Summer 2014

The internet vs. the Nation-State: Prevention and Prosecution Challenges on the Internet in Republic of TürkiyI

Ersin Elibol

Old Dominion University

Follow this and additional works at: https://digitalcommons.odu.edu/gpis_etds

Part of the Communication Technology and New Media Commons, and the International Relations Commons

Recommended Citation


https://digitalcommons.odu.edu/gpis_etds/48

This Dissertation is brought to you for free and open access by the Graduate Program in International Studies at ODU Digital Commons. It has been accepted for inclusion in Graduate Program in International Studies Theses & Dissertations by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.
THE INTERNET VS. THE NATION-STATE: PREVENTION AND PROSECUTION

CHALLENGES ON THE INTERNET IN REPUBLIC OF TÜRKİYE

by

Ersin Elibol
B.A. June 1995, Turkish National Police Academy Faculty of Security Studies
M.P.A. May 2007, Virginia Commonwealth University

A Dissertation Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

INTERNATIONAL STUDIES

OLD DOMINION UNIVERSITY
August 2014

Approved by:

David C. Earnest (Director)

Regina Karp (Member)

Avi Santo (Member)
ABSTRACT

THE INTERNET VS. THE NATION-STATE: PREVENTION AND PROSECUTION CHALLENGES ON THE INTERNET IN REPUBLIC OF TÜRKİYE

Ersin Elibol
Old Dominion University, 2014
Director: Dr. David Earnest

Social, economic, and technological developments are widely accepted as powerful forces that affect the role, power, and functions of nation-states. Being one of the most influential technological developments in the recent decades, the internet has come into prominence in this regard.

With the use of the Internet, the monopoly of media and information controlled by official ideologies, capitalist barons, or elites is seriously challenged. Consequently the power balance between individuals and authorities in the mass media and communication has been transformed in a significant way. Though their reliability may sometimes be questionable, the number and type of information resources has increased dramatically, and accessing information has become easier substantially. People are more interconnected today than ever before. They can easily find, join, or construct their personal, social or political networks. With a number of internet applications and social media, collective reactions, social movements and activities are more organized and effective today than ever before. That is why we have seen so much social fluctuation, unrest, protest, and political activism all over the world in the last few years.

Moreover new terms and phenomena like cyber-crime, cyber warfare, and cyber-attacks have urged nation-states to be more careful about the internet and increase their efforts to control it. This level of social chaos in different states and increasing cyber-crimes lead us to question the effectiveness of nation-states' controlling measures.
Focusing on one state, the Republic of Türkiye, this study analyzes two important dimensions of state control efforts, prevention and prosecution. On the prevention side, I explore the effectiveness of internet access blocking. On the prosecution side, I analyze the effectiveness of prosecution in internet child pornography.

The result of testing to measure the effectiveness of Internet website blocking reveals that there are significant gaps, complications, and dilemmas in these policies. A similar situation is also seen in the investigations of internet child pornography. Analysis conducted of the operational investigation files reveals that in most of the files, suspects could not be identified, traced or brought before judicial authorities. As seen in these two fields, state policing efforts of the Internet in a country are not absolute, and the Internet can be a vulnerable space in which any local or foreign actor or agents like criminals, opposition groups, terrorists can create problems for nation-states.
Copyright, 2014, by Ersin Elibol, All Rights Reserved.
ACKNOWLEDGEMENTS

I would like to special thanks to my chair Dr. David C. Earnest, to my committee members Dr. Regina Karp and Dr. Avi Santo. Without their advising, support and encouragement, this work would not be realized.

I would like to present my gratitude to my family Esma, E. Zulal, E. Serra for their patience.

Finally many thanks to my mother, brother and sister Hatice, Yavuz and Yasemin for their presence with me.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>THE PUZZLE AND RESEARCH QUESTION</td>
<td>4</td>
</tr>
<tr>
<td>OPERATIONALIZATION OF THE RESEARCH QUESTION</td>
<td>10</td>
</tr>
<tr>
<td>CONTRIBUTION: STATE POWER IN THE INFORMATION AGE</td>
<td>11</td>
</tr>
<tr>
<td>II. LITERATURE REVIEW</td>
<td>18</td>
</tr>
<tr>
<td>STATE POWER AND THE INTERNET</td>
<td>18</td>
</tr>
<tr>
<td>CENSORSHIP AND BLOCKING ON THE INTERNET</td>
<td>50</td>
</tr>
<tr>
<td>CIRCUMVENTION</td>
<td>58</td>
</tr>
<tr>
<td>PROSECUTING CHILD PORNOGRAPHY</td>
<td>66</td>
</tr>
<tr>
<td>III. RESEARCH DESIGN</td>
<td>74</td>
</tr>
<tr>
<td>RESEARCH QUESTION FORMALIZATION</td>
<td>75</td>
</tr>
<tr>
<td>RESEARCH QUESTIONS AND MEASUREMENT</td>
<td>76</td>
</tr>
<tr>
<td>METHODOLOGY</td>
<td>82</td>
</tr>
<tr>
<td>WHY THE REPUBLIC OF TÜRKİYE?</td>
<td>88</td>
</tr>
<tr>
<td>DEFINITIONS</td>
<td>93</td>
</tr>
<tr>
<td>IV. BRIEF ABOUT TÜRKİYE</td>
<td>97</td>
</tr>
<tr>
<td>HISTORICAL BACKGROUND OF THE INTERNET IN TÜRKİYE</td>
<td>100</td>
</tr>
<tr>
<td>V. INTERNET BLOCKING AND EFFECTIVENESS IN THE REPUBLIC OF TÜRKİYE</td>
<td>105</td>
</tr>
<tr>
<td>INTRODUCTION AND BACKGROUND</td>
<td>105</td>
</tr>
<tr>
<td>EFFECTIVENESS AND BLOCKING ON THE INTERNET IN TÜRKİYE</td>
<td>114</td>
</tr>
<tr>
<td>FURTHER ISSUES REGARDING THE SIDE EFFECTS OF INTERNET BLOCKING</td>
<td>132</td>
</tr>
<tr>
<td>VI. POLICING CHILD PORNOGRAPHY IN TÜRKİYE</td>
<td>150</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>150</td>
</tr>
<tr>
<td>EFFECTIVENESS OF POLICING CHILD PORNOGRAPHY</td>
<td>158</td>
</tr>
<tr>
<td>VII. RESULTS, CONTRIBUTIONS, AND WEAKNESSES</td>
<td>180</td>
</tr>
<tr>
<td>RESULT OF EACH ANALYSIS</td>
<td>180</td>
</tr>
<tr>
<td>OVERALL ANALYSIS AND CONTRIBUTION</td>
<td>183</td>
</tr>
<tr>
<td>WEAKNESS OF THE STUDY: LIMITATIONS AND FUTURE PROJECTIONS</td>
<td>187</td>
</tr>
</tbody>
</table>
CHAPTER I
INTRODUCTION

No other invention seems to have had the same influence within so short a time at the global level as the Internet. Some anthropologists emphasize that "this capacity-the Internet-is the most significant social development since the invention of writing over five thousand years ago."\(^1\) The Internet has become a global communication network, and it has been rapidly expanding since it was first introduced to the public. While there were about 16 million worldwide users in 1995, there were 400 million in 2001 and about 2.4 billion users as of June 2012.\(^2\) It is estimated to reach around 3 billion by the end of 2014.\(^3\)

Today, there is almost no field in our daily lives that the Internet has not penetrated. It is already one of the inseparable parts of our daily social and economic lives. The Internet can enable us to access to our banks, official departments, libraries, shopping centers, media, and entertainment centers. We can manage our banking accounts and conveniently carry out many transactions online. We can easily connect libraries and databases to conduct research. For shopping, we can find many alternative retailers and sellers, not necessarily near our homes but from anywhere in the world. We can reach newspapers, TV centers, magazines, and many kinds of media corporations.

Many of the previous media and communication services and applications have

---


been adapted to the Internet. Although the traditional ways of providing services like TV broadcasting, printing newspapers and telephone boxes still exist, the Internet has combined them all onto a unique platform to be a TV, a digital newspaper or a telephone (Voice over Internet Protocol (VoIP) calls). With smart phones running over 3G or 4G technology today, these services become mobile for individuals, and ease our lives in a significant way.

People who have messages, comments, news, ideologies, or any other ideas now have a convenient tool to amplify and share with anyone in the world. Skillful people can now use this global platform to present their skills and capabilities that can be digitalized. The mass media have started to share some of their roles with Internet-based “citizen journalism.” An individual has unique power on the internet today, what Friedman calls “uploading.”\(^4\) Without convincing any actor of the previous media order, individuals can upload any record of any subject to the internet, which can change the public agenda at the national level, or even the international level, as seen in the case of Julian Assange and WikiLeaks.

It is “nonhierarchical, interactive, and global. Its usage is also growing exponentially.”\(^5\) Because of its diffusion power and widespread use, it relatively empowers individuals more than authorities. For instance, what makes police force powerful is the use of radio communication (walky-talky) among each patrol to coordinate their collective action against criminals or in their daily activities. During the Gezi protests in Türkiye started in the end of May 2013, protesters used some of internet


applications including a walky-talky program, Zello on their smart phones for instant communication among each-others.⁶

The Internet is such a dominant medium that it is open to many new media and communication technologies. This accessibility encourages developers to make new technologies Internet compatible. Castells believes that the invention of the Internet is as important as the invention of printing press.⁷ Referring to McLuhan’s analogy of the “Gutenberg Galaxy” for the diffusion of the printing press in the West, he believes that “we have now entered a new world of communication: the Internet Galaxy.”⁸

The Internet is still quite young. Basic examples of computer networking go back to the mid-1970s in the United States. It started to be used publicly in the beginning of the 1980s and became more widespread by the 1990s. Goldfoot indicates that the word “Internet” emerged by the mid-1980s.⁹ Since then, the Internet already connected the entire world like a digital web. Between the years of 2000 and 2010, users of the Internet have increased about 444.8 % in the world.¹⁰

This popularity has also affected academia. Compared to other media and communication tools like TV, newspapers, and radio, the Internet has often been the subject of academic inquiry. Chadwick and Howard analyzed the numbers of articles available in Thompson Reuter’s ISI Web of Science scholarly article database published

---

⁸ Ibid., 3.
¹⁰ International Telecommunication Union, ibid.
between 1995 and 2006.1 A keyword search revealed that there were fewer articles published in 1995 containing the word, “Internet” than the word, “TV.” That changed in 1999, when the frequency of articles containing the word “Internet” matched the frequency of the keywords “TV,” “newspapers,” and “radio.” By 2001 the number of articles containing the word “Internet” exceeded the total number articles containing the words “TV,” “newspaper,” or “radio.”12

THE PUZZLE AND RESEARCH QUESTION

The spread of the Internet and its use have introduced new opportunities and convenience to our daily lives. At the same time Internet use has introduced significant challenges and complications. Besides complications and possible victimization at the individual level, the primary addressee and target of these negative effects is the only authority within national borders: nation-states. Authorities all over the world are developing their own national policies to maximize their benefits from the Internet, but at the same time they are trying to take measures to handle and control the externalities of this new medium. It can be expected that non-democratic states tend to take strict policies and implement harsh legal measures to regulate the Internet, whereas democratic countries prefer more liberal approaches in their Internet policies. However, strict policies and practices can also be seen in relatively democratic countries.13

12 Ibid.
13 At different times, some of the countries known as democratic and liberal are also classified by the RSF, Reporter Without Borders as enemies of the internet or where the internet is under surveillance including Australia, Türkiye, South Korea, USA, UK, France. See for instance: Clothilde Le Coz, "Reporters without Borders Issues ‘Enemies of the Internet’ List," Mediashift, 5 April 2010, and Reporters Without Borders, "Internet Enemies," (2011), and Kieran Doherty, "US, UK ‘Enemies of the Internet’ for First Time," RT, 17 March 2014.
The challenges and complications of the Internet can be seen in a variety of fields that states have fundamental interests in controlling. This might be a national security issue, like a cyber-attack to a strategic department, or a terrorist organization use of the Internet for different purposes. It could be a taxation issue for a global Internet company, e.g. Google, earning profits from local advertisement within states without paying taxes to the local government. It might be ensuring the rule of law and public order also on the internet like in preventing any of undesired idea, ideology or content within national borders for different reasons.

Today, even highly developed countries, like the United States, have serious dilemmas regarding the Internet. Although the Internet was born in the United States, and there are many well-known US-based companies in information technology, the country is having legal and technical difficulties regulating the Internet in accordance with the country’s core principles. For instance, obscenity and pornography are strictly regulated within the country "in all communications technology."\textsuperscript{14} Except its sensitivity against child sexual abuse, which is regulated in different legislation like the Children’s Internet Protection Act, similar materials are now very much available and accessible in the United States because of these difficulties. The main technical reason is “over-blocking,” which means that blocking some illegal web contents may result in blocking innocent web content, since many websites may contain both legal and illegal content. Callanan et al. stress that “it seems inevitable that legal content will be blocked where blocking is implemented.”\textsuperscript{15} While testing a blocking method, Domain Name System (DNS)


\textsuperscript{15} Cormac Callanan, Marco Gercke, Estelle De Marco, and Hein Dries-Ziekenheimer, "Internet Blocking: Balancing Cybercrime Responses in Democratic Societies," Open Society Institute, 2009, 12.
poisoning, which prevents access to unwanted websites. Dronseif figured out that almost all attempts to block websites containing hate speech made mistakes in their implementation in Germany. While some sites were closed down for hate speech, some other legal websites were blocked unintentionally.

Perhaps the most significant challenges that the Internet imposed on nation-states have been experienced in the socio-political realm. Hills notes that, “History shows that person to person instantaneous electrical communications have altered the relations of states to their citizens. Such communications can be used to organize domestic opposition to governments. They can also cross national borders creating vulnerability and threats to national security. Point to point electrical communication transfers power away from states to non-state actors in a way that the top down technology of broadcasting does not.”

In recent years, masses who were unpleased with their regime type or with the policies of their governments have created serious threats and vulnerability for some states, by also using the Internet. Together with other socio-political dynamics and reasons, effective use of the Internet has played a significant role in these incidents. The uprising called the Arab Spring started in Tunisia in the end of 2010, the incidents of Occupy Wall Street protests in the USA in the year of 2011, or the riots started in London and spread throughout England in the same year showed us clearly that the internet was the kitchen of the incidents where all the anger, hate and other negative circumstances are

---

16 Domain Name System (DNS) is a service that translates website names, which usually use alphabetical letters, into number sequences known as IP addresses.
harmonized and given stove though uploading, reporting, jogging, tweeting and where the sittings around the meal table is organized through communication, information sharing.

Even we had seen the role of the internet before, in the case of Indonesia in 1998 (the fall of Suharto regime); in the so-called Orange Revolution in Ukraine, 2004; during the Saffron Revolution in Burma, 2007; or in the incidents in Moldova, 2009 that some call the Twitter Revolution.

Kyj explains the role of the Internet in the Orange Revolution in Ukraine: “Despite lacking access to mass media, supporters of democratic change compensated through skillful use of the Internet to recruit volunteers, raise funds, organize campaigns, report breaking news, and garner the sympathy of the global democratic community.”19

Analyzing political protests in Moldova, Mungiu-Pippidi and Igor emphasize how the Internet-engaged younger generations utilized online tools and features of the Internet while organizing their political protests in 2009.20

Although it did not result in a regime change, the governments of Burma in 2007 and Iran in 2009 had similar challenges when people utilized the internet and internet applications while they were protesting their authoritarian regimes and were asking political change as well as freedom.21 During the Saffron Revolution in Burma, Chowdhury notes that “Despite efforts by the government to control all media outlets, this attempted revolution demonstrated that the Internet does not lend itself easily to

---

control." Nima believes that an independent information society that can be created by
the use of Internet features like social media tools and blogging is the only way to bring
political change to Iran in the long run.

The world also noticed recently how influential the Internet was during the Arab
Spring, particularly in Egypt, Tunis, Libya and Syria. For people on the street, the
Internet is the only effective tool on hand to mobilize disaffected masses, to organize
their reactions, and to amplify their voices to the world.

Analyzing the role of social media in political fluctuations that began in Tunisia
in the beginning of 2011, John Timpane argues how Internet use has broken the state’s
information monopoly. He cites, “One thing about information: Once it’s out, you can’t
put it back. As Richard, associate professor of communication at La Salle University,
puts it, ‘The sheer multiplicity of venues and sources makes it impossible for would-be
dictators to get the genie back in the bottle. And once info is out at all, it’s easily,
ininitely copiable.’”

Even against blocking efforts by these authoritarian governments, or the total
shutdown by these regimes, new Internet technologies were introduced and started to be
utilized in these countries. In order to circumvent government blockage of Skype calls
made from Syria, an activist used software from Psiphon, Inc. to call outside the country.
The Psiphon technology was developed by a Canadian company, funded by the United
States Department of State, and was downloaded by thousands of people in Syria during

---

22 Mridul Chowdhury, *The Role of the Internet in Burma’s Saffron Revolution*, (The Berkman Center for
23 Nima Mina, *Blogs, Cyber-Literature and Virtual Culture in Iran*, Garmisch-Partenkirchen: George C.
24 John Timpane, "Arab World Shaken by Power of Twitter and Facebook," *McClatchy - Tribune Business
a three-week period.\textsuperscript{25} Likewise, Google and Twitter have developed Internet technologies for which no internet connection is required. These became a remedy to a total Internet blackout, allowing “voice to Tweet” (a mobile application known as Voice for Twitter) capabilities for Egyptians to send short message to Twitter by calling specific telephone numbers and speaking the messages over the mobile telephone network.\textsuperscript{26}

In the end of 2010, the world experienced another example of this debate—the case of WikiLeaks. On one side there is one state, a super power—the United States. On the other side there is the Internet, a website called WikiLeaks, and an Internet activist. This case also shows how the Internet can be an influential tool in the hands of an individual, as Friedman claims in his book \textit{The World is Flat}, even to challenge a state.\textsuperscript{27}

This dissertation explores the interaction between nation-states and the Internet and explores the ways in which the Internet affects state power. State power here is operationalized as “policing.” Policing is one of the essential functions of state authority, and it has two important aspects: prevention and prosecution. While state authorities try to prevent some criminal, social, or political threats before they happen, authorities also try to trace, identify, prosecute, detain, or arrest those who involved these kinds of illegal activities. This study concentrates on one country, the Republic of Türkiye.\textsuperscript{28} For the preventive policing aspect, the study focuses on blocking measures. For the prosecution dimension, the study examines a specific crime, child pornography. This study explores empirical cases, data, and other reliable evidence to understand how the Internet has

\textsuperscript{25} Ivan Watson, "Cyberwar Explodes in Syria," \textit{CNN}, 22 November 2011.
\textsuperscript{26} Charles Arthur, "Google and Twitter Launch Service Enabling Egyptians to Tweet by Phone," \textit{Guardian}, 1 February 2011.
\textsuperscript{27} A dimension of this interaction, for instance see the declaration of Reporters Without Borders and how it condemns the blocking, cyber-attacks and political pressure against the website and its founder: Reporters Without Borders, "Wikileaks Hounded?" 4 December 2010.
\textsuperscript{28} Türkiye is the Turkish name for the country referred to as Turkey in English.
complicated traditional policing practices.

In this frame, this study analyzes two issue areas, as an example for each policing aspect: i) blocking on the Internet (prevention) and ii) prosecution of child pornography (prosecution).

OPERATIONALIZATION OF THE RESEARCH QUESTION

States have many mechanisms and tools to regulate and administer this global medium. Drezner specifies that “the Internet has generated multiple areas of governance, including the development of technical protocols, censorship, e-taxation, intellectual property, and privacy rights.” Likewise Denning indicates that “the Internet has raised numerous policy issues in such areas as privacy, encryption, censorship, electronic, commerce, international trade, intellectual property protection, taxation, Internet governance, cyber-crime, and information warfare.”

Among these policy areas, the interaction between the nation-state and the Internet is mainly argued around three areas in political science literature: i) censorship, blocking, and filtering regimes (practices of states); ii) cyber-crimes, policing, prosecution, and law enforcement difficulties; and iii) surveillance efforts. This study concerns the first two but excludes the third policy area, which is a typical state behavior: surveillance. For states, surveillance efforts are vitally important for their power and existence. Such is the case with the Internet. Many states today try to maximize their benefit from the Internet for surveillance and their national interests. Studying these kinds

---

of efforts of states would bring a broader perspective for explaining the effects of the Internet on state power. However, studying surveillance is always difficult since data and information in this field are widely confidential and closed to third parties.

Rather, this study focuses on access blocking, filtering practices, and cybercrime, specifically cybercrime investigations into the exchange of Internet child pornography, which are some of the major problems of this new medium. Blocking and filtering on the Internet are very much interrelated with many other debates, such as the Internet and democracy, and the Internet, social media, social movements, and social mobilization. Many democratic rights such as freedom of expression, freedom of speech, and privacy of communication are extensively related to censorship and filtering regimes. Analyzing these issues, exploring effectiveness and possible challenges in these regimes, will bring substantial explanations and contributions to these debates mentioned above. Also, investigation of aspects of a cybercrime will present how judicial proceedings against cybercrime are effective in solving such crimes.

CONTRIBUTION: STATE POWER IN THE INFORMATION AGE

In fact, there is already a debate in the literature about the decline in state power. Sometimes this decline has been argued within globalization dynamics, sometimes within newly emerging actors, like multi-national companies, or non-governmental organizations, or sometimes within other powerful forces like technology. As stressed

33 Thomas Risse-Kappen, Bringing Transnational Relations Back In: Non-State Actors, Domestic Structures, and International Institutions, (Cambridge Studies in International Relations. Cambridge; New
in The Economist, "Almost any discussion of international relations nowadays seems to begin and end with the same idea: the state is in retreat." Creveld classifies that states are weakening in four ways: a) losing warfare capability; b) weakening welfare capacity; c) changes brought by modern technology and communication tools; and d) difficulties sustaining public order. In the same debate, The Economist refers to two old enemies, which are stronger now than ever before: technology and ideology.

Ronald Reagan stated in a speech in London Guildhall in 1989 that, "Technology will make it increasingly difficult for the state to control the information its people receive... The Goliath of the totalitarianism will be brought down by the David of the microchip."

Nye perceives this decline as a transformation in state power and describes five trends in this transformation: economic interdependence, transnational actors, nationalism in weak states, the spread of technology, and changing political issues. Price also believes that this is a kind of transformation in state functions: "Redefined state power and changes in modes and practices of authority are more likely than what is often called state decline."

Analyzing social networks and Internet applications such as Facebook, MySpace, and Twitter, The Economist notes that, "Despite its giant population, Facebook is not

---


"The Future of the State," ibid.


Nye, ibid.

quite a sovereign state—but it is beginning to look and [to] act like one.\textsuperscript{41} The newspaper implies that, "The future is another country."\textsuperscript{42} It refers the comments of David Post, a law professor from Temple University, who specifies some interesting points: "Facebook has many implications, including commercial, for individuals or companies. Recently, the website obligated users to utilize its proprietary money system, which is a typical state feature (printing national money to circulate within national borders). Just as states tax their citizens, Facebook also taxes its users. Interestingly, while they are logged in, Facebook users can access some of different websites outside without logging in to these sites." Like using a passport (or required a valid visa) while travelling between states, \textit{The Economist} notes.\textsuperscript{43}

The magazine was reporting Facebook as having over 500 million users all over the world, coming in third after the population of China and India in 2010. As of May 1, 2013, registered users of Facebook are reportedly reached 1.11 billion. The number of existing users of another internet phenomenon, Twitter was reported as 500 million as of March 21, 2013.\textsuperscript{44}

Some scholars, on the other hand, do not agree that the Internet threatens nation-states to such an extent.\textsuperscript{45} While discussing the effects of the Internet on nation-states, Drezner indicates that "states, particularly the great powers, remain the primary actors for handling the social and political externalities created by globalization and the Internet."\textsuperscript{46}


\textsuperscript{42} Ibid.

\textsuperscript{43} Ibid.

\textsuperscript{44} For the number of Facebook members, see for instance: "Number of Active Users at Facebook over the Years," \textit{Associated Press}, 1 May 2013. For the number of Twitter users, see for instance: "Twitter in Numbers," \textit{Telegraph}, 21 March 2013.


\textsuperscript{46} Drezner, ibid., 478.
Hill notes that, "Although some theorists have argued that the internationalization of communications has eroded the power of the state, he believes that power has shifted away from domestic and international non-state civic opposition groups to increased state control." 47

In the introduction of their book, Morris and Waisbord summarize that,

"Certainly, states currently face changing and challenging conditions. The remarkable global expansion of media corporations, facilitated by liberalization and privatization of media systems worldwide and the development of cable and satellite technologies, has reduced states' ability to exercise power and maintain information sovereignty. It would be unwarranted, however, to conclude that the state no longer matters. Reports about the death of the state may be greatly exaggerated, as many contributors in this book suggest." 48

Goldsmith and Wu accept that states face serious problems because of the Internet. 49 However, they argue that these challenges are not totally different from those created by previous media and communication mediums. They also indicate that "every great technological innovation has the potential to lower the cost of violating law" and thus "these points (challenges) are unsurprising." 50

Looking at the situation in a particular country, the Republic of Türkiye, this study aims to contribute to the literature by presenting the dimensions of this interaction between the state and the Internet. Especially for some countries like China and Iran, there are quite a number of academic studies in which the effects of the Internet were subjects of inquiries. 51 The experience of Türkiye's internet blocking practices, as well as

---

49 Goldsmith and Wu, ibid.
50 Ibid, 81.
51 For China, see for instance Ho-Chun Li, "Digital Democracy in China: Evaluating Chinese Citizens' Fight for Rights via the Internet," State University of New York at Buffalo, 2008. and Zixiang (Alex) Tan,
the effectiveness of prosecution of online crimes, particularly internet child pornography, will present to the literature the experience of a developing state and its policing challenges on the Internet, both in terms of prevention, i.e. Internet blocking, and prosecution, i.e. child pornography.

This study is not a technical analysis of circumvention tools and programs in a lab environment. It is a field study where the results of blocking measures are established and where the results of circumvention tests are directly conducted. While tests and checks for blocked websites are performed in Türkiye, some sections were written in the United States.

The following second chapter presents a review of literature, divided into four sections. The first review shows how the Internet in general affects nation-states by focusing on how Internet use and activity complicate basic state functions. Classifying state functions as ensuring national security, justice and public order, and economic and social welfare, this section explores how this medium causes significant problems and challenges in these three basic fields for state authorities.

The second review of the second chapter looks at access blocking techniques and the argument about their effectiveness, discussed in more detail in the third section, about circumvention. These three sections thus explore the prevention dimension of state policing on the Internet. Finally, the literature review concludes in the fourth section, an example of a child pornography prosecution.

The third chapter includes methodology and research design. This study examines two policy areas of policing on the Internet: effectiveness of access blocking policies on

the Internet and effectiveness of prosecution of child pornography. This section also explains the methodology, how research questions are formulated, how they are measured, why the Republic of Türkiye is selected, why internet child pornography is focused on as a cybercrime, and provides some definitions of terms used in this study.

Chapter four gives introductory information for the Republic of Türkiye, the media and communication fields in general, and the historical background of the Internet in the country.

The fifth chapter presents a general overview of Internet access blocking policies in Türkiye and the effectiveness of these polices. Being one of the measurement criteria, I discuss the analysis of a YouTube case as an example for over-blocking. The chapter includes essential part of the measurement which is the circumvention tests of 25 blocked websites with three popular circumvention methods. The last part of the chapter addresses other issues and arguments about the effectiveness of Internet blocking, such as dilemmas in legal terms, access blocking terror websites, and its results as well as the circumvention tendency in the country.

In the sixth chapter, prosecution of child pornography is explored. This chapter relies on secondary data from a central police department in Türkiye. The department is a Bureau of the International Police Organization, INTERPOL, named Interpol Ankara. The department coordinates cooperation between non-Turkish departments and Turkish departments in policing and judicial matters. Looking at three years 2005, 2006, and 2007, this section analyzes how prosecution of Internet child pornography is effective both inside and outside of Türkiye, in terms of identifying criminals and bringing them before judicial authorities.
The seventh section presents overall analysis of the two aspects explored, policy implications of this study and a must "international cooperation". The final section includes weakness and limitations of the study as well as some ideas for future studies and the conclusion.
STATE POWER AND THE INTERNET

Like many technological innovations, the Internet has brought new challenges and complications. How the complications caused by the Internet are significantly different from those caused by previous communication and media technologies is a debate in the related filed literature. There are numerous scholars who believe that traditional state mechanisms are ineffective, even useless against the Internet because of its unique characteristics and features. Cairncross emphasizes that "government jurisdictions are geographic. The Internet knows few boundaries. The clash between the two will reduce what individual countries can do. Government sovereignty, already eroded by forces such as trade liberalization, will diminish further...One result: no longer will governments be able to set the tax rates or other standards they want."\(^1\) John Perry Barlow believes that, "By creating a seamless global economic zone, borderless and un-regulatable, the Internet calls into question the very idea of the nation-state."\(^2\)

Price explains that like the Internet, previous media and communication devices have caused similar problems and challenges for authorities. Border crossing radio waves including political or other kinds of undesired messages were one of the first transnational problems between states, which were later minimized by mutual negotiations and agreements. When satellites, phones, and televisions were started to be used, the conflict for national governments was again the transnational nature of the

---


technology. Although states are trying to take technical measures and develop counter technologies to cover up their air boundaries or to stop unwanted broadcasting, we may still see significant technical problems and disputes between states for these previous media and communication fields.3

To summarize the debate, Gelbstein and Kurbalija use two frames in question: “Is the Internet ‘new wine in old bottles’ or is it ‘new wine in new bottles’?”4 The “old-real” approach – or “new wine in old bottles” – argues that the Internet has not introduced anything new to the field of governance. The Internet is just another new device, from the governance perspective, no different from its predecessors: the telegraph, the telephone, or radio.

For example, in legal discussions, this approach argues that existing laws can be applied to the Internet with only minor adjustments. In the economic field, this approach argues that there is no difference between traditional and “e-commerce.” Consequently there is no need for special legal treatment of “e-commerce.”

