 47 parties. Also some police

[240] African Union. (2000). Retrieved from: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (Accessed on November 15, 2020).

[241] Council of Europe. (July 08, 2020) "EndOCSEA@Europe Project Summary" Retrieved from: https://rm.coe.int/-vc1840-project-summary-final-jul-2020/16809ef6af Accessed on November 15, 2020.

[242] Council od Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/endocsea-europe (Accessed on November 15, 2020).

organizations like INTERPOL-EUROPOL are also members of the global organization.[243]

As a result, all around the world child exploitation is a serious issue and many countries, IGOs, ICTs, and LEAs monitoring media via online virtual patrol or OSINT to protect children's future.

When it comes to iPROCEEDS-2, this project is the former version of iPROCEEDS. The stakeholders are Albania, Bosnia and Herzegovina, Montenegro, Serbia, North Macedonia, Turkey and Kosovo and funded by the COE and the EU (within the scope of the European Union project named IPA II.)[244]. When it comes to its duty like all other projects it aims to support LEA and JA to fight against online crimes. It is noted on the project summary that online crimes are increasing in the project region and changed their dimensions like a business model the most crimes observed in the region are DDoS attacks, attacks and malware against mobile or ATM devices, skimming (injection malicious code to websites), ransomware (hacking-blocking-encrypting a system in return to money), cryptojacking or wallet address stealer (think about the companies such as Binance, Cyrptopay, Bittrex, Bitcoin etc), SIM BOX frauds, identity thefts, CEO frauds (C level executives), various types of payment frauds (think about the companies such as Western Union, MoneyGram, Upt etc) and online child exploitation.[245]

The first iPROCEEDS project was carried out between the years 2016 and 2019[246] and the second phase was launched in 2020.[247] The project supplies so many

---

[243] We PROTECT Global Alliance. "WPGA Membership" Retrieved from: https://www.weprotect.org/members (Accessed on November 15, 2020)

[244] Council OF Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/iproceeds#:~:text= (Accessed on December 5, 2020).

[245] Council od Europe. (Version December 6, 2019) Retrieved from: https://rm.coe.int/2492-iproceeds-2-summary-v3/16809f3947 (Accessed on November 17, 2020).

[246] Council of Europe. (December 9-10, 2019). "iPROCEEDS: Closing Conference" Retrieved from: https://www.coe.int/en/web/cybercrime/iproceeds1/-/asset_publisher/0q0xphlFQY9G/content/iproceeds-closing-conference (Accessed on November 17, 2020).

advantages to its participants from case exercise or master degree education[248] to supply information on the academic level. Also within the scope of the project to strengthen LEA and JA, several workshops were organized in Turkey, at the workplaces of the Turkish National Police Cybercrime Department and the Ministry of Justice.[249]

Like previous projects, CyberEast is a product of cooperation and planned by the COE with the EU. The stakeholders are Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine. The scope of the project is narrow compared to others but the aim is the same as other projects.[250]

Just like CyberEast, CyberSouth is a cooperative project too. Planned by the COE with EU. It covers Southern Neighbourhood countries[251] Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestine, Syria and Tunisia.[252]

Lastly, the parties of the CyberCrime@Octopus project covers signatory states and the others who are preparing to implement the Convention on Cybercrime in their legislation. Additionally one of the founders of that project is Microsoft. Like

---

[247] Council of Europe. (February 26-28, 2020) Retrieved from: https://www.coe.int/en/web/cybercrime/-/cybereast-international-meeting-on-cooperation-with-foreign-service-providers (Accessed November 17, 2020).

[248] Council of Europe. (December 3, 2019) Retrieved from: https://www.coe.int/en/web/cybercrime/iproceeds1/-/asset_publisher/0q0xphlFQY9G/content/iproceeds-graduation-of-the-ucd-master-programme-on-forensic-computing-and-cybercrime-investigation? (Accessed on November 17, 2020).

[249]Council of Europe. (May 21-24, 2018) "iPROCEEDS: Investigating cybercrime and its financial gain under the last Cybercrime Simulation Exercise" Retrieved from: https://www.coe.int/en/web/cybercrime/iproceeds1/-/asset_publisher/0q0xphlFQY9G/content/iproceeds-investigating-cybercrime-and-its-financial-gain-under-the-last-cybercrime-simulation-exercise? (Accessed on November 17, 2020)

[250] Council of Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/cybereast (Accessed on November 18, 2020).

[251] Council of Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/cybersouth (Accessed on November 18, 2020).

[252] European Union. Retrieved from: https://ec.europa.eu/neighbourhood-enlargement/neighbourhood/southern-neighbourhood_en#:~:text= (Accessed November 18, 2020).

GLACY+ the aim of the project is spreading of Convention on Cybercrime and creates a common legal perspective.[253]

The name of the Octopus comes from Octopus Conference organized in 2004 it covered both public and private sectors to create a close relationship between parties and companies[254] and like previous ones the project is still ongoing.

3.5.1.1. Cooperation and close relation: Octopus conferences

Octopus Conferences have been organized every 12 or 18 months. The first one was organized in 2007. The conferences bring together 80 countries with cybercrime experts, cybercrime investigators, academicians, international organizations, international institutions, non-governmental organizations, public and private sectors. The aim is not only cooperating but also building and sharing the best experiences among participants.

During the international conference, several experts share their implementations and when needed different sectors can recommend something or can criticize current practices. LEA can express encountered problems and private sectors can direct them to solve any problems in an efficient way.

For example, the first Octopus Conference in 2007 (at that time it was carrying the name Octopus Interface) hosted 140 representatives from 55 countries and between them there were some nongovernmental organizations like ICMEC and INHOPE and also E-Bay, My Space and Microsoft was there.[255] The second one was organized in 2008, especially focused on the cooperation between LEA and the

[253] Council of Europe. (April 22, 2019) Retrieved from: https://rm.coe.int/summary-of-the-cybercrime-octopus/1680968ab0 (Accessed on November 18, 2020).

[254] Council of Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/octopus-conference (Accessed on November 18, 2020).

[255] Council of Europe. (June 11-12, 2007) "Octopus Interface Conference 2007 Cooperation Against Cybercrime" Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f6a08 (Accessed on November 20, 2020).

private sector.[256] In time supporters of the conference raised and in 2009 because it focused on financial crime (without disregarding other kinds of crime) Paypal and Visa joined the works.[257] In 2010, the dimension of the conference enlarged and it hosted Google.[258] (300 participants from 60 different countries)[259] 2011 was the 10th anniversary of the Convention on Cybercrime and to discuss current trends ECHR joined the meeting after that year ECHR joined nearly almost all the conferences.[260] In 2012, Octopus came to the agenda with the slogan "The Global State of Cybercrime Legislation" during the workshops there were 280 experts from 80 countries.[261] Namely, even in 2012, the organization captured nearly half of the world. In 2015, Octopus focused on the evidence in the cloud[262] and in 2016, Facebook's representatives took their chairs at the conference.[263] When it comes to the 10th conference in 2018 Amazon decided to join to support cooperation between

[256] Council of Europe. (April 1-2, 2008) "Octopus Interface Conference Cooperation Against Cybercrime" Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168026f6980 (Accessed on November 20, 2020).

[257] Council of Europe. (March 10-11, 2009) "Octopus Interface Conference Cooperation Against Cybercrime "Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168026f25c3 (Accessed on November 20, 2020).

[258] Council of Europe. (March 23-25, 2010) "Octopus Interface Conference Cooperation Against Cybercrime "Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168026f24d4 (Accessed on November 20, 2020).

[259] Council of Europe. (March 23-25, 2010) "Octopus Interface Conference Cooperation against Cybercrime" Retrieved from: https://www.coe.int/en/web/cybercrime/octopus-interface-2010 (Accessed on November 20, 2020).

[260] Council of Europe. (November 21-23, 2011) "Octopus Conference 2011 Cooperation Against Cybercrime" Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168026f2425 (Accessed on November 20, 2020)

[261] Council of Europe, (June 6-8, 2012) "Cooperation Against Cybercrime" Retrieved from: https://www.coe.int/en/web/cybercrime/octopus-interface-2012 (Accessed on November 20, 2020).

[262] Council of Europe (June 17-19, 2015) "Octopus 2015 Cooperation Against Cybercrime" Retrieved from: https://www.coe.int/en/web/cybercrime/octopus2015 (Accessed on November 22, 2020).

[263] Council of Europe, (November 16-18, 2016) "Octopus Conference 2016 Cooperation Against Cybercrime" Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168026bf0fb (Accessed on November 22, 2020).

stakeholders and Facebook increased the numbers of its participants. As of the first conference internet service providers were always there but in 2018 Vodafone sent a representative to the conference to fight against hi-tech crime and to contribute to the works of others as an internet service provider.[264] The last conference was organized in 2019 and when the time goes on the number of participants has been raised. During the conference in 2019, Apple had 3 representatives while LinkedIn had one. [265]

When it comes to Yahoo, it joined only one conference in 2009[266] Microsoft was always there but Twitter has never joined the Octopus Conference. (The policy of Twitter will be discussed in the last part.)

As stated before several times mutual assistance is an indispensable necessity when it comes to fights against cybercrime. Although several negotiations and meetings are organized to supply mutual assistance and reconciliation, the restricting structure of domestic laws causes some limitations in some cases. This also will be discussed in the next section with case examples.

Finally, there are remarkable differences among ICTs, which are willing to participate and being a part of international studies and those who are not. When ICTs joined the meetings, conferences or projects organized by international organizations and when they talk about trending problems with other public and private sectors the possibility of joint work rises. Just contrary to that, when ICTs refrain from mutual work the lack of cooperation makes them dangerous for their own customers especially like Yahoo and Twitter.

---

[264] Council of Europe. (July 11-13, 2018) "Octopus Conference 2018 Cooperation Against Cybercrime" Retrieved from: https://rm.coe.int/octopus2018-lop-11jul/16808c54d9 (Accessed on November 22, 2020).

[265] Council of Europe. (November 20-22, 2019) "Octopus Conference 2019 Cooperation Against Cybercrime "https://www.coe.int/en/web/cybercrime/octopus-interface-2019 (Accessed on November 22, 2020).

[266]Council of Europe. (March 10-11, 2019) "Octopus Interface Conference Cooperation Against Cybercrime" Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f25c3 (Accessed on November 22, 2020).

CHAPTER 4

MISSING ISSUES AND CRITICS

Even if the internet has no borders, we have legal boundaries. Even if the internet has the ability to reach other continents or countries and even if it has the ability to change its shape like social media, cryptocurrency, banking etc, we have only laws in our hands. Although it acts rapidly because of its nature, the procedures of prosecuting these crimes take remarkable time and energy both for LEA's and JA's. Therefore, like the internet does, to fight these crimes, states should be intercontinental actors. Being an intercontinental actor requires cooperation with other states and having a common legislative structure with them.

However, in practice, parties need much more. Any multinational service provider does not desire to be a haven of crime. To be a giant company and to protect their profit they first have to protect their users. In another case, these companies will lose their users and inevitably will lose their benefits. Using ICTs to commit any crime is getting popular for criminals especially those who aim to create unrest and uprising. By using the advantage of being anonymous, because they think they will never be caught, criminals damage the others, benefit from them and crime rates are rising day by day especially on some platforms used by vulnerable groups. Besides all these, users are prone to publish their even personal and private information on these platforms especially can be seen in fraud, hack, and impersonation cases.

In reality, the aim of the companies is not certainly to support any kinds of illegal actions. As expressed by Mark Zuckerberg after the Cambridge Analytica case during his testimony that "Facebook is an idealistic and optimistic company. For most of our existence, we focused on all of the good that connecting people … But it is clear now that we did not do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections and hate speech as well as developers and data privacy. We did not take a broad enough view

of our responsibility and that was a big mistake. It was my mistake and I am sorry. I started Facebook, I run it, and at the end of the day, I am responsible for what happens here… It is not enough just to connect people. We have to make sure those connections are positive. It is not enough to just give people a voice. We have to make sure that the voice is not used to harm other people or spread disinformation. It is not enough to just give people control over their information… Across the board, we have the responsibility not just to give people tools but to make sure those tools are used for good."[267]

As stated by the CEO of Facebook only giving control to people on their information stored ICTs is not enough to precautionary. Just we have seen during the Cambridge Analytica case stored information on these ICTs brings new advantages to criminals and by using this new generation of tools, they can even cause national and international disputes. In addition to all that, terms and conditions of the services prepared by these giant companies mostly can't be understood by netizens or sometimes they have never read by them and in some cases this is used by ICTs and other companies as an advantage to store private information or to get the permission of users at any time when they need.

Just for a simple example, a game company named GameStation added an article to its terms and conditions in order to control whether their customers read or not it. By approving it after April 1, 2010, 88% of the customers legally give their immortal soul to the company because they didn't read the text and so they couldn't see the article "you agree to grant Us a non-transferable option to claim, for now, and for evermore, your immortal soul".[268] Fortunately, this was only a gag. However, the case example shows us that as stressed by the CEO of Facebook only serving as a platform is not enough and to protect the customers and companies should do much more.

---

[267] YouTube. Global News, (April 18, 2018) Retrieved from: https://www.youtube.com/watch?v=YCQ_ZGxE2U4&ab_channel=GlobalNews 8Accessed December 1, 2020).

[268] FoxNews, (April 15, 2010), "7,500 Online Shoppers Unknowingly Sold Their Souls" Retrieved from: https://www.foxnews.com/tech/7500-online-shoppers-unknowingly-sold-their-souls (Accessed on December 1, 2020).

Here the words of Zuckerberg prove to us that the crimes, illegal actions and technical mistakes are also the responsibilities of these private companies. Because the main aim of the states is to protect citizens and provide a secure environment to them this is also the responsibility of the state with its units such as the Department of Justice and Department of Internal Affairs. This is a very complicated issue because the numbers of actors are equal with the number of internet users, ICTs, non-governmental organizations, and private and public entities and the number of actors is growing every passing day. Moreover, the already comprehensive issue turns much more complex one, when those turn into global problems. As neoliberal thinkers believe this inevitably leads states to cooperation.

According to the United Nations Report, which was published in 2019 large majority of cybercrimes, are committed by organized groups and in several cases, all the states in question have worked together.[269] During the fifth meeting of the UN expert group, it was handled by the participants that there is the need for dual criminality legislation on the admission of electronic evidence during criminal investigations and prosecuting.[270] Here UN's interpretation is very important because with 193 sovereign members the organization is the biggest example of cooperation. Additionally, because all the parties have equal representation it can be concluded that the things that had already been done by Convention on Cybercrime are seen as necessities by all the members.

Additionally, all the benefits and the advantages of the internet can be used by criminals to commit a crime. Here the point is very important that internet crimes are not related to only data interference, system interference, etc. It may cover so many things even homicide or suicide. A group of people may organize on a

[269] UNODC, (April 12, 2019). "Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019" Retrieved From: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Report/UNODC_CCPCJ_EG.4_2019_2_E.pdf (Accessed on December 2, 2020).

[270] UNODC, (April 4, 2018). "Expert Group to Conduct a Comprehensive Study on Cybercrime" Retrieved from: https://ccdcoe.org/uploads/2018/11/UN-180404-Expert_Group_to_Conduct_a_Comprehensive_Study_on_Cybercrime.pdf (Accessed on December 4, 2020).

Facebook group to kill someone or may use it to make terrorist propaganda. Except for that, criminals/suspects may use them for offenses against public peace. To provoke the public and to cause panic they may use those platforms. When Google's transparency report for the year 2020 was investigated, it will be seen that today all the countries fighting against criminals who publish fake or malicious content/s about COVID-19.[271] For example only in Turkey according to the Ministry of Justice report, in a week in March 2020, 1.745 accounts are investigated regarding fake news about COVID-19 and terrorist propaganda, the number of the detected accounts is 316.[272] Just in April 2020, 3.576 accounts related especially to the crimes, fake news (mostly about COVID 19) and provoking the public to hatred, hostility or degrading are investigated by the Turkish National Police Cybercrime Department, 616 of them detected and the number of prosecuted users was 229.[273] Except for that, terrorist organizations use social media to make propaganda and to recruit new members to the organization for long years. Between the time range from January 1 and August 14 the number of the investigated accounts by the Department 14.186 especially about terrorism propaganda.[274]

Except for these, criminals are also targeting especially the vulnerable groups of societies. A published report by World Health Organization shows that globally up to 1 billion children (from 02 to 17 years) are the victims of physical, sexual, or emotional violence and results of the works show that these crimes are

[271] Google, (2020). Google Transparency Report, Government Requests to Remove Content, Retrieved From: https://transparencyreport.google.com/government-removals/overview, (Accessed on December 10, 2020).

[272] The Republic of Turkey, Ministry of Internal Affairs, (April 23, 2020), "1748 Accounts That Sharing Unfounded Coronavirus News And Making Terrorist Propaganda On Social Media Were Detected". Retrieved From: https://www.icisleri.gov.tr/sosyal-medyada-asilsiz-koronavirus-paylasimlari-ve-teror-propagandasi-yapan-1748-hesap-tespit-edildi. (Accessed on December 10, 2020).

[273] The Republic of Turkey, Ministry of Internal Affairs, (April 6, 2020). "3,576 Social Media Accounts Examined 229 Persons Were Captured " Retrieved from: https://www.icisleri.gov.tr/3576-adet-sosyal-medya-hesabi-incelendi-229-sahis-yakalandi, (Accessed on December 10, 2020).

[274] The Republic of Turkey, Ministry of Internal Affairs , (August 14, 2020). "Turkish National Police Cybercrime Department Investigated 14.186 Social Media Accounts As Of January 1. " Retrieved from: https://www.icisleri.gov.tr/siber-suclarla-mucadele-daire-baskanligi-tarafindan-1-ocaktan-bugune-14186-hesap-hakkinda-calisma-yapildi , (Accessed on December 10, 2020).

"preventable".[275] To make it clear with numbers according to the report of the National Center for Missing and Exploited Children, just in 2019, 69.1 million CyberTipline reports were produced by ICTs which include child sexual abuse materials. When the company's statistics are investigated, it is seen that only Facebook supplied 15.884.511 reports to NCMEC. After Facebook, Google is the second supporter of the organization by submitting 449,283 reports while Microsoft is the third with its 123,839 reports.[276]

Besides all the benefits of ICTs, like facilitating communication, they sometimes also use to damage countries and internet users. Because states have to supply security, both real and virtual environments the cost of cybercrimes creates a burden on their economy. For instance, while the financial damage of internet crimes is rising, ICTs revenue rise. Namely, while the countries all around the world damages, companies benefitted not because of the crimes but because of the rising netizens. According to statistical research, social media companies' revenue is increasing every passing day. For example, in 2014 Facebook, the revenue of Facebook was 12,466 million dollars[277] but in 2019, the revenue of Facebook was 70,649 million dollars.[278] The amount for Google for the year 2019 was 161,8[279] moreover Apple is the first high tech company which was reached 1 trillion dollars in

[275] World Health Organization,(June 8, 2020), "Violence Against Children" , Retrieved from: https://www.who.int/news-room/fact-sheets/detail/violence-against-children, (Accessed on December 8, 2020).

[276] National Center For Missing & Exploited Children, (2020). "2019 Reports by Electronic Service Providers (ESP)" Retrieved from: https://www.missingkids.org/content/dam/missingkids/gethelp/2019-reports-by-esp.pdf (Accessed on December 8, 2020).

[277]Facebook Investor Relations, (2014) Facebook Reports Fourth Quarter and Full Year 2014 Results, Retrieved from: https://investor.fb.com/investor-news/press-release-details/2015/Facebook-Reports-Fourth-Quarter-and-Full-Year-2014-Results/default.aspx (Accessed on December 19, 2020).

[278] Facebook Investor Relations, (2019), Facebook Reports Fourth Quarter and Full Year 2019 Results Retrieved from: https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results/default.aspx (Accessed on December 19, 2020).

[279] Google Alphabet, (2019). Alphabet Announces Fourth Quarter and Fiscal Year 2019 Results Retrieved from: https://abc.xyz/investor/static/pdf/2019Q4_alphabet_earnings_release.pdf?cache=79552b8 (Accessed on December 20, 2020).

value in the world. Its revenue is bigger than the USA's annual economic deficit also exceeds the costs of several wars like the Vietnam War and the Iraq War. Comparing it with countries will make this argument more clear. Today Apple is richer than Switzerland, Saudi Arabia, Netherlands, Indonesia, and Mexico.[280] This power also makes companies "actors" in the international arena and without these hi-tech companies' cooperation on cybercrime is out of the question.

Raising the cost of cybercrime compels the states to find a solution but cybercrime is such an issue that without multinational effort and common legislation any of the players cannot escape from punishment. Here punishment means rising crimes, rising costs, rising mistrustful environment, violation of the law, and questioning of the role of states. The only solution for states to prevent their victimization was building international cooperation. As mentioned in previous parts there were several attempts to solve the problem but in the international arena the most successful one was Convention on Cybercrime and the convention is one of the best examples of neoliberal points of view to reach all win ideology.