The “new-cyber” approach—or “new wine in new bottles”—argues that the Internet is a fundamentally different communication system from all previous ones. The main premise of the “cyber” approach is that the Internet managed to de-link our social and political reality from the (geographically separated) world of sovereign states. Cyberspace is different from real space and it requires a different form of governance. In the legal field, the “cyber” school of thought argues that existing laws on jurisdiction, cybercrime and contracts cannot be applied to the Internet and that new laws must be

---

created.\(^5\)

In fact, assertive claims and exaggerated rhetoric about the transformative power of the Internet was more visible in the earliest years of the Internet when officials, politicians, and technicians faced the first challenges to govern, legalize, and nationalize this global medium. According to Seth F. Kreimer, “The first wave of legal thinking about the Internet saw millennial omens in technology. The reach of the Internet seemed to exceed the grasp of governments, and this structure heralded—or threatened—the end of censorship.”\(^6\) Castells also notes that governments were not effectively able to control this digital medium in the first years of civilian Internet use. However, government authorities increased their surveillance capacity and empowered legal mechanisms during this time.\(^7\)

The debate has many complex dimensions, and governing the Internet has brought both new opportunities and also new challenges. What is interesting in this interaction between the Internet and the nation-state is not observing how states are using traditional tools such as making laws on the Internet, founding institutions, licensing, and others. Rather, it is to observe how significant amount of Internet traffic is out of states’ control; the extent to which policies, laws, and other regulations on the Internet are applicable and effective. Further, it is important to understand why some types of states may perceive this global medium as a threat for their regime type and prefer strict censorship policies on the Internet. Likewise it is important to understand why some others are having serious legal dilemmas to regulate the Internet without damaging basic democratic and

\(^5\) Ibid, 17-18.


liberal principles. This study focuses on these kinds of complications and dilemmas for nation-states raised by the Internet. The following section explores these challenges seen in three basic functions of nation-states.

Three Main State Functions and Negative Effects of the Internet

Jackson and Sorensen classify functions that states are expected to ensure: security, individual freedoms, social order, justice and social welfare. While discussing the effect of weak states in transnational terrorism, Patrick also focuses on similar functions of nation-states: “physical security, legitimate political institutions, economic management and social welfare.”

Analytically, this section explores the effects of the Internet on nation-states based on these basic state functions: a) security, b) justice and public order, c) economic and social welfare. This classification is not a clear cut categorization to utilize for explaining the effects of the Internet on nation-states but this analytic approach is useful to frame and present this interaction between nation-states and the Internet.

National Security

Security is one of the primary concerns for nation-states and it determines state behaviors in a significant way. Being a globally open communication and media network, the Internet has raised new issue areas which tend to corrode states’ sovereignty and has

---


created new "vulnerabilities and threats" for their national security. Castells emphasizes that we are using and sharing the same network with our adversaries, criminals, and terrorists. Thus, the Internet is structurally open to all nefarious thinking anywhere in the world. Security threats through the Internet for states are analyzed in three aspects here in this section: i) the risk of being used as cyber-attacks like interstate military clashes; ii) terrorist use of the Internet; and iii) use of the internet to wage political threats against regime type and territorial integrity.

Cyber-attacks, Cyber-warfare

Cyberspace has already become a place where interstate conflicts and battles take place in asymmetric ways. The political conflict between Iran and the West, for instance, is seen to take place in cyberspace. Security experts have discovered that a virus called "Stuxnet," which is widely seen in Iran, can show that this virus was especially created to target Iran and is looking for something special there. According to Symantec (an American computer security company) records, as the Guardian noted, 60% of computers in Iran have been affected by this virus. The virus may not spread through the Internet network but is believed to be diffused in the computers and closed networks through USB ports and flash drives.

In 2007 Estonia was targeted for a series of cyber-attacks. The political disputes and conflict between Estonia and Russia at that time made some commenters suspect

---

11 Castells, ibid.
Russia was behind these attacks. But no direct link to Russia has been detected so far, nor could perpetrators be traced or prosecuted, except one Estonian student who received a fine. The computers used for this attack were spread over 100 different countries, which made prosecution complicated.\textsuperscript{13} Despite arguments whether to define it as cyber-warfare, Estonia’s unique experience affected NATO’s decision to found its cyber center in Estonia, called NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) on 14 May 2008.\textsuperscript{14}

Many of these kinds of cyber-attacks have been seen during an ongoing inter-state political conflict or a military clash. The Yugoslavian crisis showed a number of examples for cyber-attacks. During the war in Kosovo, Albanian hackers attacked and damaged about 2,000 websites.\textsuperscript{15} The \textit{Los Angeles Times} wrote that the Kosovo conflict was “turning cyberspace into an ethereal war zone where the battle for the hearts and minds is being waged through the use of electronic images, online discussion group postings, and hacking attacks.”\textsuperscript{16} When NATO launched air strikes on Serbian targets in 1999, Serbian hacker groups like the Black Hand and Serbian Angel started to attack some websites of the United States Government websites, as well as NATO’s computer networks.\textsuperscript{17} Also, the accidental bombing of the Chinese Embassy in Belgrade during the same NATO operations in Serbia in 1999 triggered attacks from Chinese hackers on some United States Government websites.\textsuperscript{18}

\textsuperscript{14} NATO Cooperative Cyber Defence Centre of Excellence, www.ccdcoe.org.
\textsuperscript{17} Ibid.
\textsuperscript{18} Ibid.
The cyber-attacks on the Georgian Internet infrastructure in 2008 were more organized and more serious than those on Estonia in 2007, according to a security expert.\textsuperscript{19} As in the case of Estonia, Russia was considered to be behind the attacks before its military forces moved into Georgia.\textsuperscript{20} According to NATO CCDCOE, cyber-attacks against Georgia included "defacement of websites," denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks, and "distribution of instructions and malicious software."\textsuperscript{21} The targets were governmental departments, financial institutions, and media outlets.\textsuperscript{22}

Despite its common use, the definition of "cyber-warfare" is not clear. Security officer Bruce Schneier believes that: "We don't have good definitions of what cyber war is, what it looks like and how to fight it."\textsuperscript{23} The OECD report also notes that incidents experienced so far in cyberspace "do not deserve the name cyber-war."\textsuperscript{24} From this perspective, cyber-warfare is an exaggerated term. However, such attacks may result in many states and security organizations taking counter measures and developing new strategies against cyber-warfare. Schneier also believes that the future wars will take place in cyberspace. Some experts worry that these kinds of cyber-attacks will become a new arms race between states.\textsuperscript{25}

"The United States officials already consider cyberspace to be a domain for warfare, similar to air, space, land, and sea."\textsuperscript{26} Speaking at a conference in Washington

\textsuperscript{20} Ibid.
\textsuperscript{22} Ibid.
\textsuperscript{24} Ibid.
\textsuperscript{26} Alex Hudson, "Is Cyber-Warfare a Genuine Threat?" \textit{BBC News}, 11 February 2011.
DC, the United States Secretary of Defense Robert Gates stressed that the United States faces a serious cyber threat that the United States Government needs to develop a security shelter, which should include private military contractors.27

NATO has started to include cyber threats in its strategic documents and develop certain policies to protect against attacks. Giving a speech to German Deutsche Welle Radio about NATO’s upcoming summit in Lisbon in 2010, NATO Secretary General Anders Fogh Rasmussen explained that in addition to conventional battles, NATO needs to be ready for the war of the future—cyber warfare. Thus, one of the important pillars of NATO’s new strategy, which he calls version 3.0, will be empowering organizational capability against all kinds of cyber threats.28

Terrorism and the Internet

Terrorism is not a new phenomenon for nation-states, but the Internet has created a new matrix for terrorists and other illegal groups to utilize. Terrorists can and are using the Internet in different ways and for different purposes. They can directly use the Internet to attack a certain targets online, which is known as “cyber-terrorism.” The term “cyber-terrorism” is the convergence of two words: cyberspace and terrorism as Denning notes.29 She defines “cyber-terrorism” as “politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. An example would be penetrating an air traffic control system and causing two planes to collide.”30

29 Denning, ibid.
Terrorists can also utilize the Internet for propaganda; data mining; fundraising; recruitment and mobilization; networking; sharing information; and planning and coordination. They can use the Internet to get knowledge and information in a particular topic from any page hosted in any country. This may include weapons, explosives, chemical substances or other kinds of tactical information. In the planning stage of any terrorist attack, they may get important details from the Internet like security points, critical times, maps, and plans of an area. Attackers may use the Internet as a propaganda tool to spread their ideology and to expand their activities. Denning indicates that in 1998, it was reported that 12 of the 30 terrorist organizations listed by the United States Department of State has an Internet presence. By August 1999, “virtually every terrorist group” had a web presence, “along with a mishmash of freedom fighters, crusaders, propagandists, and mercenaries.” Internet use is the easiest and cheapest way for groups to maintain communication with their members, volunteers, or sympathizers.

Terrorists can use the Internet for communication purposes but not necessarily in a regular and direct way. They are also aware that the web is not totally free of state control, but they develop their own techniques to perform their illegal activities. The terrorists involved in the attacks in the United States on 11 September 2001 are known to have utilized the Internet before the attack. Weimann indicates that Mohammed Atta’s last message to the other terrorists involved in the attacks of 11 September 2001 was: “The semester begins in three more weeks. We’ve obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering.” The reference to the various faculties was apparently code for the

32 Denning, ibid.
33 Ibid, 251.
buildings targeted in the attacks. Similarly, terrorists who were involved in the London bombing in 2005 are said to have communicated with each other by email. Instead of sending the messages, they saved their messages as drafts in a designated account so that the messages would be accessible to others with access to that same email account with a possible common account and/or password.

Weimann indicates the advantages of the Internet for illegal groups as

"a) easy access; b) little or no regulation, censorship, or other forms of government control; c) potentially huge audiences spread throughout the world; d) anonymity of communication; e) fast flow of information; f) inexpensive development and maintenance of a web presence; g) a multimedia environment (the ability to combine text, graphics, audio, and video and to allow users to download films, songs, books, posters, and so forth); and h) the ability to shape coverage in the traditional mass media, which increasingly use the Internet as a source for stories."

Denning believes that it is impossible to free the internet from these terror websites because of transnational structure of the Internet. Many websites blocked for terrorism-related crimes in Türkiye originate outside of the country. The separatist Liberation Tigers of Tamil Eelam in Sri Lanka has a London-based website that the Sri Lankan Government has not even attempted to shut off.

Swartz emphasized another danger on the Internet, that online access to critical military bases or important buildings through Google Earth "is alarming if not dangerous." A special agent working for Russian Federal Security Service, previously known as KGB, says "Terrorists don't need to reconnoiter about their target. Now an American company is working for them." Because of these concerns, Google, one of

---

34 Weimann, ibid.
36 Denning, ibid.
38 Ibid.
the biggest search engines on the Internet, later decided to shadow some sensitive buildings and complexes.

Political Effects

Political threats refer to the risks that the Internet can impose on states ranging from a) the possibility of revolutionary replacement of the ruling authority; b) forcing these regimes to accept serious political demands from opposition parties, minority groups, or to make significant changes in the political system; and c) putting governments in a difficult position both at home or abroad. Theoretically any state can experience these kinds of threats; however, autocratic states and dictatorial regimes are much more vulnerable to these kinds of social fluctuations. Since there is more a social consensus in democratic countries thanks to free political elections, liberal political culture, and power-sharing institutions, Internet use by the masses would not be much of a problem for them. Therefore, this aspect is very much a concern for autocratic states and is also related to the debate about whether the Internet is a democratizing agent.

"More generally, Samuel Huntington emphasizes the unprecedented importance of demonstration effects in the Third Wave of democratization, made possible by changes in global communications. Media proprietor Rupert Murdoch has even proclaimed: "Advances in the technology of telecommunications have proved an unambiguous threat to totalitarian regimes everywhere.""

Today most of the countries that apply strict censorship and intense surveillance have sensitive political concerns within their national borders. Reporters Without Borders, an international NGO that monitors Internet freedom in the world, lists 15 countries as Internet enemies, including Bahrain, Belarus, Burma, China, Cuba, Iran,

North Korea, Saudi Arabia, Syria, Turkmenistan, Uzbekistan, Vietnam. Most of these countries are considered autocratic, have a single political party, dictatorial regimes, or a weak democratic tradition. They try to control the Internet since they perceive it as a threat for their ruling authority, regime, and sovereignty. Many of them have laws that allow for the abrupt disconnection of the Internet. They have strict censorship and filtering regimes, high-level surveillance efforts, and heavy penalties for bloggers and online activists. As Reporters Without Borders reports, “The judicial or political authorities often use anti-terrorism laws to identify and monitor government opponents and activists expressing themselves online.”

The Internet and democracy

It is possible to find both pessimistic and optimistic views in the literature about the effects of the Internet on democracy. Some optimists claim that Internet promotes democracy since its decentralized structure and characteristics directly or indirectly enhance most of democratic values such as public awareness, political participation and freedom of expression. Although there are some downsides in each of these advantages, people can now find more alternative resources to get information and news, conduct online research easily, find different ways to engage politically depending on personal interests, or anonymously post ideas, images, or records on the Internet. Ultimately, the Internet is perceived as “the greatest democratizer the world has ever seen.” Castells notes: “The Internet was expected to be an ideal instrument to further democracy and still

---

41 Ibid.
42 Rodan, ibid.
The positive beliefs about the democratic effects of the Internet emerge from the rich heritage of literature about historical dynamics following the creation of the printing press, increasing print literacy, Protestant reforms, and the emergence of constitutional democracies. "Communication media, literacies, and political governance have coevolved for millennia...Communication technologies and literacies possess a power that has, on many occasions, proven mightier than physical weaponry—the potential to amplify, leverage, transform, and shift political power by enabling people to persuade and inform the thoughts and beliefs of others." Ferrall writes about the belief that the democratizing power of the Internet streams from its governing difficulty: "A Declaration of the Independence of Cyberspace, saw electronic communications technology as being inherently free and ungovernable and likely to catalyze positive social and political revolutions worldwide." 

In recent years, however, more scholars have started questioning this belief and say that "there is more hype than real change." Chowdhury believes that information abundance and peoples' awareness does not guarantee political participation. It can even cause more confusion. In a study conducted for Berkman Center in Harvard University, Chowdhury cites that "although there is a positive correlation between measures of democracy and Internet diffusion in most countries, there is still no

---

43 Castells, ibid.
47 Ibid.
convincing evidence that there is any causal relation between the two.”

Pessimists point out two important issues, which they claim limit the democratizing effects of the Internet. First is the so-called “digital divide.” Second is states’ increasing interest in surveillance and censorship policies on the Internet.

The digital divide refers to the distance between people with and without Internet access. This distance represents a new divergence both at the global and national level. The Internet has been rapidly spreading throughout the world, but this spread seems not to foster democracy as much as they emphasize. Castells notes that global web structure is significantly related with technological infrastructure, wealth and education. While the internet penetration rate in the continent of Africa was the lowest, at 15.6%, it was the highest in North America, at 78.6% in 2013. While 78% of households has internet access at home in the developed countries, it is 31% of households in the developing world.

There is also a digital divide within states. Not everyone in any society has equal opportunity to access the Internet and effectively use it for his own interests. The Internet penetration rate for China is 40.1% (out of a population of 1.34 billion, only 538 million Chinese are Internet users). The rate in Russia is 67.9 million Internet users out of a population of 142.5 million. Internet penetration rate for Russia is % 47.7. Internet penetration rate for Iran is 53.3%—42 million users out of a population of 78.8 million. In Türkiye, there are 36.4 Internet users out of a population of 79.7. Internet penetration

---

48 Ibid., 12.
49 Castells, ibid.
50 “Surfing and Site Guide Internet World Stats,” Internet World Stats, http://www.internetworldstats.com/surfing.htm. The Internet Penetration Rate corresponds to the percentage of the total population of a given country or region that uses the Internet. An Internet user is a person who must have available access to an Internet connection point and a person must have the basic knowledge required to use Internet technology.
52 Ibid.
is 45.7%.53

This situation creates new inequalities among different demographic, economic, and socio-political groups within states. Castells specifies that the Internet infrastructure is more intensive in urban areas and metropolitan regions.54 Hoctor cites that the high level of Internet use among intellectual elites in Bosnia and Herzegovina may indicate that the Internet might be is perceived as elitist. These persistent inequalities and biases mean that the Internet is far from fulfilling its role as a way to further democracy.55

Moreover, states tend to increase their surveillance capabilities, censorship practices and adopt heavy penalties against political activities on and/or through the Internet. As cited in Ferrall, “a growing area of research, known as surveillance studies, focuses on the ways in which electronic communication technologies facilitate more widespread and intense monitoring of individual citizens, limiting social freedoms and enhancing the power of oppressive regimes.”56 In Saudi Arabia, intense censorship has made the Internet more of an intranet, a limited network in a specific area or region as Drezner implies.57 Rodan notes that “such technology can also be harnessed by some states to consolidate a climate of fear and intimidation and create new opportunities to disseminate propaganda and information in their favor.”58

Different from both optimistic and pessimistic views, some scholars believe that the debate about the democratizing side of the Internet is not discussed on the right ground. In other words, they accept a normative approach and offer that we should have moderate expectations for the Internet, not to expect a revolution, regime change, or the

53 Ibid.
54 Castells, ibid.
55 Hoctor, ibid.
56 Farrall, ibid.
57 Drezner, ibid.
58 Rodan, ibid.
fall of a dictatorship. We should see how these tools are gradually opening up closed regimes to the world or how effective use of these communication devices enhances transparency, minimizes corruption, and makes the ruling regimes more responsive to their people and their demands.⁵⁹

Along with these democratic dynamics, it is impossible to question the effects of the Internet in other political issues, like the Internet use by separatist movements, and where territorial integrity is a concern for a nation-state. Today, some countries are having internal conflicts with ethnic, religious, and other minority groups. These groups demand certain political rights, religious freedom, identity recognition, or regional autonomy. Among them are the Quebec issue in Canada, the Basque region in Spain, Northern Ireland in the United Kingdom, Kurdish issues in Türkiye, and others. The virtual space has become another important space and platform for these political groups to further their political goals.

While focusing on separatist movements in East Timor and Maluku, Hill and Sen point out that the Internet was a “deciding factor in each conflict.”⁶⁰ Hill argues that “the net enabled individuals and local groups in East Timor to draw effectively upon skills and resources from supporters located far away.”⁶¹ Like in Indonesia, Hoctor notes that local opposition groups were not alone thanks to the Internet in the Chiapas conflicts in Mexico.⁶²

Domain names are another sensitive issue when these separatist minority groups are considered. The Internet Corporation for Assigned Names and Numbers (ICANN) is

---

⁶⁰ Hoctor, ibid.
⁶² Hoctor, ibid.
the private sector, non-profit United States-based corporation that issues top-level domain names. While each country has a unique domain name allocated by ICANN, new domain names for "cultural and linguistic communities" pressing for increased political rights recognition can raise new problems for some states.

"In 2003, ICANN introduced a new "cat" domain for the Catalan language. This is the first domain introduced for a language. This precedent has triggered new controversies. First, many language and cultural communities around the world are likely to request the same right. Second, in some cases language and cultural communities may have aspirations towards nationhood. This aspect may cause potential controversies and conflicts with existing states. In the case of the "cat" domain, the Spanish government did not oppose this decision."63

Justice and Public Order

Public order, public safety, and justice are essential duties that state authorities need to provide. Through different methods, institutions, and tools, states try to ensure public safety and public order. Different from previous media and communication devices, the Internet has created new challenges and dilemmas for states in ensuring these fundamental duties. As seen in social protests and revolutions in the Arab world, as well as in previous cases in Ukraine, Moldova, and Iran, the most significant complications of the Internet are in the socio-political realm.

Social Complications

Group psychology, collective action, and communication are very sensitive fields that no state can ignore. Hills notes that, "the fear of person to person communications –

63 Kurbalija and Gelbstein, ibid.
of the potential for the organization of opposition – has always been there."\(^{64}\) History shows us that technological innovations were very often influential in affecting the balance between the ruling authority and the ruled people. Before the Iranian Revolution of 1979, cassette tapes and cassette players played an important role in spreading the messages of Khomeini in Iran.\(^{65}\) Mobile phone usage and text messaging were the core instruments that unified the people of Indonesia around the fall of the Suharto regime.\(^{66}\) With the invention of the Internet this tension between the authority and citizens entered a new period. Besides interests groups, social unions, institutionalized opposition groups, NGOs, and unhappy citizens have found an effective means of communication for collective action.\(^{67}\)

Perhaps the most significant case to recognize the effects of the Internet was first seen in the case of the fall of Suharto Regime in 1998. The Internet was the essential communication medium for people to unify a mass movement against the regime through increasing awareness among the public and to organize protests against the regime.\(^{68}\)

The Internet was again on the scene when the Ukrainian Orange Revolution was emerging in the end of 2004, by ensuring effective means of communication between the crowded mass opposition groups and activists.\(^{69}\) "Despite lacking access to mass media, supporters of democratic change compensated through skillful use of the Internet to recruit volunteers, raise funds, organize campaigns, report breaking news, and garner the

\(^{64}\) Hills, ibid., 196.
\(^{65}\) Farrall, ibid.
\(^{66}\) Ibid.
sympathy of the global democratic community."

The tension between the Internet and politics was also high during the Saffron Revolution in Burma in 2007. In order to cover up violence within the country, the military junta took some measures to stop online communication. These measures were partly successful but could not totally stop the leakage of news and bloody images from the country. Thus, the government found the ultimate solution to shut down the Internet completely. The Saffron Revolution in Burma was not successful at that time, but the Internet played an important role in raising awareness about these orange-dressed monks in Burma. As Chowdhury notes “Despite efforts by the government to control all media outlets, this attempted revolution demonstrated that the Internet does not lend itself easily to control.”

Later, we witnessed the Internet shaking another country, Moldova. Analyzing political protests in this country in 2009, Mungiu-Pippidi and Munteanu indicate that the Internet was an effective tool for young protesters to communicate with each other. Thanks to the internet implications like YouTube and Twitter, the young protesters could sustain protests for several days for a political change that some journalists and scholars call this political transformation a Twitter revolution.

Both social movements in Ukraine and Moldova achieved some degree of success. Authorities revoked controversial national elections and replaced incumbent governments with new governments. Many in the West expected to see similar ends in Iran following the controversial national election in 2009; however, the Iranian

---

71 Chowdhury, ibid., 8.
government suppressed the protests by using excessive power. Although these movements in Iran could not achieve their political aims, the world witnessed how protesters utilized the Internet to amplify their voices. Independently from official Iranian media, they made personal broadcasts with their own pictures, videos, and stories.

The year 2011 became a crucial point from which to observe social booms in the Arab world, as well as to understand better the meaning of the Internet in social unrest. People who are displeased with their governments and regime types in Tunisia, Egypt, the United Arab Emirates, Saudi Arabia, people who do not believe that their governments represent them or their values found the Internet to be the perfect tool to amplify their voices, share their views and political news with like minded people, and upload pictures and videos to certain websites to attract the outside world’s attention.

Digital activists have effectively utilized the Internet. Certain websites like Facebook, Twitter, YouTube, and Daily Motion and other Internet features have had considerable success either in achieving regime change, triggering serious political reforms, or shaking old regimes in a significant way.

Social protests started in Tunis in December 2010, and President Zine El Abidine left the country in January 2011. Alexa.com is a global service that ranks websites. Some of Alexa’s website rankings for Tunis from December 2010 to January 2011 were: 1) Facebook, 3) YouTube, 6) Blogger, 12) Twitter, 13) Aljazeera.net, and 20) Daily Motion. On the same dates Egypt also experienced mass protests against President Mubarak. The incidents in Egypt started in January 2011 and President Mubarak resigned on 11 February 2011. Alexa’s rankings for the country on 04 March 2011 were: 1) Facebook, 3)
YouTube, and 7) Blogger.\textsuperscript{73}

An Egyptian NGO, “6 April,” was one of the dynamos in the events that resulted in the resignation of the 30-year old reign of the Mubarak regime. Founded in 2008 to ensure collective action among workers, they named their movement after the date of a strike that occurred on 6 April. The movement began on Facebook and later expanded to other social media like Twitter and Flicker. Declaring a national strike on 25 January 2011, it was one of the active political groups that mobilized the mass public in Egypt and was finally able to lead to the resignation of President Mubarak.\textsuperscript{74} The founder of another social media network called RNN, Ahmed Yusuf, stated that young people who did not dare protest the government before the founding of such social media networks found a place to share their opinions with others and to act collectively. Using Facebook as a platform and volunteer reporters, the number of followers of the RNN network per day was about 300,000 at the beginning of the protests.\textsuperscript{75}

A brief analysis of a website actively utilized during mass protests in Egypt in 2011

Below is detailed data about the website of the 6 April movement (www.6april.org). The data gives us a useful insight into the intense traffic to and from the site on critical dates of the social events in Egypt.\textsuperscript{76}

For the site, alexa.com interprets that, based on data and records, “compared with the overall Internet population, the site appeals more to college graduates; its visitors also tend to consist of both high- and low-income, childless men under the age of 25 who

\textsuperscript{73} Both records for Tunis and Egypt are from Alexa.com, retrieved on 4 March 2011. Alexa.com ranks the popularity of websites based on the number of visitors within the last three months.
\textsuperscript{74} BBC, "Misir'da Sokağa İnenler Kimler?" Timeturk, 28 January 2011.
\textsuperscript{75} Timuçin Mercanoğlu, "Misir Devriminin Arkasındaki Güç 'Sosyal Medya'," Timeturk, 4 February 2012.
\textsuperscript{76} "Alexa Actionable Analytics for the Web," Alexa Internet, Inc., Alexa.com.
browse from home. Visitors to it view 2.1 unique pages each day on average, and roughly 54% of visitors to 6april.org come from Egypt, where it has attained a traffic rank of 1,772.77

The popularity of the website increased dramatically by the end of January 2011.78 Since alexa.com ranks websites based on their performance in the last three months, this date in fact reflects the real traffic that started by the end of October 2011.

Reports note that social tension in Egypt has started in the end of 2010, which confirms this traffic and digital activity on this website, www.6april.org, by the end of 2010. The dramatic increase started by January 2011, which implies that online activity for the site actually started to increase by October 2010. The daily reach as a percentage increased by 330% between January and March 2011.

Upstream sites

Interesting data from alexa.com about 6april.org include upstream and downstream figures. The majority of the users for 6april.org are visiting this site after or before visiting Facebook and Twitter.

In fact, the Internet and social media were not the only influential communication and media tools during Arab Spring events. Many scholars emphasize the importance of traditional media outlets, including Al Jazeera and its Middle East-centered broadcasting. At this point, interesting cooperation and interactions occur between traditional media and Internet-based social media. While each individual and Internet user is a potential correspondent or editor on streets from which they can upload news and recordings to a

---

77 Ibid.
78 Ibid.
number of different websites, traditional media can use online news and recordings to spread and diffuse further to its audience.\textsuperscript{79} In reverse, individual Internet users can also take pictures and news from traditional media to post and upload to the Internet applications that they are using. What is surprising in this interaction is not to see the influence of so-called traditional media. Rather, it is more surprising to observe how Internet use, particularly social media, was so effective in these social upheavals during the so-called Arab Spring.

Recent revolutions, social fluctuations in the Middle East, other similar cases mentioned in this study show that the Internet can be one of the most critical media and communication platforms to inflame social unrest. The Internet or social media use itself does not directly lead to revolutions, mass movements, or regime changes. Socio-political, socio-economic reasons are still necessary for these kinds of occurrences. Rather than an independent variable, the Internet seems to be an effective communication and media tool to inflame social unrest. Without social, political, and economic reasons, the effects of Internet use alone will be limited in social unrest.

Justice and legal challenges

Like in other areas in which states have interests, authorities tend to regulate the fields related to the Internet, enforce these regulations so that legalization is ensured, and finally prosecute any possible illegality. Use of the Internet has brought new questions and challenges to the fields of justice and law. These difficulties are especially seen during the enforcement and prosecution stages.

\textsuperscript{79} During protests on Tahrir Square in Egypt in 2011, for instance, the Al Jazeera was using video records on the Internet but labeling them as “unconfirmed pictures.”
A famous phrase in this debate belongs to Nicholas Negroponte, the co-founder and director of MIT’s Media Lab, in which he asserts that “the Internet cannot be regulated. It is not that laws aren’t relevant, it is that the nation-state is not relevant.”

Likewise, Grossfeld believes that “the explosion of the Internet presents new challenges for both state regulators and self-regulatory organizations.”

According to White, “the anatomy of the Internet is unique and perhaps, impossible to regulate effectively.” Emphasizing the importance of being connected to the entire world in a global network, Grossfeld, believes that “the old parameters were intended for a telephone- and paper- based environment; the Internet challenges these traditional notions of territoriality and sovereignty.” From this point, some scholars utilize the term “cyberspace sovereignty.” Wu, for instance, notes that “Proponents of cyberspace sovereignty generally assert that it is impossible or futile” for governments to regulate the Internet.

Hollis claims that “Law cannot regulate the authors of cyber-threats because anonymity is built into the very structure of the Internet.” Hollis considers that “existing rules on cyber-crime and cyber-war do little to deter.” White notes that “the anonymity of the Internet is unique and, perhaps, impossible to regulate effectively.”

Legalization anomalies can be seen in Internet blocking measures either

---

83 Grossfeld, ibid.
86 White, ibid., 12.
implemented as prevention or for punishment purposes. In order to avoid access to illegal websites and web contents, different types of blocking techniques can be implemented. However, as summarized by Callanan et al., during these implementations it is inevitable to face some complications like over-blocking and under-blocking. There is no guarantee of totally disabling access to these undesired websites because of a variety of circumvention methods and techniques available online.\(^7\)

One of the basic principles of universal justice is the subjectivity of criminality and justice. Because of a crime or illegality, only the person(s) involved and the illegal object can be subject to criminal procedure and punishment. However, implementation of website blocking using different techniques is open to over-blocking, which means some innocent websites can be blocked along with the targeted ones.\(^8\) This inevitable complication is one of the essential reasons for authorities in the United States to approach Internet blocking cautiously because of its significant risks to damage “freedom of speech and expression,” which is strongly protected in the “First Amendment of the United States Constitution.”\(^9\)

For instance, in Meghalaya, a state in India, authorities noticed some records and postings against the local and federal government of India in a discussion group hosted by Yahoo! Groups. After the access blocking decision to the discussion group by the authorities were ordered to more than 400 Indian Internet Service Providers (ISP: business that offers customers Internet access), the ISPs shut down all Yahoo Domains

---

\(^8\) Ibid.
\(^9\) Kreimer, ibid.
and servers. Similarly, because of specific hate speech on YouTube about founder of the Turkish Republic, authorities blocked all YouTube content for a long time in Türkiye. In order to solve this problem, states can prefer a low-level blocking measure, but in this case they face another dilemma of "under-blocking," which ensures partial access to undesired websites.

In order to present the huge size and numbers of illegal Internet activities, the Intel Corporation reports that "every 60 seconds there are an estimated 135 Botnet infections and 20 new victims of identity theft" globally on the Internet. Intel also believes that for every 416 attempts at hacking, 12 of those are successful. Despite high numbers of illegal and criminal activities on the Internet, prosecution efforts and clearance rates in cybercrimes are relatively low. Kerr cites the following points about the dark side of the Internet: 1) "Although every computer connected to the Internet is subject to frequent attack by outsiders, the (United States) central government only brings criminal charges for computer hacking against about one hundred defendants per year. 2) About two-thirds of all email is unwanted "spam," unsolicited commercial email. 3) Computer viruses and malware make up about one percent of all email, although criminal prosecutions for sending out viruses or malware remain extremely rare. 4) Sophisticated pedophiles can use proxy servers and anonymous chat rooms to share images of child pornography with little fear of being caught by police. 5) Although Internet gambling is illegal in every state, millions of Americans gamble online, generating about $6 billion in revenues for the approximately two thousand Internet gambling sites. 6) Use of peer-to-


\cite{Ibid} Ibid.
peer networks remains very high despite the efforts of copyright owners to shut them down. 7) It is easy to set up an anonymous blog or email account and send threats or make false claims that are very difficult to trace.”

The Internet is open to any person from anywhere in the world and has a global structure. Thus, illegality and criminality on the Internet very often have transnational aspects. Legal difficulties seen at the national level become more complicated when the issue is transnational because of different legal structures, laws, procedures and political ideology in each state. Downloading a particular kind of software may violate a copyright law in country A. But how can authorities prosecute this kind of illegality when the downloader is from country B, web-servers and web hosting are located in country C, and the owner of the website is from country D?

When neo-Nazi propaganda was a judicial and diplomatic problem between Yahoo and France, Yahoo’s Vice President Heather Killen at that time said, “We have many countries and many laws and just one Internet.” Even today, in some of judicial disputes at the international level, we can see that this statement is not outdated and still utilized by global websites like Yahoo, Google, and YouTube when they are the subject of judicial proceedings in any state.

Kerr cites the following incidents to emphasize on these kinds of transnational legal problems.

In 2000, Onel de Guzman sent out the “Love Bug” virus from the Philippines; although the virus caused billions of dollars in damage worldwide, de Guzman was never charged because the Philippines did not have a computer crime law that allowed extradition. (Although the United States and the Philippines have an extradition treaty, Philippine law requires that both countries legally recognize a

---

94 Goldsmith and Wu, ibid.
95 Kerr, ibid.
given offense before a suspect can be extradited [and] there is no Philippine law that prevents release of a virus.)

Even for ordinary crimes like murder, theft, drug smuggling, and embezzlement, when a criminal procedure involves multiple states and/or their citizens, it is very often difficult to identify and prosecute these traditional criminal cases and bring these criminal(s) before judicial courts. In addition to jurisdiction and citizenship problems, the Internet's rapidly changing features complicate the situation further for officials trying to trace criminality and find and identify perpetrator(s) from each state.

Although there is some degree of cooperation at the international, regional, or mutual level, and some collaborative international institutions like Interpol, Europol, each state's different ideology, political traditions, national law, and diplomatic and political barriers significantly hinder criminal procedures and/or extradition of criminals to the victim state(s). Beside legal and political differences among states, there are significant technical barriers and technical capacity gaps among states to achieve such an effective level of international cooperation against criminality on the Internet. Goldfoot, claims that "it is unrealistic to believe that a global community consisting of an estimated ninety million users of almost thirty million computers spread over 196 nations and many divergent legal cultures could reach a consensus on how to govern themselves." 

Thus, new legal approaches should be developed while regulating the Internet and online activities. In his speech to the United States Senate Justice Committee, Mike Godwin, representing the Electronic Frontier Foundation, stated that he believes that it is wrong to consider the Internet in the same category as existent media and communication tools. He emphasized that the Internet has created new questions as well as problems for

---

96 Ibid.
 Likewise, Akdeniz and Altınparmak, believe that thinking of the Internet as one of the previous media and communication devices is not appropriate if lawmaking is considered on the Internet. Policy makers, lawyers, and politicians should understand the unique structure and characteristics of the Internet and new legal mentality and methods should be developed.

Also, an effective means and level of cooperation among nation-states are vitally important, as criminality on the Internet is very much transnational. Considering cooperation as a kind of concession, Castells believes that “the more a state refuses to limit its sovereignty...by international cooperation, the more it becomes vulnerable to cyber-attack.”

Economic and social welfare

The effects of the Internet on the economy are also enormous. Today, the information technology, computing, and communication sectors can compete with the prominent sectors of the previous industry era. Three of the top ten most valuable global companies in 2007 were the so-called tech companies Google, Microsoft, and IBM, and by sector ranking, the IT and technology sector comes second to the finance sector. Retail is in third place. The Internet opens national economies to the global market. Freund and Weinhold imply that directly or indirectly the Internet has positive effects on

---

98 White, ibid.
100 Castells, ibid., 160.
economic productivity and growth in the United States.\textsuperscript{102}

According to Kellner, the recent tendency to transition market capitalism into a more technology-driven model with the information superhighway, which is advocated by "Microsoftcapitalism" proponents, is very challenging.\textsuperscript{103} However, this new shape of capitalism will eventually erode the welfare state next to the liberal free market promises of more jobs, wealth, prosperity, education, information, and more democracy.

Basic principles of economy, free market and capitalism are still valid. Still we have banks, shopping centers, retailers, malls, stocks; and we have money and cheques, etc. But the World Wide Web has brought different opportunities, options, and mentalities from marketing to production; from financing to shopping, and advertising. The two important values of a free market—competition and reliable "information"—are very much being promoted and ignited through the platform of the Web 2.0.

Castells stresses that "the proper usage of the Internet is a key tool for a better competition at home and at global level."\textsuperscript{104} The Internet provides easy and fast access both for consumers and customers to find different markets, to get information about the details of a product, to compare different retailers' offers, and make their rational choice. Brown and Goolsbee note the Internet decreases "search costs by enabling price comparisons on-line."\textsuperscript{105} Although the Internet has created its new mediators from producers to consumers, Castells believes that "the Internet reduces transaction costs at

\begin{thebibliography}{9}
\bibitem{102} Caroline L. Freund and Diana Weinhold, "The Internet and International Trade in Services," \textit{American Economic Review} 92, no. 2 (May 2002): 236-40.
\bibitem{104} Castells, ibid.
\end{thebibliography}
least by 50 percent.\textsuperscript{106}

In a free market, it is also important both for sellers and buyers to access accurate information. Restricted flows of information and asymmetry of information are considered as a "market failure" as Adam Smith phrases it. When some relevant information is known by some but not all the parties involved, it causes inefficiencies in the market.\textsuperscript{107} The Internet has many advantages and positive features to minimize these inefficiencies and market failures. Rhee states that "with the advent of the Internet, almost gone are the asymmetries of information among firms."\textsuperscript{108} Varieties of alternative pages, links, and forums revoke many of the barriers to the flow of information or the asymmetry of information.

Traditionally, states tend to have quotas, customs, and tax regulations to protect their national economies. The borderless feature of the Internet has brought different dimensions and questions to the fields of economy, market, and commerce. For instance, how can Internet commerce be taxed or regulated effectively?\textsuperscript{109} Many of the leading global companies directly or indirectly related to the Internet today are United States-based companies like Google, Microsoft, IBM, Apple, and Yahoo. Others Internet-phenomena like Facebook and Twitter likewise are United States-based initiatives with global reach.

In the beginning of the 1990s, in her book \textit{The Retreat of the State}, Susan Strange claimed that states are losing negotiation power against the growing economic as well as political influence of multinational corporations (MNCs) and thus, she believed that

\textsuperscript{106} Castells, ibid.
MNCs were gradually eroding the economic and political sovereignty of nation-states.\textsuperscript{110} This claim is still apparent today, if not more serious, for the IT sector dominated by the Internet. It is very challenging for any state to stop, eliminate, or effectively tax Internet-based companies providing services and making profits from their online activities.

For a long time, the Turkish government has had taxation and legal disputes with Google and Google-owned YouTube. The Turkish Minister in charge of transportation and communication strongly criticized Google in the case of YouTube blocking and stated that, "It is not an issue of blocking or censorship on YouTube as Google claims but it is the issue of obeying local law, defending themselves in Turkish courts." The Minister added, Google "should open a local representative office in Türkiye and pay local tax."\textsuperscript{111} The Turkish government claims Google owes EUR 32 million in taxes.\textsuperscript{112} Likewise, there is a similar debate between China and the United States about Google services in China.\textsuperscript{113}

At this point, one of the important policies that some states prefer to implement is Internet blocking as a measure. Although there are political, moral, religious or health-related reasons behind Internet blocking, sometimes these measures can be considered as a non-tariff barrier against foreign companies to hinder their services within the borders of a country. As with these issues, concepts and theories of economy and marketing should be re-interpreted and even re-organized for the Internet.

As explained in this part of the chapter, the use of internet has significant and

\textsuperscript{111} "Bakan Google Ve Youtube Sert Çıktı," Haber, 11 June 2010.
\textsuperscript{112} Robin Wauters, "Turkish Government Claims Google Owes €32 Million in Taxes," CrunchBase Information, 3 November 2009.
serious effects on the basic functions of states on ensuring national security, justice and public order. The following parts explain what internet blocking is, and how it is implemented.

CENSORSHIP AND BLOCKING ON THE INTERNET

Though sometimes used in a similar context, the terms “censorship” and “blocking” on the Internet have different meanings in academic and technical terms. The Oxford online dictionary explains “censor” as “an official who examines books, films, news, etc. that are about to be published and suppresses any parts that are considered obscene, politically unacceptable, or a threat to security.”\(^{114}\) The same dictionary explains the word “blocking” as “the action of blocking or obstructing someone or something.”\(^{115}\)

From this definition, it is important to note that “censorship” occurs before an unfavorable thing is disclosed or about to be disclosed. Censorship is a general term, which can be used in broadcasting media such as TV, radio programs, or in printed media like newspapers, magazines, or even in art as well as on the Internet. The term “blocking” for the Internet is more a technical term that includes many “policies, software, hardware, and services.”\(^{116}\) “Internet blocking” is sometimes also called as “Internet filtering.” Filtering is defined as “[with an object] pass[ing] (a liquid, gas, light, or sound) through a device to remove unwanted material” in the same dictionary.\(^{117}\) Both “Internet blocking” and “Internet filtering” are used interchangeably in the literature.\(^{118}\)

Internet blocking can also be implemented in non-technical ways, like shutting

---


\(^{115}\) Ibid.

\(^{116}\) Callanan et al., ibid.

\(^{117}\) *Oxford Online Dictionary*, ibid.

\(^{118}\) Paul Greenfield, Peter Rickwood, and Huu Cuong Tran, "Effectiveness of Internet Filtering Software Products," (Sydney: CSIRO, Mathematical and Information Sciences, 2001).
down the entire Internet services by powering off routers, central servers, or Internet Service Providers (ISPs). For example, during the uprising against military junta in Bruma (Myanmar) in 2007, authorities initially blocked social media like YouTube and BlogSpot, but later the Internet was totally disconnected.\textsuperscript{119} Some reports also indicated similar situations during the Arab Spring, for instance, in Egypt and Libya in 2011. Even in these situations, there are alternative methods available to access the Internet.\textsuperscript{120} Rather than these kinds of total Internet disconnection though non-technical methods, this study examines how Internet blocking technology is effective in preventing undesired web content.

Blocking or filtering measures can be considered for different reasons by authorities. While some countries have sensitivity against ethnocentrism like in some Western states, some states prefer blocking for political reasons, religious reasons, or to minimize hate speech.\textsuperscript{121} Blocking can also be seen against copyright violations, pornography, health hazardous contents, and gambling as seen in Türkiye.

While for instance keyword filtering is a case against “Falun Gong” in China, Iran is known for its extensive internet access blocking against websites for hate speech or jogging with political and religious leaders, immoral reasons. Some European countries like Germany, France have some filtering cases against websites which may have xenophobia, Nazi contents. Many states including Canada, Denmark, the U.K., and Finland have such practices against child pornography.\textsuperscript{122}

\textsuperscript{119} Chowdhury, ibid.
\textsuperscript{121} Callanan et al., ibid.
Where it can be implemented?

Blocking can be applied at any level, including “an individual’s personal computer, an office local area network (LAN), an Internet café, an ISP, a wireless network, an SMS system, at the backbone or international gateway level, or some combination of all of these levels.” 123

The target of blocking instruments as specified by Callanan et al. are IP addresses; Domain name and DNS; Uniform Resource Locators (URLs); File content and File name; Keywords; and Content Signature (hash values).124

How to block? Blocking strategies

Greenfield et al. explain three methods for filtering Internet content: i) Inclusion filtering (white list), which runs based on the philosophy of “guilty until proven innocent.” Thus, it perceives most of the Internet websites as inappropriate except some well-known acceptable sites. The problem with this method is its allowance for access to a very small portion of the Internet. ii) Excluding filtering (black list) runs on the philosophy of “innocent until proven guilty.” This method is more common than the “inclusion” method. iii) The content filtering method dynamically analyzes the web content received and activates blocking when the content does not comply with the installed criteria. During the analysis process, the system utilizes certain keywords and/or checks certain parameters of the content. The fourth method is the combined filtering method in which all above techniques are utilized to increase the effectiveness of

124 Callanan et al., ibid.
blocking. However this latter method is not free of complications either.\textsuperscript{125}

Content filtering

Greenfield et al. analyze content filtering methods including source-based filtering and content-based filtering.\textsuperscript{126} Similarly, Deibert subdivides content filter techniques into address blocking techniques and content analysis techniques.\textsuperscript{127} Source-based filtering (address blocking technique) is a method that utilizes IP addresses (Packet filtering), domain name, DNS, and URLs while filtering objectionable websites.

The following are the details of these technical terms. Internet Protocol (IP) address is a unique numeric number given to each computer or web server that is connected to the Internet. The Internet recognizes IP numbers as the identity and addresses of the device for outgoing and incoming requests and data transfers. These unique numbers are regulated and allocated by an international non-profit agency based in the United States, The Internet Corporation for Assigned Names and Numbers (ICANN).

Today, IP numbers version 4 (IPv4) are widely used. An IP address can be seen as (x.x.x.x) where x is a number between 0 and 255.\textsuperscript{128} However, reports indicate that the capacity of IPv4 is about to be exceeded, and by the year of 2010 the next version, IPv6, was being allocated for each nation.\textsuperscript{129} While IPv4 is 32-bit, IPv6 is 126-bit, and specific IP number allocation is more possible with this latest version.

\textsuperscript{125} Greenfield et al., ibid.
\textsuperscript{126} Deibert, ibid. divides “content filter techniques” as “address blocking technique” and “content analysis technique” but with only one difference by using “address blocking technique” instead of “source based filtering” as Greenfield, ibid. does.
\textsuperscript{127} Deibert, ibid.
\textsuperscript{128} Callanan et al., ibid.
Greenfield et al. have named IP based filtering packet filtering. All data on the Internet, no matter its type—whether video, audio, image, or text—are transferred from one receiver to another server as data packets with IP addresses from both parties. When a packet includes an IP address from an undesired website, the filter blocks the packet at its final destination. This filtering can be carried out by Internet Service Providers (ISPs) in their routers.

The problem with IP-based packet filtering is its over-blocking risk. Since in general IP addresses are assigned to a computer, and a number of different websites may use the same computer or the same server, blocking an IP address because of one website may block other innocent websites that share the same device with the same IP address. It is likely that IP-based filtering may cause under-blocking or even over-blocking and thus this technique is not preferable or popular for those with such concerns.

Different from a numeric IP address, which is more appropriate for computers to communicate, the Domain Name System (DNS) is designed to be convenient to be Internet users. Rather than remembering all different groups of numbers for each website, this system allows individuals to type the name of the site. For instance, the IP address and the domain name of the ICANN website are 192.0.34.163 and www.icann.org respectively, and both can be used interchangeably to access the same website. However, instead of remembering the code numbers for a website, typing its domain name (or its abbreviation) is more easy and convenient.

A typical domain name follows generic top-level domains like .com, .org, .net,
and may follow country codes like .ba, .ge, .il, or .md. A website may have a number of separate websites and blocking based on domain names only and will be insufficient to cover up the entire website contents, including all other pages served by the same website. The same is also true when a website like www.terror.com uses different domain names like ww2.terror.com or ww3.terror.com and uses a number of different servers. It is likely that both domain name and DNS blocking to cause under-blocking or over-blocking, and for effective filtering, it is necessary to know and include all possible domain names as well as their numerical IP addresses in the lists of filtering.134

Together with domain names, the Uniform Resource Locator (URL) address shows which website the content is from and exactly on which path it is accessible. URL filtering is more accurate than IP-based filtering. It can be effective even on a single specific website and causes relatively fewer complications than IP filtering as Greenfield et al. explains.135 By this technique, it is possible to block a particular user’s unfavorable website (like www.facebook.com/users/ahacker) without blocking the entire website (www.facebook.com). When the entire website is intended to be blocked, specification for these websites should be encoded in a filtering list like a date period: www.terror.com/June2011/centrefold.html and www.terror.com/August2011/centrefold.html. While it is less likely that URL filtering may cause over-blocking, it is very likely that it may cause under-blocking errors.136

Content-based filtering (content analysis technique)

Rather than looking at the identity and addresses of the sources or destinations,

134 Ibid.
135 Ibid.
136 Ibid.
content-filtering techniques verify the contents of the Internet traffic and block the ones that include inappropriate data. Greenfield et al. specify four techniques as a content-based filtering: i) keyword filtering, ii) phrase filtering iii) profile filtering, and iv) image analysis filtering.\(^{137}\)

Keyword filtering is focusing on important words and terms in their black lists. It is widely utilized for most of the text-based Internet applications like search engines, email, URL links, and instant messaging.\(^{138}\) The challenge in this technique is to specify and include all possible variations of phrases regarding undesired web content. "Not every content or type of a file on the Internet [is] named or seen as what it is or [for] what it has in [it]."\(^ {139}\)

Keywords in a blocking list may not cover all alternatives that human cleverness can invent. To avoid key word filtering, for instance in China, Internet users are trying other way of spelling, saying, or symbols like "Tibetan@independence" or "Ti be tan in dependence" instead of "Tibetan independence" in their communications on instant messaging or chat rooms.\(^ {140} \)

Keyword filters are not without problems. For instance, including the word "sex" in a blacklist may wrongly block an academic article talking about gender, or a place like Essex in England. Moreover, keyword blocking can be bypassed by encrypting the content to make it unrecognizable by the filter and thus "a request that is blocked by a

\(^{137}\) Ibid.
\(^{139}\) Callanan et al. ibid.
keyword filter as an HTTP request will not be blocked as an HTTPS request."\textsuperscript{141}

Phrase filtering

Keyword filters can confuse and wrongly filter scientific, educational, or daily context instead of undesired web content. The word "breast," for instance, may cause blocking of news or an article about "breast cancer" by keyword filters.\textsuperscript{142} Thus, more sophisticated phrase filtering has been developed by IT vendors. This technique not only looks for a specific word but also looks for its context and how it is used. In this way, phrase filtering makes fewer mistakes than key word filters.

Both key word and phrase filters are text-based filters, and significant challenges and difficulties may be experienced in its adaptation and operations with different languages and their unique phonetic structure.\textsuperscript{143} Further, both of them can only check text but not images or video. In response, vendors have developed new techniques that can analyze some characteristics of websites and web content, such as "profile filtering" and "image analysis filtering."

Profile filtering checks some technical details of web content and blocks it when some similarities with undesired content are being tracked. Greenfield et al. notes one method, for instance, is looking at "the ratio of pictures to text" of suspected content and comparing the ration to the profiles of other similar web content before deciding whether to block.\textsuperscript{144}

Image analysis filtering also aims to close the gaps of text-based filters. It tries to capture and read specific features of unwanted images, for instance "skin tones," which

\textsuperscript{141} Roberts et al., ibid.
\textsuperscript{142} Greenfield et al., ibid.
\textsuperscript{143} Ibid.
\textsuperscript{144} Ibid.
may imply a naked body. But, this analysis may also wrongfully block an artistic image presupposing it to be a sexual image.\textsuperscript{145}

CIRCUMVENTION

Internet blocking methods do not delete or remove the undesired web content at its source. Instead they just prevent it being accessed by an Internet user. Circumvention methods try to evade these blocking barriers, commonly by hiding IP address, content signatures, the destination, or what is inside the trafficking packets.\textsuperscript{146}

Internet search engines, like many other subjects and topics, house thousands of different resources, websites, forums, and online “know-how” content available on the Internet in different formats like a video, images, or slideshows. Not every nation-state that implements some form of Internet blocking domestically takes measures against these circumvention tools.\textsuperscript{147}

Circumvention tools basically bypass blocked Internet contents by ensuring the privacy of the users’ Internet traffic. There are a number of customers or curious actors that are interested in people’s Internet habits, their preferences, and/or their connections. These can be governments, secret policing services, commercial companies, or employers.

Circumvention tools try to ensure privacy generally by utilizing encryption technology. However, encryption is not a secure enough method against Internet surveillance, which generally relies on “traffic analysis.”\textsuperscript{148} Traffic analysis utilizes

\textsuperscript{145} Ibid.
\textsuperscript{146} Roberts et al., ibid.
\textsuperscript{147} For instance in Türkiye, although there are some levels of Internet blocking, not all circumvention methods and proxies are blocked in the country as seen in this study.
\textsuperscript{148} "The Onion Routing Project," Torproject.org.
Internet data packets which have two main parts including a data “payload” for the Internet content, which can be an email, video, or a website, and the header for routing. Focusing on the headers of Internet traffic, surveillance experts can see the parties of Internet communication and the details of the communication content even though the content is encrypted. In order to overcome this risk, beside encryption, some circumvention tools utilize different server nodes in a network between the Internet user and the resource. Further, Internet traffic is set to follow different paths randomly between the nodes each time.149

There are a number of different techniques for circumvention. Callanan et al. specify some of the main methods as: proxy-servers, tunneling, hosting or URL rotation, botnets, evading DNS-based filters, and other filters.150

Proxy Servers

The most common and widespread circumvention method is using “proxy” and/or “anonymous” foreign servers, which usually operate outside national borders.151 Proxy servers play crucial roles in optimizing the Internet performance. In order to maximize the network capacity, proxies are developed to copy Internet packets during data trafficking on their records. Later, without collecting the same content from its original server, proxies use these web contents (cache) when the same content is requested by any user at future times. Thus, proxies can show which websites are being visited by any Internet users.

Different from “proxies” set by an Internet Service Provider in Internet

---

149 Ibid.
150 Callanan et al., ibid.
151 Li, ibid. and Brown, ibid.
connection, Internet users can select other proxies available on the Internet for some reasons, such as to increase performance, to ensure privacy, and especially to circumvent Internet blocking. In this situation, the proxy becomes as a demand device, generally outside national borders, and Internet traffic operate through these proxies.\textsuperscript{152}

By using a foreign proxy server, free or paid, many of which are available on the Internet, users can select another similar device abroad to fulfill access requests. The basic difference between proxies available on the Internet is their operating preference for their servers. While some proxies have their own central hosting servers for providing such a service, others do not prefer a central server but use "peer hosting servers."\textsuperscript{153}

Some proxies can hide IP addresses of the requesting Internet users from the destination and/or from the Internet Service Provider through encryption. Using such proxy servers can circumvent IP address and DNS blockings; however, Roberts et al stress that public proxies especially may not be secure in terms of privacy since they rarely use encryption.\textsuperscript{154}

Chowdhury gives the examples of people in Burma using proxy services in 2007 for circumvention since the military regime there blocked many websites, including YouTube, BlogSpot, and CNN.\textsuperscript{155} People use of proxy servers such as Glite.sayni.net, Your-freedom.net, and Yeehart.com to enable dissidents to break out of the government’s strict censorship and feed news and multimedia to the global media from inside the country. Thousands of Internet users in Burma reportedly downloaded the circumvention software of Glite.sayni.net. Consequently some call the uprising in 2007 the “GLite

\textsuperscript{152} Callanan et al., ibid.
\textsuperscript{153} Roberts et al., ibid.
\textsuperscript{154} Ibid.
\textsuperscript{155} Chowdhury, ibid.
Tunneling

Rather than using a public Internet connection that is open and unscripted, the Internet protocol named Virtual Private Networks (VPN) was originally developed for encrypting Internet communication for relatively private issues. Tunneling can be seen in other protocols, like HTTP tunnels or ssh tunnels, but the most common type of tunneling is VPN-based tunnels.\textsuperscript{157}

Dealing with some official tasks or sensitive issues, companies, public institutions, or some civic associations prefer using the VPN protocol for communicating among their agencies over the Internet. Thus, without investing and founding a separate private line, they can use regular Internet infrastructure for such private communication.

"Tunneling works by wrapping the IP packet to be sent inside another IP packet, giving the wrapper the address of an appropriate gateway computer and sending it over the Internet. When the wrapped packet reaches the gateway, the inner packet is extracted and sent on for delivery within a local or private network."\textsuperscript{158}

Callanan et al. note that due to extensive lawful usage of tunneling technology in the business and public sectors, it is not possible for internet service providers to block these tunneling servers or websites, many available online.\textsuperscript{159}

Hosting or URL rotation

This method is for website owners and content providers to bypass blocking. Some websites may periodically change their IP addresses, domain names, or URLs for
providing better service, for increasing their audience numbers, and even for evading blocking measures against them. A filter, which blocks a website based on its previous IP address, URL, or domain name, will be ineffective when a website owner changes the domain name, IP address, or URL.¹⁶⁰ This change is relatively easy and inexpensive for site owners that they may occasionally make these changes when they are blocked.

For instance, a blocking measure may rely only on the IP number to block. The website owner using this blocked IP number may evade this barrier by only changing the IP number from the same hosting company or from another. Likewise, in the case of Domain Name blocking only, the change is necessary on the website’s domain name.

Website owners can also find other available, unblocked hosting servers, generally abroad, to utilize for circumvention. There are lots of free or paid hosting servers and IP numbers available on the Internet.

Botnets

The term “bot” is short form of “robot.” Through some malicious programs, criminals may compromise an innocent computer as a “bot,” which can then be directed to operate certain processes without the knowledge of the computer’s owner. This computer is also called as a “zombie computer.” Such a takeover may result in a slowing down of the computer function.

Callanan et al. define a “botnet” as “a collection of computers configured to transmit messages to other computers on command usually for malicious reasons.”¹⁶¹

Criminals can use botnets for sending spam, spreading viruses, attacking computers or

¹⁶⁰ Ibid.
¹⁶¹ Ibid., 53.
servers; or for fraudulent purposes.

When a botnet takes a computer over, it becomes like a proxy, either as a portal or a deflector in the data traffic between the requester and the resource server. This will simply bypass IP-based blocking while ensuring anonymity. Callanan et al claim that traffic details that may identify the visitors will be hidden during this process, and these identifying details can easily be manipulated.\(^{162}\) They note that the “bot” would not track log records of the visitor.

Evading DNS based filters

It is relatively easy for a user to circumvent a DNS-based filter. In order to circumvent DNS-based blocked websites, users need to modify their computer settings, such as changing the identical number of the DNS that blocks an undesired website with another configuration of DNS servers, generally outside of the blocking country. Like many other circumvention tools, free or paid, individuals can find many alternative DNS servers and their address details on the Internet and even learn how to make such modifications in their computers for circumvention.\(^{163}\)

Following these tutorials, the steps are performed and show how DNS addresses are changed. In the last section, the default automatic DNS obtained is deactivated, and the other option “Use the following DNS server addresses” is selected. DNS change is okay when new DNS numbers, many which are available online, are encoded both for the preferred DNS server and an alternative DNS server.

\(^{162}\) Ibid.
\(^{163}\) Ibid., and Roberts et al., ibid.
The use of “proxy” servers around the globe

Hal Roberts, Ethan Zuckerman, and John Palfrey from The Berkman Center for Internet & Society at Harvard University, tested how some circumvention tools are effective to evade Internet blocking in some countries. They analyzed nine circumvention tools that use five different methods: HTTP proxy, CGI proxy, IP tunneling, re-routing, and distributed hosting. They gave the details of these pages, methods that they use, functions and other technical details.

Despite some performance problems and security concerns, the study stresses that “all of the circumvention and anonymity tools included in this study succeeded at the basic task of retrieving blocked content in a filtering country.”

It can be assumed that online circumvention services and/or bypassing websites are popular in countries where blocking policies are systematic, strict, or widespread. And the use of such websites and services are relatively less popular in countries where Internet blocking is very low or limited. In order to see the situation, this study uses data available from Alexa, a global web-ranking website for the most popular circumvention websites around the globe and from which country such websites receive visitors.