Although the Convention on Cybercrime diminishes the spending time during the prosecution process and signed/ratified by 65 countries, supported by several organizations such as G7, OECD and EU, moreover its works and projects welcomed by several ICTs such as Microsoft, Apple, and Facebook, etc. there are normally legal and democratic disputes about it.

4.1. The Main Critics of Convention on Cybercrime

The direct relation between crime prevention/investigation and privacy has always been discussed with the spreading of the internet. The dispute has been raised and gains momentum with the proliferation of ICTs. Since the reasons are listed below the Convention on Cybercrime criticized by researchers regarding several issues.

[280] Investopedia, Kolakowski, M., (Jan 06, 2020). At $1.3 Trillion, Apple Is Bigger Than These Things, Retrieved from: https://www.investopedia.com/news/apple-now-bigger-these-5-things/ (Accessed on December 21, 2020).

The main criticism about Convention mostly focuses on 5 issues such as poorness in indicating violations about data protection rules[281] extending LEA's power without establishing detailed procedural safeguards[282] serving for benefit of predetermined countries[283] limiting structure on refusing to cooperate with foreign investigations[284] allowing LEA direct accessing to personal data stored abroad without ensuring compliance with the local data privacy standards[285] and unrepresentative structure of the Convention[286] and as a new criticism I would like to mention the failure of the Convention on finding solutions among some particular states and ICTs.

4.1.1. A nutshell review on mostly criticized issues

Disputes regarding data protection issues are very common with the claims that the Convention does not apply sanctions in the case of violation of data protection in its main articles.[287] But when the Convention's legal perspective is investigated it is seen that on the background of the Convention there are several regulations on the issue of personal data protection and LEA's authority.[288] For

[281] Huey, L., & Rosenberg, R. (2004). Watching the web: Thoughts on expanding police surveillance opportunities under the cyber-crime convention. *Canadian Journal of Criminology and Criminal Justice*, *46*(5), pp.597-606.

[282] Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (Eds.). (2007). *Cybercrime: digital cops in a networked environment* (Vol. 4). NYU Press. p 207-220

[283] Baron, R. M. (2001). A critique of the international cybercrime treaty. *CommLaw Conspectus*, *10*, pp.263-277

[284] Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (Eds.). (2007). *Cybercrime: digital cops in a networked environment* (Vol. 4). NYU Press. pp 207-220

[285] Tosoni, L. (2018). Rethinking Privacy in the Council of Europe's Convention on Cybercrime. *Computer Law & Security Review*, *34*(6), pp.1197-1214.

[286] Clough, J. (2012, December). The Council of Europe Convention on cybercrime: defining crime'in a digital world. In *Criminal Law Forum* (Vol. 23, No. 4, pp. 363-391). Springer Netherlands.

[287] Huey, L., & Rosenberg, R. (2004). Watching the web: Thoughts on expanding police surveillance opportunities under the cyber-crime convention. *Canadian Journal of Criminology and Criminal Justice*, *46*(5), pp.597-606

[288] Tosoni, L. (2018). Rethinking Privacy in the Council of Europe's Convention on Cybercrime. *Computer Law & Security Review*, *34*(6), pp.1197-1214.

example, the "Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (ETS108) has been ratified by 55 parties.[289] In addition, it must be kept in mind that not only the Convention but also parties' national law regulations have rules in their inner law to protect collected data.

While Article 18 of ETS 185 indicates the production order (submitting specified computer data in that person's possession or control) Article 19 indicates the search and seizure of stored computer data by authorities like law enforcement. This means that during an investigation law enforcement can seizures and investigates someone's computer or mobile devices. Here to protect data Article 16 covers the protection of computer data and Article 17 covers the protection of traffic data.[290] Namely as indicated by the main text of the Convention during any investigation while the seizure of any data, parties should protect them from any loss, harm or modification.

According to Kozlovski the new types of crimes and the current techniques used by law enforcement to monitoring, controlling, deterring, detecting or preventing, supply a very huge ability to law enforcement. Again, according to him when internet users accept the terms and conditions of ICTs, they also allow that their information can be shared by these companies with LEAs. He criticizes that while laws guarantee personal privacy, by using prosecuting techniques LEA reaches the stored information of users even when there is no violation. According to him, this means that technology failed to hold policy accountable and transparent. During investigations, the police may use prosecutor/court order far from the main aim and can change the nature of the investigation. To prevent that, the investigation should

[289] Council of Europe, Chart of signatures and ratifications of Treaty 108, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=z2ZXeB2v (Accessed on December 24, 2020)

[290] Council of Europe, (November 13, 2001). Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on December 24, 2020).

be conducted in an accountable and transparent way.[291] Keeping limited the investigative power of LEA via conditions and safeguards is always defended by the CoE.[292]

To prevent that possibility, several international agreements pursuant to human rights were accepted by the Convention and the Convention declared its acceptance in the preamble section. Again "Recommendation No. R (87) 15" and Recommendations No R (95) 13 regulate data protection issues and draws a strict line with the power of LEA.[293] Additionally Convention on Cybercrime's Article 15 handles the issue compels the parties to protect human rights, to supply the principle of proportionality.[294]

All in all, ETS 108[295], ECHR[296] (article 8), ICCPR[297] (Article 17), Committee of Ministers Recommendations No R (87) 15[298], Committee of Ministers

[291] Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (Eds.). (2007). *Cybercrime: digital cops in a networked environment* (Vol. 4). NYU Press. pp 207-220

[292] Council of Europe, (November 1, 2013), Retrieved from: https://rm.coe.int/16802fa3e6 (Accessed on December 30, 2020).

[293] Tosoni, L. (2018). Rethinking Privacy in the Council of Europe's Convention on Cybercrime. *Computer Law & Security Review*, *34*(6), pp.1197-1214.

[294] Council of Europe, (November 13, 2001). Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on January 01,2021).

[295] Council of Europe, Chart of signatures and ratifications of Treaty 108 Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=a4fxO1c5 (total ratifications 55) (Accessed on January 01, 2020).

[296] Council of Europe, Chart of signatures and ratifications of Treaty 005, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=a4fxO1c5 (total ratifications 47) (Accessed on January 2, 2021).

[297] Council of Europe, The international covenant on civil and political rights, Retrieved from: https://www.coe.int/en/web/compass/the-international-covenant-on-civil-and-political-rights (total ratification 173 states.) (Accessed on January 2, 2021).

[298] Council of Europe, (September 17, 1987)., Committee of ministers explanatory memorandum to recommendation no. R (87) 15 Retrieved from: https://rm.coe.int/168062dfd4 (Accessed on January 3, 2021).

Recommendations No R (95) 13[299] indicates data protection issue has already been on the agenda of the Convention. Pursuant to all the regulations LEA can reach personal information in four necessities. Those are; a. legality and lawfulness b. legitimate aim c. necessity and lastly proportionality.[300]

As stressed by Baron the first draft agenda of the Convention did not mention human rights but the council noted human rights later. Baron claims that human rights may not remarkable issue for the persons who prepared it. He also criticizes it by alleging that it works dedicated to the benefit of predetermined countries and he claims that the real aim of the Convention is to complete some current blanks in western countries' law system. It was planned to increase western governments' effects by accepted unilateral procedures and lastly, he claimed all the signatory countries would be a new area to collect evidence for western countries.[301]

However, investigating and prosecuting cybercrime requires a variety of networks, such as networks between police and private sector (LEA-ICT), networks between judicial authorities and private sectors (JA-ICT), networks between police and other police organizations (LEA-LEA) etc. Namely, multi-layered cooperation is needed. Not for the benefit of some strict countries but for several organizations. So seeing the Convention as a tool of predominant countries will be a wrong identification because all parties have mutual benefits and cooperate with ICTs. Absolute meaningful differences can be observed among countries but expecting equality among them is impossible because of the fact that the numbers of cybercrimes are not the same for countries.

---

[299] Council of Europe, (September 11, 1995). Recommendation no. R (95) 13 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 (Accessed on January 3, 2021).

[300] Tosoni, L. (2018). Rethinking Privacy in the Council of Europe's Convention on Cybercrime. *Computer Law & Security Review*, *34*(6),p. 1197-1214.

[301] Baron, R. M. (2001). A critique of the international cybercrime treaty. *CommLaw Conspectus*, *10*, p.263-277

When it comes to limits on refusing cooperation, according to proponents of the Convention cooperation can be a matter only on the dual criminality.[302] Convention also gives the right to states that refuse to cooperate with Articles 25 and 27. For example, according to Article 27 parties can refuse cooperation if the investigation in question involves a political offense. In addition, states/ICTs can refuse information requests if supplying and submitting the information threatens national security and sovereignty.[303]

It is observed by cooperation theorists that if states interact constantly on a specific issue like cybercrime the situation Tit For Tat emerged. (If you help me, I will help you, if you assist me on investigations I will assist just like the same.) In Tit For Tat situation future interactions diminishes the possibility of cheating.[304] Therefore, because states know as long as they assist the other, the other one is going to assist it too. Thus, except for investigations indicated above, (such as political offense and national security if submitting of information threat national security and sovereignty) states are more prone to cooperation to prevent punishment. (Here punishment means cannot find assistance on investigations.)

When we investigate the fourth criticism because all the parties of the Convention have data protection and privacy legislation within the context of the Convention without laws indicated by the countries legislation, direct access is impossible. According to the United Nations Conference on Trade and Development (UNCTAD) all around the world, 132 out of 194 countries have legislation about the protection of data and privacy. Globally the rates of the countries with complete legislation are 66%, countries with draft legislation 10%, and countries with no

---

[302] Clough, J. (2012, December). The Council of Europe Convention on cybercrime: defining crime' in a digital world. In *Criminal Law Forum* (Vol. 23, No. 4, p. 363-391). Springer Netherlands.

[303] Council of Europe, (November 13, 2001). Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on January 01,2021).

[304] Fearon, J. D. (1998). Bargaining, enforcement, and international cooperation. *International organization*, *52*(2), pp.269-305.

legislation 19%.[305] When the signed and ratified countries were investigated, all of them without any exception have personal data privacy legislation in their legislation system. Therefore, for LEAs without legal permission accessing any kind of data is out of the question.

Additionally, as stressed above 55 of 65 member states also signed and ratified the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" with reference to ETS 108. With ETS 108 all parties accept that producing personal data should be legal and only on the specific conditions the data can be transferred across national borders.[306]

Moreover to prevent compelling ICTs by states Stored Communications Act' (hereinafter SCA) was approved. SCA also protects ICTs from producing content data or traffic data and brings strict rules. For example, Article 18 U.S. Code § 2702 gives permission to agencies' disclosure of data to some extent especially in the condition of emergency with the articles b/8, c/4.[307] Also, article 2703 mentions about disclosure of data when a court needs information. According to the article any company can supply info to a law enforcement agency when a proper court order, search warrant or prosecutor order is supplied to them. Especially, section c/2 explains the extent of the information that can be shared and preserved.[308] Also, the

[305] UNCTAD, (April 2, 2020). Data Protection and Privacy Legislation Worldwide Retrieved from: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (Accessed on January 4, 2021).

[306] Council of Europe, (January 28, 1981), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 (Accessed on January 04, 2021).

[307] Cornell Law School, 18 U.S. Code § 2702 - Voluntary disclosure of customer communications or records, Retrieved from: https://www.law.cornell.edu/uscode/text/18/2702 (Accessed on January 04, 2021).

[308] Cornell Law School, 18 U.S. Code § 2703 - Required disclosure of customer communications or records Retrieved from: https://www.law.cornell.edu/uscode/text/18/2703 (Accessed on January 04, 2021).

18 U.S. Code § 2705 regarding delay notice to the customer, aims to protect stored data so that LEA can reach it before it is altered or deleted by suspect/s.[309]

The combination of all rules proves to us that the requester party first has to base the information request on its local rules and after that, to supply needed information ICTs have to obey SCA rules. This may look so hard and complicated but to protect personal privacy and to protect human rights this is needed.

According to the ITU, Convention on Cybercrime has a limited structure and the impact of the Convention can not be measured only by the number of signatory states.[310] Skeptics also touch on the same issue and according to them the countries that are signed the agreement are not the problematic ones. Cybercrimes like hacking or damaging the systems and computers via viruses mostly come from Russia, China, Vietnam or North Korea and the creator of the "I love You" virus is never prosecuted because of legal border problems.[311] Criticism about the representation problem is one of the most touched issues. Even if the Convention is well known by the international community, compared to the UN, the ratification number is highly low.[312] Especially the absence of some countries such as Russia, China, Brazil, and India is often criticized because of the fact that the number of cybercrime, cybercriminals and cyberattacks are remarkably high in these countries.[313]

---

[309] Cornell Law School, 18 U.S. Code § 2705 - Delayed notice, Retrieved from: https://www.law.cornell.edu/uscode/text/18/2705 (Accessed on January 04, 2021)

[310] International Telecommunication Union, (November 2014). Understanding cybercrime phenomena challenges and legal response, Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf (Accessed on January 5, 2021).

[311] Archick, K., & Foreign Affairs, Defense, and Trade Division. (2005). Cybercrime: The council of Europe convention. Congressional Research Service, Library of Congress.

[312] Clough, J. (2012, December). The Council of Europe Convention on cybercrime: defining crime' in a digital world. In *Criminal Law Forum* (Vol. 23, No. 4, pp. 363-391). Springer Netherlands.

[313] Vatis, M. A. (2010, June). The Council of Europe Convention on Cybercrime. In *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy http://www. nap. edu/catalog/12997.html. p 219-220*

The Council of Europe's works and Convention on Cybercrime are open to all the countries both the members and non-member states. It is seen that with invitations and projects Council of Europe tries to increase parties too. This is also necessary because those are fighting against global extended crimes. Overall, when the signatory countries are investigated although they are mostly located in Europe, the Convention has parties from all around the world and all the continents. The parties from the Asia region such as Japan or Pakistan have highly important cooperative relations with Facebook and Apple etc.

When time goes on because different and new needs came to the agenda some issues indicated in the Convention became discussable. Today there are three kinds of hacking and they resemble hat colors. Black hat hackers exploit systems and benefited from them, grey hat hackers are a combination of white and black versions and while they exploiting a system they generally inform the companies or public sector regarding exigencies. Lastly, white ones today also known as ethical hackers or IT guys work with organizations. Like black and grey hats they exploit the system to find a backdoor so that companies fix it.[314] However, either this or that way they exploit the system and it is accepted as a crime in the Convention. If we run with this ideology, all ethical hackers are criminals. So some regulations are needed on the Convention.

For example, Apple announced that it will give a prize, up to 200,000 dollars, to a person who finds a security vulnerability in the Apple system.[315] This call in the literature as Bug Bounty and several companies support this, to prevent any damage in their system. When we look at the case from the perception of the Convention all the people who try to fix the system's default are criminals because they illegally access the systems and several companies like Apple supports persons who violate the rules.

---

[314]EC-Council, (November 2020), Retrieved from: https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/ (Accessed on January 05, 2021).

[315] The Guardian, (August 12, 2019), Bug bounty': Apple to pay hackers more than $1m to find security flaws, Retrieved from: https://www.theguardian.com/technology/2019/aug/12/apple-hackers-black-hat-conference (Accessed on January 07, 2021).

In addition, some companies leave alone the ethical hacker after they used them. A case about that happened in Hungary. According to the news, an ethical hacker found some mistakes in the system at the beginning although the company supports the hacker's action it reported that as illegal activity and the prosecutor asked fine about the hacker here there is a dilemma. But in the end, instead of prison, he is fined to pay 600,000 HUF (1,996,75 dollars).[316]

Some providers especially located in the USA region can supply direct information to requested countries where they are offering services even if the request comes from a different jurisdiction. We call this "voluntary cooperation" and in such requests, providers can decide on whether the request in question is lawful or not. ICTs such as Apple, Microsoft and Facebook receive a huge amount of information requests from different jurisdictions so direct cooperation is getting important.[317] However, cooperation is based on free will and knowing the ICTs restrictions and structures is important for LEAs.

To make cooperation more effective firstly LEAs should understand the business model of ICTs and should know what kinds of data can be available or not. Secondly building a trusted relationship between ICTs and LEAs depends on the quality of requests. Thirdly, it should be accepted that because cooperation is based on free will if an ICT receives an information request from a country with a poor human rights record, it could reject and advise to use the MLAT process.[318]

In some cases, LEAs try to compel ICTs to take the needed information from them. Even there are examples of illegal demands. For example, crime prevention

[316] Hungary Today, (July 12, 2019), Kaszás, F., Instead of jail time, ethical hacker fined for exposing vulnerability in telekom's system Retrieved from: https://hungarytoday.hu/instead-of-jail-time-ethical-hacker-fined-for-exposing-vulnerability-in-telekoms-system/ (Accessed on January 07, 2021).

[317] Council of Europe, (February 17, 2016), Cloud evidence group, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8 (Accessed on January 07, 2021).

[318] Council of Europe, (August 30, 2017), Study on Strategy of Cooperation with Multinational Service Providers, Retrieved from: https://rm.coe.int/09000016808f1e16 (Accessed on January 07, 2021).

controls in the USA reshaped changed drastically and turn freakiness in time after the 9/11 attack. On December 02, 2015, another terrorist attack happened in the USA, California's San Bernardino region. 14 people lost their lives and 22 people were injured.[319] After the disaster's following days FBI asks help for from Apple to investigate the suspect's mobile phone. During the investigation, Apple published a letter claiming that they have no sympathy for terrorists and they did whatever they can to help the FBI with the investigation. In the message published by Apple for its customers, Apple complained the FBI to the world because the agency demand installing a backdoor to the iPhone and last words of Apple was "While we believe the FBI's intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect. "[320] the Apple case is one of the best examples that LEAs forces companies to obtain information.

Because cybercrimes are hi-tech crimes, findings and following tracks left by criminals are difficult for LEA and this causes the need for expertise in the private sector or academia. They need timeless cooperation with companies. Because online crimes happen at any time of the day police have to work and have to be ready at any time and have to make online patrols to prevent any undesirable results.[321]

Additionally as reported by LEA, the other problem of the organization is that because of personal data privacy issues companies warn their users and informs them regarding the ongoing investigation. In this situation, suspects or those who violate the law can damage evidence, can delete their accounts, or destroy their tools. Also as a part of personal privacy issues while warning the suspects' companies supply detailed information to the suspects about LEA such as name, agency, rank, position,

---

[319] Wikipedia, 2015 San Bernardino attack, Retrieved from: https://en.wikipedia.org/wiki/2015_San_Bernardino_attack Accessed on January 8, 2021.

[320] Apple, (February 16, 2016), A message to our customers, Retrieved from: https://www.apple.com/customer-letter/ (Accessed on January 8, 2021).

[321] Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*. 29(2) : pp. 408-433

email address, and location information. In some cases, investigations may be related to terrorist organizations, and to protect their agencies ICTs disclose LEAs information.[322] Although the requester LEA can ask the ICT to keep the investigation confidential, this causes wasting the time of LEAs and JAs.

In addition to all problems and disputes about the Convention on Cybercrime and along with that, in addition to all the problems among LEAs, JAs, ICTs when the transparency reports which are regularly publishing by ICTs investigated it has been found that currently there are disputes among states and some ICTs. It seems that the Council of Europe and the Convention's endeavor is not enough to solve that problem.

Although the problems among states and ICTs have been tried to solve by the Convention's Article 18 (production order) and with the capacity building works within the framework of Council of Europe, with the supports both other international/regional organizations and companies it seems that all the works are not enough in reality.

Moreover, even though the TCY committee touched on the problem several times and supplied a series of training about the issue they could not solve the problem in an efficient way. Surely when the numbers of requests were investigated as of 2014, there are remarkable improvements in the relations of ICTs and LEA. (except for some ICTs.) The problematic companies investigated, especially like Twitter and Yahoo, we will realize that the companies either have never joined the capacity building works or were join only one of them. For example, Twitter has never joined Octopus and Yahoo was joined only one meeting in 2009. This is not absolutely can be the only one reason but as indicated in the previous part joint works are very important to improve cooperation among stakeholders and the case examples show that although the organization collects nearly half of the world it has

[322] Council of Europe, (August 30, 2017), Study on Strategy of Cooperation with Multinational Service Providers, Retrieved from: https://rm.coe.int/study-on-strategy-of-cooperation-with-multinational-service-providers/16808f1e16 (Accessed on January 8, 2021).

failed to catch some companies and also has failed to solve disputes among some particular countries and ICTs.

In order to make the argument visible, investigating transparency reports of some companies will be beneficial. The tables shared below show the most information requested countries. The countries were restricted with the first ten requesters for the period only 2019. In addition, the first column shows the name of countries second column is shared their total request numbers and the last one shows compliance rates respectively. In addition, because these companies share transparency reports two times in a year, the term which covers the time range January and Jun named H1, and the last term which covers July and December named H2. (* means not a party of Convention on Cybercrime)

4.1.2. Twitter

Table 4. 1. Twitter transparency report.[323]

January Jun 2019 (H1)		
Country	Total Request	Compliance
USA	2120	71 %
Japan	1742	52 %
UK	658	67 %
France	549	56 %
India*	474	5 %
Germany	458	18 %
Turkey	350	0 %
Spain	150	33 %
Korea*	132	32 %
Brazil	105	10 %

July December 2019 (H2)		
Country	Total Request	Compliance
USA	2271	62 %
Japan	1961	45 %
France	1057	66 %
India*	789	2 %
Korea*	484	30 %
Turkey	478	0 %
UK	433	51 %
Germany	400	19 %
Spain	107	20 %
Poland	91	1 %

[323] Twitter, Transparency, Retrieved from: https://transparency.twitter.com/ (Accessed on February 01, 2021).

As shared by Twitter, during the term H1 the company received 5822 regular information requests, the number of emergency requests is 1478. Disclosed information rate for the regular request is 47,6% this rate for emergencies is 46,4% namely total disclosure rate for the term H1 is 47%.[324]

Additionally, for the term, H2 total regular information requests are 6952 the compliances of these requests 45,2%. When it comes to an emergency, Twitter received 1867 emergency requests and the compliance rates of these requests are 22.8% namely global compliance rate is 40%.[325]

When the numbers are evaluated it is seen that although Turkey tries to fight against criminals and shows a high endeavor to make Twitter's environment safer Twitter does not respond to the requests made by Turkish authorities. Nonsense, Twitter does not support investigations of some countries except for a few like Germany, France, Japan or South Korea and absolutely the USA. When the numbers are evaluated, it is also seen that the most requested countries are located in some specific locations. Those are North America, Asia Pacific, and Western Europe mostly. The only country from the Middle East Region is Turkey.

When the comprehensiveness of cybercrimes is considered, the conclusion that can be drawn here is that Twitter does not support several countries to fight against criminals and it is a haven for those who violate the law. Those requests made by Turkey, India, Brazil, Poland or even the USA etc. may be related to child exploitation, sexual harassment or even may be related to any possible suicide or terrorist attack. Moreover, we have an example with the John Doe case. According to the news published by Newyorkpost, Twitter refused to remove an improper video of

---

[324] Twitter, Transparency, Information requests, Retrieved from: https://transparency.twitter.com/en/reports/information-requests.html#2019-jan-jun (Accessed on January 10, 2021).

[325] Twitter, Transparency, Information Requests, Retrieved from: https://transparency.twitter.com/en/reports/information-requests.html#2019-jul-dec (Accessed on January 10, 2021).

the child, which was recorded without the knowledge and consent of the victim when he was only 13 years old.[326]

It seems that if all these huge amounts of crimes are not happening in certain countries/locations, those are not important to deserve Twitter's attention.

4.1.3. Facebook

Table 4. 2. Facebook transparency report.[327]

January Jun 2019 (H1)		
Country	Total Request	Compliance
USA	50741	88 %
India*	22684	54 %
UK	3397	90 %
Germany	7302	58 %
France	5782	70 %
Brazil	5683	67 %
Italy	2547	61 %
Mexico*	2337	69 %
Turkey	2060	73 %
Pakistan*	1849	51 %

July December 2019 (H2)		
Country	Total Request	Compliance
USA	51121	88 %
India*	26698	57 %
UK	8378	88 %
Germany	8013	63 %
France	7001	83 %
Brazil	6549	66 %
Poland	4688	63 %
Turkey	4306	79 %
Italy	2466	65 %
Mexico*	2153	59 %

When the statistics of Twitter and Facebook are evaluated, while Twitter's statistics show a meaningful difference, Facebook's statistics are more homogenous. Compliance rates show similarities and most importantly, countries which are reported crimes to the company are supported to some degree. While Turkey's

[326] NewYorkPost, Twitter refused to remove child porn because it didn't 'violate policies': lawsuit, Retrieved from: https://nypost.com/2021/01/21/twitter-sued-for-allegedly-refusing-to-remove-child-porn/ (Accessed on July 18, 2021)

[327] Facebook, Transparency, Retrieved from: https://transparency.facebook.com/ (Accessed on February 01, 2021).

requests have been totally and completely rejected by Twitter interestingly, the county has one of the higher compliance rates in the global extend and has efficient relation with Facebook. The world statistics investigated and evaluated during the H1 Turkey has the 3rd compliance rate. This also means that the crimes reported by Turkey's requester authorities at the same time were accepted as a violation of the law by the USA because Facebook is located in the jurisdiction of that country. From there, it can be alleged that there is a democratic dilemma. Moreover, when the second term, H2 investigated Turkey similarly among the top 10 countries which are fighting against criminals and again it has the 3rd compliance rate.

During the term H1, received regular information requests numbers by Facebook are 116,4 K and the total number of emergency requests 12.2 K. Facebook responded to these requests with compliance rates respectively 73,7% and 70,10 %.[328] Also during the second term, H2, the company totally received 140,878 requests the compliance rate for regular requests was 74,5% and the rate for emergencies was 73,7%.[329]

By using these numbers, it can be alleged that because there is a more homogenous frequency among the Top 10 requested countries Facebook has a much more objective structure compared to Twitter and supports countries and LEAs more equally than Twitter to make Facebook's environment safer.

[328] Facebook, Transparency, Government requests for user data, Retrieved from: https://transparency.facebook.com/government-data-requests/jan-jun-2019 (Accessed on January 10, 2021).

[329] Facebook, Transparency, Government requests for user data, Retrieved from: https://transparency.facebook.com/government-data-requests/jul-dec-2019 (Accessed on January 10, 2021).

4.1.4. Verizon media/YAHOO!

Table 4. 3. VerizonMedia transparency report.[330]

January Jun 2019 (H1)		
Country	Total Request	Compliance
USA	6341	81 %
Germany	1287	29 %
Taiwan*	1011	84 %
UK	873	59 %
India*	629	47 %
France	523	52 %
Brazil*	216	71 %
Australia	212	42 %
Italy	189	16 %
Spain	98	17 %

July December 2019 (H2)		
Country	Total Request	Compliance
USA	5807	78 %
Germany	1385	25 %
Taiwan*	1175	83 %
UK	1107	48 %
India*	696	40 %
France	623	46 %
Australia	250	72 %
Brazil*	196	55 %
Italy	153	19 %
Singapore*	120	34 %

When we focus on YAHOO's statistics, it is seen that like Twitter it has complicated numbers while it supports the investigations in the USA, Taiwan and Brazil its attitude shows meaningful differences from a country to another. YAHOO publishes its transparency report as of 2017 and all of them are available on its web page. When the numbers are investigated just like Twitter there are incredible differences. For example, as of 2017, Korea, Sweden, Poland, Romania, Lithuania, Netherlands and Malta have never received any response to their information requests. Another example the countries Turkey, Austria, Switzerland, Greece, Japan, and Norway could receive only one response to their request for 3 years. (for all the terms and years[331])

[330] VerizonMedia, Transparency, Retrieved from: https://www.verizonmedia.com/transparency/index.html (Accessed on February 01, 2021).

[331] Verizonmedia, Government Data Requests, Retrieved from: https://www.verizonmedia.com/transparency/reports/government-data-requests.html (Accessed on 10, 2021).

In addition, when we take a gaze at the tables shared above the orders of the top 10 requested countries have very similar structure just one exception on the term H2 with Singapore.

When the relation between Turkey and YAHOO was investigated, in 2017's H1 term Turkey totally made 3 requests and asked for information about 4 YAHOO accounts. YAHOO disclosed only one of them and supplied information about only one account and the other 3 accounts' requests were rejected. After then although Turkey obeys international law and create legal court order or prosecutor order and submit them legally as indicated on Convention on Cybercrime it's all requests rejected.

According to YAHOO's transparency report the company received 11,677 K information requests during the term H1 and the compliance rate of the received demands explained as 67% and these numbers for the second half respectively 11,868K with the compliance rate 61,70%.

4.1.5. Google

Table 4. 4. Google transparency report.[332]

January Jun 2019 (H1)			July December 2019 (H2)		
Country	Total Request	Compliance	Country	Total Request	Compliance
USA	26964	82 %	USA	26186	83 %
Germany	10011	68 %	Germany	11160	70 %
India *	8547	63 %	India*	10891	62 %
France	6777	79 %	France	7405	81 %
UK	4645	84 %	UK	5954	81 %
Brazil*	2961	61 %	Brazil*	3606	64 %
Australia	2367	83 %	Australia	2009	88 %
Spain	1618	59 %	Poland	1881	60 %
Italy	1509	47 %	Spain	1538	61 %
Poland	1409	52 %	Italy	1486	50 %

[332] Google, Transparency, Retrieved from: https://transparencyreport.google.com/?hl=tr (Accessed on February 01, 2021).

When we focus on Google's numbers and when we compare the two tables, it is easy to observe that there is a clear order among the top 10 requested countries. Firstly, in all two tables finding a different country is impossible. "This means that cybercrimes occur in all these countries with an order!" However, absolutely this is not possible. The only mindful answer can be that "Google has highly good cooperation with some specific countries" to support this argumentation again Turkey's rate is important.

During the term, H1 Turkey made 526 information requests and Google did not supply even once a positive answer.[333] Moreover for the second term, H2, Turkey made 499 information requests to the company not surprisingly Google did not answer any of them.[334] For the cases regarding the imminent risk of death/suicide or terrorist activity during the term H1 Turkey made 4 emergency disclosure requests and Google supplied only two of them[335] when it comes to the second term Turkey made two times more requests, and Google answered only 3 of them.[336] When the numbers are compared with global compliance rates of all requested countries, they are seriously low. Because for the first term, the global compliance rate was 73% and for the second term, the rate was 74%[337] while Turkey's respectively were 0% and 1%.

[333] Google, Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=series:requests,accounts;authority:TR;time:Y2019H1&lu=user_requests_report_period (Accessed on January 11, 2021).

[334] Google, Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=series:requests,accounts,compliance;authority:TR;time:Y2019H2&lu=user_requests_report_period (Accessed on January 11, 2021).

[335] Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=series:requests,accounts;authority:TR;time:Y2019H1&lu=user_requests_report_period (Accessed on January 12, 2021).

[336] Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=series:requests,accounts,compliance;authority:TR;time:Y2019H2&lu=user_requests_report_period (Accessed on January 12, 2021).

[337] Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr (Accessed on January 13, 2021).

To make much clearer the circumstance Russia's rate is much higher than Turkey's. Its answered request rates are for H1 15% and H2 23%.[338] When it comes to China the countries last information request is shown in H1/2014 with 2 requests 50% compliance rate.[339] Just like Turkey, Bulgaria also suffers from the attitude of Google for H1 the country's compliance rate is 0 and for H2 Bulgarian authorities made 4 requests only two of them positively answered.[340] Compared to other countries Turkey's rates are similar to Iran[341], Moldova[342], Thailand[343], and Hungary[344] because all of them are 0 % of all the terms except for scarcely amount of emergencies.

[338] Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=authority:&lu=user_data_produced&user_data_produced=authority:RU;series:compliance (Accessed on January 13, 2021).

[339] Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=authority:&lu=user_data_produced&user_data_produced=authority:CN;series:compliance (Accessed on January 13, 2021).

[340] Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=authority:&lu=user_data_produced&user_data_produced=authority:BG;series:compliance (Accessed on January 13, 2021).

[341] Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_data_produced=authority:IR;series:compliance&lu=user_data_produced (Accessed on January 13, 2021).

[342] Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_data_produced=authority:MD;series:compliance&lu=user_data_produced (Accessed on January 13, 2021).

[343] Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_data_produced=authority:TH;series:compliance&lu=user_data_produced (Accessed on January 13, 2021).

[344] Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_data_produced=authority:HU;series:compliance&lu=user_data_produced (Accessed on January 13, 2021).

4.1.6. Microsoft

Table 4. 5. Microsoft transparency report.[345]

January Jun 2019 (H1)		
Country	Total Request	Compliance
USA	4860	54 %
Germany	3774	59 %
France	3656	41 %
UK	3011	71 %
Brazil*	1278	30 %
Turkey	1190	31 %
Australia	887	72 %
Spain	693	33 %
Italy	479	31 %
India*	458	49 %

July December 2019 (H2)		
Country	Total Request	Compliance
USA	4315	55 %
UK	3312	74 %
Germany	3310	62 %
France	2470	58 %
Brazil*	1162	45 %
Turkey	1159	67 %
Australia	898	71 %
India*	604	35 %
Argentina	544	69 %
Spain	525	38 %

During the term H1, Microsoft globally received 24,175 information requests and it positively responded to the request with the degree 53% the company supplied content data to some countries to support ongoing investigations with the rate of 5%. In some cases because of technical issues or because users delete the account which has been used by suspects during the violation of law the rate of no data found request is 14% rejected request rate is 26% namely totally of 6469 requests were rejected by the company.[346]

[345] Microsoft, Transparency, Retrieved from: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (Accessed on February 01, 2021).

[346] Microsoft Corporate Social Responsibility, Law Enforcement Requests Reports, Retrieved from: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (Accessed on January 15, 2021).

For the second term, the total numbers of received requests by Microsoft are 21,781K and the global compliance rate is 58 %. While the rejected request rate is 20% total rate of which no data found is 15 %.[347]

When the top requested ten countries investigated for the two terms it can be seen that there are some differences among countries this means that Microsoft has a relatively open structure. For the first term, Italy receives attention and for the second term, Argentina joins the list. When Turkey's numbers were investigated, it is obvious that compared to the H1 time interval the country reached a significant compliance rate for H2 and raised its compliance rate from 31% to 67%. Moreover, for the H1 term of 2020s compliance rates with the degree 73%[348] show us that Turkey is decisively fighting against cybercrimes and cooperates with ICTs to supply a secure virtual environment.

However, things are not the same for some countries such as China, Russia, Moldova, Slovakia and Bulgaria the countries' relations with Microsoft are not cooperative although some of the members of the Convention and joined cooperation works and capacity building efforts of the organization.

The differences among the companies can be explained only by subjective reasons because while the investigations of Turkey supported by Facebook, Microsoft (especially email service) and Apple (especially for financial information investigations Turkey supported by Apple with a high compliance rate for all the two terms Turkey is the 7th country with the 65% compliance rate[349]) with the high

[347]Microsoft Corporate Social Responsibility, Law Enforcement Requests Reports, Retrieved from: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (Accessed on January 15, 2021).

[348] Microsoft Corporate Social Responsibility, Law Enforcement Requests Reports, Retrieved from: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (Accessed on January 15, 2021).

[349] Apple, Transparency, Financial Identifier Requests, Retrieved from: https://www.apple.com/legal/transparency/financial-identifier.html (Accessed on January 15, 2020).

compliance rate although they are located in just the same jurisdiction Twitter, Google and Yahoo have never supported the investigations in Turkey.

Child exploitation is accepted as an emergency issue by several countries and to supply the security of children with the supports of the INHOPE Foundation, all around the world totally 48 hotline services established. Despite all the works of the INHOPE and all the supports of the IWF, today total of 149 countries has not hotline to combat internet facilitated CSAM. However, when it comes to Turkey, the country is one of the 48 countries in the world having a hotline called "Ihbar Web" within the scope of the Information and Communication Technologies Authority. As of 2007, the hotline received almost one million reports regarding prohibited materials, nearly 45.000 of which were concerning CSCAM. For example, only in the year 2014, the number of reports was 9.000.[350] According to NCMEC, the numbers of child exploitation materials on the internet are rising every passing day. Only between the years 2014 and 2015 the numbers of reports increased by 90 %. Again compared to 2014 the sextortion reports were raised up to 150 %. The results of sextortion are fear, anxiety, hopelessness, and depression in children. Even as indicated by 13 % CyberTipline reports, about 1 in 3 of victims had engaged in self-harm or suicide.[351] In addition, as expressed by NCMEC, the Internet companies are the most frequent reporters to the CyberTipline with the rate of 71%.[352]

In 2019, NCMEC helped families and law enforcement agencies with more than 29,000 cases of missing children. As stated earlier, CyberTipline received more

[350] National Center for Missing & Exploited Children, (2016), Global Research Project: A Global Landscape of Hotlines Combating Child Sexual Abuse Material on the Internet and an Assessment of Shared Challenges, Retrieved From: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/grp.pdf (Accessed on December 10, 2020).

[351] National Center for Missing & Exploited Children, (2015), Trends identified in CyberTipline sextortion reports https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf (Accessed on December 10, 2020).

[352] National Center for Missing & Exploited Children , (2017), The Online Enticement of Children: An In-Depth Analysis of CyberTipline Reports https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel1.pdf , (Accessed on December 10, 2020).

than 16.9 million reports in 2019.[353] When the reports sent by ICTs to NCMEC CyberTipline were examined, it was seen that Facebook sent 15,884,511 reports, the total case reported by Google were 449,283 and this number for Microsoft were 123,839, while Twitter reported only 45,726 cases.[354]

These numbers show us that criminals are using ICTs platforms not only to get in touch or communicate but also to benefit from the vulnerable groups. Child exploitation numbers are used here to illuminate only one type of crime. If we could investigate the other crimes, I am sure that the numbers would have been more devastating. The number of reports produced by Twitter shows that this crime is common all around the world. While it's so common type of crime worldwide, is it possible for Turkey to refrain from that problem? While Google reports 449,283 cases, because of the compliance rate of Turkey, can we understand from the situation that "no one of them was not regarding violation of law"?

According to Twitter Inc. The mission of Twitter is "… give everyone the power to create and share ideas and information instantly without barriers. Our business and revenue will always follow that mission in ways that improve and do not detract from a free and global conversation."[355] Controversially, just for the term January-July 2019, Twitter received 7.3 K information requests and the total compliance rate was only 47.3 %. When it comes to Turkey for the same term, the total information request number was 350 with 0 % compliance rate.[356] Is that mean

[353] National Center for Missing & Exploited Children , About NCMEC, https://www.missingkids.org/footer/media/keyfacts (Accessed on December, 10, 2020).

[354] National Center for Missing & Exploited Children, (2020), 2019 Reports by Electronic Service Providers (ESP) https://www.missingkids.org/content/dam/missingkids/gethelp/2019-reports-by-esp.pdf (Accessed on December 10, 2020).

[355] Twitter, FAQ, Retrieved from: https://investor.twitterinc.com/contact/faq/default.aspx , (Accessed on December 11, 2020).

[356] Twitter, Transparency Report, Information Requests, https://transparency.twitter.com/en/reports/information-requests.html#2019-jan-jun (Accessed on December 11, 2020).

none of the reported contents relate to child exploitation or not violates human rights? Are that Turkish authorities completely wrong for all 350 cases?

Political contents are one of the always discussed issues by states. During the last election, several people published content against the political structure of the USA. This caused disputes in that country. For example, the contents published by the New York Post on Twitter about Joe Biden's son were removed by that company for the reason that the published materials were captured illegally and because of the reason, these contents violate its platform's terms and rules.[357] The order was given by the CEO of Twitter Jack Dorsey, but soon after because of the rising disputes, he announced that their action against New York Post was wrong.[358]

That is not the only case example of that ICTs intervene in the elections. By alleging that, Donald Trump provokes the public to hatred, hostility or degrade Twitter announced if Trump does not delete the contents in question, the account will be deleted.[359] After two days, Twitter announced the account of Donald Trump was permanently deleted.[360] How can we call this if it does not an example of preventing freedom of thought and expression?

This situation is just the same for Google and Twitter. While these companies interesting in political disputes they are ignoring some countries' problems on their platform. While cybercrimes are rising, while the crimes causing even suicide attempts of children, the political structures of some countries, or the companies' subjective beliefs about states are affecting the investigations of public authorities.

---

[357] Business Insider, (2020). Jack Dorsey says the New York Post Twitter account will remain locked until it deletes the original tweet featuring its Hunter Biden story, https://www.businessinsider.com/jack-dorsey-ny-post-remains-locked-out-twitter-hunter-biden-2020-10 (Accessed on January 12, 2021).

[358] Twitter, Jack Dorsey, (@jack) (October 15, 2020) Retrieved from: https://twitter.com/jack/status/1316528193621327876 (Accessed on January, 12, 2021).

[359] Twitter, Twitter Safety, (@TwitterSafety) (January 7, 2021) Retrieved from: https://twitter.com/TwitterSafety/status/1346970431039934464 (Accessed on January 13, 2021).

[360] Twitter, Twitter Safety, (@TwitterSafety), (January 9, 2021) Retrieved from: https://twitter.com/TwitterSafety/status/1347684877634838528 (Accessed on January 10, 2021).

These make them a haven for criminals, cause rising of crimes on their platforms and cause delaying of justice. Just like said by Mark Zuckerberg during his testimony "… we didn't take a broad enough view of our responsibility and that was a big mistake."[361]

Suggesting a single and proper approach to receive information from ICTs is not possible. It can be easily observed that some companies try to cooperate with LEA others do not respond at all to requests or treat them according to their political regime, ideology, or something else without thinking about the victims in their platform. These numbers also support LEAs arguments regarding the problems of cooperation. According to LEAs, many ICTs do not respond at all to some countries and taking decisions based on their subjective view of a country rather than a legal basis.[362]

It is seen by the examples that although the Convention on Cybercrime supplied several things to its parties like substantive and procedural law along with international cooperation and although it organized meetings and projects wits ICTs, it remained incapable to solve some problems among ICTs and some particular states.