Alexa categorizes and ranks global websites based on their area of activities. For instance, Alexa places its section on hosted proxy services under the topic titled “proxying and filtering.” That section is located under the heading “Internet” under the heading “Computers.” Alexa ranks websites based on their popularity under this classification. Only the five most popular website are taken into consideration based on their rankings on 01 April 2011. The top five website and their areas of service are

164 Roberts et al., ibid.
165 Ibid., 22.
166 Ibid., 85.
167 Alexa, ibid.
reported as follows: 1) Anonymouse: Free anonymous surfing, email and usenet posting; 2) Vtunnel: Web proxy supporting SSL via the HTTPS encryption protocol; 3) Ktunnel: Turkish Cgi Proxy which supports watching YouTube and other video sites; 4) Proxify anonymous proxy: Proxify is a web-based anonymous proxy service; 5) Proxy.org: Contains various lists of web based proxies, as well as a forum to discuss topics.\(^{168}\)

For the degree of internet blocking, this study utilizes classifications from an independent NGO, Reporters without Borders (RSF), which monitors Internet freedom in the world. It has two lists in which countries are identified as “Internet enemies-strict censorship” or “countries under surveillance-having some kinds of blocking and filtering.” While China, Iran, Saudi Arabia and Cuba were reported within the first list; Australia, Russia and Türkiye were in the second list.\(^{169}\) Countries in any of these two lists by the RSF are called RSF-classified countries. Countries that are not listed by the RSF are considered non-RSF countries.

Proxy usage for circumvention and bypassing is not only popular and widespread in countries where strict internet blocking policies are preferred (countries listed by the RSF) but also popular among the countries in non-RSF countries, which are known as relatively liberal and democratic.

Being in the list of RSF, listed as “country under surveillance,” Türkiye is the first country in terms of the total percentages of visitors for the two websites above, ktunnel.com and vtunnel.com. Not classified by RSF, the percentage of US visitors are highest for three of the other websites, anonymouse.org, proxify.com, proxy.org. Likewise, the second and third countries are both from RSF or non-RSF countries like

---

\(^{168}\) Ibid.
\(^{169}\) Reporters Without Borders, 2011, ibid.
India and Russia for anonymouse.org; China and India for vtunnel.com; Azerbaijan and Germany for ktunnel.com; Australia and Canada for proxify.com; India and the United Kingdom for proxy.org.170

PROSECUTING CHILD PORNOGRAPHY

Though states have taken so many legal, technical measures and though there is a wide international consensus against it, child pornography is still a significant problem on the Internet. An independent organization, Telefono Arcobaleno, which has focused on the issue of online pedophilia since 1996, issued a report in 2008 that presents the alarming situation.171 The report claims that pornographic material on European servers increased 406% since 2003, and there are 20 billion online transactions that include 1.7 million records of 36,149 child-victims, 42% of whom are under seven years old and 77% of whom are under nine years old.172 The report also stresses that either free or with credit cards, these kinds of materials are easily accessible and purchasable online.

A special report, issued for the United Nations by Najat Maalla M'jid'in in 2009, notes that the number of child-victims in this crime is between 10,000 and 100,000. Turla and Özkanlı claim that child-victims under the age of 16 number between 300,000 and 600,000.173 The number of websites hosting some form of child pornography content increased to 480,000, between the years of 2001 to 2004.174

170 Ibid.
172 Ibid.
A specific child pornography site could receive a million hits in a month.\textsuperscript{175} Turla and Özkanlı believe that the crime was a USD three million business in 2005.\textsuperscript{176} They report that 300,000 credit card transactions conducted for the purchase of child pornography in the same year from 66 countries. Beside these numbers it is important to stress that the total amount of trade of child pornography on the Internet is unknown.

Prosecution magistrates' courts have been low—only 113 in 1995 and 235 in 1997 in the UK. Susan S. M. Edwards stresses the difficulties of policing, identifying, and detecting child pornography access on the Internet.\textsuperscript{177} Mr. Arena, president and founder of Telefono Arcobaleno, states that "less than 1\% of victims of child sexual abuse images have been detected, therefore it is necessary to divert all available resources and energies towards identifying, recuperating, curing and socially reintegrating all abused children."\textsuperscript{178} The United Nations Special Report on the Sale of Children, Child Prostitution and Child Pornography from 2004 even stresses that a considerable number of countries do not have legislation on this issue.\textsuperscript{179}

Criminality against children

Criminality against children is argued in a broad context in the literature. Essentially, it is considered in two main dimensions. One track explores how children are involved, or induced into certain types of crimes or as subjects of crime. The other track examines crimes against children, where children are victims, as is the case with child

\textsuperscript{176} Turla et al., ibid.
\textsuperscript{178} "Child Slavery on the Internet Is Still Growing," ibid.
\textsuperscript{179} International Resource Centre (IRC), www.internationalresourcecentre.org/.
pornography.

As cited in Chase and Statham, the sexual exploitation of children can take many forms, "including: trafficking, prostitution, sex tourism, mail-order bride trade, involvement in pornography, stripping, battering, incest, rape and sexual harassment."\textsuperscript{180} And the Internet can facilitate many of these types of sexual abuse in a significant way including Internet child pornography.\textsuperscript{181}

The 2000 UN Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography, explains the term "child pornography" in Article 2(c) as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child, the dominant characteristics of which is depiction for sexual purpose."\textsuperscript{182} For analytical purposes, Wortley and Smallbone accept the general definition of child pornography as "any record of sexual activity involving a prepubescent person."\textsuperscript{183}

Internet child pornography

In terms of the Internet, child pornography should be understood as digital forms of any pornographic record involving a prepubescent person. These records can be digital files, photographs, videos, or audio recordings. Legal perceptions may vary, but there are ten different degrees of these kinds of records from non-sexualized pictures to sadistic records as Wortley and Smallbone cite and internet child pornography includes

\textsuperscript{180} Elaine Chase and June Statham, "Commercial and Sexual Exploitation of Children and Young People in the UK?" \textit{Child Abuse Review} 14, no. 1 (2005): 4-25.
\textsuperscript{181} Wortley and Smallbone, ibid.
\textsuperscript{183} Wortley and Smallbone, ibid.
possession, production and/or distribution of such records. Excluding other kinds of sex crimes against minors like illegal detention, child marriage, harassment etc. this study covers any crime against minors committed on or through the internet and internet applications such as messengers with webcams, file sharing applications, or email.

Possession and production

Many images and records of child pornography on the Internet are old ones, generally reproductions of images from older magazines and films. Relatively new ones are frequently made in the developing countries. Some individuals may use webcams or other video hardware for making amateur recordings.

Images of children taken from the Internet can be combined in the form of a pornography slideshow. In a judicial case in the United States, Ashcroft v. Free Speech Coalition, the United States Supreme Court decided that “computer generated child pornography” is not illegal. It is necessary for law enforcement agencies to demonstrate that the victim depicted in a digital record is not digital but an actual real child.

Once these records are created or obtained, digital versions of such records are stored in different ways in personal computers, on CDs, on DVDs, and on external drives. In addition to digital fingerprints of Internet activities, forensic analysis of such tools, when put to use, is very important for judicial investigation. The digital forensic field is a new area for experts and high tech companies to develop new technological methods to detect or identify criminal activities, even when evidence is deleted or damaged.

184 Ibid, 7.
185 Ibid.
186 Ibid.
187 "Çocuk Pornosuna Karşı Nası Savaş Verirsiniz?" SDN, 14 April 2011.
188 International Resource Centre, Ibid.
Distribution

The Internet is a perfect tool for child pornographers to market and disseminate pornography. The very complicated network structure of the Internet enables such perpetrators to utilize the servers or computers of others from any country. Perpetrators use websites, chat-rooms, newsgroups, email, email groups, instant messages, bulletin boards, and peer-to-peer (P2P) networks for different purposes in this crime. They can digitally hide themselves from law enforcement agencies for prosecution thanks to their technical skills.

The most common application on the Internet is websites with hyperlinks. It is uncommon for ordinary Internet users to encounter child pornography while surfing the Internet. Purveyors of child pornography use temporary websites, servers, links, and different techniques to avoid police detection. Sometimes they provide passwords for certain types of files. These passwords are shared through the other Internet applications such as e-groups and bulletin boards.

Webcam compatible instant messaging programs like MSN and Yahoo Messenger are a significant threat to be used in this crime. Teenagers or children can be victims of certain types of sexual harassment while they are chatting, usually with a webcam. Their accounts may be hacked, and their peers may be deceived by criminals into providing photos or other kinds of sexual acts through webcams. Such photos and activities can be recorded, modified, or shared among networks. They may also be used

---

189 A newsgroup is the same as a forum, an on-line discussion group. On the Internet, there are thousands of newsgroups covering every conceivable interest. A news reader program is necessary to connect users to a news server and to view and post messages to a newsgroup.
190 A bulletin board is an electronic message center. Most bulletin boards serve specific interest groups. Users can review messages left by others, and leave messages.
191 Wortley and Smallbone, ibid.
192 Ibid.
as blackmail.

Pornographers use email methods, but do not directly post or attach such records to their messages. Instead they use email for communication or information exchange to share their interests. Sometimes they can use this method as a means of blackmailing the victim. Most of the time, they use pseudonyms and may use public computers to avoid police detection.

Bulletin Board Systems (BBS) are used for posting information or hyperlinks to child pornography access resources. Detecting such postings in these bulletin boards can be problematic and impossible for system administrators. Closed and password-protected chat rooms and peer-to-peer (P2P) networks are the digital platforms on the Internet where perpetrators share pornography and find victims.\(^{193}\)

The recent challenge for law enforcement agencies are e-groups and Internet search engines. The danger is that the amount of password protected content is increasingly common in these groups since access to such content is only possible when a person shares new content with the group.\(^{194}\)

Internet newsgroups are a common method that perpetrators in this crime utilize for distribution. There are some famous newsgroups that both users and officials know, and authorities sometimes take measures against these groups. However, computer-savvy perpetrators can use these groups without leaving their identity or IP number.\(^{195}\)

In addition to the tools mentioned above, pornographers are starting to utilize new Internet phenomena such as social media. A recent article stresses that social media is one of the most critical methods utilized in this crime along with file sharing programs.

\(^{193}\) Ibid, 10-11.
\(^{194}\) "Çocuk Pornosuna Karşı Nasıl Savaşı Verirsiniz?", ibid.
\(^{195}\) Wortley and Smallbone, ibid.
and e-groups for children. The article cites FBI data showing that child-victims are lured by perpetrators assuming the identities of celebrities. Perpetrators also bribe child-victims with money, toys, movie tickets, or other enticements.196

Edwards specifies seven unique challenges that complicate child pornography investigations for law enforcement: the global structure of the Internet, uncertainty of its political borders, lack of regulation, legal differences, expertise of offenders, sophistication and constant change in Internet technology, and the scale, size, volume of the Internet and Internet activities.197

Wortley and Smallbone have some advice for the police departments on which to concentrate.198 First of all is the importance of technical knowledge and experience. Since the Internet is very much a technical field, law enforcement personnel dealing with these kinds of crimes should be well educated and trained about the tricks of the crime. Beyond these efforts, police agencies should have good contacts and cooperation with other related agencies, especially with internet service providers. They also advise that police units should prioritize their activities considering the size and dimensions of the crime. For example, one area of concentration of police efforts might be known sex offenders and their involvement in child pornography.199

In the view of the literature review above, the following chapter explains how research questions are formalized, how they are operationalized for analytical purposes, and how they are measured. As well as definitions of some terms used in this study, the following chapter also covers explanations of how specific circumvention tools are selected, how blocked websites are selected for testing, and significance of the country

196 "Çocuk Pornosuna Karşı Nasıl Savaş Verirsiniz?", ibid.
197 Edwards, ibid.
198 Wortley and Smallbone, ibid.
199 Ibid, 35-36.
for this research.
CHAPTER III
RESEARCH DESIGN

The effectiveness of state control on the Internet has been the subject of a number of previous studies.¹ While examining Internet policies in Singapore, Rodan finds the following questions important to explore:

"First, can access to the Internet be effectively controlled, or will it have the sort of snowballing political effects predicted by some? Second, to what extent is control of the Internet a technical question alone and how important are social and political structures in shaping the Internet's impact? Do the particular characteristics of authoritarianism in Singapore render it more capable than most authoritarian regimes of restricting the Internet's liberalizing potential? Third, has the Internet's potential political significance been over-estimated? Does a plurality of individual political and social views on Internet necessarily translate into organized political and social action?²"

Wu also asks similar questions: "Is it possible for nation-states to regulate the Internet? Assuming that it is possible; will nation-states regulate the Internet? …to what extent will states choose to regulate cyberspace?"³ While discussing the role of the Internet on economic growth in China, Tan et al asks: "How can the government use the Internet to promote economic growth while maintaining its political and economic control?"⁴

It is not unusual for scholars, however, to exclude an uncertain area that is vulnerable to new questions while explaining their positive or negative arguments in this

---

³ Wu, ibid.
debate. For instance, Denning indicates that "Chinese authorities block access to websites that are considered subversive to government objectives. This has been only partially effective, however, and Chinese activists have found ways of slipping information past the controls."\textsuperscript{5} The amount or size of the term "partly" is not very clear here though.

Likewise, Goldsmith and Wu explain their position by excluding the same point as "our discussion of the techniques of government control over the Internet is not meant to suggest that the techniques always work perfectly. They do not. Nor do we mean to suggest that government control over Internet activities will always be as successful as when these activities take place outside the Internet. They will not."\textsuperscript{6} While discussing legal dilemmas on the Internet, White articulates that "it is more difficult, if not impossible, to trace the source of some material for the purpose of regulation."\textsuperscript{7}

This study focuses on this uncertain area. To what extent is the Internet outside of state control? To what extent are there leaks or failures in state polices? To what extent is the lack state of control over the Internet reasonable or acceptable for states? How effective are these controlling and regulating mechanisms? Do the aspects that states have difficulty controlling pose a threat for states? To what extent is this gap different from those caused by previous media and communication tools?

RESEARCH QUESTION FORMALIZATION

Questions in this debate can be formalized as threat/complications emphasis questions like: Is the Internet a threat to national governments? What kinds of

\textsuperscript{6} Goldsmith and Wu, ibid.
complications might it lead to, and how will these challenges affect nation-states? There are also authority emphasis questions like: How does the Internet affect authority? Will it empower or weaken authority? There are control emphasis questions like: To what extent is the Internet outside of state control? To what extent is the lack of control over the Internet reasonable or acceptable for states? There are also policy/law/law enforcement emphasis questions like: How is law applicable in the online world? To what extent and which of nation-states' policies and laws to control and regulate the Internet are effective?

RESEARCH QUESTIONS AND MEASUREMENT

For analytical purposes, the study prefers to focus on the “policy, law and law enforcement” emphasis question, particularly the last group phrased above. Thus, the main question of this study is how much policing and law enforcement is effective to prevent and prosecute crimes committed on/through the Internet?

Prevention and prosecution are the two essential functions of any state authority. For any type of criminality, prevention is the priority for authorities. When they fail to prevent crime, the second state power tool, prosecution, applies. Thus, any inquiry questioning authority on the Internet should consider these two dimensions—the effectiveness of prevention through blocking measures and the effectiveness of prosecution when prevention fails.

Likewise, policing has two main purposes and aspects: i) prevention (to prevent crimes from being committed), and ii) investigation (to identify perpetrators, to collect evidence, and to transfer criminals to judicial authorities).

In terms of prevention, this study analyzes access blocking efforts and policies on
the Internet in Türkiye. Although internet access blocking can sometimes also be applied as a result of a prosecution (punishment), it is widely used as a preventive measure in the country.

In terms of prosecution, this study explores how the Turkish police are effective in identifying, tracing and ensuring the prosecution of a cybercrime. For the previous prevention aspect, this study selected websites which have contents like ideology, political, pornography, gambling and blocked for some legal reasons. In connection with these tested websites, internet child pornography is the only crime content which there is a wide range of international consensus on. There are significant political and legal approach differences among states for the other crime subject materials mentioned above. Internet child pornography is also one of the first crimes that make each country to consider internet filtering for prevention as well as accept it as a crime to be penalized.

Since the internet is a global network of networks and is transnational due to its structure, it is important to make analysis to an extent of covering this transnational dimension. At this point a national unit of Interpol Ankara becomes an ideal unit to conduct this research in. Moreover, file classification on this unit does not have a unique specific code that covers all kinds of cybercrimes. Rather each crime committed on/through the internet are given code as the same given to offline crime, like both fraud and online fraud cases are given FKA. One exception of a cybercrime is internet child pornography which is specifically given the code as KCC. For analytical reasons, thus, evaluation of the second research question can be performed based on these specific KCC files.
Effectiveness of Internet Blocking (Prevention)

One of the essential methods of preventive measures on the Internet is the blocking technique. Many countries in the world legalize some degree of blocking for different reasons. Although its use has spread, the effectiveness of this measure is questionable. In this part, this question is being explored.

Research Question 1: To what extent do blocking measures on the Internet effectively prevent access to undesired websites and web content?

Measurement discussions in literature

Internet blocking can target either the producers or the consumers but this study is concerned with consumers and Internet users. Callanan et al. laid out perfectly certain parameters to evaluate the effectiveness of blocking measures and stressed some important points. "It is not possible to express effectiveness as the amount of content that is blocked correctly in comparison to the total amount of available illegal content since the total volume of available illegal content is unknown...Since it is often unclear where hits on a website come from, figures quoting volume of hits on an existing list are a very crude indicator at best."8

Excluding limitations noted above, Callanan et al. specified the following levels of analysis to approach the question of effectiveness of blocking measures. This study makes its evaluations based on these following factors: 1) "Analysis of over-blocking and under-blocking potential can be used as indicator of the effectiveness of Internet blocking technologies." 2) "Another indicator for effectiveness is the ease of circumvention of a

---

block. If it is easy to circumvent or disable a block, the availability of the blocked material is likely to remain unaffected." 3) “The availability of alternative methods of access to the same content, by whatever means, can be seen as a measure for effectiveness of blocking in the absence of precise data. 4) The availability of other enforcement options that offer other more effective methods of preventing access to the material can also be assessed - especially if they are less costly, less intrusive or more effective towards the availability of the material.”

This study analyzes the effectiveness of blocking based on the first three criteria. The fourth criterion is a preference of the administrative authority, which needs to be evaluated based on a broad analysis of price, capacity, speed, complication, and other technological variables. Since this criterion is not of direct interest in this study, it was considered for further analysis. The remaining three criteria and how they are measured in this study include the first criteria quoted in Callanan et al., analysis of over-blocking and under-blocking potential can be used as an indicator of the effectiveness of Internet blocking technologies.

Measurement developed in this study based on above criteria

This part is measured under the title of “Analysis of over-blocking and under-blocking.” Qualitatively this section explores empirical evidence of such complications (over-blocking and under-blocking) from independent resources. YouTube, which was the subject of blocking in the country for about two and a half years, is the focus here as a case study.

---

9 Ibid.
10 Ibid.
The second and third criteria quoted in Callanan et al are: 2) the ease of circumvention of a block. If it is easy to circumvent or disable a block, the availability of the blocked material is likely to remain unaffected. 3) The availability of alternative methods of access to the same content, by whatever means, can be seen as a measure for effectiveness of blocking in the absence of precise data.11

Measurement developed in this study based on above criteria

This two criteria “b and c” are combined here as “Ease of circumvention of a block and the availability of alternative methods of access to the blocked websites.” For measuring this part, the study utilizes a previous study’s tools, particularly by Roberts et al.’s 2009 study for the Berkman Center at Harvard University.12 They have tested the effectiveness of some types of web-based circumvention tools. Taking examples of circumvention tools for each method, this study checks whether circumvention tools are effectively retrieving a sample of the blocking websites in Türkiye. How easy is it to circumvent websites that are blocked in the country? This section further analyzes and focuses on a specific issue area, terrorism and blocked terror websites, including circumvention tendencies in the country and legal dilemmas.

Prosecution of Internet child pornography

Child pornography is the main undesired content on the Internet that filters target. However, despite all preventive policies and blocking measures against child pornography, it is still one of the primary problems on the Internet. While the previous

11 Ibid
research question inquires about the effectiveness of Internet blocking, this part questions how effective policing is when such blocking systems fail.

Research Question 2: How effective are the police in identifying, tracing and bringing criminals involved in child pornography before judicial authorities?

Measurement

The Internet is a global medium, and most of the complications of the Internet stream from its transnational structure. "Cybercrime is very much a transnational crime," and so is child pornography.13 A study exploring the challenges of investigations about child pornography should see the subject from international and transnational perspectives. This study analyzed the issue based on digital files from Interpol Ankara. INTERPOL is the acronym of the International Police Organization, headquartered in Lyon, France. The organization has 190 member states. Staffed by member states’ law enforcement personnel, each country has an Interpol National Bureau (National Central Bureau, called as NCB) within their homeland. The study conducted searches for the years of 2005, 2006, and 2007. Looking at each of these cases, this study checked how police investigations either in Türkiye, or investigations abroad are successfully concluded. How successful are investigations in identifying, tracing, and bringing suspects before judicial authorities? Considering the fact that investigations take time, and considering that this part of the study was conducted in June 2011, the files opened in 2005, 2006, and 2007 were selected. The situation is not promising, as will be described in the coming sections.

METHODOLOGY

Measuring effectiveness of Internet blocking

Research Question 1: To what extent have blocking measures on the Internet effectively prevented access to undesired websites and web content?

Hal Roberts, Ethan Zuckerman, and John Palfrey from the Berkman Center for Internet & Society at Harvard University tested how effective some circumvention tools are for some countries.14 They analyzed nine web-based proxy servers that use five different methods: HTTP proxy, CGI proxy, IP tunneling, re-routing, and distributed hosting. Despite some performance problems and security concerns, the study by the Berkman Center stresses that: “all of the circumvention and anonymity tools included in this study succeeded at the basic task of retrieving blocked content in a filtering country.”15

In a lab environment, Roberts et al. evaluated above mentioned circumvention tools based on six criteria: 1) “Utility (Does it retrieve filtered websites? How fast is it compared to unmediated browsing? How well does/will performance scale?) 2) Usability (How easy it for novice users to learn? How easy is it to use?) 3) Security (How well does the tool protect the user from surveillance at various points in the network?) 4) Promotion and marketing of the tool (How well is knowledge of the tool pushed out to users in filtered countries?) 5) Fiscal sustainability of the project (To what degree is the project on a path toward fiscal self sustainability?) 6) Openness (Is the code open source? Are the developers approachable and forthright about their techniques and future

14 Roberts et al., ibid.
15 Ibid.

Selection of circumvention tools

Taking these circumvention tools from this list, this study proposes to test how these tools are working in Türkiye to bypass blocking measures. It is important to check if these tools are significant for Türkiye. Thus, I checked all of these tools (websites) at alexa.com and looked for their popularity in Türkiye. Checks reveal that only the third place web tool, Ultrareach, and the seventh place web tool, Tor, have some degree of popularity in Türkiye. Thus I selected Ultrareach and Tor for additional analysis. While Ultrareach is an HTTP proxy (http://ultrasurf.us/), Tor is a re-routing proxy (https://www.torproject.org/).

In order to select one example for the other types of proxy servers (CGI proxy and IP tunneling), I check the top list of global proxy websites and establish how popular these proxies are in Türkiye. This check reveals that among the five global proxies,

---

16 Ibid.
17 Türkiye is the fifth most popular country for Ultrareach software. Ultrasurf ranked 39,012, and Türkiye is the seventeenth most popular country for Tor, ranked 11,181. "Alexa Actionable Analytics for the Web," Alexa Internet, Inc., Alexa.com.
Turkish users make use of three of the following. Ktunnel is a Turkish CGI proxy. Turkish visitors make up the majority of visitors to the site, ranking at 88.4% of total visitors. Anonymouse is a free anonymous surfing, email, and Usenet posting site. 3.4% of visitors came from Türkiye, coming in at eighth place among visitor source countries. Vtunnel is a web proxy supporting SSL via the HTTPS encryption protocol. Türkiye provided a plurality of visitors, 21.6%. Because of its popularity in Türkiye, both in terms of country ranking and percentage of visitors, I chose Ktunnel as a CGI proxy. The three circumvention tools selected in this study are: Ultrarech, Ktunnel, and Tor Project.

Selection of blocked websites

In order to test how circumvention tools are working, the following blocked websites have been selected from an independent website that monitors blocked websites in Türkiye. According to engelliweb.com, which monitors Internet blockings within Türkiye, 15,596 websites are blocked for different reasons as of 2 March 2012. Among them, 12,772 websites are reported by the administrative authority called Telekomünikasyon İletişim Başkanlığı (TIB). 2,326 are by judicial authorities. Among them, 26 websites are hosted by WordPress, 48 are hosted by Blogger or Blogspot, and 47 are IP addresses. The result of testing and its analysis are further explored in the following section.

Measuring effectiveness of prosecution

Research Question 2: How effective are police in identifying, tracing, and

---

18 Usenet is a worldwide bulletin board system that can be accessed through the Internet or through many online services. The USENET contains more than 14,000 newsgroups (see definition in Chapter II). It is used daily by millions of people around the world.
bringing criminals involved Internet child pornography before judicial authorities?

The following measures are offered by Wortley and Smallbone to measure the degree of success for law enforcement agencies while they are policing child pornography:20 "The followings are potentially useful measures of the effectiveness of responses to Internet child pornography: 1) reduced number of complaints from the public about Internet child pornography. Initially, you might want to see an increase in complaints from the public if you have reason to believe the problem is underreported; 2) reduced number of child pornography sites and images on the Internet; 3) reduced number of new child pornography images on the Internet; 4) reduced level of severity of the child pornography images on the Internet; 5) reduced number of images possessed by offenders who are arrested for downloading child pornography; 6) reduced level of severity of the images possessed by offenders who are arrested for downloading child pornography; and 7) reduced level of involvement (possession, distribution, or production) of the offenders arrested for Internet child pornography crime.

Other measures are important for tracking official actions taken to address the problem. Among them are: 1) the number of offenders arrested for Internet child pornography crimes; and 2) the number of victims portrayed in Internet child pornography who are identified and assisted."21

Since this study concerns more on the investigation side of the issue rather than complaints, images, or websites, for analytical purposes, the measurement of effectiveness focuses on the offender side. Thus, effectiveness in this section is measured as the success of investigations to identify, trace, or arrest the offenders involved in

---


21 Ibid., 32-33.
reported cases. Looking at both incoming and outgoing requests to Interpol Ankara will
give a good insight to evaluate this effectiveness in such a transnational crime.

INTERPOL plays an important role to ensure cooperation among police
organizations of all countries in the world. With its 190 member states, the organization
and the INTERPOL network of National Central Bureaus (NCBs) help to communicate
directly with each other, to share information about any transnational crime, and to
submit requests for investigation from each other.

This part of the study was conducted in The National Central Bureau of Interpol
Ankara (NCB Ankara) for one week between 27 June 2011 and 1 July 2011 with official
permission dated 21 June 2011. Because of legal concerns and time limitations, I selected
files from the years 2005, 2006 and 2007. A four to six-year time period is appropriate to
anticipate that a regular police investigation will be concluded. Thus, analysis and
evaluations are not conducted based on new cases that may be ongoing, but rather on
cases considered to be concluded.

How does the NCB of Interpol Ankara work?

This department operates under the General Directorate of National Police in
Ankara. The department has about 100 personnel, and its working languages are English
and French. It coordinates policing and legal cooperation between national departments
with their foreign counterparts. It receives requests from national police, judicial units,
and other official departments and directs appropriate inquiries to related country’s NCB.
It also receives requests from foreign Interpol departments (NCBs) to convey them to
related national units.

Any criminal or legal issue, either a request from national bodies or from outside
the country, results in a new file being opened in the department. Depending on the types of crimes, these files are assigned reference codes for easy archiving. FKA is the code for forgery cases. GPE is the code for human smuggling. ST is for drug smuggling. The code KCC is for cases involving child sexual abuse and child pornography. Among the six different sections at the Interpol department in Ankara, the Public Safety and Order Section handles KCC-labeled crime.

File selection and digital archive

Looking at the years 2005, 2006 and 2007, this study checks the new files opened as KCC. These checks and analyses are conducted in the digital archive but not in regular files. Paper-based files of the same digital file would be complementary and would show other small details of the cases. However, the digital archive includes all the significant writings and processes of a case saved and accessible in a closed internal network within the department. Only insignificant documentation about a case is excluded from the digital file. It is kept instead in a paper-based physical file. Examples of such documents are forms requesting the status of an investigation, requests to speed up an investigation, or a negative result from one of the units that conducted the investigation. In some cases there is action required for these types of documents. In other cases, it may not be helpful to convey these types of requests to related national or foreign units. Thus, significant information and data conducted in any case is included in the digital files, and no relevant information is excluded.

Analysis of files

For each year, there are digital files named 2005, 2006, and 2007 in the digital
archive. Cases opened in each year were given a case number with corresponding crime code such as KCC-356 or KCC-278 and saved as a MS Word documents within the corresponding year file in the digital archive. Thus, the total number of MS Word documents in a year file represents the total number of cases subject to investigation by Interpol investigators.

Checks conducted of the digital archive files for the years 2005, 2006, and 2007 reveal that there are respectively 35, 35 and 85 new cases subject to investigations by NCB Ankara. These numbers do not reflect the total documents received by the Bureau each year. The real number of documents pertaining to the same crime may be higher. However, this study only concerns the operational side of police investigation of the crime. Thus, the informative and secondary documents held in paper-based files have little or no value for this analysis.

Interpol investigations can be essentially divided into two main groups, Requests of National units from Foreign Interpol Bureaus (outgoing requests) and Requests of Foreign Interpol Bureaus from national units (incoming requests)

After this classification as outgoing requests and incoming requests, all cases are opened for content analysis. Each case has been checked based on the following questions and aspects: From where did the request come? What was the request? To where was it conveyed? When police investigations are successful in identifying criminals, are possible perpetrators brought before judicial authorities? What are possible difficulties and barriers during these police investigations and proceedings?

WHY THE REPUBLIC OF TÜRKİYE?

While examining the geopolitics of blocking trends in 2009, Deibert stresses that
although Internet filtering policies are very common around the globe, information about each state's experience from these policies is limited.\footnote{Ronald J. Deibert, The Geopolitics of Internet Control: Censorship, Sovereignty and Cyberspace, Routledge Handbook of Internet Politics. Edited by Andrew Chadwick and Philip N. Howard (London: Routledge, 2009).} There are not many reliable resources available on this complex issue, and the number of empirical studies is quite limited. Transparency and accountability for these policies are very low for most of the countries.