Lastly, except for the problematic relations shared above, statistics show us that the Convention on Cybercrime supports the stakeholders in a really remarkable degree and the next and the last chapter of this thesis will focus on the positive effects of the Convention on criminal matters.

---

[361] YouTube, (GlobalNews), (April 11, 2018), Retrieved from: https://www.youtube.com/watch?v=YCQ_ZGxE2U4&ab_channel=GlobalNews (Accessed on January 10, 2021)

[362] Council of Europe, (2017), Study on Strategy of Cooperation with Multinational Service Providers https://rm.coe.int/study-on-strategy-of-cooperation-with-multinational-service-providers/16808f1e16 (Accessed on January 10, 2021).

CHAPTER 5

BENEFITS AND IMPACTS OF THE CONVENTION ON COUNTRIES

As mentioned before when the issue is cybersecurity from a state's perspective cooperation is necessary to prevent crimes and to supply criminal justice. International Telecommunication Union indicates five pillars to supply cybersecurity those are respectively legal, technical, organizational measures, capacity building, and lastly cooperation. Legal measures are deal with legal institutions and frameworks. Technical ones indicate technical institutions and frameworks. The third one, the organizational measures, means national-level policy coordination, institutions and strategies. Capacity building includes education, training and academic research etc. When it comes to cooperation, the pillar is based on the existence of a partnership, information sharing and absolutely cooperation among states[363] or in general terms mutual assistance as used by the CoE.

Just like defined by ITU, the CoE focuses on these five pillars to supply cybersecurity too. As before mentioned in the fourth part of this thesis, to reach the first aim namely to create cybercrime legislation, Convention on Cybercrime was prepared. Before mentioned projects which have been organized by the CoE and the EU are some of the best examples of technical supports and capacity-building endeavors. Lastly, cooperation among parties always defends by the organization and just because of that there are several countries that signed the Convention. Although as mentioned in the previous part of this thesis, some cultural or legal differences, changing trends on cybercrime and even the attitude of ICTs against states or their political views cause procedural discrepancies between ICTs and public sectors. However, except for these disputes when the case examples are investigated it is going to be seen that participant agencies highly benefitted from this cooperation structure.

---

[363] International Telecommunication Union, (2018), Global Cybersecurity Index, Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (Accessed on December 5, 2020). p 8

In this context according to ITU's Global Cybersecurity Index (Hereinafter referred to as GCI.) being a part of an international organization is important for countries. Also when the GCI index investigated countries that have high global rank are mostly parties of the Convention on Cybercrime. In the index, Turkey is the 20th country (total number is 194 with Palestine) and from the other 19 countries which have higher GCI rates investigated 7 of them are not the signatory of the convention. Here the numbers show that the countries that are the member of the Convention show better commitment to cybersecurity.[364]

According to the World Economic Forum's The Global Risks Report 2020, cybersecurity problems and the products of the internet are evaluated as short-term risks.[365] However, eliminating the risks of cybersecurity is not the duty of only one organization. At a country's border, LEA and JA should work together. In addition, without legal rules that give the authority to law enforcement getting in touch with other organizations from the public to private sectors, without the authority to seizing and investigating data or without training, experience etc. waiting for successful crime prevention or crime detection from LEAs will be volatile. To have qualified crime investigators, being a part of international agreements and projects that are aiming for capacity building is important. All crime investigators should have qualified international education because they have to work internationally. For example, LEAs of France, Germany and Turkey, all the three public entities, that work internationally, have lines among them and acting in harmony when they detect or try to prevent a crime. Without qualified international education, support and training like EndOCSEA or iPROCEEDs and international meetings such as Octopus this can't be possible.

To fight against this problem we see that the Convention on Cybercrime and its very cooperative works, also the projects behind it are one of the best examples of

[364] International Telecommunication Union, (2018), Global Cybersecurity Index, Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (Accessed on December 5, 2020).pp 63.

[365] World Economic Forum, Executive Summary, Retrieved From: http://reports.weforum.org/global-risks-report-2020/executive-summary/ (Accessed on December 5, 2020).

how states, institutions, NGOs, public and private sectors act in a cooperative way to solve the global problem. With 65 parties the CoE brought together several states all around the world along with their institutions. In addition, it is extending in every passing year. Moreover, with the projects aforementioned in this thesis' 3rd chapter the dimension of cooperation carried one step further. This is not all because of all the mentioned ongoing projects funds by countries and other organizations and even private companies.

5.1. What the Countries Gain from the Convention on Cybercrime

In democratic countries, every investigation should be based on law. If the investigation in question, related to transnational crime this creates the need for an international system. To do that the Convention on Cybercrime supplies three basic things those are respectively substantive law, procedural law and international cooperation. Here substantive law covers the articles from 2 and 12 and criminalizes some computer offenses. Procedural law permits efficient investigations and using electronic evidence during investigations. While substantive law defines the crime and supplies common legislation to countries procedural law defines investigation ways and lastly international cooperation, namely the Articles from 23 and 35 limits by safeguards and conditions to prevent abuse the authority and brings some necessities such as proportionality judicial supervision. Domestic legislation reaches international standards of all parties to facilitate international cooperation through the agreement.[366]

With the works of capacity building, the parties can change the situation to their benefit. They can have legislation and improve their international cooperation in line with the Convention on Cybercrime because of the fact that classic solutions lost their popularity in time.[367] Here capacity building aims to strength rule of law

[366] Council of Europe,(2013)., Capacity building on cybercrime, Retrieved from: https://rm.coe.int/16802fa3e6 (Accessed on November 1, 2020)

[367] Seger, A., (November, 20-22, 2019). Council of Europe, Results of capacity building and impact on legislation, Retrieved from: https://rm.coe.int/090000168098e27b (Accessed on January 15, 2021).

and human rights, enhancing cybersecurity, reducing poverty, raising human development and supplying democratic governance.

When it comes to ICTs because so many aspects of social life are exhibited on platforms especially like Facebook and Instagram police can obtain evidence from them and by using ICTs technologies investigators have enhanced their capacity. This is also one of the aims of the Convention. Because there are a series number of technics used by police agencies to detect suspects or prevent crimes and all the parties have to be sure the techniques used by police are legitimate. Because this thesis focuses on virtual evidence collectible via public-private cooperation (Hereinafter referred to as PPP) it is focused on these methods and those are; reaching online publicly available data, getting in touch with ICTs to obtain private data, and using OSINT or similar techniques to collect data automatically.[368]

ICTs' general structure can supply unique information to police agencies such as location information, metadata, sentiment analysis, images, (facial recognition) names uploaded to social media (to detect real users) and relational data. In the case of legal demand when a prosecutor or judge demands information about a suspect, LEA is fully authorized to directly getting touch with private companies to supply adequate information to the investigation.[369] To some extend law enforcement especially those located western region realized the contributions and capacity of service providers to collect evidence and the CoE aims to support all countries because a weak link in the chain, threatens whole the body. To prevent that Convention on Cybercrime indicates some necessities to ISPs in order to support police and investigations.[370]

---

[368] Trottier, D., & Fuchs, C. (Eds.). (2014). *Social media, politics and the state: protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube*. Routledge. pp.209-224

[369] Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the US criminal justice system. *Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. Priority Criminal Justice Needs Initiative. Rand Corporation*.

[370] Huey, L., & Rosenberg, R. (2004). Watching the web: Thoughts on expanding police surveillance opportunities under the cyber-crime convention. *Canadian Journal of Criminology and Criminal Justice*, *46*(5), pp.597-606.

As an example, police use content data to detect some specific content related crimes like child exploitation, threat, romance scam, insult etc. One of the best case examples of that issue happened in Turkey. A Skype group named "SEX" was detected and police organized synchronous operations in 17 provinces in Turkey. Without the supports of Microsoft and the information supplied by that company, this could not be possible.[371] Convention compels ICTs to share some information including identity, location, telephone number, access method, billing and payment information, the type of service and length of service.[372] Article 16 obliges the companies to keep and preserve the requested data as long as needed time. However, restricts the time range to 90 days to enable the competent authority to demand its disclosure.[373] Shortly while article 16 obliges to parties preservation of data article 17 mentions disclosure sufficient amount of data to detect service providers. Also within the scope of articles 18, 19, 20 and 21 parties can reach the needed data during investigations.

Traffic data is generally used to detect log info to prevent an imminent threat like suicide or terrorist attacks. A very important example of the importance of cooperation happened in the USA. Police were called by Facebook about a suicide attempt so that they prevent it. Like the case, according to news published by The New York Times, Indian police received similar calls from Facebook.[374] Is it possible? Absolutely! ICTs have Artificial Intelligent (AI) systems coding and

[371] Sözcü, ATAM, H., (October 10, 2020). Police conducted operations in 17 provinces, 22 criminals were arrested, Retrieved from: https://www.sozcu.com.tr/2020/gundem/17-ilde-cocuk-pornosu-operasyonu-22-kisi-yakalandi-6075151/ (Accessed on: January 17, 2021)

[372] Smith, S. W. (2004). *U.S. Patent No. 6,771,971*. Washington, DC: U.S. Patent and Trademark Office.

[373] Council of Europe, (November 23, 2001) Convention on Cybercrime Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on January 17, 2021).

[374] The New York Times, Retrieved from: https://www.nytimes.com/2018/12/31/technology/facebook-suicide-screening-algorithm.html (Accessed on January 18, 2021).

classifying the published contents.[375] (1) they can create an alert, (2) report the case to experts and (3) they get in touch with their 24/7 contact point and share traffic data so that police find the location of the person through the system. [376] Moreover, to protect its netizens Facebook created an alert page[377] and like Facebook, Twitter[378] Instagram[379] WhatsApp[380] has similar alert pages. Namely, ICTs can detect the users via AI and through close relations with ICTs, LEA can save a person's life only via log data.

5.2. Ways to Receive Information from ICTs

The Budgets of ICTs' are oriented toward innovation and transformation of the market. Namely, whose main aim is not assisting LEAs. So the number of staff who are working in the crime detection departments is lower compared to the other departments. When a company received a request from a country it is revived by a person. The employee is not interested in only one country's request but resembles a region. Therefore, the only way to proper communication is English among the parties. The language issue is a difficulty for LEAs and to some extend interesting in the whole region brings a burden for the employee because s/he needs to understand all particularities of the whole region.[381] In addition, all of the ICTs do not have

[375] Facebook, (September 10, 2018) How Facebook AI Helps Suicide Prevention, Retrieved from: https://about.fb.com/news/2018/09/inside-feed-suicide-prevention-and-ai/ (Accessed on January 18, 2021).

[376] Facebook, (March 1, 2017)., Building a Safer Community With New Suicide Prevention Tools Retrieved from: https://about.fb.com/news/2017/03/building-a-safer-community-with-new-suicide-prevention-tools/ (Accessed on January 18, 2021).

[377] Facebook Help Center, Report Suicidal Content, Retrieved from: https://www.facebook.com/help/contact/305410456169423 (Accessed on January 19, 2021).

[378] Twitter, Help Center, Report suicidal content, Retrieved from: https://help.twitter.com/forms/report_self_harm (Accessed on January 18, 2021).

[379] Instagram, Self-injury, Retrieved from: https://www.facebook.com/help/instagram/553490068054878 (Accessed on January 18, 2021).

[380] WhatsApp, Staying safe on WhatsApp, Retrieved from: https://faq.whatsapp.com/general/security-and-privacy/staying-safe-on-whatsapp (Accessed on January 18, 2021).

[381] Council of Europe, (August 30, 2017), Study on Strategy of Cooperation with Multinational Service Providers, Retrieved from: https://rm.coe.int/09000016808f1e16 (Accessed on January 19, 2020).

offices in every region of every country, unlike Microsoft. (Microsoft Offices[382]) Even if these ICTs have offices in a particular country this not always means that they are interesting law enforcement's requests. Those offices are work on the quality of services and products in the country. As a simple example, Twitter has offices both in India (one of them in Mumbai the other one in Bengaluru) and in the United Arab Emirates (in Dubai). The company during the term 2019/H2 (July-December) received information requests from India with the number 789 (662 regular 127 emergencies) and the compliance rate of the requests for regular ones 13 for emergency only 1. Namely, although Twitter has 2 offices in the country it responded to only 14 requests. When it comes to the United Arab Emirates although the country made 10 emergency requests, Twitter did not answer any of them just like Singapore.[383] Shortly having an office is not a solution to supply cooperation. Here worth noting that although Twitter has two offices in İndia and although the law 18 U.S. Code§2702 permits to share info in case of emergency Twitter did not respond to 126 emergency requests of that country.

In order to receive information from multinational service providers countries follows two ways the first and the older one is known as the "Mutual Legal Assistance Treaty" (Hereinafter referred to as MLAT.). To follow this way states should have an agreement, after then the state which is investigating any crime applies to the other's justice department. The receiver state launches the investigation to compel the private company. If any problem emerges, to fix it, the process turns its start line namely to the requester country. When the Mutual Legal Assistance Treaty compared with the extent of internet access it is can be seen easily that the MLAT solution cannot be enough to solve the problems. [384] It takes much more time

---

[382] Microsoft, Microsoft office locations around the world, Retrieved from: https://www.microsoft.com/en-us/worldwide.aspx (Accessed on January 20, 2021).

[383] Twitter, Transparency, Information Requests, Retrieved from: https://transparency.twitter.com/en/reports/information-requests.html#2019-jul-dec (Accessed on January 19, 2021).

[384] Republic of Turkey, Ministry of Justice, Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü Retrieved from: https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/ikili.html (Accessed on January 21, 2021).

and during this process, criminals may violate much more laws, may swindle more people may cause much more damage and manual process slowdowns ongoing investigations.

According to TC-Y's report dated 2014 that contains 42 countries' responses, when states applied the MLAT procedure to take information from a different jurisdiction it delays the investigations around 6 or 24 months and after the time consume, companies may reject the requests. This is causing significant delays during the investigations, also in some cases especially because of rising crime rates some countries give up and leave the investigation. When the numbers investigated belongs to 2012 Turkey received 11 MLAT requests and the total sending requests are 364. (In 2011, the numbers respectively were 7 and 232 and this is highly more compared to other countries that submit their numbers.) When the crimes are In 2013 Norwegian police called the Italian police and reported that a person investigated it is seen that there are several kinds of crime topics in Turkey such especially as Illegal access, hacking website, blackmail, computer sabotage, computer fraud, website forgery, threat, defamation, misuse of credit card, payment fraud, violation of privacy, violation of secrecy, illegal recording and tapping of communications, terrorism, smuggling etc.[385] This means that with the MLAT procedure prosecuting all the crimes listed above are delayed.

The MLAT's problems were also discussed by the European Commission and to reach a faster solution to collect e evidence Commission strictly recommended direct cooperation way with ICTs. To improve cross-border access to e-evidence Commission criticized current investigation tools, limits of them, legal borders, the slowness of MLAT procedure, ICTs different procedures and legal uncertainty. The solutions recommended by the EU were enhancing cooperation among EU members, using a single platform among EU parties for secure communication, organizing regular meetings, promoting the exchange of best practices etc. to solve problems

[385] Council of Europe, T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c (Accessed on January 23, 2021).

especially legislative one's Commission accepted that measures could be complemented with by agreements with some key countries, in particular the Convention on Cybercrime of the CoE.[386]

Also on a meeting of the CoE, it is reflected by a representative of a county that, as a small and partly poor country finding resources to negotiate all the bilateral agreements is not possible for them. Therefore, the Convention supplies dozens of partners who are instantly bound to provide assistance.[387] Although the Convention cannot solve all the problems it helped improve the situation and contributed to successful cooperation and as stated by that person ıt supplies several partners to states as recommended by the EU Commission.

To solve the problems Convention on Cybercrime recommends "Mutual Assistance among Parties". One of the examples of cooperation covering Italian and Norwegian police has been highly announced in the press.[388] In 2013 Norwegian police called the Italian police and reported that a person killed his wife. After he escaped from Norway, it is detected with his Skype connection and with his mobile phone IP addresses that the person arrived in Rome. In the case, Norwegian police supplied IP addresses and photos of the suspect then an Italian prosecutor requested real-time traffic data of the suspect. In the end, the person was arrested as a result of direct mutual cooperation between parties. [389]

---

[386] European Commission, (June, 11, 2017), How can we improve cross-border access to e-evidence? Retrieved from: https://ec.europa.eu/home-affairs/news/how-can-we-improve-cross-border-access-e-evidence_en (Accessed on January 23, 2021).

[387] Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed on October 02, 2020).

[388] NewsinEnglish, (June 16, 2013)., Murder suspect arrested in Rome Retrieved from: https://www.newsinenglish.no/2013/06/16/murder-suspect-arrested-in-rome/ (Accessed on October 02, 2020).

[389] Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed on October 02, 2020), pp:16

When the issue is international mutual assistance, it is seen that within the scope of the Convention Turkey has several good experiences. According to the same report prepared by the CoE, Turkey both received information from other countries and support other countries to prevent imminent risk of harm.

For example, the Online Notice System of the Turkish National Police received a notice regarding a bomb attack. The system automatically captured the source IP. When the IP address was investigated, it is understood that it was resolved to an ICT company in the USA. After direct communications with the company in question, it is disclosed that the IP resolving an American cruise company and came from a vessel that is in another country at that time. The suspect was captured by investigating security cameras on the board, his visa was canceled and he was arrested at the airport on return to Turkey. In another example, the TNP supplied spontaneous information to the Netherlands regarding a highly possible bomb attack planned by PKK terrorist organization in Schiphol Airport. The TNP warned the Netherlands so that they could take precautions to prevent harm.[390]

To receive information from service providers the second way is voluntary cooperation. In this method, police, prosecutor and the company work in harmony. Prosecutor gives the order to the police, after the police received the proper order s/he submits it to the company, and then the process turns the other way run. The company supplies requested information to the police, and the police give the documents to the prosecutor. In this system, police can warn the prosecutor when they find a mistake or when the prosecutor request improper information due to police have much more experience on data request issue. For example, the second way is only acceptable when the needed information covers only subscriber data. If a prosecutor needs traffic data or content data, she should follow the MLAT procedure. (Article 18)

[390] Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed on October 02, 2020), pp:18-19

The reason for the difference between (1) subscriber information and (2) traffic data along with (3) content data, 2 and 3 cover the more detailed information and to prepare these data, companies need more time and more information about the investigation. Also According to the US Department of Justice, the drafters of the Electronic Communication Privacy Act in other words Wiretap Act (hereinafter ECPA) saw greater privacy on content data compared to subscriber data. Direct cooperation can be used only for serious crimes because of the restriction ECPA (1986). This law restricts the USA-based multinational service providers to share the information stored in the USA.[391] However, as can be seen, the law has been launched in 1986 and during that time, there were no ICTs giants such as Facebook or Google.

5.3. Convention on Cybercrime's Role on Voluntary Cooperation

Communication with these multinational and powerful companies is a highly different and detailed issue. This duty requires different thinking and skills for law enforcement officials because the companies' terms and conditions can show differences, needs better understanding and better relationship and most importantly trust among parties. If a company does not trust LEA, or if LEA makes mistakes during the process, the relation between the company and LEA will get harm. The bridge between a company and the prosecutor will collapse without LEA.[392]

Lack of cooperation, namely when the bridge collapsed among parties causes new problems and can change the nature of the dispute. One of the best examples of it is the dispute between Germany and ICTs. In German law, the country can fine ICTs up to 50 million Euros, if they do not remove illegal contents especially including hate speech. According to the law, ICTs have only 24 hours to remove

[391] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, Electronic Communications Privacy Act of 1986 (ECPA), Retrieved from: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 (Accessed on October 03, 2020).

[392] Council of Europe, (August 30, 2017)., Study on Strategy of Cooperation with Multinational Service Providers, Retrieved from: https://rm.coe.int/09000016808f1e16 (Accessed on October 03, 2020).

reported content that includes hate speech and xenophobic materials. If the content less obviously violates the law, ICTs have only seven days to remove them. If cooperation among the parties (in other words the bridge) does not use an effective way this kind of sanctions will be common.[393]

To solve possible disputes both between parties and ICTs, the Council of Europe decided to organize the Cybercrime Convention Committee (Hereinafter referred to as TC-Y). The decision to create this committee is based on the Convention on Cybercrime's Article 46. According to Article 46 "parties consult periodically in order to guarantee; "the effective use and implementation of this Convention, including the identification of any problems thereof …"[394] With article 46 it is can be alleged that the possibility of an "outdated agreement" can be eliminated because all the parties periodically work and discuss on issues. Within the scope of Article 46 states and ICTs can explain their problems periodically with the works of TCY.

TC-Y represents all the parties to Convention on Cybercrime and has members from all of them.[395] It has also three working groups called Protocol Drafting Group, Cloud Evidence Group, and Transborder Group with three basic aims; a) facilitating effective use and implementation of the convention, b) exchange of information, c) consideration of future amendments.[396]

Cloud Evidence Group's (Hereinafter referred to as CEG.) recommendations regarding cooperation with ICTs and LEAs are important to reach a faster solution.

---

[393] German Law Archive, (September 01, 2017)., Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG), Retrieved from: https://germanlawarchive.iuscomp.org/?p=1245 (Accessed on October 03,2020).

[394] Council of Europe, (November 23, 2001), Convention on Cybercrime Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on October 03, 2020).

[395] Council of Europe, Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY, Retrieved from: https://www.coe.int/en/web/cybercrime/parties-observers Accessed on October 03, 2020.

[396] Council of Europe, Cybercrime Convention Committee, Retrieved from: https://www.coe.int/en/web/cybercrime/tcy (Accessed on October 04, 2020).

On September 16, 2020, CEG prepared a series of recommendations to TC-Y and it was accepted by the committee during its 16th Plenary. The recommendations included; inviting parties to full implementation of Article 18 (Production order), taking the practical solution to build more coherent relation with ICTs to prevent wasting time with MLAT, more simple procedure to reach subscriber data on the MLAT process, creating an international production order, holding annual meetings with providers, direct cooperation with service providers on information, preservation, and emergency request and creating much more clear framework and stronger safeguards of transborder access to data.[397]

Currently, there are only two solutions to receive information from ICTs as mentioned above the difficult and time-consuming one is the MLAT process the other one is the voluntary disclosure model. The voluntary disclosure model can be investigated with the transparency reports of the companies as we did in the fourth chapter of this thesis. However, it will be seen that while some companies are very cooperative and have high responds rates, the others have different approaches, especially in some countries. Even some of them do not respond to particular countries just because of subjective reasons.

5.4. Examples of Cooperation and Complex Interdependence

Before exploring the benefit of the Convention with the case examples discussing to what extend the Convention brings benefits to countries will be better. The impact of the Convention when the issue is ICTs can be many folds. Firstly as mentioned, all the members having the same domestic legislation to prosecute these crimes and having the same procedure for collecting electronic evidence from networks. Convention supplies multi-stakeholders to investigate the crimes internationally with the workshops, meetings and projects including both public and private sectors the cooperation's dimension can extend. With the training by

[397] Council of Europe, (November 14-15, 2016)Cybercrime Convention Committee, Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cd270 (Accessed on October 04, 2020).

following the other footprints and methods by used the other agencies, the time spent can be diminished remarkably. Also with the experiences of other countries and departments, states can easily get in touch with private companies this both diminishes spending time and build confidence between the requester and responder. By using the same methods and the same procedures reaching equal level cybersecurity may be possible.

States that have adopted the Convention during the prosecution process may attribute to the treaty and the articles of it. However, this is not the more proper one, because courts refer to articles of domestic law so the Convention can be used during international cooperation provision. However, there are successful examples the articles of the Conventions used too. For example, Bosnia and Herzegovina used Articles 29 and 30 to seek data preservation and Article 31 to take subscriber information from ICTs. In 2019, crime investigators received data from an ICT regarding the distribution of child exploitation materials. The investigation resulted that the suspect has 1000 items of storage media (42 hard discs, computers, mobile phones, etc.) to store child exploitation materials. Just like Bosnia and Herzegovina, the French used the Convention on Cybercrime to find the criminals who produce and sell some kinds of illegal drugs and fake cigarettes.[398]

Another two other interesting cases were solved with the assistance of respectively Facebook and Apple in Hungary. In the first case, two suspects convinced an underage victim to get off the bus with them in exchange for a cigarette. Because the victim seems to used sedatives and under the effect of alcohol, s/he accepted the offer and then she was abused by the suspects. By using the security camera records of the bus investigators reached the photos and related information of the suspects on Facebook in accordance with Article 32. The second case was related to a murder. A murderer killed his/her mother and throw the body into a septic tank. To find the murderer investigators seized the suspect's iPhone and iWatch to find evidence. By using cloud data the criminal is found by the authorities.

[398] Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed on October 02, 2020), pp:9

According to Hungary without the use of Article 32 finding the criminal with the classic methods will be time-consuming.[399] Here it is worth that there are several examples of the convention's articles used by LEAs and JAs to solve the cases.

However, it should be kept in mind that this mostly depends on the companies. Any agency or any state cannot force ICTs to share info with them just like happened Apple/USA case and just like what happened Facebook/Germany case. Convention supplies the legal basis for international cooperation with pieces of training, projects, meetings etc. not force any ICTs to help and support countries. Parties and states that had access to that treaty may become priority countries and benefit from the capacity building.

Countries that are the signatories of the Convention use Article 18 as a legal basis to reach subscriber information because ICTs offer service in the territory of the Party. Many of them are aware that if the information is stored in the USA, without MLAT, ICTs have the authority to disclosure some kinds of data. When it comes to ICTs, before disclosure of data the providers explicitly consider whether the country is a party of the Convention or not. As stated by several countries (such as Bosnia and Herzegovina, Chile, France etc.) with the Convention PPP raised among them, most companies set up contact lines and now they have better relations with private sectors.[400] Nearly almost all ICTs prone to think that signing the Convention means the requester has the same legal structure as the USA.

[399]Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed on October 02, 2020), p:10

[400] Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed on October 02, 2020). p: 12

CONCLUSIONS

According to criminal theorists Wilson and Kelling if a window in a building is broken and if it is left unrepaired this means the other windows are condemned to break. This theory in crime literature is called Broken Windows theory if punishment does not supply promptly and if the damages do not compensate all rest of the windows will soon be broken. If a state or an authority ignores a criminal problem when it occurs, this crime will continue to increase and the cost of eliminating it will rise too.[401] When we think of cybercrimes from that point of view, it seems that this is acceptable.

If a cybercrime regardless of the dimension and the cost of crime, does not punish or prosecute this will bring much more crime. When we think of the state as a building, in time the state will lose all of its windows eventually if it does not take precautions. To supply a safer democratic environment in this globalized connected world, to protect the "windows" of the state, cybersecurity is indispensable for all the stakeholders.

Because the entire world is connected to each other, a missing party means a haven for criminals. In this context, it is obvious that the crimes which happen in the haven will affect others, threaten the netizens, causes asking the role of the state, will raise the costs and the situation will continue until all the windows are crashed. So fighting against cybercrimes brings the need for cooperation on the international level to protect all the parties. A missing party causes losing building and this will turn the situation to the start line repeatedly. To protect all the buildings five things are indispensable. Those are legal, technical, organizational measures along with capacity building and cooperation.

The issue is investigated from the neoliberal perspective, as advocated by neoliberal thinkers multinational cooperation and global institutions are important to

[401] Kelling, G. L., & Wilson, J. Q. (1982). Broken windows. *Atlantic monthly*, *249*(3), pp.29-38.

provide cooperation. To act in a harmony, as defended especially by neoliberals, governance without government is indispensable. State-based constitutional rules or penal codes cannot be the proper solution to protect the internet society.

While on the one hand internet and ICTs affecting the world to a globalized extend and turning things into international issues and on the other hand while criminals bomb any location of the world only by using a little device, mentioning legal borders will be nonsense. As a regulative local authority, states should always be there but to supply security and to protect human rights. However, they should have the ability to act internationally too. International cooperation can effectively supply international organizations. With technology especially with the proliferation of Information and Communication Technologies, states become connected to each other and this causes mutual interdependence.

Moreover, with the powerful and rich private actors (even richer than states) this mutual interdependence turns into a complex situation. Namely, with modernization, innovation and globalization not only states, NGOs, universities but also public/private sectors have been involved in the scene. However, the actors which are involving the scene can benefit from the situation with their own connections to some extent such as Mutual Legal Assistance. However, this cannot be enough to fight against the global problem for a state which acting alone or acting with a few partners while it should have acted globally.

Convention on Cybercrime supplies multi-functional benefits to states. By cooperating all the parties can protect their internet society and this also provides a dual benefit to them and raises the possibility of benefit from the other. Additionally, the shadow of the future makes the parties more prone to cooperation. Increasing crimes and the rising cost of fixing the systems, or the cost of prosecuting the hi-tech crimes make states “prisoners”. In this situation in order to refrain from punishment and to refrain from prisoner dilemma, the only way is cooperation.

In the globalized world with the excessive prevalence of MSPs, it should also be accepted that the concept of power changed from the hard one to the soft one. Technological adaptation leads to new kinds of innovations that supply human development, free and fast communication. Borders are eliminated, cultural figures are transported, with the internet and MSPs people's choices are enlarged, authorities are held accountable, and information can be carried, shared without any cost. However, if the advantages of ICTs turn reverse the havoc can destroy a huge amount of parties even with a trojan.

Convention on Cybercrime provides a legal framework to countries that are located on every continent. While the regular MLAT process takes remarkable time around 6-24 months between the countries, with the Convention this time wasting is reduced. Countries indicate this as a benefit in their case examples. Especially with the conferences, the Council of Europe brings together public and private organizations, universities, NGOs, and most importantly ICTs in a place to discuss current trends, problems among the LEA, JA, ICT, etc. to make the cooperation efficient.

With the projects organized by the Council of Europe within the context of capacity building measures, hundreds of thousands of LEA and JA members trained, all these training workshops organized in different countries, so all the participants can benefit from the other's experiences and can build friendly relations.

From Keohane’s and Nye’s perspective in cooperation, the relation among all the parties and stakeholders is far from a state-centric interaction pattern and very close to transnational interactions and interstate politics. Just like that, the structure of the Convention does not focus only on governments as agencies. In addition, in the structure of the convention, parties know each other with interstate interactions, organizations/companies participate in meetings, supply funds to make technological measures more effective, play a direct role, and cooperates with states as Microsoft does.

The Cybersecurity works of the Convention are very important but it must be improved also. For example, Yahoo joined only one Octopus Conference in 2009 and Twitter has never joined the conference. Therefore, when the transparency reports of these companies are investigated it will be seen that the two companies' relation, with some countries is getting worse in time. The lack of communication or political problems should not affect the criminal investigations this will not be ethical and will make them haven for criminals. Therefore, the Council of Europe should invite many more companies especially the most used ones by netizens to the meetings, workshops and conferences.

BIBLIOGRAPHY

Açar, K.V., Avrupa konseyi budapeşte sözleşmesi kapsamında saklama talebi ve Türkiye uygulamaları çalıştayı, Retrieved from: https://www.researchgate.net/publication/336578876_Avrupa_Konseyi_Budapeste_Sozlesmesi_Kapsaminda_Saklama_Talebi_ve_Turkiye_Uygulamalari_Calistay_Raporu (Accessed on October 14, 20220).

Adena, M., Enikolopov, R., Petrova, M., Santarosa, V., & Zhuravskaya, E. (2015). Radio and the Rise of the Nazis in Prewar Germany. *The Quarterly Journal of Economics*, *130*(4), p.1885-1939

African Union. (2000). Retrieved from: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (Accessed on November 15, 2020).

African Union. Retrieved from: https://au.int/en/overview (Accessed on November 15, 2020).

Altvater, E. (2008). The Roots Of Neoliberalism. *Socialist Register*, *44*.

Apple, (February 16, 2016), A message to our customers, Retrieved from: https://www.apple.com/customer-letter/ (Accessed on January 8, 2021).

Apple, Transparency, Financial Identifier Requests, Retrieved from: https://www.apple.com/legal/transparency/financial-identifier.html (Accessed on January 15, 2020).

Archick, K., & Foreign Affairs, Defense, and Trade Division. (2005). Cybercrime: The council of Europe convention. Congressional Research Service, Library of Congress.

Axelrod, R., & Dion, D. (1988). The further evolution of cooperation. *Science, 242*(4884), p.1385-1390.

Axelrod, R., & Hamilton, W. D. (1981). The evolution of cooperation. *science*, *211*(4489), p.1390-1396.

Axelrod, R., & Keohane, R. O. (1985). Achieving cooperation under anarchy: Strategies and institutions. *World politics*, *38*(1), p.226-254.

Axelrod, R., & Keohane, R. O. (1985). Achieving cooperation under anarchy: Strategies and institutions. *World politics*, *38*(1), p.226-254.

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (Eds.). (2007). *Cybercrime: digital cops in a networked environment* (Vol. 4). NYU Press. p 207-220

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (Eds.). (2007). *Cybercrime: digital cops in a networked environment* (Vol. 4). NYU Press. p 207-220

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (Eds.). (2007). *Cybercrime: digital cops in a networked environment* (Vol. 4). NYU Press. (pp 207-220)

Barnett, C. (2000). The measurement of white-collar crime using uniform crime reporting (UCR) data. *US Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division*.

Baron, R. M. (2001). A critique of the international cybercrime treaty. *CommLaw Conspectus*, *10*, p.263-277

Baron, R. M. (2001). A critique of the international cybercrime treaty. *CommLaw Conspectus*, *10*, p.263-277

Baylis, J. (2020). *The globalization of world politics: An introduction to international relations*. Oxford university press, USA. p 240-245

Baylon, C. (2014). Challenges at the intersection of cyber security and space security. *International Security*. p. 10-15

Baysal, T. (2017). Neo-Liberalizm Tartişmalari Çerçevesinde Kamu Yönetiminin Dönüşümü: Türkiye Pratiği. *Kafkas Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *8*(15), pp. 171-195

BBC News, (January 8, 2019) Facebook ad campaign helped Donald Trump win election, claims executive, Retrieved from: https://www.bbc.com/news/technology-51034641

Briggs, A., & Burke, P. (2009). *A social history of the media: From Gutenberg to the Internet*. Polity. p.13-61

Briggs, A., & Burke, P. (2009). *A social history of the media: From Gutenberg to the Internet*. Polity.p.61-67

Briggs, A., & Burke, P. (2009). *A social history of the media: From Gutenberg to the Internet*. Polity. p.265

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*. 29(2) : p. 408-433.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*. 29(2) : p. 408-433

Business Insider, (2020). Jack Dorsey says the New York Post Twitter account will remain locked until it deletes the original tweet featuring its Hunter Biden story, https://www.businessinsider.com/jack-dorsey-ny-post-remains-locked-out-twitter-hunter-biden-2020-10 (Accessed on January 12, 2021).

Castells, M. (1999). *Information technology, globalization and social development* (No. 114). Geneva: UNRISD. P.4-7

Castells, M. (1999). *Information technology, globalization and social development* (No. 114). Geneva: UNRISD. P.10

Castells, M. (1999). *Information technology, globalization and social development* (No. 114). Geneva: UNRISD. P.7

Castells, M. (2013). *Communication power*. OUP Oxford. 238-239

Castells, M. (2013). *Communication power*. OUP Oxford. pp 240-243

Castells, M. (2013). *Communication power*. OUP Oxford. pp 243-246

Cerezo, A. I., Lopez, J., & Patel, A. (2007, August). International cooperation to fight transnational cybercrime. In *Second international workshop on digital forensics and incident analysis (WDFIA 2007)* p. 13-27. IEEE.

Cerezo, A. I., Lopez, J., & Patel, A. (2007, August). International cooperation to fight transnational cybercrime. In *Second international workshop on digital forensics and incident analysis (WDFIA 2007)* p. 13-27. IEEE.

Cerezo, A. I., Lopez, J., & Patel, A. (2007, August). International cooperation to fight transnational cybercrime. In *Second international workshop on digital forensics and incident analysis (WDFIA 2007)* p. 13-27. IEEE.

Clement j.," Number of monthly active Facebook users worldwide as of 2nd quarter 2020", *Statista*, August 10, 2020., https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide, (Accessed on October 07, 2020).

Clough, J. (2012, December). The Council of Europe Convention on cybercrime: defining crime in a digital world. In *Criminal Law Forum* Vol. 23, No. 4, p. 363-391. Springer Netherlands.

Clough, J. (2012, December). The Council of Europe Convention on cybercrime: defining crime' in a digital world. In *Criminal Law Forum* Vol. 23, No. 4, p. 363-391. Springer Netherlands.

Clough, J. (2012, December). The Council of Europe Convention on cybercrime: defining crime' in a digital world. In *Criminal Law Forum* Vol. 23, No. 4, p. 363-391. Springer Netherlands.

COE, Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Accessed on January 15, 2020)

Convention on Cybercrime, (2001), Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561, (Accessed on January 15, 2020)

Convention on Cybercrime, (2001), Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561, (Accessed on January 15, 2020)

Cornell Law School , Legal Information Institute, 17 U.S. Code § 506 - Criminal offenses, Retrieved from: https://www.law.cornell.edu/uscode/text/17/506 (Accessed on March 02, 2021)

Cornell Law School , Legal Information Institute, 18 U.S. Code § 1029 - Fraud and related activity in connection with access devices, Retrieved from: https://www.law.cornell.edu/uscode/text/18/1029 (Accessed on March 01, 2021)

Cornell Law School , Legal Information Institute, 18 U.S. Code § 1030 - Fraud and related activity in connection with computers, Retrieved from: https://www.law.cornell.edu/uscode/text/18/1030 (Accessed on March 02, 2021)

Cornell Law School , Legal Information Institute, 18 U.S. Code § 2251 - Sexual exploitation of children, Retrieved from: https://www.law.cornell.edu/uscode/text/18/2251 (Accessed on March 02, 2021)

Cornell Law School , Legal Information Institute, 18 U.S. Code § 2421 - Transportation generally Retrieved from: https://www.law.cornell.edu/uscode/text/18/2421 (Accessed on March 02, 2021)

Cornell Law School , Legal Information Institute, 18 U.S. Code § 3121 - General prohibition on pen register and trap and trace device use; exception, Retrieved from: https://www.law.cornell.edu/uscode/text/18/3121 (Accessed on March 4, 2021)

Cornell Law School , Legal Information Institute, 18 U.S. Code § 3127 - Definitions for chapter https://www.law.cornell.edu/uscode/text/18/3127 (Accessed on March 4, 2021)

Cornell Law School , Legal Information Institute, 18 U.S. Code § 2703 - Required disclosure of customer communications or records https://www.law.cornell.edu/uscode/text/18/2703 (Accessed on March 4, 2021)

Cornell Law School , Legal Information Institute, 18 U.S. Code § 2518 - Procedure for interception of wire, oral, or electronic communications https://www.law.cornell.edu/uscode/text/18/2518 (Accessed on March 4, 2021)

Cornell Law School , Legal Information Institute, 18 U.S. Code § 2511 - Interception and disclosure of wire, oral, or electronic communications prohibited, https://www.law.cornell.edu/uscode/text/18/2511 (Accessed on March 4, 2021)

Cornell Law School , Legal Information Institute, Rule 41. Search and Seizure https://www.law.cornell.edu/rules/frcrmp/rule_41 (Accessed on March 4, 2021)

Cornell Law School, 18 U.S. Code § 2702 - Voluntary disclosure of customer communications or records, Retrieved from: https://www.law.cornell.edu/uscode/text/18/2702 (Accessed on January 04, 2021)

Cornell Law School, 18 U.S. Code § 2703 - Required disclosure of customer communications or records Retrieved from: https://www.law.cornell.edu/uscode/text/18/2703 (Accessed on January 04, 2021)

Cornell Law School, 18 U.S. Code § 2705 - Delayed notice, Retrieved from: https://www.law.cornell.edu/uscode/text/18/2705 (Accessed on January 04, 2021)

Cornell Law School, Legal Information Institute, 15 U.S. Code § 1644. Fraudulent use of credit cards; penalties Retrieved from: https://www.law.cornell.edu/uscode/text/15/1644 (Accessed on March 01, 2021)

Cornell Law School, Legal Information Institute, 15 U.S. Code § 45 - Unfair methods of competition unlawful; prevention by Commission, Retrieved from: https://www.law.cornell.edu/uscode/text/15/45 (Accessed on March 01, 2021)

Cornell Law School, Legal Information Institute, 18 U.S. Code § 1030 - Fraud and related activity in connection with computers, Retrieved from: https://www.law.cornell.edu/uscode/text/18/1030 (Accessed on March 01, 2021)

Council of Europe. (Version December 6, 2019) Retrieved from: https://rm.coe.int/2492-iproceeds-2-summary-v3/16809f3947 (Accessed on November 17, 2020).

Council of Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/endocsea-europe (Accessed on November 15, 2020).

Council of Europe (June 17-19, 2015) "Octopus 2015 Cooperation Against Cybercrime" Retrieved from: https://www.coe.int/en/web/cybercrime/octopus2015 (Accessed on November 22, 2020)

Council of Europe, (November 14-15, 2016)Cybercrime Convention Committee, Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cd270 (Accessed on October 04, 2020).

Council of Europe, (November 23, 2001), Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on March 4, 2021)

Council of Europe, (November 23, 2001), Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on March 4, 2021)

Council of Europe, (2017), Study on Strategy of Cooperation with Multinational Service Providers https://rm.coe.int/study-on-strategy-of-cooperation-with-multinational-service-providers/16808f1e16 (Accessed on January 10, 2021).

Council of Europe, (April 20, 1959). European Convention on Mutual Assistance in Criminal Matters, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016800656ce (Accessed on February 24, 2021)

Council of Europe, (August 30, 2017), Study on Strategy of Cooperation with Multinational Service Providers, Retrieved from: https://rm.coe.int/09000016808f1e16 (Accessed on January 07, 2021).