Each state has unique characteristics, with different cultural, historical, and political heritages and traditions. Studying how Turkish authorities manage to control and regulate the Internet, particularly its blocking experience, collection of important cases, and empirical evidence from the country, will be helpful to enrich the literature in this field.

Being a democratic, secular and developing country, Türkiye has a rich culture and history. It is situated in a very strategic place between Europe to the West, Russia to the North, and in the Arabian Peninsula to the Southeast. Many call the country the bridge between Europe and Asia. It has a growing economy, ranked 17th in the world as measured in nominal GDP, according to the World Bank. It is the second most populated country in Europe with a population around 72 million. It has relatively a young population compared to other European countries. Türkiye's diverse social, political, and economic characteristics create a rich profile that potentially reflects interesting evidence about experiences and patterns of the effects of the Internet.

Political debates about the Internet discuss widely the blocking policies of different states. Türkiye's internet access blocking policy and its implications present different patterns and empirical evidence worth bringing to the literature. Türkiye's practices is interesting to explore since it is not as strict as in China, Iran, or Saudi
Arabia, nor does it resemble more liberal Internet policies like those in Western Europe. According to an international non-profit organization, Reporters Without Borders, which monitors freedom of the press and the Internet, Türkiye is not among the countries that are “enemies of the Internet.” However, the organization included Türkiye among the “countries under surveillance.”

In fact, Turkish authorities did not have many options to consider against undesired websites and web content that violate national laws. Authorities either close their eyes to these illegalities and other negative effects or they enforce the law, including Internet access blocking, despite some of the complications discussed in this study.

Engelliweb.com, which monitors Internet blocking in Türkiye, reported that access to 7,221 websites was blocked for different reasons on 29 August 2010. On 04 March 2011, about six months later, and the check revealed that 9,151 sites were being restricted. As of 13 June, 2014, total number of blocked websites found by the same resource reached to 48,412.

Internet access blocking in Türkiye can be done based on Law No. 5651 regarding “Regulation of Publications on the Internet and the Struggle against Crimes Committed on the Internet” or based on related sections of other laws. Among those which are restricted based on law no. 5651, the biggest percentage of blocking, 96.3 %, is done for obscenity, pornography, and child sexual abuse. The remaining websites are blocked for hate speech, gambling, and other health related reasons like encouraging suicide, or the use of narcotics.

---

24 "Engelli Web.", ibid.
25 Ibid.
26 The law came into effect on 23 November 2007.
Blocking policies in Türkiye are also open to public denunciation by the Turkish administrative authority TIB. The TIB can directly restrict access to the website once they find allegations that apparently violate related law. Decisions to block access to any website can be handed down by the TIB and by judicial authorities, either by prosecutors or by courts.

Implementation of Internet blocking, however, has raised public questions about the effectiveness of these measures since access may still be possible despite being blocked. For instance, YouTube is restricted based on different court verdicts and was closed for a long time. However, during the time that the websites was being blocked, alexa.com reports showed that the website was one of the most popular within Türkiye.

Access to these websites, blocked for obscenity, social networking, or gambling, may be a secondary concern, but this gap also seems to be open for websites encouraging terrorism and violence. Türkiye has been suffering from terrorism by the Marxist-Leninist terrorist organization PKK since the beginning of the 1980s. Türkiye’s struggle against this terrorist organization faced a different challenge when a TV channel, ROJ TV, propagandizing PKK, started to broadcast from Denmark. Authorities were used to taking measures against such publications or broadcasting within national borders, but this transnational broadcasting to the potential audience within the country created a new challenge for Turkish authorities. Türkiye urged Danish authorities to close ROJ TV, but the country faced legal and political barriers in Danish national legislation. Later the television channel moved its center to other European states and changed the satellite it

---

28 Turkish acronym of Telekomünikasyon İletişim Başkanlığı, the Turkish telecommunications headquarters.
29 YouTube was the sixth most popular website in Türkiye as of 21 March 2010, although the website was blocked based on the decision by 1st Peace Criminal Court in Ankara since 5 May 2008. "Alexa Actionable Analytics for the Web.", ibid.
was broadcasting from. It was a significant subject of legal and political dispute between Danish authorities and Türkiye for a long time.\(^{30}\)

Through the Internet and its multimedia features, such kinds of broadcasting have become more complicated for Turkish authorities. The Internet has increased the number of websites acting as the voices of the terrorist organization PKK. In the case of ROJ TV, Türkiye needed to convince one or two states to close off this television broadcasting. But because of the Internet, Turkish authorities need to talk—and negotiate—with a number of states with different legal, political and economic regimes to stop these websites from using servers in their country.

Authorities are also taking measures to prevent domestic access to these websites. However, these websites still receive a significant number of domestic visitors despite being blocked domestically by authorities. There are a number of alternative ways people circumvent Internet blocking. People can use proxy websites, online anonymous services for circumvention. They can also change their modem or computer settings for the same purpose.

It is worth noting here that information and websites that provide circumvention techniques are also open access, and so far, authorities have not taken any measures against these kinds of websites. People can easily find these circumvention techniques on the Internet. For instance, ktunnel.com, a proxy website that circumvents Internet blocking, is the 60th most popular website in Türkiye according to alexa.com.\(^{31}\) This shows that people in Türkiye are using these kinds of tools and services available on the Internet to access blocked websites.

\(^{30}\) "ROJ TV Davasında Sona Doğru," Sabah, 7 December 2011.

\(^{31}\) The popularity ranking of the website within the country was 3330 on 12 February 2014. "Alexa Actionable Analytics for the Web.", ibid.
In addition to these blocking dilemmas and problems, law enforcement agencies face different challenges while investigating criminal issues committed on or through the Internet, as seen in police investigations against child pornography. This crime is one of the primary reasons authorities consider Internet blocking. It is such a sensitive issue that almost in every country, it is admitted as a serious crime. So it is in Türkiye. Authorities take this crime very seriously and utilize all technical and scientific capabilities to investigate, identify and prosecute such crime allegations.

This study has a chance to explore digital files of investigation requests of Interpol Ankara. These investigation requests have two sides. It can be investigation requests of foreign Interpol Bureaus from Interpol Ankara (incoming requests) or it can be investigation requests of Interpol Ankara from other Interpol Bureaus (outgoing requests). Looking at investigations for three years, 2005, 2006, and 2007, this study checked how many cases either outside the country or inside the country successfully identified criminals involved in this crime and handed over to judicial authorities.

DEFINITIONS

Definitions and terminology matter in any study, especially when it is academic. It is important to specify what this study means when talking about certain terms, like the Internet, Internet blocking, effectiveness, and Internet child pornography.

The Internet: In their study DiMaggio et al. define the Internet as "the electronic network of networks that links people and information through computers and other digital devices allowing person-to-person communication and information retrieval."\(^{32}\)

---

The Internet is both a communication and a mass medium. Previously, media and communication disciplines used to be studied and taught separately. Now the Internet has unified these disciplines. Although there are some similarities with older media and communication devices such as telephones, fax, television, and radio, the Internet has many distinct characteristics. White indicates that:

"The Internet is not a tangible device, no one entity manufactures or produces it and it is not allowed or controlled by any government or corporation...The computers which form the Internet are connected by many different methods...fiber optic cables, twisted pair copper wire, wireless signals ... The information travelling on these networks is translated by a computer into a universal protocol called TCP/IP, which uses a common name and enables other computers to find and understand the information.... It is these protocols that really define the network. The machines that talk to one another using IP and their connections are the Internet."33

Hick and McNutt describe the Internet as "a global pool of information and services, accessible locally through individual computer stations, each of which is part of global system of interconnected computer networks."34 Callanan et al. say: "The Internet is a vast complex network of networks with a myriad of hardware systems, protocols and services implemented."35 While studying the effects of the Internet in social movements, Huang specifies the use of Internet technology as the use of "the World Wide Web, websites/websites, email, real time chat, blogs, VoIP, and discussion forums."36

The Internet is a global network of networks that enables users from all over the world to interact and connect through the Internet applications, devices, and tools of communication technology. Internet applications implies the use of World Wide Web

33 White, ibid.
35 Callanan et al., ibid.
(Web 2.0), blogging, social networking sites, any kind of forums, messengers, instant chat, email, VoIP, multimedia, peer to peer (P2P) networking, and Usenet Newsgroups. Devices and tools of communication technology include all kinds of equipment necessary for Internet infrastructure and connection to the Internet, such as computers, modems, wireless capabilities, cables, mobile phones, and the like.

Blocking policies can target Internet applications such as websites/webpages, email, Usenet, search, and peer to peer (P2), as Callanan et al. analyzed in their study.\(^{37}\) For analytical purposes, this study specifically focuses on one of the important applications of the Internet, websites, while examining blocking measures. Callanan et al. also stress, "Websites are one of the foremost distribution methods of all types of content on the Internet."\(^{38}\) Moreover "many filtering products are based on lists of Websites that are supplied by their vendor[s]."\(^{39}\)

Blocking on the Internet: Blocking covers "a broad range of policies, hardware, software, and services, and it would be a mistake to think that all types of Internet blocking are the same or equally effective, legally equivalent, or even that one system can easily be used in relation to more than one type of content."\(^{40}\) In this study, blocking essentially refers to authorities' technical measures to prevent access to undesired websites and web content. This study is not a lab analysis of blocking techniques or circumvention methods. It uses the words "blocking" and "filtering" interchangeably, as seen in the literature.

Effectiveness: In order to talk about effectiveness in a positive or negative sense,

\(^{37}\) Callanan et al., ibid.

\(^{38}\) Ibid.


\(^{40}\) Callanan et al., ibid.
there should be an accurate and reliable measure. While this term basically refers to the level of success, how it is measured is explained for each research question based on criteria from the literature.

The next chapter gives information about brief political history of the country, and some background about media and communication sector. This chapter also includes historical information about how the internet was first introduced to the country and how it has been governed by related institutions.
CHAPTER IV
BRIEF ABOUT TÜRKİYE

Following the First World War, the six century old Ottoman Empire broke apart. Founded in 1923, the Republic of Türkiye chose many political, legal, and economic models from Western states to form a new governmental and institutional structure. Türkiye kept itself away from involvement in the Second World War and gave priority to industrialization and developing its economy. Becoming a NATO member in 1952, Türkiye was one of the frontlines of the Alliance and played a strategic role during the Cold War. Geographically, Türkiye is in an important region in the Middle East, Caucasus, Black Sea, Europe, and the Mediterranean. It has a population of about 76 million,\(^1\) which makes the country the second most populous nation in Europe and among the most populous in the Middle East. Türkiye is the only pluralist secular democracy in the Muslim world.

The European Union (EU) has become one of the successful civilization projects in the last century. From the very beginning, Türkiye wanted to be a part of this project. The relationship between Türkiye and the EU goes back to 1963 when the Association Agreement signed in Ankara between the two parties (at that time the Union was called as the EEC). Since then, it has undertaken extensive political and economic reforms and has become a part of European institutions, such as the Organization for Security and Cooperation in Europe (OSCE), the European Court of Human Rights, and the Council of Europe Parliamentary Assembly (PACE). Türkiye applied for full membership to the EU

\(^1\) As of 31 December 2012, the population is 75,627,384. Turkish Statistical Institute, "Adrese Dayali Nüfus Kayıt Sistemi Sonuçları, 2012," www.tuik.gov.tr/PreHaberBultenleri.do?id=13425.
in 1987, and was recognized as a candidate state during the EU Helsinki Summit in 1999. After a long and hard discussion at the Copenhagen Summit in 2004, the European Council finally specified a date for accession talks with Türkiye to be held in 2004 but without guarantee of a full membership.

Irrespective of whether full membership is ever granted, Türkiye is advancing its democratic standards, promoting human rights standards, and improving its economic development. The end of Cold War has opened up a wide hinterland for the country to expand economic relations and diversify its foreign policy in its region. Both for Turkish people and for politicians, the popularity and credibility of the European Union seems to be decreasing. Thus, any response in the future will not be surprising for the country, as it might have been one or two decades ago.

Liberal policies in the country were intensified in the beginning of 1980s. Free and competitive market principles were intensified in economic policies during this time, and the state’s role and involvement in the economy began to be minimized afterward. Privatization of many of the State Economic Enterprises (abbreviated KIT in Turkish), liberalization of the circulation of foreign currency within the market, and ensuring convertibility of the Turkish Lira in the international market are some of the important policies of this term. Although the country has not become a full member of the EU, the country signed the Customs Union agreement with the European Union, which came into force at the beginning of 1996. This liberalization movement is not only seen in economy. The country has made significant transformations in a variety of legal and political areas. The death penalty has been abolished and individual applications to the European Human Rights Court have been accepted under certain conditions.
Both the media and communication sectors have been very much affected by these liberalization policies. As seen in most of issue areas, technology was very much ahead of the law. Although there is no legal framework for broadcasting private TV and radio channels, a number of private TV and radio channels have emerged and undermined the monopoly of the state-run, official voice of Turkish Radio and Television (abbreviated TRT in Turkish). It was up until 1993 that private TV and radio broadcasting have been regulated based on an amendment to the constitution. Since then, private TV and radio channels have been very influential on the country’s progress in democracy, civil rights, freedom, and institutionalization. The Turkish Radio and Television High Commission (abbreviated RTUK in Turkish) reports that 249 Territorial Analog Television stations are licensed by the RTUK. Of those, 24 are national, 15 are regional, and 210 are local TV channels. RTUK licenses 1,062 FM radio stations. Of those, 35 are national, 98 are regional, and 929 are local.\footnote{Radio and Television Supreme Council, (Radyo Televizyon Ust Kurulu, RTUK) Annual Report (2009-2010)}

Because of serious political and legal disputes, privatization of the state owned Postal, Telephone and Telegraph (abbreviated PTT in Turkish) progressed slowly and was realized only realized after a number of postponements. For this purpose, telecommunication services have been separated from the postal service, and Turk Telekom A.S. was founded in 1994.\footnote{Hasan Serindag, "Turk Telekomunikasyon Sektorunde Liberalizasyon Ve Regulasyon Kurumlarinin Fonksiyonlari," In 2008 Bilisim Konferansi. Ankara, 2008.} There are 443 licensed companies operating in a free and competitive Turkish telecommunication market. Using three communication satellites, one of which is national GOKTURK, the country allocates a considerable
amount of resources to advance its space and satellite technology.{}

HISTORICAL BACKGROUND OF THE INTERNET IN TÜRKİYE

Having significant growth, progress, and development, the media and communication sectors in Türkiye have entered into a new transformation trend that was essentially shaped and dominated by the Internet. The Internet has changed and diversified previous communication habits and gained a critical place in transforming this balance of the new media order. Increasing popularity, especially among younger generations in the country, has urged authorities and private endeavors to spread Internet services and advance infrastructure throughout the entire state.

The first transnational computer network in Türkiye, called TUVAKA (Turkish Networks of Universities and Research Institutes), was established in 1986. It was a BITNET connection that first connected the University of Ege in Izmir, Türkiye to EARN (European Academic and Research Network) in Italy. More universities from other parts of the country joined the same network later, but technical and operational problems within the network made resulted in it being insufficient to respond to necessary demands at that time.

In 1991, a well-known national research institute in Türkiye, TUBITAK (The Scientific and Technical Research Council of Türkiye) and one of the leading universities

---

4 "Ministry of Transportation (Türkiye Cumhuriyeti Ulaştırma)," www.ubak.gov.tr/.
of the country, METU (Middle East Technical University)\textsuperscript{8} initiated a project called TR-NET. They were able to test connection with the Netherlands in October 1992.\textsuperscript{9} On 12 April 1993, the first Internet connection using the TCP/IP protocol\textsuperscript{10} was made between METU/TUBITAK and the NSFNet (National Science Foundation Network) in the United States through a 64-kbps leased line.\textsuperscript{11}

Since then Internet infrastructure and Internet users in the country have increased noticeably. In 1995, the number of individual Internet connections was about 1,300, and total daily Internet users numbered between 10,000 and 15,000. In 1997, about 30,000 computers were connected to the Internet. This number was 100,000 in the beginning of 2000.\textsuperscript{12} Mestçi notes that Internet users numbered about 293,000 in 1998. That increased to 1.78 million in 2000 and 10 million in 2004.\textsuperscript{13}

The Turkish Statistics Institution (TUIK) began conducting an address-based survey in 2007. A survey conducted that year reveals that 19.7% of Turkish households had Internet access. ADSL was the most used connection type by 78.5%.\textsuperscript{14} In 2009, the percentage of Internet-connected households increased to 30% of the total households. The same year, the total population of the country was 71,517,100 and average family size was around four. From these numbers, officials estimated that there were 18 million households in Türkiye, meaning that approximately 5.4 million households had Internet

---

\textsuperscript{8} In Turkish: Orta Doğu Teknik Üniversitesi (ODTU).
\textsuperscript{9} "Türkiye'de Internet.", ibid.
\textsuperscript{11} Akdenizli, ibid. and "Türkiye'de Internet.", ibid.
\textsuperscript{12} "Turkish Ministry of Education (Milli Eğitim Bakanlığı)," http://www.meb.gov.tr/.
\textsuperscript{14} "Turkish Statistical Institute Database," http://www.turkstat.gov.tr/PreTabloArama.do?metod=search &araType=vt.
access in 2009. In December 2009, Bulent Hicsonmez, Head of Google Türkiye, estimated that Turkish Internet users numbered about 28 million.

In 2010 the percentage of households with Internet access increased to 41.6% of total households—7.48 million homes. That increased to 47.2% in 2012. The rate for cities is 55.5%, and the rate in rural areas is 27.3%.

Besides Internet access from individual homes, public Internet use, such as in Internet cafés, is very common around the country. For example, there are more than 800 internet cafés in Ankara with more than five users per café per day and almost 2000 internet cafés in Istanbul with more than six users per café per day.

The “e-state” project, a government initiative to combine all official departments into one main gateway has encouraged officials to develop their own websites and provide some services on the Internet. The Ministry of Transportation, which is in charge of communication in the country, recently notes that with 40 million Internet users, Türkiye is 12th in the world and 5th in Europe in terms of Internet penetration. While the number of broadband Internet subscribers exceeds 8 million, the number of cable Internet subscribers exceeds 200,000. 3G technology makes mobile Internet access convenient and popular in the country, and mobile subscribers have reached 16.6 million.

comScore, Inc. (the initial “c” is not capitalized), a global Internet traffic ranking and measuring website, reports that in April 2009 Türkiye had the 7th largest online audience among Internet visitors from 17 European states. “Spending an average 32

---

16 "Türkiye'nin İnternet Nüfusu 28 Milyon," Timeturk, 7 December 2009.
17 Güvenli Web, "Internet Abone Sayıları," http://www.guvenliweb.org.tr/istatistikler/content/internette-abone-say%C4%B1lar%C4%B1. Of the 71,517,100 inhabitants, 50.2% are male and 49.8% are female. There are about 18 million households in the country.
18 Ibid.
19 "İstatistik Bilgileri," ibid.
20 All data from "Ministry of Transportation (Türkiye Cumhuriyeti Ulaştırma)," ibid.
hours and viewing an average 3,044 pages of content per month” makes Türkiye the most engaged Internet visitors in Europe and the 5th most engaged in the world. 21

Institutions and the Internet

The Internet urged politicians and bureaucrats to create a unique and special institution and law to regulate the Internet. The Presidency of Telecommunication Communication (Telekomünikasyon İletişim Başkanlığı (TİB)) was founded based on amendment law number 5397, approved by the Turkish Parliament and published in the Official Gazette on 3 July 2005. The TİB is under the direct supervision of the President of the BTK (Bilgi Teknolojileri ve İletişim Kurumu—the Turkish Information and Communications Technologies Authority) both of which operate under Ministry of Transport Maritime Affairs and Communications.

The law on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications, number 5651 published on 23 May 2007, directly assigns the TİB to enforce the related provisions of the law about the Internet. The Internet Department Directorate is founded under the TİB.

The TİB’s duties and responsibilities are stipulated in law number 5651, Article 10, Paragraph 4. These duties are to ensure coordination between the Ministry, Law Enforcement Agencies, related Directorates, and NGOs to prevent illegal activities and publications of content published on the Internet, as described in the law. Like at home, the Presidency (TİB) is to facilitate cooperation and coordination with institutions abroad. Establishing the level, time, and means of monitoring Internet publications, the TİB is obligated to monitor Internet publications and take appropriate access-blocking measures

against any criminality as described in the law. It establishes systems and procedures for registration, filters, and other administrative requirements for commercial public Internet providers.

Law number 5651, article 10, paragraph 5 provides the foundation of the Internet Board, made up of members from the Ministry of Justice, Ministry of Interior, Ministry of State Responsible for Women, Children and Family, from other related Ministries and organizations, and members from Internet Service Providers and NGOs. The law calls for the TIB to ensure cooperation and coordination with this board in designating websites to block and with collecting suggestions, measures, and decisions from similar situations.

After presenting introductory information about internet access blocking, related law, blocking examples and concerns, the following chapter includes analysis of the first research question which is the effectiveness of internet blocking. As a case study, YouTube access blocking was explained here as an example for over-blocking. Utilized some of the tools tested in the literature, this chapter includes testing circumvention tools to access some of blocked websites. This chapter also looks the effects of blocking on blocked websites, focusing on those with violence, ideology or terror contents.
CHAPTER V

INTERNET BLOCKING AND EFFECTIVENESS IN THE REPUBLIC OF TÜRKİYE

INTRODUCTION AND BACKGROUND

Technology develops faster than law.¹ Law making comes after public use of technology. Such is the case with Internet use in Türkiye. During the early years of Internet use in Türkiye, there were no specific laws or regulation. In a short time, legal disputes and cases involving the Internet started coming before judicial authorities. In this period, judges and prosecutors utilized previous laws and regimes to solve these legal problems.²

The first judicial cases can be considered as “the Internet vs. the state.” In these cases, the Internet was the medium where alleged crimes against the existence and solidarity of the state were prosecuted.³ One of the cases in this regard was the case of Emre Ersoz in 1998. Because of his posting to a forum of an Internet Service Provider (ISP), he was sentenced ten months imprisonment for “publicly insulting state security forces” based on Turkish Penal Code 159/1. He defended himself by explaining that the forum is not open to the public but only open to its users. His sentence was postponed on the condition that he not be charged for similar charge in five years.⁴

In 1999, another similar case arose known as the case of Coskun Ak. As the administrator of a forum in an Internet portal belonging to an ISP named Superonline, he

---

⁴ Ibid.
refused to remove an anonymous comment criticizing human rights in the country after a user complained and asked for its removal. Since Coskun Ak refused to take down the comment, the complaining user took the issue to the court. Considering a parallel to the regulations of previous media, the prosecutor claimed that as the administrator of the forum, Coskun Ak’s responsibility was similar to that of an editor of a published newspaper. Ak defended himself on the principle of “nullum crimen nulla poena sine lege – no crime, no punishment without a previous penal law.” Although he was found guilty, the decision was overturned by the Supreme Court. The local court upheld its first decision, but once again it was overturned by the Supreme Court. At the end, Ak was not sentenced, but only because of an amendment in the Turkish Penal Code, Article 159 at that time.5

Akdeniz and Altinparmak notes that some twenty websites, among them yolsuzluklar.org, soygun.com, turkbet.com, pkk.org, cjb.net, cunta.org, superbahis.com, bahismerkezi.com, hizb-ut-tahrir.org, al-ummah.org, akademya.org, ucbucuk.com, akparti.gen.tr, altinrehber.com, otuken.org, soyguncular.com, dindusmanlari.com, aloihbar.org, were blocked between 2001 and 2004.6

With the legal mentality that considers the Internet analogous to previous media forms, new regulations were introduced to the public at the beginning of the 2000s. After long discussions during the law-making process, the first regulation was prepared as amendment number 4676,7 which was first overturned by the president. When it was for a second time admitted by the Turkish Parliament, the president was left one choice to

6 Akdeniz et al., ibid.
ratify and bring it to the Supreme Court. Finally, the Court changed some of its articles and the law number 4656 came into force in 2002.8

In the year 2005, blocking was intensely seen as an effort to protect copyrights. Between 2005 and 2007, based on applications of the Turkish Phonographic Industry Society (MUYAP), access to some 1,500 websites was blocked.9 Blocking for copyright violations even reached well known global websites like myspace.com and bloger.com. These two sites would not be in service in Türkiye for a while. In 2008 alone, 52 websites, including muzikhaber.bloggum.com and mp3evin.com were blocked by the Beyoglu Prosecutor’s Office for violation of copyrights based on above MUYAP’s application.10

During this time, increasing crimes committed through the Internet, especially public sensitivity on child pornography and suicide, mobilized Parliament to make a specific law about the Internet.11 Although two drafts prepared by NGOs and the Ministry of Justice could not come to the Assembly’s agenda for voting, a draft prepared by Ministry of Transportation came to the Assembly and was admitted after voting.12 Law number 5651 on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications, approved by Parliament on 4 May 2007, was published in the Official Gazette number 26030 on 23 May 2007 and came into force on 23 May 2007.13 On 30 November 2007, its ordinance was admitted and came into force.

The law number 5651 provides definitions of Internet actors, such as Internet

---

9 Sanstür Sansür, ibid.
11 Akdeniz et al., ibid.
12 Sansür Sansür, ibid.
Service Provider (ISP), Internet Content Provider, Hosting Provider, and Commercial Internet Public Use Providers in Article 2, as follows:

Access provider: Those operators and real or legal entities providing the Internet public use providers as well their subscribers with the possibility of accessing to the Internet, Content provider: Real or legal entities producing, modifying and providing all kinds of information or data provided to the users on the Internet, Hosting provider: Real or legal entities providing and operating the systems hosting the services and contents on the Internet, Commercial Internet public use providers: Real or legal entities who provide the service as an Internet public use in a certain place for a certain time.

Under the obligation of Information, Article 3, the commercial or economic purpose content providers, hosting providers, and access providers are liable to maintain and update their identity information accurately and make them completely accessible on their own Internet services. Responsibilities and obligations of the content providers, hosting providers, and access providers are further explained in the following articles (4, 5, and 6). Article 4 is called, “Obligations of the content provider.” Clause 1 states, “The content provider shall be responsible for all and any content it provides for use on the Internet.” Clause 2 states, “The content provider shall not be responsible for the contents of another person for whom it provides a link. However, the content provider shall be responsible as per the general provisions if it is explicitly understood from the way of presentation that it adopts the content for which it provides a link and aim that the users access such content.”

Article 5 is called “Obligations of the hosting provider. Clause 1 states, “The hosting provider shall not be obliged to control the content for which it hosts or to investigate whether an unlawful action is realized there or not.” Clause 2 states, “The hosting provider shall be obliged to remove the unlawful content from publication when it is notified based on Article 8 and 9 of this law and to the extent it has the technical
possibility of blocking the access, without prejudice to the provisions related to penal
liability for the content it is hosting.”

Article 6 is titled “Obligations of the access provider.” Clause 1 states, “The
access provider shall be obliged to a) block the access to the unlawful content published
by any of its users provided that it is notified based on provisions in this law and to the
extent it has the technical possibility of blocking the access, b) save the traffic
information of the provided service described in the ordinance, maintain the accuracy,
integrity and privacy of these information for a period in the ordinance, not less than 6
months, not more than two years, c) notify the case to the Authority, content providers
and their customers at least three months before the date when it will stop its operation
and submit to the Authority the records regarding the traffic information based on
provisions and procedures described in the ordinance.” Clause 2 states, “The access
provider shall not be obliged to control whether the content of the information accessed
through it is unlawful or requires responsibility or not.” Clause 3 states, “Any access
provider which violates any obligations in (b) and (c) of this paragraph shall be fined
between ten thousand Turkish Liras up to five thousand Turkish Liras.”

Law number 5651, article 8 specifies that “There shall be a decision on blocking
the access regarding the publication on the Internet the content of which poses substantial
cause for suspicion that they constitute the following crimes:” 1) inducement to suicide,
2) sexual abuse of children, 3) access to narcotics and stimulants, 4) supplying substances
dangerous to health, 5) obscenity, 6) prostitution, 7) supplying place and opportunity for
gambling, and 8) crimes against Ataturk, the founder of the Republic of Türkiye. The
crimes specified in this law are called as catalog crimes by the Turkish administrative
organization, the TIB, and blocking measures can be taken against any website content
that is criminal according to the law.\footnote{Ibid.}

According to the law number 5651, blocking decisions during the investigation stage, can be handed down by judges. During the inquiry stage they can be handed down by the court. In immediate cases with potential undesired results, public prosecutor can also adjudicate a blocking decision. In this situation, the prosecutor should present the decision for the judge’s approval within twenty-four hours. The judges must reach a verdict twenty-four hours after submission. If it is not approved by the judge, blocking removal needs to be requested immediately by the prosecutor. Being a measure, the appeal procedure against the blocking decision is open based on Turkish Penal Code number 5271 dated 4 December 2004.\footnote{Serhat Koç and Selva Kaynak, "Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet Ve Kişisel Güvenlik," In Akademik Bilişim Konferansı 2010. (Muğla, 2010).}

According to a lawyer, Atamer, access blocking is a measure against a site, not a penalty.\footnote{Ilker Atamer, “5651 Sayılı Yasa Ve Erişim Engelleme Kararları,” In 2008 Bilişim Konferansı. (Ankara, 2008).} Access blocking decisions taken based on this law can be taken by judicial institutions like the Prosecutor’s Office or Criminal Courts but at the same time by an administrative institution, the TIB. However, the TIB can directly decide blocking measures only when the alleged crime on the website is one of the crimes specified in the law, and when the website’s hosting servers or content provider are outside the country. When they are inside the country, the TIB can directly decide blocking only for crimes of sexual abuse of children and obscenity. The TIB later asks a judge for approval of the decision. Blocking decisions given based on this law by courts are implemented by the TIB.\footnote{Telekomünikasyon İletişim Başkanlığı, ibid.}

The blocking procedure is also open to public denunciation. People can report
suspicious websites or contents to the TIB. These reports are evaluated based on criteria specified in law number 5651 and other legal frameworks, technical dimensions, the degree of traffic to the website from the country, and ease of access by children. After evaluation, the TIB decide to block the content directly or refer it to the judicial authorities.

The appeal procedure is open against the blocking measure. Completing the judicial and/or administrative procedure, the blocked websites can be reopened for access. Article 8, paragraph 9, of law number 5652 explains the appeal procedure against blocking decisions. Once an appeal is admitted by judicial authorities, the decision for removal of blocking measures is sent to the TIB. Accordingly the TIB conveys the appeal decision to all Internet Service Providers in the country. The appeal application against blocking decisions directly handed down by the TIB can be made to the TIB or to the judicial authorities.

According to Akdeniz and Altinparmak, the essential problem with Internet blockings is not those blocked based on law number 5651 but rather other blocking examples carried out based on other laws. They note that especially these kinds of blocking occur based on Civic Law (individuals’ rights, insulting etc.) and based on laws regarding copyrights. The TIB also provides statistics for blocked websites as seven catalog crimes specified in law number 5651 but not for those blocked based on other laws, which are more controversial.

The number of blocked websites in the country has reached about 31,000, according to independent website engelliweb.com, which monitors blocking measures in

---

18 Ibid.
19 Ibid.
20 Akdeniz et al., ibid.
21 Telekomünikasyon İletişim Başkanlığı, ibid.
Türkiye. Among them, 26,877 websites are blocked by the TIB, 1,730 websites are blocked by the courts and the Prosecutor’s Offices, and 1,274 websites display no information. Further, 158 IP addresses, 69 Wordpress Blogs and 165 Blogger and Blogspot pages are reported as blocked. For 115 websites, blockings are known that were later cancelled. The same source, engelliweb.com was reporting 9,115 blocked websites on 15 March 2011, 39 of which were Blogger or BlogSpot pages, 20 of which were Wordpress pages, and 47 of which were IP addresses. In almost two years, between March 2011 and June 2013, the numbers of blocked websites increased more than three times to some 31,000.

Internet access blocking in the country is generally performed through Türk Telecom which is the biggest ISP in Türkiye, with the method of IP address blocking. Included among these blocked websites, there are globally well known websites like youtube.com, dailymotion.com, ustream.com, blogger.com, blogspot.com, myspace.com, tagged.com, google.groups.com, myspace.com, wordpress.com, blogger.com that host thousands of separate pages, and millions of images, data, and records.

The symbolic figure of the blocking policies in the country is the case against YouTube. The YouTube case contains many empirical parameters to explain the question of the state vs. the Internet. Because of a few specific video records uploaded to the website, YouTube was blocked different times based on different court decisions. Blockings were seen between March 2007 and October 2010, and the longest blocking

---

23 Websites that display no information can be considered blocked by courts. Ibid.
24 Ibid.
26 These websites have been reported in different resources as being subjects of blocking on different dates for different periods.
was between May 2008 and October 2010. The last YouTube blocking was because of hate speech and insults against Ataturk, the founder of the Turkish Republic.

The two parties, representatives from YouTube and from the Ministry tried to resolve the issue. It is against YouTube policy to remove undesired video records. The Turkish side claimed that the issue is a judicial matter, and YouTube itself should appeal the blocking decisions of independent local courts. For some time, both sides maintained their positions, and YouTube was kept blocked during this period.27 If there is any winner in the YouTube case is further explained in the coming section as a case study.

In fact, the law no 5651 also confesses this situation in its texture by excluding the situation of incapability. While specifying one of the three responsibilities of Internet Service Providers in Article 6, the law stipulates: "Shall block access to the contents that is published in any unlawful way by its users, when it is notified in accordance with the provisions of this Act and to the extent that is technically able to block." The Article 5 of the same law indicates that Hosting Providers are responsible to remove unlawful contents as technically as possible when it is notified.

Likewise the Article 10/4.g. regulate the duties of the administrative body, the TIB, and says:

"The Presidency shall provide all kinds of assistance and coordination required within the framework of its technical possibilities to the competent and assigned law enforcement officers and investigation authorities in order to prevent the promotion, entering into the country, maintaining, letting for rent or sale of all and any representative images, texts or sounds with the subject of the crimes provided for in the first paragraph of article 8 of the Law."

These articles are the essential parts of the Law no. 5651 which regulates access blocking and investigation aspects which are also the subjects of this study. What is

technically possible and what is not is a constantly changing matter. Depending on human resources, devices, software or hardware, technical capacity of an access provider or a hosting provider may be different from the others. This exclusion included in the law better makes it change its name as: “Law on the Internet to the extent of technically possible.”

Increasing numbers of blockings on the Internet receive many criticisms both at home and abroad. Analyzing implementation of blocking policies, Akdeniz and Altinparmak believe that because the unique nature of the Internet could not be well perceived by authorities, a number of legal anomalies and dilemmas are being experienced because of blockings. Labeling the situation censorship, Tevetoğlu emphasizes that blocking does not remove undesired content from the Internet, and thus “it looks like an ostrich hiding its head in sand.” The following chapter discusses this essential question in detail.

EFFECTIVENESS AND BLOCKING ON THE INTERNET IN TÜRKİYE

Analysis of over-blocking and under-blocking

The Internet is a global borderless network, and it is unrealistic to consider that all the Internet content is equally acceptable in different parts of the world. That is why Internet access or its content can be subject to restrictions for legal, ethical, cultural, religious, and ideological reasons. These restrictions on the Internet are widely implemented with filtering technology in the world. However, the size, scope, and nature

28 Akdeniz et al., ibid.
29 Koç et al., ibid.
of the Internet create significant challenges for these kinds of preventive restrictions.

These challenges are especially problematic for countries where liberal and democratic values are widely accepted and institutionalized. It is almost inevitable to experience mistakes when this technology is an option for restriction and prevention on the Internet. As Callanan et al. explain, all blocking systems may be either "negative errors" (not all undesired Internet content can be blocked, some undesired Internet content may be outside blocking capabilities), or "positive errors" (some innocuous Internet content may be unintentionally blocked).\footnote{Callanan et al., ibid.}

Callanan et al. tested different blocking techniques for a number of Internet applications including websites, email, search engines, UseNet, and p2p.\footnote{Ibid.} They found that the degree may vary, but these techniques are not free from errors.

Among the seven web blocking techniques, DNS, Domain, URL, IP, Dynamic, Signature, and Hybrid (IP, Signatures/URL), they found four very likely blocking complications for DNS, Domain, IP, and Dynamic blocking techniques. It is less likely that the remaining three blocking techniques overreach.\footnote{Ibid, 20.}

There are no results considered "less likely" that cause under-blocking for any website blocking techniques that Callanan et al. evaluated.\footnote{Ibid.} Thus, the under-blocking complication is almost inevitable (very likely and likely) when the web blocking techniques here are implemented. Over-blocking complications, on the other hand, can be minimized to the degree of less likely only when URL, Signature, and Hybrid (IP, Signatures/URL) Web blocking techniques are implemented. As for circumvention, all Web blocking techniques present medium-level difficulties except one. DNS blocking is

\footnote{\textsuperscript{30} Callanan et al., ibid.} \footnote{\textsuperscript{31} Ibid.} \footnote{\textsuperscript{32} Ibid, 20.} \footnote{\textsuperscript{33} Ibid.}
considered as easy to circumvent.

Akdeniz, a professor at the University of Leeds, Faculty of Law, stated in a TV program that Internet blocking implementation methods cause disproportional results, as seen in the case of YouTube and Geocities. These disproportional results are unacceptable in a democratic country. He stresses that blocking in the country is implemented either at the level of ISPs or at the Internet gateway of the country. The TIB reports that access blocking is implemented on domain name servers (DNS) through domain names or IP addresses (based on submitted “access list” to the routers). Stressing the implementation of IP blocking can be problematic since this blocks all other, possibly innocent domain names using the same IP address. The Director of the TIB stated that the department pays attention to these kinds of risks in their direct blocking decisions, especially when some other domain names are known using the same IP, or when the situation is unknown.

It is very unfortunate that a measure that can cause such serious complications is used at the discretion of an administrative agency, even though conditions are limited. According to Atamer, in their blocking decisions courts should also need to specify how blocking is implemented. Akdeniz and Altiparmak believe that “technical infrastructure for Internet access in the country is not appropriate for blocking or censorship.” They further stress that no other system is perfect. Even expensive methods currently in use for blocking are not free from risks and complications.

Over-blocking has side effects beyond making innocent websites are inaccessible.

34 "Herkes Kendi Güvenliğini Kendi Sağlamah!" NTVMSNBC, 24 June 2008.
33 Telekomünikasyon İletişim Başkanlığı, ibid.
36 The TIB can directly block websites when websites’ servers are outside of the country and when their content is pornographic.
37 Atamer, ibid.
38 Akdeniz et al., ibid, 62.
It also blocks innocent web content and pages hosted within the undesired and blocked website. Many critics in the country emphasize this situation in blocking cases on the Internet. Akdeniz and Altiparmak note that, among the many cases checked, they found blockings are enforced based on only a single file, a single website, a single blog posting, or a 30-second video record, like in the cases of YouTube, Geocities, WordPress, Blogger, and Blogspot. The YouTube case is a wonderful example to explain these kinds of anomalies in practice. Because of a few undesired and/or illegal video records, the entire website hosting millions of records is vulnerable to blocking.

An over-blocking issue: case study of YouTube blocking

YouTube is one of the most popular video sharing websites on the Internet. It hosts millions of videos recorded and uploaded by millions of Internet users. Although the website and video records were initially used for entertainment purposes, today it can be utilized for a variety of reasons ranging from education to health and business to advertisement.

YouTube is also very popular in Türkiye. As of March 2012, it was the third most popular website in the country according to Alexa.com. According to a statistical analysis on 12 March 2007, Türkiye ranks fourth for video uploading at 3.4%, after the United States at 34.5%, the UK at 6.9%, and the Philippines at 3.9%. Looking at the size, capacity, and spread of use, blocking the entire website for one or a few video records was very controversial in the country in that it contradicts the basic principles of universal law and the subjectivity of crime.

39 Akdeniz et al., ibid, 62.
The YouTube ban became the symbol of blocking policies. Many public arguments centered on this subject. It also has symbolic importance for foreign media and NGOs. For instance, although the Annual Report of RSF for 2007 does not mention any Internet issues for Türkiye, the 2009 Report mentions the YouTube blocking issue. This is evidence that the YouTube case attracts foreign attention to the country, and blocking practices in the country has become more internationalized with this policy.

Turan Mentes, chair of the NGO Informatics Association of Türkiye, thinks that blocking YouTube is like banning the entire library because of a few books. This anomaly also shows how a state is incapable of implementing a law precisely when authorities find a specific crime agent on the Internet. Such is a video record among the many in YouTube case.

Since state authorities cannot punish the person(s) who uploaded such criminal record(s), or take the criminal record(s) out of the website’s servers, authorities prefer to block access to the entire website within the borders of the country, for Turkish Internet users, even though it is globally accessible beyond Turkish borders.

These kinds of challenges and anomalies remind us of the famous comments of Nicholas Negroponte in his discussion about the law and the Internet: “the Internet cannot be regulated. It’s not that laws aren’t relevant, it’s that the nation-state is not relevant.” The YouTube case in the country shows this dilemma in an apparent way. Tevetoğlu states that “it is not the perpetrators, who uploaded the criminal video records to the website, [who] are punished; the Turkish Internet users are punished in this case.

---

44 Koç et al., ibid.
through blocking access to the website."\(^{46}\)

The first blocking decision against YouTube was because of a video consisting of hate speech against the founder of the Turkish Republic, Atatürk, in March 2007. When the video was reported in Turkish media and newspapers, the public prosecutor’s office in Istanbul requested legal action from the court to prevent access to this particular video, which is claimed to violate law number 5816 (Law on Crimes Against Atatürk, the founder of Turkish Republic), and law number 5237, article 300 (Turkish Penal Code/Crimes against Turkish Flag).\(^{47}\) Based on this application, the First Peace Criminal Court in Istanbul decided to block access to this video record and sent the decision to the TIB.\(^{48}\) Since the TIB could not remove the video record or block access to this particular record, it had to block the entire website by blocking domain address of the website.\(^{49}\) YouTube made a press release that such videos are also a violation of their policy, and they removed the video. YouTube expected that Turkish authorities would lift their decision to block all of YouTube.\(^{50}\) In March 2007 access to YouTube was restored by the TIB after they received a new judicial decision.

This first YouTube blocking was not conducted based on law number 5651 “Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications” since this law did not exist at the time. In the second instance, YouTube was blocked based on law number 5651 by the Twelfth Peace Criminal Court in Ankara, decision number 2008/55 dated 17 January 2008, again for hate speech against

\(^{46}\) Koç et al., ibid.
\(^{47}\) Akdeniz, ibid.
\(^{48}\) “Hakaret Videosu Kalkarsa, Yasak Biter,” CNN, 7 March 2007.
\(^{49}\) Akdeniz, ibid.
\(^{50}\) “Youtube'a Erişim Yasağı Getirildi,” CNN, 7 March 2007.
Ataturk and the Turkish Flag.\textsuperscript{51} Just after this blocking decision was revoked, another blocking decision was enforced against YouTube by the Second Peace Criminal Court in Sivas, decision number 2008/11 dated 16 January 2008.\textsuperscript{52}

In January 2008, the Second Criminal Court in Erzurum decided to block the website forever for propagandizing terrorist organization PKK based on decision number 2008/192.\textsuperscript{53} In March 2008, it was reported to be blocked by the First Peace Criminal Court in Ankara. Both IP and DNS blocking methods are implemented to prevent access to the website by the TIB.\textsuperscript{54} Between March 2007 to June 2008, Akdeniz and Altinparmak note 17 different blocking decisions against YouTube by different courts in Türkiye.\textsuperscript{55} The longest period in which the website was inaccessible started 5 May 2008 based on a decision by the First Peace Court in Ankara for about two and a half years.

In June 2010, the YouTube blocking case had gained a new alarming dimension. Critics about the effectiveness of blocking of YouTube, as presented in this study, urged authorities to revise blocking measures against YouTube and realized that the website uses other IP numbers. They decided to block 44 new IP addresses to cover up critics of the media about the effectiveness of YouTube blocking. However, the result reached to a point of blocking the world’s most popular search engine Google. Because some of Google services were using the same IP addresses as YouTube, Internet users in Türkiye started having problems accessing Google websites, including Google Analytics, Google Maps, Google Docs, Google Translate, and Google Earth. Users also had problems with speed of access to Google services such as using Google tool bar and the Google search

\textsuperscript{51} "Youtube'a Erişim Engellendi," Hurriyet, 19 January 2008.
\textsuperscript{52} Gökçer Tahincioğlu, "Ankara Kaldırdı, Sivas Yasakladı!" Milliyet, 22 January 2008.
\textsuperscript{53} "Erzurum Da Youtube'yi Kapattı," Haber 61, 25 January 2008.
\textsuperscript{54} "Youtube'a Erişim Engellendi," Sabah, 13 March 2008.
\textsuperscript{55} Akdeniz et al., ibid.
These over-blocking problems further disturbed Internet users and online activists in the country. Both Akdeniz and Altinparmak applied to the BTK with a petition that the process of the TIB, which negatively affected some of Google websites and services, was unlawful and violated freedom of speech, freedom of access to knowledge, and freedom of communication protected by the constitution and international law. Gülin Yıldırımkaya, editor of Internet news website haberturk.com, believes that it is shame that while initially the issue was limited to the problem of YouTube blocking, is created another problem of Google. Aylin Duruoğlu, director of Vatan Internet News Website, stated that the TIB act as if it is an institution which is in an open a war against the Internet.

The Institution of Information and Communication Technology (Bilgi Teknolojileri ve İletişim Kurumu, BTK), which is the governing institution of the TIB, defended itself by claiming that the process was just updating IP addresses of the blocked website, YouTube, and that the situation was not their fault but rather the preference and responsibility of the company (YouTube and Google) for sharing the same IP with a website subject to blocking measures by the judicial authorities.

An NGO, the Association of Internet Technology (Internet Teknolojileri Derneği, INETD) claimed that the over-blocking problem stemmed from the decision of the TIB to update IP numbers for YouTube without asking judicial authorities. According to the

---

57 "Google Sansüründe İtiraz," Kanal D Haber, 8 June 2010.
58 "Youtube Yasakının Ucu Google'a Dokundu.", ibid.
59 Ibid.
60 Ibid.
INETD. the TIB did not have authority to interpret the two-year-old court decision. The TIB had to get a new decision from the court if a new implementation or change on the previous blocking decision was necessary. The TIB later said it applied for a court decision for the additional 44 blocked IP address seems after they faced the over-blocking problem. Akdeniz believes that this situation is best be explained by a Turkish saying: “He who steals a minaret (tower) from a mosque before knowing how to conceal the stolen object.”\footnote{Noyan Ayan, "Youtube’a Geçit Yok!" NTV/MSNBC, 17 June 2010.}

For a long time, there were no representatives in the country to defend YouTube in Turkish courts. During this time, authorities called on YouTube, and later its owner Google, to open a representative office in the country. The international company was not able to respond for a long time.\footnote{“Ulaştırma Bakan'ından Sert Google Açıklaması,” Chip Online, 8 June 2010.}

In the end of October 2010, the Germany-based International Licensing Service announced that it revoked the disputed videos against Ataturk on YouTube, by purchasing the copyrights. Following this news on Turkish media, the prosecutor’s office asked the police to confirm if these illegal records were removed. Later, the office asked the TIB to revoke all blocking measures against YouTube since 5 May 2008. Binali Yıldırım, Minister of Transportation, stated that this case showed how authorities were right to call for obedience of the law and how Türkiye is a country with rule of law. Yıldırım also added that the administrators of the company finally decided to act, and once everyone obeys the rules there is no problem at all.\footnote{“Darısı Diğerlerinin Başına!” NTV/MSNBC, 30 October 2010.}

However, a press release by Google stated that the last YouTube situation in Türkiye was not related to them but a third company, which removed the disputed video
records based on automatic copyrights complaints, and they were examining how this was appropriate to their policy.\textsuperscript{64}

It is not clear who was the winner in this case. As cited in Akdeniz and Altiparmak, the TIB statistics dated 26 May 2008 show that YouTube revoked 67 video records among the disputed 111 records. This shows that to some degree, Internet companies can cooperate with states, but under what conditions is a subject for another study. In a workshop in Abant, Türkiye, Nadi Turkaslan, a press prosecutor from the Prosecutor’s Office in Ankara, stated that in some disputed cases, YouTube may only prevent accesses to a disputed video from the country, i.e. Türkiye, but it does not completely remove it from its global servers.\textsuperscript{65}

Despite blocking measures, it is difficult to claim that the popularity of YouTube in the country declined during the term in which access was blocked. The longest YouTube was closed to access within the country was between May 2008 to October 2010. Interestingly, alexa.com, which ranks websites’ popularity, reported YouTube as the sixth most popular website within Türkiye on 21 March 2010 and as third most popular on 22 September 2010.\textsuperscript{66}

Ease of circumvention and the availability of alternative methods

As explained in Chapter III, three circumvention tools are included in the 2009 study by the Berkman Center: 1) Ultrareach (ultrasurf.us); 2) Ktunnel (ktunnel.com); and 3) Tor (torproject.org).\textsuperscript{67} I have chosen them for this study to test whether circumvention is possible to access blocked websites in Türkiye.

\textsuperscript{64} "Youtube’dan Şartlan Açıklama," BilisimLive, 31 October 2010.
\textsuperscript{65} "Youtube’u Kapattıran Savcı Konuştu," Hüriyet, 18 June 2008.
\textsuperscript{66} "Alexa Actionable Analytics for the Web.", ibid.
\textsuperscript{67} Roberts et al., ibid.
In order to see how web content matters in this test, the selection is made based on web contents including political and hate speech, terror, sex and pornographic, game and gambling, and other (health, copyrights, hackers).68

Checks were conducted in Sanlurfa, Türkiye in April and May 2013. The test was conducted with a personal laptop running Intel Pentium CPU, 2.13GHz, 2GB RAM, and Windows 7 (32-bit) Ultimate operating system. The web browser was Internet Explorer 8 (Version 8.0.7600.16385) with 256-bit encryption. The security level of Internet options was set for medium-high, and the privacy settings were also set as medium. Flash player is version 11.4.402.265. Java version is 6 Update 30, and Scripting of java applets is enabled, as is the default for medium-high security level.

Initially, I tried to access each blocked website without using circumvention tools. I checked all websites and confirmed that they are blocked on the date of testing. Each blocked website and its contents are different, so I checked the following criteria during the circumvention tool test to access the blocked website. Is the first page accessible (links, images, or texts are broken or clear)? Are links on the first page are working (i.e. opens the linked page)? Is video available and accessible? Are images on the first page available and visible? Is audio available and accessible (voice records, radio, songs)? Is downloading available and possible (PDF, video, zip)? Is membership required for any of above requested access?

Possible outcomes are: the answer is positive (access is possible, links are working, etc.); the answer is sometimes positive, sometimes negative, which means the tool is partly working for the criteria in question; the answer is negative; encountered some errors (including servers, computer or network connection), including the tool itself.

---
68 “Engelli Web.”, ibid.
gives error; and the criteria in question are not available or are irrelevant for accessing the blocked website.

Overall, if most criteria during the test are positive, the outcome is considered positive, which means access to the blocked website is possible. If some criteria are positive but not others, access to the blocked website is partly possible. When most criteria are negative during the test, access to the blocked website is not possible through the used circumvention tool.

However, there needs to be exception in this measurement since being able to playing a game in a gaming website is more important than some broken pictures or audio file errors. Likewise, being able to shopping is important than audio or video playing on the same website. In this situation, the measurement is made based on the importance of the criteria for the website itself.

It is important to note that no game is tried for testing in gambling websites. Nor, an actual order is performed for shopping in any websites. For gambling websites, the test is conducted up until trying to download software but noting further. For shopping websites (tobacco, cigarettes marketing), the test is performed up until checking out, but not confirming payment.

During testing, it has seen that some websites are just for directing visitors to other classified websites and/or domains. Directed website can be an alternative domain of the same website or a totally different website. In this situation, testing criteria becomes misleading since the domain address is changed. Furthermore, the directed website can be found not blocked within the country when checked. Thus, these websites are excluded from the evaluation and marked as “Excluded”.
Testing circumvention of block with Ultrasurf

Ultrasurf is a product of Ultrareach Internet Corporation. It claims to be one of the world’s most popular anti-censorship, pro-privacy software, with millions of people using it to bypass Internet censorship and protect their online privacy. It is for anonymous surfing and browsing. Ultrasurf hides IP address, clears browser history, cookies, and more. It uses industry standard, strong end-to-end encryption to protect data transfer from being seen by third parties. It allows users to Bypass Internet censorship to browse the Internet freely. It is portable and does not require installation. It can be run over a USB drive or SD card for cameras in an Internet cafe, for instance.69

Ultrasurf is selected as an example of an HTTP proxy circumvention tool. It requires software download and install. It is compatible with Internet Explorer, and while Internet surfing, a yellow image of a lock is visible on the bottom right of the page. The version of the software tested in this study is U13.01.

By clicking the Ultrasurf Icon on the desktop, which I created during software installation, an Ultrasurf Key and the Ultrasurf homepage open with Internet Explorer. For each access—or lack of access—to the blocked websites using the circumvention tool, the study uses screen captures taken during the test. Screen captures sometimes are also taken for illustrating that downloading is possible, videos are playing, or pdf files are accessible. The evaluation of Ultrasurf during the test to access blocked websites reveals the following results.

Among the 23 blocked websites, the two of which are excluded here, the test with Ultrasurf reveals that sixteen websites and their contents are almost entirely accessible. These accesses are satisfactory to an extent that almost the entire content of the website

can be accessible with some missing content or services. Two of them, hizb-ut-tahrir.org and hpg.kk5.org give audio and video errors, i.e. audio and video on these websites could not be played during the test. However, the test results for these two sites are considered positive, since there is not much video or audio content on the websites.

Although access and checking content from the two websites ioyun.com and cigarexport.com are possible, playing games at ioyun.com and pre-ordering steps for online purchasing tobacco at cigarexport.com are not possible through the use of Ultrasurf. Since these are the essential services of the websites, circumvention is evaluated as negative for these two websites. Ultrasurf is seen as not supporting pornographic websites, as seen for five websites.

The two websites, 777-online-gambling.net and cyberturk.net are excluded from the evaluation of this method since these domains directs to other websites which are different from the tested one.

Categorically, more than at least one website from all four categories, including hate speech and politics, terror, games and gambling, and the others like hacking, copyrights, etc. are accessible. No site from the category of sexual and pornographic is accessible through Ultrasurf since it does not support such websites.

Testing circumvention of block with Ktunnel

The second tool Ktunnel is selected as an example of a CGI Proxy. The website explains itself thus: “I run a website-based proxy on my server, and you connect to it to retrieve websites, generally blocked by schools, corporations, or governments.” This website, ktunnel.com, is a mediator between the visitor’s computer and the target web server. The website also claims to protect anonymity and privacy of users. Downloads are
possible, the site claims, unless abuse is a problem. Its owner is reported to be running a computer repair shop in Fairbanks, Alaska in the United States.  

Ktunnel requires no software, installation or special browser configurations. It runs on Internet Explorer. The website provides an address bar embedded on its homepage. The target website, which may be blocked, is accessed by typing the website's domain name on this embedded address bar within ktunnel.com. For each access to the blocked websites through ktunnel.com, this study produces screen captures. The evaluation of ktunnel.com during the test to access blocked websites reveals the following results.

Among the 22 blocked websites, the three of which are excluded here, the test with ktunnel.com reveals that nine websites and their contents can be accessed almost entirely. While seven of them can partly be accessed, six websites and their contents cannot properly be accessed. Three websites are excluded from evaluation.

Among the ones for which circumvention is possible, sosyalistforum.org displays a video error and pkkonline.com displays an audio error. In other words, on these sites video and audio records on these websites could not be played during the test. The study ignores these, since video or audio content for these websites is not very significant within the entire message of the websites.

As for the seven websites evaluated as partly working, they sometimes give video and audio errors, some hyperlinks may not work, or some images are missing. The remaining six of the websites and their contents could not properly be accessed and evaluated as negative for circumvention through ktunnel.

Categorically, at least one website from all five categories including hate and

---

political, terror, game and gambling, sexual and pornographic, and the others like hacking and copyrights can be accessed through ktunnel.com.

Testing circumvention of block with Tor

The third tool Tor is selected as a re-routing proxy. It is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It hides browsing habits as well as the location of the clients through random communication paths in its anonymous network. In order to use Tor, it is necessary for clients to download Tor software and install it on their computers. Tor has its own browser, which comes with software installation. This study worked with Tor browser 2.3.25-5_en-US_2.71

The evaluation of Tor during the test to access blocked websites reveals the following results. Among the 22 blocked websites, the three of which are excluded here, the test with the Tor test reveals that fifteen websites and their contents can be accessed almost entirely through the use of Tor. Three websites and their contents cannot properly be accessed and they are evaluated as being partly accessible. Access test for one website gives the error message: “unable to connect.” Three websites are excluded from the evaluation here: www.red-movies.com (redirects to other websites); www.777-online-gambling.net (redirects to other gambling website); and http://cyberturk.net (redirects to another domain: www.masterhack.org which is not blocked yet in the country on testing date).

Among the ones for which circumvention is evaluated as possible through the use

71 For a detailed description of how Tor works, see "Tor: Overview." https://www.torproject.org/about/overview.html.en.
of Tor, hizb-ut-tahrir.org displays an audio error and hpg.kk5.org displays a video error. The study ignores these errors because of the insignificance of audio and video for the website itself.

The same video error is considered as significant for three pornographic websites, and the three websites in which videos are not working are evaluated as partly working through the use of Tor.

Since audio is important for music website stereomood.com, audio error is evaluated as circumvention not being possible, although the first page is accessible, photographs are visible, and links function. The other two websites which are evaluated as “access not possible” are the two game websites ioyun.com and cigarexport.com.

At least one website from all five categories, including hate and political, terror, game and gambling, sexual and pornographic, and the others like hacking and copyrights can be accessed through Tor. Although one shopping website cigarexport.com does not work through the use of Tor, gerard-pere-et-fils.com works for ordering tobacco.

Overall analysis of three circumvention tools

As indicated in the above evaluations, blocking measures against undesired websites are not effective to an extent that most of the blocked websites can be accessed through circumvention methods. Access tests to the undesired blocked websites can reach up to 71% through the circumvention tool Tor (15 websites could be accessed among the 21 blocked websites excluding the one with technical error and the three specified as “Excluded”). If the ones which are evaluated as “partly possible” are also considered satisfactory, this percentage reaches 85%. In other words, among the 21 blocked websites, 18 of them can be accessed by Internet users with the use of Tor.
Access tests through the circumvention tool Ultrasurf gives similar performance. The percentage of access through the use of this tool is about 69%. (16 websites could be accessed among the 23 blocked websites, excluding the two ones). In fact, if the five websites for which the tool does not support are also excluded from the sample size, the percentage of access for this tool reaches 88%. In other words, among the 18 blocked websites, 16 of them can be accessed with the use of Ultrasurf.

Access tests with the use of Ktunnel reveals the lowest possible access to 9 blocked websites which constitute about 40% of all the tested sites excluding the three excluded. The test with Ktunnel also reveals the highest score of partly accessed websites which is seven. If the ones which are evaluated as “access partly possible” are also considered satisfactory, this percentage reaches 72%.

While there is no website which is evaluated as partly accessible with the use of Ultrasurf, the result with the use of Tor is seven. As for the results for inaccessibility with the tested tools, Ktunnel has the highest 6 websites which cannot be accessible, it is three for Tor and two for Ultrasurf.