Council of Europe, (August 30, 2017), Study on Strategy of Cooperation with Multinational Service Providers, Retrieved from: https://rm.coe.int/study-on-strategy-of-cooperation-with-multinational-service-providers/16808f1e16 (Accessed on January 8, 2021).

Council of Europe, (August 30, 2017), Study on Strategy of Cooperation with Multinational Service Providers, Retrieved from: https://rm.coe.int/09000016808f1e16 Accessed on January 19, 2020.

Council of Europe, (August 30, 2017)., Study on Strategy of Cooperation with Multinational Service Providers, Retrieved from: https://rm.coe.int/09000016808f1e16 Accessed on October 03, 2020.

Council of Europe, (December 11, 1981) Recommendation no. R (81) 20, Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804c66e0 (Accessed on February 27, 2021)

Council of Europe, (December 13, 1957). European Convention on Extradition Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680064587 (Accessed on February 24, 2021)

Council of Europe, (December 3, 2014). T-CY Guidance Note 3, Retrieved from: https://rm.coe.int/16802e726a (Accessed on November 12, 2020).

Council of Europe, (February 17, 2016), Cloud evidence group, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8 Accessed on January 07, 2021.

Council of Europe, (January 28, 1981), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 Accessed on January 04, 2021

Council of Europe, (January 28, 2003) Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f (Accessed on March 10, 2021)

Council of Europe, (July 01, 2010). Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201 (Accessed on March 10, 2021)

Council of Europe, (July 13, 2020), The Budapest Convention on Cybercrime: benefits and impact in practice https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed on March 7, 2021)

Council of Europe, (July 13, 2020), The Budapest Convention on Cybercrime: benefits and impact in practice https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac (Accessed on March 7, 2021)

Council of Europe, (June 28, 1985) Recommendation no. R (85) 10, Retrieved from: https://rm.coe.int/09000016804e6b5e (Accessed on February 27, 2021)

Council of Europe, (June 6-8, 2012) “Cooperation Against Cybercrime” Retrieved from: https://www.coe.int/en/web/cybercrime/octopus-interface-2012 (Accessed on November 20, 2020)

Council of Europe, (March 15, 2013). Computer-related forgery and computer-related fraud: the need to build and include these new criminal types in a modern penal code, Retrieved from: https://www.coe.int/en/web/octopus-old2019/blog/-/blogs/computer-related-forgery-and-computer-related-fraud-the-need-to-build-and-include-these-new-criminal-types-in-a-modern-penal-code/ (Accessed on March 01, 2021)

Council of Europe, (March 17, 1978). Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680077975 (Accessed on February 24, 2021)

Council of Europe, (March 24, 1997). Implementation of recommendation No. R (89) 9 on computer related crime, Retrieved from: https://rm.coe.int/0900001680928683 (Accessed on February 27, 2021).

Council of Europe, (Marrch 1, 2017), T-CY Guidance Note #10 Production orders for subscriber information https://rm.coe.int/16806f943e pp: 5 (Accessed on March 4, 2021)

Council of Europe, (May 01, 2008).Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198 (Accessed on March 10, 2021)

Council of Europe, (May 14, 1993). Motion for a recommendation on economic crime, Retrieved from: https://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewHTML.asp?FileID=7197&lang=en (Accessed on February 27, 2021)

Council of Europe, (November 1, 2013), Retrieved from: https://rm.coe.int/16802fa3e6 Accessed on December 30, 2020.

Council of Europe, (November 13, 2001). Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 Accessed on December 24, 2020.

Council of Europe, (November 13, 2001). Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 Accessed on January 01,2021.

Council of Europe, (November 16-18, 2016) "Octopus Conference 2016 Cooperation Against Cybercrime" Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806bf0fb (Accessed on November 22, 2020)

Council of Europe, (November 23, 2001) Convention on Cybercrime Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on January 17, 2021).

Council of Europe, (November 23, 2001) Convention on Cybercrime, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on February 28, 2021)

Council of Europe, (November 23, 2001) Explanatory Report, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on November 12, 2020).pp: 54-55

Council of Europe, (November 23, 2001), Convention on Cybercrime Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 Accessed on October 03, 2020.

Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on March 01, 2021)

Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on March 01, 2021)

Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on February 28, 2021)

Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on March 02, 2021) p 6-7

Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on March 01, 2021) p 8-10

Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on March 01, 2021) p. 18-19

Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from:https://rm.coe.int/16800cce5b (Accessed on March 3, 2021) p: 21

Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from:https://rm.coe.int/16800cce5b (Accessed on March 3, 2021) p: 25-26

Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from:https://rm.coe.int/16800cce5b (Accessed on March 3, 2021) pp: 28-30

Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on March 3, 2021) pp: 28

Council of Europe, (November 23, 2001). Explanatory report to the Convention on Cybercrime, Retrieved from: https://rm.coe.int/16800cce5b (Accessed on February 3, 2021)

Council of Europe, (October 01, 1985). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (Accessed on March 10, 2021)

Council of Europe, (September 11, 1995) Recommendation no. R (95) 13, Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 (Accessed on February 27, 2021)

Council of Europe, (September 11, 1995). Recommendation no. R (95) 13 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 Accessed on January 3, 2021.

Council of Europe, (September 13, 1989) Recommendation no. R (89) 9, Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094 (Accessed on February 27, 2021)

Council of Europe, (September 17, 1987) Recommendation no. R (87) 15, Retrieved from: https://rm.coe.int/168062dfd4 (Accessed on February 27, 2021)

Council of Europe, (September 17, 1987)., Committee of ministers explanatory memorandum to recommendation no. R (87) 15 Retrieved from: https://rm.coe.int/168062dfd4 Accessed on January 3, 2021.

Council of Europe, (Status as of March, 2021). Reservations and Declarations for Treaty No.185 - Convention on Cybercrime Retrieved from: https://www.coe.int/en/web/conventions/recent-changes-for-treaties/-/conventions/treaty/185/declarations (Accessed on March 4, 2021)

Council of Europe, Chart of signatures and ratifications of Treaty 185, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Upslst88 (Accessed on January 15, 2020).

Council of Europe, Chart of signatures and ratifications of Treaty 108, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=z2ZXeB2v (Accessed on December 24, 2020).

Council of Europe, Chart of signatures and ratifications of Treaty 108 Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=a4fxO1c5 (total ratifications 55) (Accessed on January 01, 2020).

Council of Europe, Chart of signatures and ratifications of Treaty 005 , Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=a4fxO1c5 (total ratifications 47) (Accessed on January 2, 2021).

Council of Europe, Cybercrime Convention Committee, Retrieved from: https://www.coe.int/en/web/cybercrime/tcy (Accessed on October 04, 2020).

Council of Europe, Details of treaty no 185, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Accessed on Ocober 13, 2020).

Council of Europe, Details of treaty, Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (Accessed on February 27, 2021)

Council of Europe, Octopus Interface, (September 15-17, 2004). Computer related offences, Retrieved from: https://www.cybercrimelaw.net/documents/Strasbourg.pdf (Accessed on February 27, 2021).

Council of Europe, Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY, Retrieved from: https://www.coe.int/en/web/cybercrime/parties-observers Accessed on October 03, 2020.

Council of Europe, Protocol Negotiations, Retrieved from: https://www.coe.int/en/web/cybercrime/t-cy-drafting-group (Accessed on March 4, 2021)

Council of Europe, Search in database, Retrieved from: https://www.coe.int/en/web/conventions/recent-changes-for-treaties/-/conventions/treaty/185/declarations (Accessed on November 13, 2020).

Council of Europe, T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c Accessed on January 23, 2021.

Council of Europe, The international covenant on civil and political rights, Retrieved from: https://www.coe.int/en/web/compass/the-international-covenant-on-civil-and-political-rights (total ratification 173 states.) Accessed on January 2, 2021.

Council of Europe,(2013)., Capacity building on cybercrime, Retrieved from: https://rm.coe.int/16802fa3e6 (Accessed on November 1, 2020)

Council of Europe,(2013)., Capacity building on cybercrime, Retrieved from: https://rm.coe.int/16802fa3e6 (Accessed on November 1, 2020)

Council of Europe,(July 13, 2020)., The budapest convention on cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac Accessed on January 15, 2021.

Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac Accessed on October 02, 2020.

Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac Accessed on October 02, 2020, p:16

Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac Accessed on October 02, 2020, p:18-19

Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac Accessed on October 02, 2020, p:9

Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac Accessed on October 02, 2020, p:10

Council of Europe,(July 13, 2020)., The Budapest Convention on Cybercrime: benefits and impact in practice Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac Accessed on October 02, 2020. p: 12

Council of Europe. (2000). "Assembly backs protocol on strengthening personal data protection" Retrieved from: https://rm.coe.int/0900001680962597 (Accessed on November 12, 2020).

Council of Europe. (April 1-2, 2008) "Octopus Interface Conference Cooperation Against Cybercrime" Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f6980 Accessed on November 20, 2020.

Council of Europe. (April 22, 2019) Retrieved from: https://rm.coe.int/summary-of-the-cybercrime-octopus/1680968ab0 Accessed on November 18, 2020

Council of Europe. (December 3, 2019) Retrieved from: https://www.coe.int/en/web/cybercrime/iproceeds1/-/asset_publisher/0q0xphlFQY9G/content/iproceeds-graduation-of-the-ucd-master-programme-on-forensic-computing-and-cybercrime-investigation? Accessed on November 17, 2020.

Council of Europe. (December 9-10, 2019). "iPROCEEDS: Closing Conference"

Council of Europe. (February 26-28, 2020) Retrieved from: https://www.coe.int/en/web/cybercrime/-/cybereast-international-meeting-on-cooperation-with-foreign-service-providers Accessed November 17, 2020.

Council Of Europe. (January 28, 2003) "Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems" Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 Accessed on November 13, 2020

Council of Europe. (July 08, 2020) "EndOCSEA@Europe Project Summary" Retrieved from: https://rm.coe.int/-vc1840-project-summary-final-jul-2020/16809ef6af Accessed on November 15, 2020.

Council of Europe. (July 11-13, 2018) "Octopus Conference 2018 Cooperation Against Cybercrime" Retrieved from: https://rm.coe.int/octopus2018-lop-11jul/16808c54d9 Accessed on November 22, 2020

Council of Europe. (June 11-12, 2007) "Octopus Interface Conference 2007 Cooperation Against Cybercrime" Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f6a08 Accessed on November 20, 2020.

Council of Europe. (March 10-11, 2009) “Octopus Interface Conference Cooperation Against Cybercrime “ Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f25c3 Accessed on November 20, 2020.

Council of Europe. (March 10-11, 2019) “Octopus Interface Conference Cooperatin Against Cyberbercrime” Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f25c3 Accessed on November 22, 2020

Council of Europe. (March 23-25, 2010) “Octopus Interface Conference Cooperation against Cybercrime” Retrieved from: https://www.coe.int/en/web/cybercrime/octopus-interface-2010 Accessed on November 20, 2020.

Council of Europe. (March 23-25, 2010) “Octopus Interface Conference Cooperation Against Cybercrime “ Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f24d4 Accessed on November 20, 2020.

Council of Europe. (May 21-24, 2018) “iPROCEEDS: Investigating cybercrime and its financial gain under the last Cybercrime Simulation Exercise” Retrieved from: https://www.coe.int/en/web/cybercrime/iproceeds1/-/asset_publisher/0q0xphlFQY9G/content/iproceeds-investigating-cybercrime-and-its-financial-gain-under-the-last-cybercrime-simulation-exercise? Accessed on November 17, 2020

Council of Europe. (November 20, 2016). "Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime" Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806bf0f8 Accessed on November 15, 2020.

Council of Europe. (November 20-22, 2019) "Octopus Conference 2019 Cooperation Against Cybercrime "https://www.coe.int/en/web/cybercrime/octopus-interface-2019 Accessed on November 22, 2020

Council of Europe. (November 21-23, 2011) "Octopus Conference 2011 Cooperation Against Cybercrime" Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2425 Accessed on November 20, 2020

Council of Europe. (November 23, 2001) "Convention on Cybercrime" Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on November 12, 2020).

Council of Europe. (November 23, 2001) "Convention on Cybercrime" Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Accessed on November 12, 2020.)

Council of Europe. (November 23, 2001) "Convention on Cybercrime" Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 Accessed on November 13, 2020.

Council Of Europe. (Status as of November 30, 2020) Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=7tZMZRq7 Accessed on November 13, 2020

Council of Europe. “Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY “ Retrieved from: https://www.coe.int/en/web/cybercrime/parties-observers Accessed on November 12, 2020.

Council of Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/capacity-building-programmes Accessed on November 15, 2020.

Council of Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/glacyplus Accessed on November 15, 2020.

Council OF Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/iproceeds#:~:text= Accessed on December 5, 2020.

Council of Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/cybereast Accessed on November 18, 2020

Council of Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/cybersouth Accessed on November 18, 2020

Council of Europe. Retrieved from: https://www.coe.int/en/web/cybercrime/octopus-conference Accessed on November 18, 2020.

Csonka, P. (2006). The council of europe's convention on cyber-crime and other European initiatives. *Revue internationale de droit penál*, *77*(3), p.473-501.

DaCosta, F., & Henderson, B. (2013). *Rethinking the Internet of Things: a scalable approach to connecting everything* Springer Nature. p. 42.

Dreher, A., Gaston, N., & Martens, P. (2008). Measuring Globalisation. *Gauging its Consequences Springer, New York*.

Dreher, A., Gaston, N., & Martens, P. (2008). Measuring Globalisation. *Gauging its Consequences Springer, New York*. P.16-17

Drezner, D. W., & Drezner, D. W. (1999). *The sanctions paradox: Economic statecraft and international relations* (No. 65). Cambridge University Press. p 7-9

EC-Council, (November 2020), Retrieved from: https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/ Accessed on January 05, 2021

Eltantawy, N., & Wiest, J. B. (2011). The Arab spring| Social media in the Egyptian revolution: reconsidering resource mobilization theory. *International journal of communication*, *5*, 18.

ENISA, (September 2017). ENISA overview of cybersecurity and related terminology, Retrieved from: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology. Accessed on February 18, 2021

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations:(IR) relevant theory?. *International political science review*, *27*(3), p.221

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR) relevant theory?. *International political science review*, *27*(3), 221-244.

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations:(IR) relevant theory?. *International political science review*, *27*(3), 224

EU, Cybercrime, Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en (Accessed on February 18, 2021)

European Commission, (June, 11, 2017), How can we improve cross-border access to e-evidence? Retrieved from: https://ec.europa.eu/home-affairs/news/how-can-we-improve-cross-border-access-e-evidence_en Accessed on January 23, 2021.

European Union, (December 15, 1997) "Directive 97/66/EC Of The European Parliament And Of The Council Concerning The Processing Of Personal Data And The Protection Of Privacy In The Telecommunications Sector" Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=en Accessed on November 10, 2020.

European Union, (October 16, 1996) "Illegal and harmful content on the Internet" Retrieved from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0487:FIN:en:PDF Accessed November 10, 2020.

European Union, (October 24, 1995) “Directive 95/46/EC Of The European Parliament And Of The Council” Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN Accessed on November 10, 2020

European Union. (2013). “Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace” Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52013JC0001&from=HU Accessed on November 10, 2020

European Union. (December 8, 199). “eEurope - An Information Society for All” Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24221&from=FI Accessed on November 8, 2020

European Union. (January 12, 2005) “Regulation (Ec) No 184/2005 Of The European Parliament And Of The Council On Community Statistics Concerning Balance Of Payments, International Trade In Services And Foreign Direct Investment” Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005R0184&qid=1605006979191&from=EN Accessed on November 10, 2020.

European Union. (March 7, 2002) “Directive 2002/19/EC Of The European Parliament And Of The Council On Access To, And Interconnection Of, Electronic Communications Networks And Associated Facilities (Access Directive)” Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0019&qid=1606722783130&from=EN Accessed on November 10, 2020

European Union. “Cybercrime” Retrieved from: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en (Accessed on November 10, 2020).

European Union. Retrieved from: https://ec.europa.eu/neighbourhood-enlargement/neighbourhood/southern-neighbourhood_en#:~:text= Accessed November 18, 2020

Facebook Help Center, Report Suicidal Content, Retrieved from: https://www.facebook.com/help/contact/305410456169423 Accessed on January 19, 2021.

Facebook Investor Relations, (2014) Facebook Reports Fourth Quarter and Full Year 2014 Results, Retrieved from: https://investor.fb.com/investor-news/press-release-details/2015/Facebook-Reports-Fourth-Quarter-and-Full-Year-2014-Results/default.aspx Accessed on December 19, 2020

Facebook Investor Relations, (2019), Facebook Reports Fourth Quarter and Full Year 2019 Results Retrieved from: https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results/default.aspx Accessed on December 19, 2020.

Facebook, (March 1, 2017)., Building a Safer Community With New Suicide Prevention Tools Retrieved from: https://about.fb.com/news/2017/03/building-a-safer-community-with-new-suicide-prevention-tools/ Accessed on January 18, 2021.

Facebook, (September 10, 2018) How Facebook AI Helps Suicide Prevention, Retrieved from: https://about.fb.com/news/2018/09/inside-feed-suicide-prevention-and-ai/ Accessed on January 18, 2021.

Facebook, Help Center, Retrieved from: https://www.facebook.com/help/224562897555674?helpref=faq_content (Accessed on March 4, 2021)

Facebook, Transparency, Government requests for user data, Retrieved from: https://transparency.facebook.com/government-data-requests/jan-jun-2019 Accessed on January 10, 2021.

Facebook, Transparency, Government requests for user data, Retrieved from: https://transparency.facebook.com/government-data-requests/jul-dec-2019 Accessed on January 10, 2021.

Facebook, Transparency, Retrieved from: https://transparency.facebook.com/ Accessed on February 01, 2021.

Fearon, J. D. (1998). Bargaining, enforcement, and international cooperation. *International organization*, *52*(2), p.269-305.

Finkelstein, L. S. (1995). What is global governance?. *Global Governance: A Review of Multilateralism and International Organizations*, *1*(3), p.367-372.

FoxNews, (April 15, 2010), "7,500 Online Shoppers Unknowingly Sold Their Souls" Retrieved from: https://www.foxnews.com/tech/7500-online-shoppers-unknowingly-sold-their-souls Accessed on December 1, 2020.

Freeman, M. (2015). Neoliberal Policies and Human Rights. *Dokuz Eylul Universitesi Hukuk Fakultesi Dergisi*, *17*, p.141.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society* (pp. 3-540). London: Addison-Wesley.

G7 Information Center, (July 21-23, 200) “G8 Okinawa Summit: Documents” Retrieved from: http://www.g7.utoronto.ca/summit/2000okinawa/ Accessed on November 4, 2020.

G7 Information Center, (June 29, 1996) “Lyon Summit Documents” Rete-rieved from: http://www.g7.utoronto.ca/summit/1996lyon/chair.html. Accessed on November 4, 2020.

G7 Information Center. (July 7–9, 2008). “Hokkaido Toyako Summit” Retrieved From http://www.g7.utoronto.ca/summit/2008hokkaido/index.html Accessed on November 5, 2020.

G7 Information Center. (June 17, 1995) “Halifax Summit Documents” Retrieved from: http://www.g7.utoronto.ca/summit/1995halifax/chairman.html Accessed on November 4, 2020.

G7 Information Center. (June 8, 2007) “Heiligendamm Summit” Retrieved From http://www.g7.utoronto.ca/summit/2007heiligendamm/g8-2007-ct.html Accesed November 5, 2020

Gercke, M. (2016). Understanding cybercrime: a guide for developing countries. ITU, (pp 89-91)

German Law Archive, (September 01, 2017)., Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG), Retrieved from: https://germanlawarchive.iuscomp.org/?p=1245 Accessed on October 03,2020.

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the US criminal justice system. *Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. Priority Criminal Justice Needs Initiative. Rand Corporation*.

Google Alphabet, (2019). Alphabet Announces Fourth Quarter and Fiscal Year 2019 Results Retrieved from: https://abc.xyz/investor/static/pdf/2019Q4_alphabet_earnings_release.pdf?cache=79552b8 Accessed on December 20, 2020.

Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=authority:&lu=user_data_produced&user_data_produced=authority:CN;series:compliance Accessed on January 13, 2021

Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=series:requests,accounts;authority:TR;time:Y2019H1&lu=user_requests_report_period Accessed on January 12, 2021.

Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=series:requests,accounts,compliance;authority:TR;time:Y2019H2&lu=user_requests_report_period Accessed on January 12, 2021

Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr Accessed on January 13, 2021.

Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=authority:&lu=user_data_produced&user_data_produced=authority:RU;series:compliance Accessed on January 13, 2021.

Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=authority:&lu=user_data_produced&user_data_produced=authority:BG;series:compliance Accessed on January 13, 2021.

Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_data_produced=authority:IR;series:compliance&lu=user_data_produced Accessed on January 13, 2021.

Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_data_produced=authority:MD;series:compliance&lu=user_data_produced Accessed on January 13, 2021.

Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_data_produced=authority:TH;series:compliance&lu=user_data_produced Accessed on January 13, 2021.

Google Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_data_produced=authority:HU;series:compliance&lu=user_data_produced Accessed on January 13, 2021.