This test also showed that circumvention tools are especially unsuccessful in playing multimedia content. Although circumvention tools can make it possible to access a website, to surf with hyperlinks, and to download, they can very often give multimedia failures and/or errors. Blocking is especially ineffective in terms of circumvention for text and document-intense websites, such as ideological, hate speech, pro-terrorism, and pro-racist websites.
A specific issue area: terror websites and wide-effects of Internet blocking

This section explores how blocking policies in Türkiye affect the websites of the pro-terrorist organization PKK and/or its sympathizers. How effective are blocking policies in preventing access to these websites from the country? How have these websites, their popularity, and audience have been affected after blocking measures? What does the current picture of the interaction between a state and the Internet look like in terms of blocking terrorist websites?

This section utilizes data and information from open sources, well known global websites like alexa.com, websitetrafficspy.com (which provides traffic rates of websites from different sources like alexa.com, compete.com, and Google Trends), and ipaddress.com (which gives available information about hosting, ownership, and addresses as well as other hostnames for the same IP number that a website is using).

For blocked pages in Türkiye, the study uses a Turkish website, engelliweb.com, which monitors blocked websites in the country. This analysis was conducted both in Türkiye and in the United States. The blocked websites, their blocking details as well as some methods to circumvent blocking, were checked and tested in Ankara, Türkiye. Other analysis about these websites was checked and concluded in the United States. Testing dates for each check are mentioned in the foot notes.

Sample size and selecting a representative sample are vitally important for any academic study, which is also the case for this section. In order to establish which

---

72 Not all the websites here have direct and organic links with the organization. Some websites here are even registered and giving service within Türkiye and may be blocked because of a few specific illegal contents.
websites support, encourage, or sympathize with the Marxist-Leninist separatist terrorist organization PKK, this part of the study utilizes Alexa records. A search for the name of terrorist organizations within Alexa found the website pkk-online.net, which was ranked by Alexa. Using the features of alexa.com (related links, click stream, and sites link in) reveals a network of websites, shown below. Since Alexa ranks websites from most popular (a combination of average daily visitors and page views on a particular website) to least popular, this network of websites does/should significantly represent all active and popular websites within the context explored here.

Later, the study checked if access to each of these websites was being blocked in Türkiye, and if so, when and by whom they were being blocked. All of the websites specified above were found blocked by different courts in Türkiye at different times. Blocking details below are noted from the first page of these websites when access attempts were made in Türkiye. The rankings of the each website within Türkiye and the percentage of visitors for each page from within Türkiye have been taken from alexa.com.

In order to see how blocking affects these websites over time, the study conducts a longitudinal analysis. Ranking of the specified websites, particularly for Türkiye, have been taken on three different dates: February 2010, September 2010, and March 2011. This approximate one-year time frame is assumed to minimize possible data fluctuations in alexa.com and can give more reliable results. During this time, it was also possible to observe and analyze which websites were closed, which domain names have changed,

73 Although there are some exceptions, the blocked authority, date, and reference number appear on the page at the time of access to the blocked site in Türkiye. This information appears on the screen also gives two references: Telekomünikasyon İletişim Başkanlığı, www.tib.gov.tr/ and Turkish Information and Communication Technologies Authority, Telecommunications Presidency, Internet Regulations Department, "İhbar Web: Telecommunications Presidency Internet Hotline," Telekomünikasyon İletişim Başkanlığı, www.ihbarweb.org.tr.
and how blocking measures by Turkish authorities have shaped these kinds of websites.

In this way, the following 11 popular but blocked websites in Türkiye have been specified. They are: gerila.tv, rojaciwan.com, roj.tv, ygk-info.com, yeniozgurpolitika.com, pkk-online.net, hpg-online.net, atilim.org, firatnews.com, gunlukgazetesi.com, and pdk-xoybun.com.

Gerila.tv

The decision number 2008/5517 dated 07 October 2008, handed down for gerila.tv within the context of protection measure of Ankara 11. Ağır Ceza Mahkemesi was implemented by Telekomünikasyon İletişim Başkanlığı.

At the time of the first check on 28 February 2010, Gerila.tv was ranked 18,734 in Türkiye.74 62.4% of users visiting Gerila.tv came from Türkiye.

No rank data or visitors profile is available on alexa.com for the Gerila.tv check on 01 September 2010. However, the study found that with its original address name, an error message appears in Türkiye (Domain name is not active anymore).

The Gerila.tv check on 01 September 2010 revealed that no rank data or visitors profile was available on Alexa.com. The domain name was not active anymore.

Rojaciwan.com

Testing for Rojaciwan.com showed that the blocking date and authority were unknown.75 The following message appears: “Access to this website is restricted based

---

74 Ranking of a website in a country is a combination of average daily visitors and page views on a particular website for the past three months. "Alexa Actionable Analytics for the Web.", ibid.
75 Percentage of visitors from Türkiye to the website decreased to some degree from 34.8% to 31.1%. This may suggest that regular Internet users from the country could not access the website and percentage of visitors from Türkiye gradually declined. However popularity ranking (combination of average daily visitors and page views) in Türkiye increased some from 13,642 to 13,208 (lower is better popularity than
on a court decision."

At the check on 28 February 2010, Rojaciwan.com was ranked 8,074 in Switzerland, 13,642 in Türkiye, 54,692 in Germany, 114,977 in France, and 247,926 in United Kingdom. Rojaciwan.com users came from these countries: 34.8% from Türkiye, 25.4% from Germany, 25.1% from Switzerland, 3.9% from France, 3.3% from the United Kingdom, and 7.5% from other countries.

At the test on 1 September 2010, Rojaciwan.com was ranked 5,422 in Switzerland, 9,767 in Türkiye, 11,201 in Finland, 14,780 in Denmark, 28,953 in Germany, 108,806 in the United Kingdom. Rojaciwan.com users come from these countries: 26.3% from Germany, 25.3% from Türkiye, 21.7% from Switzerland, 7.5% from Finland, 5.6% from Denmark, 5.1% from the United Kingdom, and 8.5% from other countries.

At the test on 25 March 2011, popularity of Rojaciwan.com was tabulated as 6,303 in Finland, 12,601 in Belgium, 13,208 in Türkiye, and 150,829 in Germany. Visitors by country for Rojaciwan.com as a percent of site traffic included Türkiye (31.1%), Finland (25.7%), Belgium (16.1%), Germany (13.3%), and other countries (13.8%).

Roj.tv

Access to this website was blocked based on the decision number 2008/4687 dated 21 August 2008, which was handed down for roj.tv within the context of the protection measure of Ankara 11. Ağır Ceza Mahkemesi was implemented by
At the test on 28 February 2010, Roj.tv’s popularity rankings were 22,414 in Türkiye, 27,412 in Switzerland, 31,525 in the United Kingdom, 38,389 in Germany, 65,164 in France, 89,466 in China, and 89,842 in the Netherlands. Roj.tv users come from these countries: 31% from Germany, 22.8% from the United Kingdom, 16.1% from China, 22.4% from Türkiye, 3.8% from France, 3.6% from Switzerland, 2.4% from the Netherlands, and 7.2% from other states.

At the test on 1 September 2010, Roj.tv was ranked 20,980 in Türkiye, 74,249 in Germany, 117,399 in France, and 203,617 from the United Kingdom. Roj.tv users come from these countries: Germany (40.2%), Türkiye (27.1%), the United Kingdom (8.7%), France (7.2%), and other countries 16.7%.

At the test on 25 March 2011 Roj.tv’s popularity ranking were given as 3,366 in Finland, 10,686 in Belgium, 28,668 in Türkiye, 51,034 in Germany, and 63,980 in the United Kingdom. The percentage of visitors by country for Roj.tv include Finland at 27.5%, Germany at 19.2%, the United Kingdom at 12.7%, Belgium at 9.3%, Türkiye at 6.3%, and other countries at 24.8%.

Ygk-info.com

The block was based on the decision number 2008/531 dated 2 April 2008, which was handed down for ygk-info.com within the context of protection measure of Eskisehir 3. Sulh Ceza Mahkemesi was implemented by “Telekomünikasyon İletişim Başkanlığı.”

At the test on 28 February 2010, Ygk-info.com ranked 104,124 in Türkiye, with

---

76 Decline is seen in popularity ranking in Türkiye (from 22,414 to 28,668) and percentage of visitors from the country (13.1% to 6.3%).
100% of users coming from Türkiye.

At the test on 1 September 2010, only a global ranking was available which was 7,327,170, but there was no regional ranking or visitors profile available.

The study accessed the website through a proxy (ktunnel.com) in Türkiye, on 1 September 2010. The domain name was active.

At the test on 25 March 2011 Alexa ranked Ygk-info.com globally at 17,500,453. There was no regional rank or visitors profile available. The domain name was still active.

Yeniozgurpolitika.com

Blocked based on decision number 2008/2815 dated 9 May 2008, which was handed down for yeniozgurpolitika.com within the context of the protection measure of Ankara 11. 77 Ağır Ceza Mahkemesi was implemented by “Telekomünikasyon İletişim Başkanlığı.”

At the test on 28 February 2010, Yeniozgurpolitika.com ranked 31,340 in Türkiye, 39,517 in Switzerland, 51,107 in Sweden, 67,963 in Germany, and 74,858 in France. Yeniozgurpolitika.com users come from Germany (42.8%), Türkiye (29.6%), France (10.8%), Switzerland (8.1%), Sweden (7.0%), and 1.8% from other countries.

At the test on 1 September 2010 Yeniozgurpolitika.com ranked 3,874 in Sweden, 8,520 in Switzerland, and 111,556 in Türkiye. Yeniozgurpolitika.com users come from Sweden (57.8%), Switzerland (33.2%), Türkiye (4.7%), and other countries (4.2%).

At the test on 25 March 2011, Yeniozgurpolitika.com’s Regional Traffic Rank was 101,432 for Türkiye. 10.8% of visitors to Yeniozgurpolitika.com were from Türkiye

77 Decline is seen in popularity ranking in Türkiye (from 31,340 to 111,556) and percentage of visitors from the country (29.6% to 10.8%).
and 88.9% were from other countries.

Pkk-online.net

This site was blocked based on two court decisions. One decision was number 2009/6163-1 dated 19 October 2009, handed down for pkk-online.net within the context of the protection measure of Ankara 11. Ağır Ceza Mahkemesi was implemented by “Telekomünikasyon İletişim Başkanlığı.” The other was decision number 2009/7088 dated 04 November 2009, handed down for pkk-online.net within the context of the protection measure of Ankara 11. Ağır Ceza Mahkemesi was implemented by “Telekomünikasyon İletişim Başkanlığı.”

At the test on 28 February 2010, Pkk-online.net ranked 22,536 in Türkiye. Pkk-online.net users come from Türkiye (76.3%) and 23.3% from other countries.

At the test on 1 September 2010, only a global rank was available. The Alexa Traffic Rank was 11,694,421. There was no regional rank or visitors profile is available.

The test on 25 March 2011 indicated that there was not enough data to display the traffic metrics for pkk-online.net. With its original address name, the “Domain name is not active anymore” message appears in the United States.

Hpg-online.net

The blocking date and authority are unknown. The following message appears: Access to this website is restricted based on a court decision.

The test on 28 February 2010 showed that Hpg-online.net ranked 9,321 in Türkiye, 308,486 in the United Kingdom, and 337,111 in Germany. Hpg-online.net users come from Türkiye (84.5%), Germany (7.5%), and the United Kingdom (4.2%).
The test on 1 September 2010 revealed a global Alexa Traffic Rank of 1,567,794. There was no regional rank or visitors profile available.

At the test on 25 March 2011, Hpg-online.net’s three-month global Alexa traffic rank is 4,215,954. The site is located in Germany. With its original address name the “Domain name is not active anymore message” appears in the United States.

Atilim.org

The blocked is based on decision number 2009/632 dated 04 April 2009, handed down for atilim.org within the context of the protection measure of Istanbul 9. Ağır Ceza Mahkemesi was implemented by “Telekomünikasyon İletişim Başkanlığı.”

At the test on 28 February 2010, Atilim.org ranked 3,404 in Türkiye, 54,895 in Belgium, and 292,212 in France. Atilim.org users came from Türkiye (94%), Belgium (1.4%), France (0.8%), and 3.8% from other countries.

At the test on 1 September 2010, the Alexa Traffic Rank was 354,930. Atilim.org’s worldwide traffic ranked 5,151 for Türkiye and 350,160 for Germany. Visitors for Atilim.org include 85.9% from Türkiye, 5.4% from Germany, and 8.6% from other countries.

At the test on 25 March 2011, Atilim.org’s Regional Traffic Rank was 10,914 for Türkiye. Visitors by country for Atilim.org include 81.9% for Türkiye and 8.1% from other countries.

---

78 Decline is seen in popularity ranking in Türkiye (from 3,404 to 10,914) and percentage of visitors from the country (94% to 81.9%).
Firatnews.com

This site was blocked based on decision number 2008/2815 dated 9 May 2008, handed down to firatnews.com within the context of the protection measure of Ankara 11. Ağır Ceza Mahkemesi was implemented by "Telekomünikasyon İletişim Başkanlığı." 79

At the test on 28 February 2010, Firatnews.com was ranked 1,070 in Türkiye, 3,878 in Tunisia, 10,225 in Switzerland, 10,478 in Sweden, 28,785 in the United Kingdom, 34,301 in China, 34,403 in Germany, 50,551 in Russia, 71,737 in France, and 594,465 in the United States. Firatnews.com users come from Türkiye (60.6%), China (10.7%), Germany (8.7%), the United Kingdom (5.3%), Sweden (3.2%), Russia (2.6%), Switzerland (2.1%), the United States (1.0%), France (1.0%), Tunisia (1.0%), and 3.6% from other countries.

At the test on 1 September 2010, the Firatnews.com’s Worldwide Traffic Rank was 1,048 from Azerbaijan, 1,214 from Albania, 1,254 from Türkiye, 2,508 from Iraq, 2,825 from Sweden, 3,687 from Switzerland, 4,256 from Austria, 13,722 from Germany, 32,136 from France, 55,065 from Canada, 174,467 from the United Kingdom, and 483,168 from the United States. Visitors by Country for Firatnews.com as a percent of site traffic were Türkiye (41.1%), Azerbaijan (13.9%), Germany (12.8%), Sweden (9.8%), Switzerland (5.3%), Austria (5.3%), France (2.9%), Iraq (2.7%), Albania (1.3%), Canada (1.1%), Austria (5.3%), France (2.9%), Iraq (2.7%), Albania (1.3%), Canada (1.1%), the United States (1.1%), the United Kingdom (0.9%), and other countries (1.8%).

79 Decline is seen in popularity ranking in Türkiye (1,070 to 1,705) and percentage of visitors form the country (60.6% to 38.3%).
For the test on 25 March 2011, Firatnews.com's Regional Traffic Ranks are Türkiye at 1,705, Belgium at 2,213, Sweden at 3,403, Germany at 12,982, the Netherlands at 26,600, France at 29,466, Greece at 32,440, and the United Kingdom at 187,374. Visitors by country for Firatnews.com were 38.3% from Türkiye, 23.9% from Germany, 11.4% from Sweden, 10.1% from Belgium, 5.7% from France, 2.8% from the Netherlands, 1.1% from the United Kingdom, 0.9% from Greece, and 5.8% from other countries.

Gunlukgazetesi.com

The block is based on decision number 2009/7088 dated 4 November 2009, handed down to gunlukgazetesi.com within the context of the protection measure of Ankara 11. Ağır Ceza Mahkemesi was implemented by “Telekomünikasyon İletişim Başkanlığı.”

At the test on 28 February 2010, Gunlukgazetesi.com was ranked 12,318 in Türkiye, 67,068 in France, 85,672 in China, and 234,780 in Germany. Gunlukgazetesi.com users came from Türkiye (49.1%), China (29.0%), France (8.6%), Germany (8.3%), and 4.9% from other countries.

At the test on 1 September 2010 no regional or other data was available.

At the test on 25 March 2011 Gunlukgazetesi.com’s three-month global Alexa traffic rank was 18,088,952. No regional or other data was available. With its original address name, the “Domain name is not active anymore” page appears when accessed in the United States.
The block was based on decision number 2008/6731 dated 28 November 2008, handed down to pdk-xoybun.com within the context of the protection measure of Ankara 11. Ağır Ceza Mahkemesi was implemented by "Telekomünikasyon İletişim Başkanlığı."

In the test on 28 February 2010, pdk-xoybun.com ranked 74,643 in Türkiye. 42.5% of visitors to the site came from Türkiye, and 57.5% came from other countries.

In the test on 1 September 2010, no regional or other data was available.

In the test on 25 March 2011, pdk-xoybun.com's three-month global Alexa traffic rank was 3,585,233. This site's content placed it in the "Parti" category of websites. The site has been online for at least eight years. The domain name is active.

Overall analysis of the websites

The six websites experienced dramatic decline in their popularity rankings, which is a combination of average daily visitors and page views on a particular website for the past three months (Gerila.tv; Ygk-info.com; Pkk-online.net; Hpg-online.net; Gunlukgazetesı.com; and Pdk-xoybun.com). Five websites were suffering some kind of decline both in their popularity ranking and percentage of visitors from the country. (Rojaciwan.com; Roj.tv; Yeniozgurpolitika.com; Atilim.org; and Firatnews.com; although popularity ranking of the second website, rojaciwan.com was seen as some increase in the country, this website is also considered as suffering some decline since the percentage of visitors from the country declined slightly).

The test also checked on its final check in March 2011, whether the domain addresses were affected from these access-blocking measures. It showed that despite some decline in their popularity, the domain addresses of five websites were still active.
Among the six websites which were having dramatic declines in their popularity, four domain addresses were seen as deactivated (Gerila.tv; Pkk-online.net; Hpg-online.net; and Gunlukgazetesi.com). Despite dramatic declines in their popularity, the domain addresses of two websites were still active on the date of final check (Ygk-info.com and Pdk-xoybun.com).

These checks however, do not provide the entire picture about the results of blocking access to these websites. Further checks reveal that these websites have other alternative domain addresses attached their IP number(s). The following part of this dissertation explores this issue in detail.

Blocked websites and alternative domain addresses

This section is an analysis of alternative domain names for the same websites. For this analysis, ipaddress.com was utilized as a source that gives all technical, registration, and administrative details. Ipaddress.com also gives other hostnames for a website by looking at the registered IP addresses of the same website. Checks on ipaddress.com reveal that most of these websites analyzed above have other (alternative) sub-domain names and addresses. During this analysis, five websites were found using only one domain name, but the other seven websites have at least one other alternative domain name. Rankings and percentage of visitors for each domain name are checked again three different times on alexa.com. Gerila.tv was blocked on 7 October 2008. Gerillatv.com was blocked on 3 April 2008.

Verification revealed that in addition to gerila.tv, the website had two other domain addresses, gerillatv.com and gerillatv.net. Also, it was established that both
domain names, gerila.tv and gerillatv.com, are not active anymore but the (same) site was still online under a third domain name, gerillatv.net on the final check in March 2011.

No court decision was known against this domain name at that time, and the website was accessible from Türkiye. The website was still online at that time although two of its domains were blocked and not active anymore.

Verification revealed that beside rojaciwan.com, there was another domain address of the same website, hezaciwanan.com (blocked on 28 January 2009). The website rojaciwan.com is blocked in Türkiye, but this domain address was still active and online outside Türkiye. Blocking details were unknown.

The same website also uses the domain name hezaciwanan.com, which seems to be blocked as of 28 January 2009 within the country. Overall, the website was still active in March 2011.

Despite some decline in terms of popularity and ranking within Türkiye, the website Roj.tv was still active with this domain (blocked 21 August 2008) and had no alternative domain addresses on the date of the final verification.

Despite dramatic decrease in terms of popularity and ranking within Türkiye, the website Ygk-info.com was still active with this domain and had no alternative domain addresses at that time (blocked on 2 April 2008.

The website with yeniozgurpolitika.com had another domain extension with (.org) in March 2011. Although both domains were blocked on 9 May 2008, the website was still online at that time.

Pkk-online.net was blocked in Türkiye (19 October 2009 to 4 November 2009) and this domain address was not active anymore in March 2011. Alternative domain addresses (pkkonline.net, blocked on 18 June 2010 and pkkonline.com, details are not
known) were also blocked within the country. The website was still online then with these two alternative domain addresses.

In addition to Hpg-online.net (blocked but details are not known), an alternative domain hpg-online.com (blocked but details are not known) was inactive in March 2011. However, the same website was still online with a third domain address hpg.kk5.org at that time (blocked 28 November 2008).

Despite some decline in its ranking within Türkiye, the website Atilim.org (blocked 4 April 2009) was still active with this domain and had no alternative domain addresses on the date of verification.

It was established that besides firatnews.com (blocked 9 May 2008), the website was using Firatnews.eu (blocked 10 January 2008) as another domain address. Access to either domain address was blocked in Türkiye but both domains were active and the website was online on the date of verification.

Blocked on 4 November 2009, the domain gunlukgazetesi.com was inactive on the date of verification. The website has another domain name gunlukgazetesi.net. No court decision blocking this site was known to be in effect against this domain name and the website was accessible from Türkiye. The website was still online at that time.

Despite a dramatic decrease in terms of popularity and ranking within Türkiye, the website Pdk-xoybun.com was still active with this domain despite being blocked on 28 November 2008 and had no alternative domain addresses at that time.

Evaluation of data

All of the terror websites specified in this study are experiencing decrease in their rankings and popularity according to alexa.com. Decreases for six of them are dramatic
enough that alexa.com does not provide regional rankings or global rankings.\textsuperscript{80} Ranking and popularity decreases for the other five websites are not as dramatic, but there is nonetheless some degree of decrease in popularity and ranking between February 2010 and March 2011.

Among 11 websites, only four of them had declines in popularity enough to deactivate their domain names. The other seven sites (among them 2 sites experiencing severe decline, five experiencing some decline) have not yet deactivated their domain names as of March 2011. The four which deactivated their domain names have at least one alternative domain name, according to ipaddress.com. However, none of the websites checked here have shut down their servers.

Either making changes in their domain addresses, servers, or IP numbers, these websites were able to pursue a range of technological alternatives to remain accessible. Access blocking measures against the websites date back to 2008 and 2009. Despite these measures, however, the sites continued to receive some of its audience and remained online at least for the period between February 2010 and March 2011.

Circumvention tendency, particularly in Türkiye

As explored in already in this study, for each blocking technique, there are bypassing methods which allow users to access blocked websites and web content. The Internet provides access to information about these circumvention methods and instructions for how to use them. Ordinary Internet users familiar with search engines can find information about these methods and access these resources.

For instance, a Google search revealed 94,600 results in 0.17 seconds for how to

\textsuperscript{80} "Alexa Actionable Analytics for the Web.", ibid.
circumvent blocked websites (without quotation marks). Google Turkish (Google.tr) revealed 16,400 results in .22 seconds for a similar search in Turkish ( İnternette sansür nasıl aşıılır). Yahoo found 1,330,000 resources for the same English phrase and 53 results for the same Turkish phrase. A Turkish search engine, Arabul, found 210 results with the English language search string how to circumvent blocked websites and 570 results for the Turkish search string İnternette sansür nasıl aşıılır (without quotation marks). 

These results provide hundreds or thousands of different resources for Internet users. These resources sometimes include video, photos or step-by-step instructions for how to circumvent Internet blocking. Because of this, some countries also try to prevent access to these kinds of online resources, either by blocking them directly or using key word search blocking at search engines. So far, these measures against circumvention websites or online resources are unknown in Türkiye.

The most widespread method for circumvention seems to be using online proxy servers, which can also be located through search engines. Google.com found 126 million results in 0.12 seconds for the term proxy. Google.com.tr suggested ten alternative search phrases as the user typed the word proxy (in English): proxy, proxy list, proxygizlen (proxyhide), proxy nedir (what is proxy?), proxy server, proxy ayarları (proxy settings), proxy switcher, proxy site, proxy sites, and proxyhideout.com. While google.com.tr found 124 million results in 0.05 seconds for proxy (in English), it found 361 thousand results in 0.34 seconds for proksi (In Turkish).

As seen in Appendix-2, Turkish visitors were accustomed to using three of the top five proxy servers, ktunnel, vtunnel, and anonymous. The proxy server ktunnel received

---

81 I checked the sites in the United States on 4 April 2011 without quotation marks.
82 I conducted the searches in the United States on 1 April 2011 without using quotation marks in the search string.
88.4% of its visitors from Türkiye. This is also observable in alexa.com website rankings for each country. While ktunnel is one of the top 100 most popular websites, vtunnel.com ranked 294th in popularity in Türkiye.

The effects in the case of YouTube cannot be ignored when considering the spread of proxy usage in Türkiye. The YouTube case, which became a symbol of blockings in Türkiye, was often a subject of discussion and news in the media as well as on the Internet in blogs, forums, and other Internet sites. Most of these resources discussed the dilemmas in YouTube's blocking as explained in this study and provided alternative ways to access the website.\(^{83}\) While some of them suggest proxy servers for circumvention, others explain methods like changing DNS settings and adjusting computer settings. These resources are also available for pro-terrorism websites.

As explained in this chapter access blocking to undesired websites are not effective to an extent that many of the blocked websites can be accessible through different tools and technics. Access blocking to undesired websites within a national border do not necessarily lead the website to totally shut down their services and servers. It is not effective to use access blocking as a measure since it is open to possible errors like over-blocking or under-blocking. If it does not cause an error, access blocking can be un-proportional and unacceptable since it seriously violates fundamental rights and freedom as explained in the case of YouTube blocking. Thus, the effectiveness of prevention aspects of internet policing is open to significant questions and doubts.

The following chapter examines how much prosecution is effective in identifying,

---

tracing or detaining suspects/perpetrators of a cybercrime, particularly internet child pornography. After giving introductive information about the crime, legal framework, national institutions and international regimes this part of the study explores how much policing is successful in child pornography investigations.
CHAPTER VI
POLICING CHILD PORNOGRAPHY IN TÜRKİYE

INTRODUCTION

Compared to most of the EU member countries, Türkiye has a young population. Of the 75.6 million inhabitants in 2012, 18.8 million were under 14 years old, about 25% of the population.¹

Culturally, family is very important in Turkish society, and families give much importance to their children and their children’s health, wellbeing, and upbringing in accordance with socio-cultural values. The Ministry of Families and Social Policies is the highest bureaucratic institution in the country that deals with policies regarding the family, children, the disabled, and the aged.²

Occasionally there are news stories involving child victims. These stories rarely involve child sexual abuse. For instance, in connection with investigations conducted by German Interpol, a suspect downloading child pornography from the Internet was identified based on IP numbers and found to be located in Türkiye. Police investigation of the address found files containing child pornography. A 65-year old man was imprisoned after prosecution in Trabzon in 2012.³

According to news reports, a 31-year old man identified himself as a child in chat rooms where he engaged with children and obtained recordings from them containing images of the children undressing. The man used MSN and Facebook to access files of

³ Osman Şişko, "Doçente Porno Cezası," Gazete Vatan, 17 February 2012.
children undressing. He was transferred to judicial authorities for prosecution in Bursa.⁴

Recently an adult using the pseudonym “Begum10” identified himself as a 10-year old girl in a chat room and received approximately a hundred messages in half an hour, some of which included sexuality.⁵

Related departments and NGOs

Children’s rights and protection from victimization should not be solely the responsibility of authorities, and solutions should include society and civic actors. In recent years, universities, civil-society organizations, and non-governmental organizations have started to play roles in this sensitive issue.

The Bar Associations of Istanbul and Ankara have founded the Center of Children Rights.⁶ Other groups include the Organization of Child Abuse and Neglect;⁷ the Organization of Children and Information Security;⁸ and the Organization of Protecting Children from Abuse and Rehabilitation (ÇIKORED).

Operating since 2001 under a different name, the Research, Practice and Protection Center for Children was officially opened in 2006 at the University of Gazi in Ankara.⁹ Likewise, the Ankara Children Protection Institution (AÇOK) was founded in 2005 at the University of Ankara. It deals with children, who are subjects of abuse in different ways. Unveren cites that the center received 164 victims between 2005 and May

---

⁴ Budakoğlu, Selahattin, and Bursa - Doğan Haber Ajansı (Dogan News Agency), "Bilgi İşlem Sorumlusundan Çocuklara Tuzak," Milliyet, 4 February 2011.
⁵ "10 Yaşındaki Çocuğa Seks Təklif Edenler..." haber365.com, 28 March 2011.
&DocumentIndex=merkezler/chm.htm.
⁷ "Çocuk İstismarı Ve İhmalini Önleme Derneği," http://www.cocukistismari.org/.
⁸ "Çocuk Ve Bilgi Güvenliği Derneği," cbgd.org.
2009.\textsuperscript{10} Among them, 53% were male and 46% were female. Ages vary from infant to 16 years old, while the average age was seven. Among the victims, 33% of them were sexually abused, 33% were physically abused, 3% were mentally abused, and 30% of cases featured other kinds of abuse.\textsuperscript{11}

The University of Erciyes founded the Prevention of Children Neglect and Abuse, Research and Practice Center (ÇITEM) in 2009. The center hires specialists and experts.\textsuperscript{12}

National legal framework

Turkish Criminal Code, No.5237 dated 26 September 2004, Official Gazette No.25611 dated 12 October 2004 defines child as a person under the age of eighteen in Article 6 and regulates criminality specifically in terms of child involvement in different articles. The term child pornography is not used by the code. Instead the code uses the term child sexual abuse as penalized in Article 103. The code also uses the term indecency, which includes production, advertisement, selling, storing, or broadcasting of obscene materials of children in Article 226: 

\begin{verbatim}
Obscenity
ARTICLE 226-(1) Any person who involves in an unlawful act; a) By allowing a child to watch an indecent scene or a product, or to or hear shameful words, b) By displaying these products in places easy to reach by children, or reading the contents of these products, or letting other to speak about them, c) By selling or leasing these product in such a way open for public review, d) By selling, offering, or leasing these products at places other than the markets nominated for sale of these product, e) By gratuitously supplying or distributing these
\end{verbatim}

\textsuperscript{11} Ibid.
\textsuperscript{12} "Erciyes Üniversitesi Çocuk İhmalı Ve İstismarını Engelleme Uygulama Ve Araştırma Merkezi Yönetmeliği," http://bilgiedinme.erciyes.edu.tr/cocuk_ihmal_istismari_engellemeye_merkezi.asp.
products along with other goods or services, f) By making advertisement of these products, is punished with imprisonment from six months to two years.