Google, (2020). Google Transparency Report, Government Requests to Remove Content, Retrieved From: https://transparencyreport.google.com/government-removals/overview, Accessed on December 10, 2020.

Google, Policies, Retrieved from: https://policies.google.com/terms/information-requests (Accessed on July 17, 2021)

Google, Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=series:requests,accounts;authority:TR;time:Y2019H1&lu=user_requests_report_period Accessed on January 11, 2021.

Google, Transparency Report, Retrieved from: https://transparencyreport.google.com/user-data/overview?hl=tr&user_requests_report_period=series:requests,accounts,compliance;authority:TR;time:Y2019H2&lu=user_requests_report_period Accessed on January 11, 2021.

Google, Transparency, Retrieved from: https://transparencyreport.google.com/?hl=tr Accessed on February 01, 2021.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20. https://www.coe.int/en/web/octopus-old2019/blog/-/blogs/computer-related-forgery-and-computer-related-fraud-the-need-to-build-and-include-these-new-criminal-types-in-a-modern-penal-code/ (Accessed on March 01, 2021)

Huey, L., & Rosenberg, R. (2004). Watching the web: Thoughts on expanding police surveillance opportunities under the cyber-crime convention. *Canadian Journal of Criminology and Criminal Justice*, *46*(5), 597-606.

Hughes, C. W., & Lai, Y. M. (Eds.). (2011). *Security studies: a reader*. Routledge. pp. 157-162

Hungary Today, (July 12, 2019), Kaszás, F., Instead of jail time, ethical hacker fined for exposing vulnerability in telekom's system Retrieved from: https://hungarytoday.hu/instead-of-jail-time-ethical-hacker-fined-for-exposing-vulnerability-in-telekoms-system/ Accessed on January 07, 2021.

Instagram, Self-injury, Retrieved from: https://www.facebook.com/help/instagram/553490068054878 Accessed on January 18, 2021.

International Telecommunication Union, (2018), Global Cybersecurity Index, Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf Accessed on December 5, 2020. p 8

International Telecommunication Union, (2018), Global Cybersecurity Index, Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf Accessed on December 5, 2020 pp 63.

International Telecommunication Union, (November 2014). Understanding cybercrime phenomena challenges and legal response, Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf Accessed on January 5, 2021

Investopedia, Kolakowski, M., (Jan 06, 2020). At $1.3 Trillion, Apple Is Bigger Than These Things, Retrieved from: https://www.investopedia.com/news/apple-now-bigger-these-5-things/ Accessed on December 21, 2020.

Isnarti, R. (2016). A Comparison of Neorealism, Liberalism, and Constructivism in Analyzing Cyber War. *Andalas Journal of International Studies (AJIS)*, *5*(2), p. 155

Isnarti, R. (2016). A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. *Andalas Journal of International Studies (AJIS)*, *5*(2), p.158-160

İstanbul Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı, (September 7, 2013)., Retrieved from: https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarih%C3%A7esi Accessed on October 13, 2020.

ITU, (April 18, 2008) Retrieved form: https://www.itu.int/rec/T-REC-X.1205-200804-I Accessed on February 18, 2021.

Janczewski, L., & Colarik, A. (Eds.). (2007). *Cyber warfare and cyber terrorism*. IGI Global.

Jervis, R. (1978). Cooperation under the security dilemma. *World Politics: A Quarterly Journal of International Relations*, 167-214.

Jessop, B. (2002). *Liberalism, Neoliberalism, and Urban Governance: A State-Theoretical Perspective. Antipode, 34(3), 452–472*. doi:10.1111/1467-8330.00250

Johnson, D. G. (2002). Globalization: what it is and who benefits. *Journal of Asian Economics*, *13*(4), 427-439.

Jørgensen, K. E. (2017). *International relations theory: A new introduction*. Macmillan International Higher Education.184-187

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons*, *53*(1), p.59-68.

Kelling, G. L., & Wilson, J. Q. (1982). Broken windows. *Atlantic monthly*, *249*(3), 29-38.

Kemmerer, R. A. (2003). *Cybersecurity. 25th International Conference on Software Engineering, 2003. Proceedings.* pp.3

Kendall, G. (2003). From liberalism to neoliberalism. In *Social Change in the 21st Century 2003 Conference Refereed Proceedings* (pp. 1-14). Centre for Social Change Research, School of Humanities and Human Services QUT.

Keohane, R. (2011). Neoliberal institutionalism. *Security studies: A reader*. pp. 157-164.

Keohane, R. O. (1984). *After hegemony: Cooperation and discord in the world political economy*. Princeton university press. p. 89-90

Keohane, R. O. (2003). *Global governance and democratic accountability* p. 130-156.

Keohane, R. O., & Nye Jr, J. S. (1998). Power and interdependence in the information age. *Foreign Aff.*, *77*, 81.

Keohane, R. O., & Nye Jr, J. S. (2000). Globalization: What's new? What's not? (And so what?). *Foreign policy*, 104-119.

Keohane, R. O., & Nye, J. S. (1987). Power and Interdependence revisited. *International organization*, *41*(4), 725-753.

Keohane, R. O., & Nye, J. S. (1987). Power and Interdependence revisited. *International organization*, *41*(4), 725-753.

Keohane, R. O., & Nye, J. S. (1987). Power and Interdependence revisited. *International organization*, *41*(4), 725-753.

Kierkegaard, S. M. (2007). International Cybercrime Convention. In *Cyber warfare and cyber terrorism* (pp. 469-476). IGI Global.

Kissel, R. (Ed.). (2011). *Glossary of key information security terms*. Diane Publishing. p. 57

Koziarski, J., & Lee, J. R. (2020). Connecting evidence-based policing and cybercrime. *Policing: An International Journal*.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22-31.

Lev Grossman, "Person of the Year 2010: Mark Zuckerberg," *Time*, 15 December 2010, http://content.time.com/time/specials/packages/article/0,28804,2036683_2037183_2037185,00.html Accessed on October 7, 2020

Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. *Center for Strategic and International Studies*. pp.1

Li, J. X. (2017). Cyber crime and legal countermeasures: A historical analysis. *International Journal of Criminal Justice Sciences*, *12*(2), 196-207.

Li, J. X. (2017). Cyber crime and legal countermeasures: A historical analysis. *International Journal of Criminal Justice Sciences*, *12*(2), 196-207.

Li, X. (2007). International actions against cybercrime: Networking legal systems in the networked crime scene. *Li, Xingan." International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene." Webology*, *4*(3).

Li, X. (2007). International actions against cybercrime: Networking legal systems in the networked crime scene. *Li, Xingan." International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene." Webology*, *4*(3).

Marson, S. M. (1997). A selective history of Internet technology and social work. *Computers in Human Services*, *14*(2), p.35-49

McAfee, Lewis j. (February 18). Economic impact of cybercrime no slowing down, Retrieved from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf Accessed on November 1, 2020)

Mercado,S.C. (2007). Sailing the sea of OSINT in the information age, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html#top. Accessed on July 17, 2020

Mestçi A., (2007). Turkey's internet report in 2007, Retrieved from: http://inet-tr.org.tr/inetconf12/kitap/Bildiriler/30_24_inet07.pdf Accessed on September 7, 2020.

Microsoft Corporate Social Responsibility, Law Enforcement Requests Reports, Retrieved from: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report Accessed on January 15, 2021.

Microsoft, Microsoft office locations around the world, Retrieved from: https://www.microsoft.com/en-us/worldwide.aspx Accessed on January 20, 2021.

Microsoft, Transparency, Retrieved from: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report Accessed on February 01, 2021.

Monge, Peter and Contractor, Noshir (2003) Theories of Communication Networks. Oxford: Oxford University Press.

Morozov, E. (2009). Iran: Downside to the" Twitter revolution". *Dissent*, *56*(4), 10-14.

National Center for Missing & Exploited Children , (2017), The Online Enticement of Children: An In-Depth Analysis of CyberTipline Reports https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel1.pdf , Accessed on December 10, 2020.

National Center for Missing & Exploited Children , About NCMEC, https://www.missingkids.org/footer/media/keyfacts Accessed on December, 10, 2020.

National Center for Missing & Exploited Children, (2015), Trends identified in CyberTipline sextortion reports https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf Accessed on December 10, 2020.

National Center for Missing & Exploited Children, (2016), Global Research Project: A Global Landscape of Hotlines Combating Child Sexual Abuse Material on the Internet and an Assessment of Shared Challenges, Retrieved From: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/grp.pdf Accessed on December 10, 2020.

National Center for Missing & Exploited Children, (2020), 2019 Reports by Electronic Service Providers (ESP) https://www.missingkids.org/content/dam/missingkids/gethelp/2019-reports-by-esp.pdf Accessed on December 10, 2020.

National Center For Missing & Exploited Children, (2020). "2019 Reports by Electronic Service Providers (ESP)" Retrieved from: https://www.missingkids.org/content/dam/missingkids/gethelp/2019-reports-by-esp.pdf Accessed on December 8, 2020.

NewYorkPost, Twitter refused to remove child porn because it didn't 'violate policies': lawsuit, Retrieved from: https://nypost.com/2021/01/21/twitter-sued-for-allegedly-refusing-to-remove-child-porn/ (Accessed on July 18, 2021)

NewsinEnglish, (June 16, 2013)., Murder suspect arrested in Rome Retrieved from: https://www.newsinenglish.no/2013/06/16/murder-suspect-arrested-in-rome/ Accessed on October 02, 2020.

Nye, J. S., & Keohane, R. O. (1971). Transnational relations and world politics: An introduction. *International organization*, *25*(3), 24-26

Odysseos, L. (2010). Human rights, liberal ontogenesis and freedom: producing a subject for neoliberalism?. *Millennium*, *38*(3), 747-772.

OECD, (1992) “OECD Guidelines for the Security of Information Systems, 1992” Retrieved from: http://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm Accessed November 7, 2020. (Replaced in 2002 as OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security)

OECD, (April 19, 2006). “Report Of The OECD Task Force On Spam: Anti-Spam Toolkit of Recommended Policies and Measures” Retrieved From: http://www.oecd.org/digital/consumer/36494147.pdf Accessed on November 8, 2020.

OECD, (January 14, 2020) “Reducing Systemic Cybersecurity Risk” Retrieved From: https://www.oecd.org/newsroom/46894657.pdf Accessed on November 8, 2020.

OECD, (July 25, 2002) “OECD Guidelines for the Security of Information Systems and Networks TOWARDS A CULTURE OF SECURITY” Retrieved from: http://www.oecd.org/digital/ieconomy/15582260.pdf Accessed on November 8, 2020.

OECD, (September 23, 1980) “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” Retrieved From: http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm Accessed on November 7, 2020. (Updated in 2013)

OECD, “National Terrorism Risk Insurance Programmes Of OECD Countries With Government Participation Main Features” Retrieved from: https://www.oecd.org/daf/fin/insurance/Terrorism-Risk-Insurance-Country-Comparison.pdf Accessed on November 8, 2020

OECD, “OECD Guidelines for Consumer Protection in the Context of Electronic Commerce Frequently Asked Questions (FAQ)” Retrieved from: https://www.oecd.org/sti/consumer/2091663.pdf Accessed on November 8, 2020.

Ozbek, M. (2015). The Impacts of European Cybercrime Convention on Turkish Criminal Law. *GSI Articletter*, *13*, 73.

Parker, D. B., Abt Associates, & SRI International. (1989). *Computer crime: Criminal justice resource manual*. US Department of Justice, National Institute of Justice, Office of Justice Programs.

Parmar, I., Miller, L. B., & Ledwidge, M. (Eds.). (2009). *New directions in US foreign policy*. Routledge. pp 48-57

Pieterse, J. N. (1996). Globalisation and culture: Three paradigms. *Economic and political weekly*, 1389-1393

Princeton University Press. Retrieved from: http://assets.press.princeton.edu/chapters/i9827.pdf Accessed on Janury 23, 2021

Princeton University,” Introduction” Retrieved from: http://assets.press.princeton.edu/chapters/i9827.pdf Accessed on February 20, 2020.

Republic of Turkey, Ministry of Internal Affairs , (August 14, 2020). "Turkish National Police Cybercrime Department Investigated 14.186 Social Media Accounts As Of January 1. " Retrieved from: https://www.icisleri.gov.tr/siber-suclarla-mucadele-daire-baskanligi-tarafindan-1-ocaktan-bugune-14186-hesap-hakkinda-calisma-yapildi , Accessed on December 10, 2020.

Republic of Turkey, Ministry of Internal Affairs, (April 23, 2020), "1748 Accounts That Sharing Unfounded Coronavirus News And Making Terrorist Propaganda On Social Media Were Detected". Retrieved From: https://www.icisleri.gov.tr/sosyal-medyada-asilsiz-koronavirus-paylasimlari-ve-teror-propagandasi-yapan-1748-hesap-tespit-edildi. Accessed on December 10, 2020.

Republic of Turkey, Ministry of Internal Affairs, (April 6, 2020). "3,576 Social Media Accounts Examined 229 Persons Were Captured " Retrieved from: https://www.icisleri.gov.tr/3576-adet-sosyal-medya-hesabi-incelendi-229-sahis-yakalandi, Accessed on December 10, 2020.

Republic of Turkey, Ministry of Justice, Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü Retrieved from: https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/ikili.html Accessed on January 21, 2021.

Retrieved from: https://www.coe.int/en/web/cybercrime/iproceeds1/-/asset_publisher/0q0xphlFQY9G/content/iproceeds-closing-conference Accessed on November 17, 2020.

Rosenau, J. N., Czempiel, E. O., & Smith, S. (Eds.). (1992). *Governance without government: order and change in world politics* (Vol. 20). Cambridge University Press.

Sabah, (January 31, 2020) We are online around 7,5 hours in a day, Retrieved from: https://www.sabah.com.tr/teknokulis/haberler/2020/01/31/gunde-75-saat-internetteyiz (Accessed on November 1, 2020)

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 53-74.

Schulzrinne, H., & Rosenberg, J. (1999). Internet telephony: Architecture and protocols–an IETF perspective. *Computer Networks*, *31*(3), 237-255.

Seger, A. (2012) "Cybercrime Strategies". Rerieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e1 Accessed on November 1, 2020

Seger, A., (February 25-27, 2019), Council of Europe, Retrieved from: https://rm.coe.int/09000016809326ac Accessed on November 1, 2020.

Seger, A., (November, 20-22, 2019). Council of Europe, Results of capacity building and impact on legislation, Retrieved from: https://rm.coe.int/090000168098e27b (Accessed on January 15, 2021).

Seger. A. (2012) "Cybercrime Strategies". Rerieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e1 Accessed on November 1, 2020

Seger. A. (2012) "Cybercrime Strategies". Rerieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e1 Accessed on November 1, 2020.

Simon Kemp (18 February 2020), Digital 200: Turkey, retrieved from: https://web.archive.org/web/20200612160417/https://datareportal.com/reports/digital-2020-turkey Accessed on September 7, 2020.

Smith, S. W. (2004). *U.S. Patent No. 6,771,971*. Washington, DC: U.S. Patent and Trademark Office.

Sözcü, ATAM, H., (October 10, 2020). Police conducted operations in 17 provinces, 22 criminals were arrested, Retrieved from: https://www.sozcu.com.tr/2020/gundem/17-ilde-cocuk-pornosu-operasyonu-22-kisi-yakalandi-6075151/ Accessed on: January 17, 2021

Statista, Number of network connected devices per person around the world from 2003 to 2020, Retrieved from: https://www.statista.com/statistics/678739/forecast-on-connected-devices-per-person/, Accessed on January 17, 2021

Statista, Richter. F., (August 2, 2012), The rapid rise of social media, https://www.statista.com/chart/521/the-rapid-rise-of-social-media/ Accessed on September 01, 2020

Steans, J., Pettiford, L., Diez, T., & El-Anis, I. (2013). *An introduction to international relations theory: Perspectives and themes*. Routledge.

Taber, J. K. (1978). On Computer Crime (Senate Bill S. 240), 1 Computer LJ 517 (1978). *The John Marshall Journal of Information Technology & Privacy Law*, *1*(1), 16.

The Atlantic. Barber R. B. Retrieved From: https://www.theatlantic.com/magazine/archive/1992/03/jihad-vs-mcworld/303882/ Accessed on November 5, 2020

The Guardian, (2014). https://www.theguardian.com/technology/2014/jul/12/chinese-man-charged-with-hacking-into-us-fighter-jet-plans. Accessed on July 27, 2020.

The Guardian, (April, 8, 2009) Moldova forces regain control of parliament after 'Twitter revolution' Retrieved from: https://www.theguardian.com/world/2009/apr/08/moldova-protest-election-chisinau Accessed on September 9, 2020.

The Guardian, (August 12, 2019), Bug bounty': Apple to pay hackers more than $1m to find security flaws, Retrieved from: https://www.theguardian.com/technology/2019/aug/12/apple-hackers-black-hat-conference Accessed on January 07, 2021.

The Harvard Crimson. Kaplan A. Katherine, (November 19, 2003) https://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/ Accessed on September 1, 2020

The New York Times, (April 4, 2018), Facebook says Cambridge analytica harvested data of up to 87 million users, Retrieved from: https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html

The New York Times, (October 21, 2000) A Filipino linked to love bug talks about his license to hack. Retrieved from: https://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html (Accessed on February 28, 2021)

The New York Times, Retrieved from: https://www.nytimes.com/2018/12/31/technology/facebook-suicide-screening-algorithm.html Accessed on January 18, 2021.

Tosoni, L. (2018). Rethinking Privacy in the Council of Europe's Convention on Cybercrime. *Computer Law & Security Review*, *34*(6), 1197-1214.

Trottier, D., & Fuchs, C. (Eds.). (2014). *Social media, politics and the state: protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube*. Routledge. (209-224)

Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. *Journal of democracy*, *28*(4), 46-59.

TUİK. (04 February 2020). Adrese Dayalı Nüfus Kayıt Sistemi Sonuçları, 2019, Retrieved from: https://data.tuik.gov.tr/Bulten/Index?p=Adrese-Dayali-Nufus-Kayit-Sistemi-Sonuclari-2019-33705, Accessed on November 11, 2020.

Turkish National Assembly, (February 21, 2001), Law of Intellectual Property Rights, Retrieved from: https://www.tbmm.gov.tr/kanunlar/k4630.html (Accessed on March 8, 2021)

Turkish National Assembly, (September 26, 2004), Turkish Criminal Code, Retrieved from: https://www.tbmm.gov.tr/kanunlar/k5237.html (Accessed on March 8, 2021)

Twitter, @benjami2533977, (Februay 18, 2020 responded to @samuelhunningt1) Retrieved from:https://mobile.twitter.com/benjami25333977/status/1229671592181063681 Accessed on November 5, 2020

Twitter, @samuelhunningt1, (February 18, 2020) Retrieved from: https://mobile.twitter.com/samuelhunningt1/status/1229670935273377793 Accessed on November 5, 2020.

Twitter, @SchimelfenigX, (February 18, 2020 responded to @samuelhunningt1 and @benjami2533977)https://mobile.twitter.com/SchimelfenigX/status/1229672055227940864 Accessed on November 5, 2020

Twitter, Defending and respecting the rights of people using our service, Retrieved from: https://help.twitter.com/en/rules-and-policies/defending-and-respecting-our-users-voice Accessed on January 23, 2021.

Twitter, FAQ, Retrieved from: https://investor.twitterinc.com/contact/faq/default.aspx , Accessed on December 11, 2020

Twitter, Help Center, Report suicidal content, Retrieved from: https://help.twitter.com/forms/report_self_harm Accessed on January 18, 2021.

Twitter, Jack Dorsey, (@jack) (October 15, 2020) Retrieved from: https://twitter.com/jack/status/1316528193621327876 Accessed on January, 12, 2021.

Twitter, Transparency Report, Information Requests, https://transparency.twitter.com/en/reports/information-requests.html#2019-jan-jun Accessed on December 11, 2020.

Twitter, Transparency, Information requests, Retrieved from: https://transparency.twitter.com/en/reports/information-requests.html#2019-jan-jun Accessed on January 10, 2021.

Twitter, Transparency, Information Requests, Retrieved from: https://transparency.twitter.com/en/reports/information-requests.html#2019-jul-dec Accessed on January 10, 2021.

Twitter, Transparency, Information Requests, Retrieved from: https://transparency.twitter.com/en/reports/information-requests.html#2019-jul-dec Accessed on January 19, 2021.

Twitter, Transparency, Retrieved from: https://transparency.twitter.com/ Accessed on February 01, 2021.

Twitter, Twitter Safety, (@TwitterSafety) (January 7, 2021) Retrieved from: https://twitter.com/TwitterSafety/status/1346970431039934464 Accessed on January 13, 2021.

Twitter, Twitter Safety, (@TwitterSafety), (January 9, 2021) Retrieved from: https://twitter.com/TwitterSafety/status/1347684877634838528 Accessed on January 10, 2021.

U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, Electronic Communications Privacy Act of 1986 (ECPA), Retrieved from: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 Accessed on October 03, 2020.

UN, Cybercrime, Retrieved from: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html (Accesssed on February 18, 2021.)

UN. (April 10-17, 2000). "Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders" Retrieved from: https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf Accessed on November 1, 2020

UNCTAD, (April 2, 2020). Data Protection and Privacy Legislation Worldwide Retrieved from: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide Accessed on January 4, 2021.

United Nationas (January 22, 2001) "55/63. Combating the criminal misuse of information technologies" Retrieved From: https://undocs.org/en/A/RES/55/63. (Accessed on November 02, 2020)

United Nationas (January 23, 2020) "56/121. Combating the criminal misuse of information technologies" Retrieved from: https://undocs.org/en/A/RES/56/121. (Accessed on November 02, 2020)

United Nationas (January 23, 2020) "56/121. Combating the criminal misuse of information technologies" Retrieved from: https://undocs.org/en/A/RES/56/121. Accessed on November 02, 2020.

United Nationas, (May 17, 2005). "Eleventh United Nations Congress on Crime Prevention and Criminal Justice" Retrieved from: https://www.unodc.org/documents/congress/Documentation/11Congress/ACONF203_18_e_V0584409.pdf (Accessed on November 02, 2020)

United Nations (January 22, 2001) "55/63. Combating the criminal misuse of information technologies" Retrieved From: https://undocs.org/en/A/RES/55/63. Accessed on November 02, 2020.

United Nations, Member States, Retrieved from: https://www.un.org/en/member-states/ (Accessed November 2, 2020)

University of Toronto G8 Information Centre, (May 11, 2001) "Genoa Summit" Retrieved from: http://www.g7.utoronto.ca/summit/2001genoa/dotforce1.html Accessed on November 5, 2020.

UNODC, (April 12, 2019). "Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019" Retrieved From: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Report/UNODC_CCPCJ_EG.4_2019_2_E.pdf Accessed on December 2, 2020.

UNODC, (April 4, 2018). "Expert Group to Conduct a Comprehensive Study on Cybercrime" Retrieved from: https://ccdcoe.org/uploads/2018/11/UN-180404-Expert_Group_to_Conduct_a_Comprehensive_Study_on_Cybercrime.pdf Accessed on December 4, 2020.

Ünver, M., Canbay, C., MİRZAOĞLU, A. G., ÇETİNKAYA, E., & Teknolojileri, B. (2009). Uluslararası Kuruluşların Siber GüvenliN Faaliyetleri. *Konulu makale*, 10.

Van Dijck, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford University Press.

Van Dijck, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford University Press.

Vatis, M. A. (2010, June). The Council of Europe Convention on Cybercrime. In *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy http://www. nap. edu/catalog/12997.html. p 219-220*

Verizonmedia, Government Data Requests, Retrieved from: https://www.verizonmedia.com/transparency/reports/government-data-requests.html Accessed on 10, 2021.

VerizonMedia, Transparency, Retrieved from: https://www.verizonmedia.com/transparency/index.html Accessed on February 01, 021.

Viotti, P. R., & Kauppi, M. V. (2019). *International relations theory*. Rowman & Littlefield.

Watson Amy, Jun 23 2020, Share of adults who use social media as a source of news in selected countries worldwide as of February 2020, Statista, https://www.statista.com/statistics/718019/social-media-news-source/, Accessed on October 8, 2020.

We are Social, (Jan 2020) Dily time spent using social media. Retrieved from: https://wearesocial-net.s3.amazonaws.com/uk/wp-content/uploads/sites/2/2020/01/10-Social-Media-Daily-Time-%E2%80%93-DataReportal-Digital-2020-Global-Digital-Overview-Slide-92.png Accessed on February 17, 2020

We are Social. (Jan 2020). Time per day spent using the internet. Retrieved From: https://wearesocial-net.s3.amazonaws.com/uk/wp-content/uploads/sites/2/2020/01/02-Internet-Daily-Time-%E2%80%93-DataReportal-Digital-2020-Global-Digital-Overview-Slide-43.png Accessed on February 17, 2020

We PROTECT Global Alliance. “WPGA Membership” Retrieved from: https://www.weprotect.org/members Accessed on November 15, 2020

Weber, A. M. (2003). The Council of Europe's Convention on Cybercrime. *Berkeley technology law journal*, *18*(1), 425-446.

Weber, A. M. (2003). The Council of Europe's Convention on Cybercrime. *Berkeley technology law journal*, *18*(1), 425-446

Weiss, L. (2005). The state-augmenting effects of globalisation. *New Political Economy*, *10*(3), 345

WhatsApp, Staying safe on WhatsApp, Retrieved from: https://faq.whatsapp.com/general/security-and-privacy/staying-safe-on-whatsapp Accessed on January 18, 2021.

Wikipedia, 2015 San Bernardino attack, Retrieved from: https://en.wikipedia.org/wiki/2015_San_Bernardino_attack Accessed on January 8, 2021.

Wikipedia, Retrieved from: https://en.wikipedia.org/wiki/Facebook Accessed on September 1, 2020.

World Economic Forum, Executive Summary, Retrieved From: http://reports.weforum.org/global-risks-report-2020/executive-summary/ Accessed on December 5, 2020.

World Health Organization,(June 8, 2020), “Violence Against Children” , Retrieved from: https://www.who.int/news-room/fact-sheets/detail/violence-against-children, Accessed on December 8, 2020

YouTube, (GlobalNews), (April 11, 2018), Retrieved from: https://www.youtube.com/watch?v=YCQ_ZGxE2U4&ab_channel=GlobalNews Accessed on January 10, 2021

YouTube, The Obama White House, (May, 29, 2009). President Obama on Cybersecurity, Retrieved from: https://www.youtube.com/watch?v=wjfzyj4eyQM&ab_channel=TheObamaWhiteHouse (Accessed on March 10, 2021).

YouTube. Global News, (April 18, 2018) Retrieved from: https://www.youtube.com/watch?v=YCQ_ZGxE2U4&ab_channel=GlobalNews Accessed December 1, 2020.

Zacher, M. W. (1990). Toward a theory of international regimes. *Journal of International Affairs*, 139-157

TURNITIN REPORT

Fatma AKIN AKILLI

ORİJİNALLİK RAPORU

%12	%10	%5	%7
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	inba.info İnternet Kaynağı	%1
2	wetten.overheid.nl İnternet Kaynağı	%1
3	www.gonullyourself.org İnternet Kaynağı	<%1
4	www.dud.de İnternet Kaynağı	<%1
5	Submitted to Loyola Marymount University Öğrenci Ödevi	<%1
6	Submitted to Tobb University of Economics & Technology Öğrenci Ödevi	<%1
7	www.internetjurisdiction.net İnternet Kaynağı	<%1
8	Submitted to Atilim University Öğrenci Ödevi	<%1
9	rm.coe.int İnternet Kaynağı	<%1

10	www.washingtonpost.com İnternet Kaynağı	<%1
11	Submitted to Tilburg University Öğrenci Ödevi	<%1
12	www.govinfo.gov İnternet Kaynağı	<%1
13	afyonluoglu.org İnternet Kaynağı	<%1
14	www.itu.int İnternet Kaynağı	<%1
15	Submitted to National Model United Nations Öğrenci Ödevi	<%1
16	Submitted to CSU, San Jose State University Öğrenci Ödevi	<%1
17	Submitted to University of College Cork Öğrenci Ödevi	<%1
18	adlisicil.adalet.gov.tr İnternet Kaynağı	<%1
19	Submitted to King's College Öğrenci Ödevi	<%1
20	Submitted to University of Salford Öğrenci Ödevi	<%1
21	"Miscellaneous", Commonwealth Law Bulletin, 2010	<%1

22	www.coe.int İnternet Kaynağı	<%1
23	Submitted to Napier University Öğrenci Ödevi	<%1
24	Submitted to Queen Mary and Westfield College Öğrenci Ödevi	<%1
25	www.scribd.com İnternet Kaynağı	<%1
26	Luca Tosoni. "Rethinking Privacy in the Council of Europe's Convention on Cybercrime", Computer Law & Security Review, 2018 Yayın	<%1
27	www.cyber-rights.org İnternet Kaynağı	<%1
28	www.europol.europa.eu İnternet Kaynağı	<%1
29	openknowledge.worldbank.org İnternet Kaynağı	<%1
30	link.springer.com İnternet Kaynağı	<%1
31	www.tandfonline.com İnternet Kaynağı	<%1

32	Submitted to Embry Riddle Aeronautical University Öğrenci Ödevi	<%1
33	www.europarl.europa.eu İnternet Kaynağı	<%1
34	Submitted to University of Edinburgh Öğrenci Ödevi	<%1
35	Submitted to Longwood College Öğrenci Ödevi	<%1
36	citeseerx.ist.psu.edu İnternet Kaynağı	<%1
37	conventions.coe.int İnternet Kaynağı	<%1
38	digital.lib.washington.edu İnternet Kaynağı	<%1
39	Submitted to National University of Singapore Öğrenci Ödevi	<%1
40	Ruwantissa Abeyratne. "Aviation in the Digital Age", Springer Science and Business Media LLC, 2020 Yayın	<%1
41	Submitted to Trident University International Öğrenci Ödevi	<%1
42	apnews.com İnternet Kaynağı	<%1

43	www.webology.org İnternet Kaynağı	<%1
44	irep.ntu.ac.uk İnternet Kaynağı	<%1
45	libres.uncg.edu İnternet Kaynağı	<%1
46	research.edgehill.ac.uk İnternet Kaynağı	<%1
47	Submitted to Rikkyo University Öğrenci Ödevi	<%1
48	Ahmed Patel. "International Cooperation to Fight Transnational Cybercrime", Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007), 08/2007 Yayın	<%1
49	LexisNexis Yayın	<%1
50	Submitted to University College London Öğrenci Ödevi	<%1
51	cybilportal.org İnternet Kaynağı	<%1
52	ratingacademy.com.tr İnternet Kaynağı	<%1
53	blog.sunnyboy.me İnternet Kaynağı	<%1

54	Submitted to Holborn College Öğrenci Ödevi	<%1
55	rocor-trenton.com İnternet Kaynağı	<%1
56	www.conventions.coe.int İnternet Kaynağı	<%1
57	www.oecd.org İnternet Kaynağı	<%1
58	Submitted to University of Maryland, University College Öğrenci Ödevi	<%1
59	dspace.lib.uom.gr İnternet Kaynağı	<%1
60	rakovski-defcol.mod.bg İnternet Kaynağı	<%1
61	slate.com İnternet Kaynağı	<%1
62	Submitted to Universiteit van Amsterdam Öğrenci Ödevi	<%1
63	dergipark.org.tr İnternet Kaynağı	<%1
64	etd.lib.metu.edu.tr İnternet Kaynağı	<%1
65	mafiadoc.com	

66	spectrum.library.concordia.ca İnternet Kaynağı	<%1
67	www.mi.fu-berlin.de İnternet Kaynağı	<%1
68	Submitted to The Blake School Öğrenci Ödevi	<%1
69	Submitted to University of Nevada, Las Vegas Öğrenci Ödevi	<%1
70	Submitted to University of West London Öğrenci Ödevi	<%1
71	www.cirdi.org İnternet Kaynağı	<%1
72	www2.unescobkk.org İnternet Kaynağı	<%1
73	yayinlamaozgurlugu.org İnternet Kaynağı	<%1
74	Submitted to University of Technology, Sydney Öğrenci Ödevi	<%1
75	Submitted to Vrije Universiteit Brussel Öğrenci Ödevi	<%1
76	digitalcommons.library.umaine.edu İnternet Kaynağı	

77	etheses.whiterose.ac.uk İnternet Kaynağı	<%1
78	storre.stir.ac.uk İnternet Kaynağı	<%1
79	Submitted to Istanbul Medeniyet Ãniversitesi Öğrenci Ödevi	<%1
80	Submitted to Laureate Higher Education Group Öğrenci Ödevi	<%1
81	Submitted to Southern Illinois University Öğrenci Ödevi	<%1
82	Submitted to Webster University Öğrenci Ödevi	<%1
83	catalog.hathitrust.org İnternet Kaynağı	<%1
84	www.missingkids.com İnternet Kaynağı	<%1
85	"Handbook of Communication for Development and Social Change", Springer Science and Business Media LLC, 2020 Yayın	<%1
86	Submitted to Leiden University Öğrenci Ödevi	<%1

87	Submitted to NALSAR University of Law Hyderabad Öğrenci Ödevi	<%1
88	Submitted to University of Cambridge Öğrenci Ödevi	<%1
89	Submitted to University of Johannsburg Öğrenci Ödevi	<%1
90	Submitted to University of London External System Öğrenci Ödevi	<%1
91	Submitted to University of Northampton Öğrenci Ödevi	<%1
92	Submitted to University of Strathclyde Öğrenci Ödevi	<%1
93	www.thirdway.org İnternet Kaynağı	<%1
94	Jelena Bäumler. "Chapter 60 The WTO's Crisis: Between a Rock and a Hard Place", Springer Science and Business Media LLC, 2020 Yayın	<%1
95	John Hunt. "The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them", Information & Communications Technology Law, 2011	<%1

96	Submitted to Middle East Technical University Öğrenci Ödevi	<%1
97	Submitted to Uganda Christian University Öğrenci Ödevi	<%1
98	Submitted to University of Santo Tomas Öğrenci Ödevi	<%1
99	clok.uclan.ac.uk İnternet Kaynağı	<%1
100	e-spacio.uned.es İnternet Kaynağı	<%1
101	www.beccaria-portal.org İnternet Kaynağı	<%1
102	"Data Protection in the Internet", Springer Science and Business Media LLC, 2020 Yayın	<%1
103	"International developments", Commonwealth Law Bulletin, 2002 Yayın	<%1
104	Submitted to Grand Canyon University Öğrenci Ödevi	<%1
105	Submitted to University of Central England in Birmingham Öğrenci Ödevi	<%1
106	Submitted to University of Nottingham	

107	baselinescenario.com İnternet Kaynağı	<%1
108	orbilu.uni.lu İnternet Kaynağı	<%1
109	www.dekyo.or.jp İnternet Kaynağı	<%1
110	"Rethinking Cybercrime", Springer Science and Business Media LLC, 2021 Yayın	<%1
111	Daniele Cangemi. "Procedural law provisions of the council of Europe convention on cybercrime 1", International Review of Law Computers & Technology, 7/1/2004 Yayın	<%1
112	Rainey, Bernadette. "Jacobs, White, and Ovey: The European Convention on Human Rights", Oxford University Press, 2020 Yayın	<%1
113	www.end-violence.org İnternet Kaynağı	<%1
114	www.interpol.org İnternet Kaynağı	<%1
115	www.open-access.bcu.ac.uk İnternet Kaynağı	<%1

116	Beril Dedeoglu. "Bermuda triangle: comparing official definitions of terrorist activity", Terrorism and Political Violence, 2003 Yayın	<%1
117	Ghernaouti, . "The Fight Against Cybercrime", Cyber Power Crime Conflict and Security in Cyberspace, 2013. Yayın	<%1
118	ir.canterbury.ac.nz İnternet Kaynağı	<%1
119	vx.netlux.org İnternet Kaynağı	<%1
120	www.ftaa-alca.org İnternet Kaynağı	<%1
121	www.law.cornell.edu İnternet Kaynağı	<%1
122	www.missioncriticalmagazine.com İnternet Kaynağı	<%1
123	www.mysciencework.com İnternet Kaynağı	<%1
124	www.nmun.org İnternet Kaynağı	<%1
125	www.theiacp.org İnternet Kaynağı	<%1

126	İnternet Kaynağı	<%1
127	Delphine Defossez. "chapter 23 Regulations for Cybercrimes", IGI Global, 2021 Yayın	<%1
128	Fernanda Mello Mena. "Actors and incentives in cannabis policy change: an interdisciplinary approach to legalization processes in the United States and in Uruguay", Universidade de Sao Paulo, Agencia USP de Gestao da Informacao Academica (AGUIA), 2020 Yayın	<%1
129	Vanessa Kirch. "Social Networks - The Modern-Day Family", Springer Science and Business Media LLC, 2021 Yayın	<%1
130	aeiseguridad.es İnternet Kaynağı	<%1
131	docplayer.net İnternet Kaynağı	<%1
132	dspace.unive.it İnternet Kaynağı	<%1
133	lawforcomputerscientists.pubpub.org İnternet Kaynağı	<%1
134	undocs.org İnternet Kaynağı	<%1

135	www.estig.ipbeja.pt İnternet Kaynağı	<%1
136	www.saintleo.edu İnternet Kaynağı	<%1
137	"Regulating eTechnologies in the European Union", Springer Nature, 2014 Yayın	<%1
138	Submitted to Chapman University Öğrenci Ödevi	<%1
139	Csaba Rada. "Introvertált külpolitikától regionális puha hatalmi ambíciókig. A török külpolitika átalakulásának elemzése", Corvinus University of Budapest, 2017 Yayın	<%1
140	Joseph Savirimuthu. "Online Child Safety", Springer Science and Business Media LLC, 2012 Yayın	<%1
141	M ERBSCHLOE. "Global cyberspace security cooperation", Implementing Homeland Security for Enterprise IT, 2004 Yayın	<%1
142	Melaku Bayu Workie, Destaw Bayable Yemer, Minwuyelet Andualem Desta, Meslo Sema Berhanu et al. "The Impacts of Social Media Usage on Health Professionals' Healthcare Services", Research Square, 2021	<%1

	Yayın	
143	Nikos Koutras. "chapter 2 The Copyright", IGI Global, 2020 Yayın	<%1
144	Oliver Westerwinter, Kenneth W. Abbott, Thomas Biersteker. "Informal governance in world politics", The Review of International Organizations, 2020 Yayın	<%1
145	Roderic Broadhurst. "Developments in the global law enforcement of cyber_crime", Policing: An International Journal of Police Strategies & Management, 2006 Yayın	<%1
146	Submitted to University of Malaya Öğrenci Ödevi	<%1
147	chicagounbound.uchicago.edu İnternet Kaynağı	<%1
148	cryptome.org İnternet Kaynağı	<%1
149	eprint.ncl.ac.uk İnternet Kaynağı	<%1
150	eprints.bournemouth.ac.uk İnternet Kaynağı	<%1
151	eprints.soton.ac.uk İnternet Kaynağı	<%1

152	eucyberdirect.eu İnternet Kaynağı	<%1
153	library.aceondo.net İnternet Kaynağı	<%1
154	philpapers.org İnternet Kaynağı	<%1
155	propertibazar.com İnternet Kaynağı	<%1
156	psulibrary.palawan.edu.ph İnternet Kaynağı	<%1
157	rd.springer.com İnternet Kaynağı	<%1
158	www.awarenetwork.org İnternet Kaynağı	<%1
159	www.cairn.info İnternet Kaynağı	<%1
160	www.globalresearch.ca İnternet Kaynağı	<%1
161	www.kcnorthares.org İnternet Kaynağı	<%1
162	www.kids-o-rama.com İnternet Kaynağı	<%1
163	www.lets-go-virtual.com İnternet Kaynağı	<%1

164	www.pura.gm İnternet Kaynağı	<%1
165	www.registercitizen.com İnternet Kaynağı	<%1
166	www.sagecertification.org İnternet Kaynağı	<%1
167	www.sfb597.uni-bremen.de İnternet Kaynağı	<%1
168	www.unodc.org İnternet Kaynağı	<%1
169	www30.tau.ac.il İnternet Kaynağı	<%1
170	zombiedoc.com İnternet Kaynağı	<%1
171	"Dark Web Investigation", Springer Science and Business Media LLC, 2021 Yayın	<%1
172	Borka Jerman Blažič, Tomaž Klobučar. "Investigating crime in an interconnected society: will the new and updated EU judicial environment remove the barriers to justice?", International Review of Law, Computers & Technology, 2019 Yayın	<%1

173	"The Palgrave Handbook of International Cybercrime and Cyberdeviance", Springer Science and Business Media LLC, 2020 Yayın	<%1
174	Submitted to American Public University System Öğrenci Ödevi	<%1
175	Dirk Brand. "Algorithmic Decision-making and the Law", JeDEM - eJournal of eDemocracy and Open Government, 2020 Yayın	<%1
176	Dr. Chat Le Nguyen, Dr. Wilfred Golman. "Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'", Computer Law & Security Review, 2021 Yayın	<%1
177	Masike Malatji, Annlizé L. Marnewick, Suné von Solms. "Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa", Sustainability, 2020 Yayın	<%1
178	reset-bibliography.ca İnternet Kaynağı	<%1
179	www.informatica-juridica.com İnternet Kaynağı	<%1

CURRICULUM VITAE

Name and Surname: Fatma AKIN AKILLI

Place and Date of Birth:

Foreign Languages: English

Email:

Education

Degree	Field	University	Year
Undergraduate	Social Sciences Teaching	Amasya University	2012
Undergraduate	Security Sciences	Şehit Önder Güzel Police College	2017
Graduate	International Relations	Atılım University	2021

Work Experience

Work Place	Position	Year
Turkish National Police Department of Cybercrime	Police/Cybercrime Investigator	2017 / -