Section two states: The persons who publicize indecent scenes, words, or articles through press and broadcast organs or act as intermediary in publication of the same is punished with imprisonment from six months to three years. Section three states: Any person who uses children in production of indecent scenes, words or articles is punished with imprisonment from five years to ten years, and also imposed punitive fine up to five thousand days. Any person who engage in import, duplication, transportation, storage, export of these products, or presents the same to other’s use, is punished with imprisonment from two years to five years, and also imposed punitive fine up to five thousand days.

Section four states: Any person who produces products containing audio-visual or written material demonstrating abnormal sexual intercourse by using sex, or with animals, or body of a death person, and engages in import sale, transportation storage of the same and presents such material to other’s use, is punished with imprisonment from one year to four years. Section five states: Any person who publicizes the contents of the products mentioned in third and fourth subsections through press and broadcast organs, or acts as intermediary in publication of the same, or lets children to read, hear, or see this material is punished with imprisonment from six months to ten years, and also imposed punitive fine up to five thousand days.

Neither Turkish law no. 5651 on Regulation of Publications on the Internet nor the law on Combating Crimes Committed by Means of Such Publications dated 23 May 2007 specifically define child pornography. Both laws refer to the Turkish Criminal Code, No.5237, which penalizes child sexual abuse in Article 103 and obscenity in
Law no. 5651 regarding the Internet regulates access blocking measures on some conditions, such as specific crimes committed or whether addresses of content and hosting servers are within Türkiye or located outside of the country. Under limited conditions, this measure can directly and immediately be implemented by the administrative institution, the TIB, and later the issue details are submitted to the judicial authorities for further investigation and a verdict. Tracing a record of child pornography on the Internet is among the conditions under which the TIB can immediately block a website, irrespective of whether its content provider or hosting server is within Türkiye or abroad. TIB detections of these types of web contents are performed through routine checks and on the basis of tips submitted by individuals.

National police institutions

Judicial authorities may receive reports of cases including child pornography from individuals, victims, through administrative departments, or police or gendarmerie units for prosecution. The Department of Interpol Ankara is the gateway in Türkiye for such judicial investigations when the alleged crime has transnational aspects, for example when IP numbers, victims, suspects, email addresses, or servers originate outside of Türkiye. The Department of Interpol Ankara operates under the General Headquarter of Turkish National Police. The official name is “Interpol Europol Sirene Department Directorate.” These cases are dealt with by the Section of Public Security.13

Recent developments in information and telecommunication technologies and the concomitant shift in criminality toward cyberspace resulted in the Turkish National

Police establishing the Department of Struggling against Information System Crimes in 2011. It was renamed the Department of Struggling against Cybercrimes in 2013. The department has a center under the MHQ of Turkish National Police in Ankara and has established sections in 82 Turkish cities as City Police Directorates.14

In the past, operational child pornography investigation requests in Türkiye by foreign Interpol departments tended to be directed toward the Department of Public Security, and in urgent cases, to the Police Directorates in cities as well. The reverse for operational investigation requests from foreign Interpol departments were received by Interpol Ankara from the Department of Public Security, Police Directorates in cities, and the prosecutor’s office.15 Currently, this process includes the new Department of Struggling against Cyber-crimes and its subsections in cities.

International regimes and Türkiye’s participation

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, opened for signatures on 25 October 2007 in Lanzarote and came into force in Türkiye on 1 April 2012, after ratification on 7 December 2011. The convention advises signatory countries to develop preventive policies and programs and criminal and legal frameworks against various forms of children sexual abuse, children prostitution, and pornography.

Instead of limiting scope to the Internet, the Convention extends to information and communication technologies writ large. Article 20 of the Convention, under the title “Offences concerning child pornography” advises parties to “take the necessary

15 Unveren, ibid.
legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised: a) producing child pornography; b) offering or making available child pornography; c) distributing or transmitting child pornography; d) procuring child pornography for oneself or for another person; e) possessing child pornography; [and] f) knowingly obtaining access, through information and communication technologies, to child pornography.” The same article also has an exemption for the final paragraph (f) that “Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f.”

On 10 November 2010, Türkiye signed the Council of Europe Convention of Cyber Crimes, CETS No. 185, and opened for signatures in Budapest on 23 November 2001 but has not yet ratified the Convention as of 17 July 2013. The convention is considered to be the first international treaty regarding crimes committed through the Internet and other computer networks and focuses on violations of copyrights, computer-related fraud and forgery, child pornography, and interception of computer networks and information systems. Convention CETS No. 185 also specifies criminalized actions for the above crimes in Convention CETS No. 201, except paragraph f (further are exceptions stipulated in Article 9/4).

The term child pornography, the Convention notes, shall include pornographic material that visually depicts a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; or c) realistic images representing a minor engaged in sexually explicit conduct. According to the Convention, minor means all persons less than 18 years of age (or less than 16 years old, if a signatory

---

party requires a lower age limit).\textsuperscript{17}

Türkiye is also a signatory of United Nations Convention on the Rights of Children dated 20 November 1989. Türkiye signed the convention on 14 September 1990 and ratified it on 4 April 1995 with reservations.\textsuperscript{18} Formerly known as SHCEK, CHGM is the coordinating department in Türkiye assigned to follow up on issues relevant to the Convention. Together with other related departments and institutes, the first report issued by the department was submitted to the UN Children’s Rights Committee in 1999, and the Committee issued its evaluations of the report based on Article 44 of the Convention.\textsuperscript{19}


In their evaluation based on the submitted report, the Committee expresses its contentment with the amendments in the Turkish Criminal Code in terms of new effective provisions that specify child trade, prostitution, and pornography. But the Committee emphasizes some missing items and gaps in the national legal framework regarding Internet child pornography, and suggests new legal provisions that specify the crime in order to empower the legal system in combating these crimes. It also stresses the importance of Türkiye's submitting to the Council of Europe Convention of Cyber

\textsuperscript{17} "Convention on Cybercrime Cets No.: 185." http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=19/07/2013&CL=ENG.
\textsuperscript{20} United Nations Treaty Collection, ibid.
Crimes, which opened for signatures in Budapest on 23 November 2001 and the Council of Europe Convention on Action against Trafficking in Human Beings, which opened for signature in Warsaw on 16 May 2005. Türkiye signed both Conventions; however, as of 17 July 2013 neither have been ratified.

EFFECTIVENESS OF POLICING CHILD PORNOGRAPHY

Beside the complications involved with blocking Internet content, which is essentially a preventive measure of policing, Internet content presents significant challenges to prosecution efforts. Rather than looking at all kinds of crimes and their prosecution, this study focuses on child pornography on the Internet and its prosecution.

Different from most of the other types of crimes and their punishment, there is a broad international consensus on defining child pornography as a crime and having legal punishment against offenders. This study has analyzed digital files, each of which is opened as a specific file for different child pornography cases in Interpol Ankara.

Interpol is the second biggest international organization after the United Nations in terms of members. Each country has its own National Central Bureau or NCB to coordinate cooperation between national units with foreign units in criminal and policing issues.

Unveren conducted a descriptive study about child pornography in his Master’s dissertation. Based on records from the Interpol Department in Ankara, Unveren notes that there are a total of 136 cases between 1999 and 2006 and 85 files in 2007, 128 files in 2008, 51 files in 2009, and 5 files in 2010 (up until January 22, 2010). The average

---

21 Unveren, ibid.
22 Ibid., 31. (This study has found two duplicate files that means totally 83 new files opened in the year 2007)
number of cases opened in each year for the past ten years (between 1999 and 2009) is about 40 files.

According to Aydin, the first known arrest resulting from an Interpol request was conducted in Konya, Türkiye in 2000, but the suspect was released on bail. Unveren’s study was important to understand the transnational aspects of the crime. However, Unveren did not go in depth to explore the details of the investigations, their results, problems, or other barriers in these files. Focusing on the files of specific cases initiated in 2005, 2006 and 2007, this study presents readers with more details of these investigations. Rather than looking at specific successful cases, it analyzes all cases to see the overall picture regarding these investigations.

Internet child pornography here covers any crime against minors committed on or through the internet and internet applications such as messengers with webcams, file sharing applications, or email. The study excludes files that include other kinds of sex crimes against minors such as illegal detention, child marriage, rape, harassment, or peeping. These non-Internet crimes are specified below for each year. This study likewise does not include non-operational messages sent only for information, fingerprint or criminal record checks, or address or language errors.

Analysis of 2005

Records in the digital archive show that 31 new Internet-based child pornography files were opened in 2005. Not all these cases are operational, i.e. resulting in a request of police and legal action. This study excludes those cases which are non-operational and thus irrelevant for this study. In 2005, 13 cases were considered non-operational since

23 Ibid.
these files may include criminal background check for a person, general information
inquiries from Interpol departments, or wrong addresses.

As for operational cases, among the 31 case files, five cases were the result of
requests for police and legal action from foreign Interpol Bureaus (outgoing requests).
Thirteen cases were incoming requests from different national Interpol Bureaus for police
and legal action.

Most of the requests, both outgoing and incoming, involve websites established to
host child pornography on their servers, or have links to pornographic images. Each case
may concern a single website or more. Besides police departments, these requests may
came from the legal units of any Interpol member country. Interpol uses its secure
communication system for transmitting these kinds of messages. Requests include all
available details from the websites, their domain names, web address, IP numbers, crime-
related photos, videos, and other technical details about the servers. Investigation requests
for legal or police action may only be addressed to one or more NCB as well as to the
General Secretariat in Lyon, France.

Outgoing requests

Outgoing requests have been addressed to a number of NCBs, including
Germany, Australia, the United States (three times), Russia (twice), Portugal, France, and
in one case to all Interpol NCBs. These requests include some web pages determined to
be hosting or distributing child pornography and have servers registered abroad, such as
in the country where the NCB is located. Cases were initiated by two units in Türkiye, the
local police of Ankara, and the Police Department of Public Order. Checks made of text
documents reveal that no results could be achieved in five cases.
A complicated procedure of "rogatory commission"

In one case, Interpol Washington requested a rogatory commission (a detailed judicial file and documents about the case and requests sent through a diplomatic channel) for the investigation in Türkiye. Preparing a rogatory commission for a transnational case is a complex task that is both a time- and resource-consuming procedure. Political and diplomatic tensions among countries involved in such cases may prevent these procedures from proceeding further. Time is very much a concern for any judicial investigation, but more so for crimes committed on and through the Internet. By the time the judicial file is prepared and translated into the language of the address country, the subject website or records could be deleted, moved, or changed.

Different legal systems among the countries are another barrier for initiating such a procedure. Even when a judicial file is prepared and translated into the language of the target country, it is not always guaranteed that all requests in these files will be admitted by the judicial authorities of the addressed country.

In some cases, a rogatory commission is requested after the first immediate police action is conducted, but it is not a prerequisite for police or legal action. In such a situation, as seen in successful cases from 2005, suspects may be identified and evidence could be collected before they disappear or are deleted.

While in some cases, investigations were about a single website, in some others a number of websites were subject to inquiry. For instance in one case, investigations for five websites were addressed to three Interpol NCBs (Portugal, Russia, and the United States). Another case regarded a website sent only to Interpol United States. Unfortunately, there were no results established in digital files for these cases. Paper-based files of these digital files may include insignificant replies from Interpol NCBs. But
the absence of these writings in the digital archive implies no legal or police action could be achieved based on the requests of Interpol Ankara.

Incoming requests

There were 13 operational incoming requests (cases) received in 2005. That year incoming requests exceeded outgoing. Among them, only three of the investigations conducted in Türkiye resulted suspects being identified and transferred to the judicial authorities.

For the other ten cases, no results could be achieved. In four of them, the information submitted was insufficient to conduct investigations in Türkiye. In this situation, further information was requested back from the original Interpol Bureaus. However, no messages were recorded back from these countries to further the investigation in the country. The other six files were notified related units. Non availability of further information in these ten files imply no significant result could be achieved in none of them.

Successful cases

Three cases in 2005 were investigated successfully, and suspects involved in these reported cases were identified or brought before judicial authorities. The first case regarded a message from Interpol Madrid about a suspicious IP address distributing child pornography. This request was sent to local police in İzmir, Türkiye, and all details and investigations conducted in İzmir established the user and owner of the IP number. After receiving court permission, local police in İzmir conducted a search of the suspect’s
home and computer. He was transferred to court but released afterwards when no evidence found.

In the second case, the initiator of the investigation was in the UK and concerned emails sent to an underage adolescent from an email address in Türkiye. One or more individuals was suspected of sending explicit sexual images and photos to teenagers in the UK. The request from Interpol London was sent to local police of Zonguldak, Türkiye with copies of images from emails and the details of IP numbers and emails attached. Local police identified two suspects and transferred them to the Prosecutor’s Office in Zonguldak, Türkiye. The file shows that the Prosecutor’s Office requested a rogatory commission from competent authorities of the UK for the case.

The third case was from German Interpol and involved two teenagers aged 14 and 15. Some pornographic images and photos were sent to these teenagers from a person they while they were chatting on the Internet. Based on available email addresses and IP numbers submitted to Interpol Ankara by German Interpol, local police in Aksaray were notified, and the suspect was identified. The file shows that the Prosecutor’s Office requested further details of the investigation with a rogatory commission from German authorities through diplomatic channels.

Unsuccessful cases

All of these ten cases concerned websites containing photos and videos of child pornography or have links to other websites with similar content. These requests were from Ireland, Germany (five cases), Spain, Finland (two cases), and Portugal. These requests received from outside Interpol Bureaus were sent to competent bodies in Türkiye along with images and records of the crime with other technical details.
Many IP numbers from different countries involved

In one case, Finland Interpol had a request in which 78 different countries were involved. Based on an investigation conducted for child pornography in this country, about 2,200 IP numbers were established to have some kind of connections with a suspect being prosecuted in that country. Since some IP numbers notified by Finland Interpol were from Ankara, Türkiye, local police in Ankara were provided with all the details of the case accordingly. So far the result is unknown. Likewise the result for Finland is not in its file.

Lack of necessary information, date and time problems, internet cafe involvement

Among the ten cases in this situation, it is apparent that for some cases, ambiguities about the time and date of the investigation conducted by the initiator of the investigation abroad was the main reason to launch further investigations in Türkiye because Internet cafés were involved in the commission of the alleged crime. For four cases of the ten, competent bodies in Türkiye informed the Interpol Bureau in Ankara that further information was needed to conduct investigations in Türkiye. In these four cases, Interpol Ankara requested additional information (IP numbers, further crime details, and available material) from the Interpol office originating the investigation. No response from foreign Interpol departments is available for these four cases, nor is a result known in their file.

For the remaining six operational cases, no necessity or reason is reported and available in their files. Overall, no positive results could be achieved for ten operational cases.
Analysis of 2006

The number of cases in 2006 was 33. Among the cases in that year, five were initiated from Interpol Bureaus outside of Türkiye (outgoing requests) for police and legal action. Incoming requests, on the other hand, were 28—more than in the previous year. Among them, 21 cases were operational, resulting in a request for police and legal action. The other seven include non-operational files and other kinds of sexual crimes against minors, as explained above.

As with cases in the previous year, most of the requests (both outgoing and incoming) in 2006 concerned websites determined to be hosting pornographic records, images, or photos involving children, or have links to such websites. Cases may concern one or more websites. Requests may come from legal units, courts or prosecutor’s office in any Interpol country, as well as police departments.

Outgoing requests

Outgoing requests in 2006 were addressed to Interpol Bureaus of the United States (three), Germany, Canada, the UK, Slovakia, Mexico, the Netherlands, Poland, Australia, Sweden, Denmark, Uruguay, Russia, and Czech Republic in five different cases. All the cases requested to be investigated in these countries concerned websites registered in or connected to servers located in these countries. Sometimes servers, registration, or other contact details of a website may refer to one country or more countries. Cases from 2006 were initiated by two local police departments, in Ankara (four) and in Istanbul (one).
Many countries involvement

Like cases in the previous year 2005 for outgoing requests, no significant results could be achieved in these cases either. Among them, one case was interesting to note here since twelve different countries were involved. The case was about a web-site which was hosting child pornography on two domain addresses registered or has servers abroad. The request was to conduct simultaneous police operations against the registered addresses of these websites in different states. Based on legal and technical reasons, no country responded to Interpol Ankara expressing willingness to join a police operation. While US Interpol responded that material submitted to them was not enough to initiate such an action, Polish Interpol mentioned technical barriers for such an operation. Uruguay Interpol responded that they will join such an operation after their initial investigations. Digital files of this case also show that language barriers (especially in the attached documents which include technical, registration, and log details), time zone and date differences, as well as address errors, were the subject of message trafficking in the case. Only UK Interpol responded, stating that based on a request from Interpol Ankara, they had conducted investigations in the UK of related IP numbers but could not find individuals who accessed or downloaded records from the websites in question.

For the other four outgoing cases, a number of websites have been reported to the related Interpol Bureaus by Interpol Ankara. However, no success could be achieved in these cases.

Incoming requests

There were 21 operational requests (cases) received in 2006. In six of them, investigations conducted in Türkiye were successful in identifying suspects or in bringing
them before the judicial authorities. However, for fifteen cases, no significant result could be achieved according to the digital archive.

Lack of necessary information

Out of fifteen cases, four contained files that seemed to hinder further investigations in Türkiye. In three of those four cases, crime subject records such as videos, photos, and chat and email records were missing. For one case, technical and registration details of the website and IP number were missing. In all four cases, requesting NCBs were notified by Interpol Ankara requesting further documents and necessary information. In some cases, related NCBs responded back to Interpol Ankara that they had no further information or records. In others, no response was provided for the requests for additional information.

For the other eleven operational cases, information as well as all available records and documents were sent to competent bodies and local police in Türkiye. However, no replies in these files show significant results. Regardless of whether there were reported reasons or no replies available, no significant results could be achieved in these cases according to their files.

Successful cases

Half of the six successful cases in 2007 were related to investigations in the Netherlands. On behalf of Interpol The Hague, Interpol General Secretariat (IP SG) in Lyon, France notified all NCBs in a diffusion message to all member countries that monitoring of some websites hosting child pornography revealed that approximately 2,800 IP numbers were detected accessing these sites and downloading child
pornographic records from these sites. IP SG requested all related NCBs to make appropriate investigations of these Internet users from several countries. The operation was called Operation Balendo.

Interpol Ankara checked the IP numbers and found that 387 IP numbers came from Türkiye. Interpol Ankara informed the Department of Public Peace and Order, the competent body in Türkiye, about the case and submitted to them all available documents, a CD, passwords, and details of IP numbers received. Following investigations in Türkiye, users and owners of eight IP numbers were identified and transferred to the judicial authorities in Istanbul, Ankara, and Antalya.

In an operation called Operation Lancer, investigators revealed that the case prosecuted in the Netherlands had connections to Türkiye. Interpol The Hague informed Interpol Ankara about these suspicious IP addresses and submitted all available documents for appropriate legal action. Based on this request, competent bodies in Türkiye conducted investigations in seven different cities. In the end, four persons were arrested in four different cities, Hatay, Burdur, Mugla, and Canakkale. Some evidence was detected in the computers of the other persons in Istanbul, Kriklareli and Mersin, but they were released on bail.

Again in another operation in the Netherlands, IP addresses and copied records and images submitted by Interpol The Hague were checked and investigations initiated in Türkiye. At the end of the investigations, the users and registered owners of the IP numbers were identified in Usak and Denizli in Türkiye. While no evidence could be detected in the investigations in Denizli, the perpetrator was identified in Usak and he or she was arrested by judicial authorities.
In another case, Interpol Vienna informed Interpol Ankara that 22 IP numbers from Türkiye were detected while they were purchasing pornographic records from a website. Since some information and documents were missing, Interpol Ankara requested additional documents and information from Interpol Vienna. Later Interpol Ankara received all available information to initiate an investigation in Türkiye. The case was called Operation Flo, and it was transferred to the Department of Public Peace and Order for investigation and action. For eleven IP users, no evidence could be found to charge them before court. For the other eleven IP numbers, investigations revealed some child pornographic images and other kinds of evidence to bring them before judicial authorities. Although the prosecutions regarding the case were reported to be ongoing, the suspects were released on bail.

In an operation called Smasher, Interpol Wiesbaden requested appropriate investigations against some IP numbers from Interpol Ankara that were suspected of dealing in child pornography. The Department of Public Peace and Order received the case with all CD and documents from Interpol Ankara, and they identified 53 Internet users of the IP numbers in 21 different cities in Türkiye. For 25 users, no evidence could be detected to bring charges against them. Sixteen other users from different cities were arrested. In computers of ten of the users, illegal content was detected. The accused were released on bail by judicial authorities. Because two IP addresses were used in internet cafés, users of these two IPs could not be identified.

Interpol Canberra informed Interpol Ankara that while using a chat program, a minor female received inappropriate sexual images from a person whose email address and IP numbers were originating from Türkiye. The case was transferred to competent
bodies in Türkiye. The perpetrator was identified in Denizli, and a judicial proceeding was initiated against the person, who was arrested.

Unsuccessful cases

These cases were basically about websites hosting photos, videos of child pornography, or have links to other websites with similar content. While German Interpol had four investigation requests, Spanish Interpol had three requests from Interpol Ankara. All of these investigations concerned websites and IP numbers linked to marketing, distributing, or otherwise involved in downloading child pornography. Italy sent a message about a website registered in Türkiye. Likewise Swiss, Dutch, and Polish Interpol Bureaus sent requests about IP numbers in Türkiye to be investigated. In only one case, which was from Germany, the investigation was concerned with the use of a chat program. Checks on these files found no significant information, which implies negative results for these cases.

Analysis of 2007

The highest number of cases opened was 83 in 2007—more than in 2005 and in 2006. Among the 83 documents from 2007, fifteen cases were operational requests from foreign Interpol Bureaus (Outgoing requests) for police and legal action.

Incoming Requests totaled 69. Among these incoming requests, 52 cases were operational, involving requests for police and legal action. Among the incoming cases, eight cases were considered non-operational, and nine cases concern other kinds of sexual crimes against minors.
Outgoing requests

Total outgoing requests in 2007 numbered 14. These file requests were sent to Interpol Bureaus in the United States (five times), Germany (three times), Panama (three times), Russia (two times), the UK, Holland, Canada, Saudi Arabia, and Vietnam, and copied to the Interpol headquarters in Geneva (seven times only for information). Most of these requests called for investigation of websites determined to be hosting child pornography. In addition, two cases involved a video sharing web application, rapidshare.com, through which child pornography was claimed to be uploaded or downloaded. In one case, an email account was used for the same crime. Cases in 2007 were initiated by local police in Ankara (four cases), and Istanbul (six cases), by the Department of Public Peace and Order (two cases), and by judicial authorities in Türkiye (two cases). In two cases, Interpol Ankara received responses requesting that investigations not continue. National units dealing with these two cases were notified about these messages and any additional details requested by foreign Interpol Bureaus. In the other twelve files there are no responses.

Time and date barrier

One of the cases concerns a file-sharing website. The Prosecutor’s Office in Ankara established that a link for a child pornography file was uploaded and shared on this file-sharing website. The administration of the website had noticed the file and removed it from their servers. Submitting all available information including date and time of the uploaded file, Interpol Ankara requested that German Interpol identify the user who uploaded the file by submitting all technical details of the uploading including IP number, user name, and sign-up email address. However, since the file was removed
and deleted by the website administration. Interpol Wiesbaden informed Interpol Ankara that it was not possible to have the file again.

Transnational involvement and rogatory commission

The other unsuccessful case involved marketing a sex video of a child victim on the Internet. Based on inquiry by judicial authorities in Türkiye, Interpol Ankara requested from a number of NCBs and IP SG to assist in identifying the victim in the photo. Interpol Ankara also requested that Interpol France identify the IP number of a suspect whose email address was known. German and Dutch Interpol Bureaus and IP SG were not able to identify the child in the photo. Canadian and US Interpol replied they could not compare and check the video in their records. Interpol France responded that the IP number belongs to an Internet Service Provider (ISP) in their country, and a rogatory commission about the request for the case was necessary to further investigations in France.

In the other twelve cases, a number of websites were subject to inquiries from foreign Interpol Bureaus. All of these cases were reported to the related foreign Interpol Bureaus with all available information and documents, including recorded photos, videos, or other kinds of digital files on CD or DVD, domain addresses, IP numbers, the original Internet Service Provider (ISP), and other contact information (postal addresses, phone numbers, and email addresses). These Interpol Bureaus were asked to make appropriate investigations and notify Interpol Ankara of their results. However, no significant response or result has been received or achieved so far in these cases.
Incoming Requests

Total incoming requests in 2007 were 69. Among them, 52 cases concerning child pornography on the Internet were operational and resulted in requests for appropriate police or judicial action. While eight cases were non-operational requests, nine cases in 2007 involved other kinds of sexual crimes against children.

Among the 52 operational cases, only nine cases resulted in significant success in identifying suspects and transferring them to judicial authorities. For the remaining 43 operational cases, no significant results could be achieved. Among the 43 cases, in six cases, there were reasons and barriers mentioned in the digital archive that investigations could not be furthered. For the remaining 37 cases, no result or a reason was recorded in the files.

Successful cases

Interpol London notified Interpol Ankara that an email address and phone number from Türkiye were found to be related to an investigation against child pornography in the UK and submitted eight pages of details of the investigation to Interpol Ankara. It was easy to identify the subscriber of the phone number in a province of Türkiye, but the person was not the user of the email. Based on information supplied by the subscriber of the phone number, the user of the email account was identified. Checks by local police revealed such photos and records in the person’s computer. He was transferred to the public prosecutor’s office, and released afterwards.

A nine page message attached with a CD sent by German Interpol stated that one IP number from Türkiye was downloading crime related records from the video sharing websites FrostWire and BearShare. The department of Interpol Ankara conveyed the
message to the related department and local police. The user of the IP number was identified and traced to Karabuk. The person was interrogated by the police and stated that he was just storing these records but not distributing them. He was transferred to the public prosecutor’s office and released afterwards.

In a message from Interpol Canada, it was stated that an 11-year-old child was chatting with a person from Nevsehir, Türkiye. The person gave the victim his phone number and wanted to take a photo and recording of her while chatting. Local police in Nevsehir established that the phone number belonged to another person who denied knowing either the perpetrator or the incident. No judicial action is known in this case, although the alleged persons were identified.

Another criminal investigation of a chat program was reported by Interpol London to Interpol Ankara. Identifying himself as the teenaged victim’s cousin, an individual requested photos from the victim. Later the individual began blackmailing the victim and requested more naked photos. Interpol London submitted all available information about the case, the blackmailer’s IP number and other available details. The offender involved in this case was identified and traced to Kocaeli, Türkiye. Checks of the person’s computer found inappropriate photos and recordings. For further judicial proceedings against the person, Interpol Ankara requested judicial documents from Interpol London through diplomatic channels.

Providing a CD, protected with a password, Interpol London identified criminal proceedings in their country to Interpol Ankara against child pornography. Based on information and records submitted by Interpol London, Ankara police investigated and identified seven persons. They were transferred to judicial authorities and released afterwards.
In a similar case, reported by German Interpol, a person was arrested by judicial authorities but released afterwards.

Another similar case was reported by Interpol Austria. Investigations were conducted based on submitted IP numbers, CD, and other available information in Türkiye. Thirteen suspects were identified and transferred to judicial authorities. While two of them were arrested, the others were released.

In a message from Interpol London, it was reported that on a website, a person whose nickname and email account is known was trying to incite underage girls to pose on a webcam and provide their email addresses. Interpol London submitted all available records, dates, and times of the incidents, as well as the IP numbers of the user. Interpol Ankara conveyed this information to related departments. The user was later identified, and a lawsuit was initiated against the person. He was released, but prosecution was ongoing without arrest.

Interpol Canada notified Turkish authorities that from an email account, naked photos and video recordings of an underage girl of 15 were sent to an individual’s email address in Canada. After the given information was submitted to competent bodies in Türkiye by Interpol Ankara, the user of the email account was identified. He was transferred to the prosecutor’s office. He was released, but the prosecution against him was on-going at the time.

No results cases

As stated above, except from nine cases (out of total 52), in 43 operational cases, no significant result could be achieved. Among these 43 cases, in six cases, some reasons are reported and known which may hinder investigations. For the other 37 operational
cases, investigations by competent bodies in the country revealed no significant result. If we look at negative cases resulted because of some barriers, we see the following cases:

Problem of Internet café and date-time of the crime

Interpol Hong Kong reported to Interpol Ankara that a person on a web-cam showed some sexual behaviors to a girl and sent some sexual pictures to her email account. Based on given IP number by Interpol Hong Kong, investigations conducted in Türkiye established that the IP number belongs to an internet café. Since the date and time of the crime is not clear it was impossible to check all the visitors of the internet café and establish the perpetrator(s) in this case.

Corporation barriers (email account)

According to information received from Interpol London, a person showed some inappropriate sexual behaviors on MSN while chatting with a teenager, aged 12. Investigations in Türkiye checked the person’s email account and IP number but no useful information could be received from Microsoft Corporation. Because of that, no further proceedings could be carried out by authorities.

Problem of dynamic IP numbers and date-time of the crime

Interpol Poland submitted a DVD and all available information in their hand regarding an investigation in their country against child pornography on the web. They submitted a number of IP numbers as well as all documents of all technical details of web pages. Investigations by competent bodies in Türkiye found that submitted IP numbers are dynamic which can be used by different persons on different date and time. Thus,
missing information such as the accurate connection time period of IP numbers, connection date and time details hindered investigations to proceed in Türkiye. Moreover, the attached document's language received from Interpol Poland was another problem since they were in the Polish language.\(^{24}\)

Likewise, Interpol Belgium sent an investigation request to Interpol Ankara about an email that included child pornography. Because of lack of information about date and time of the crime reported, no investigations could be carried out in Türkiye.

Lack of information

Canadian Interpol notified a number of other Interpol National Bureaus that investigations in their country established that one person was distributing and sharing images of child porn with 56 users within Canada and 576 other user/person(s) from 42 different countries. It was reported that three were from Türkiye. Investigations could not be furthered because of lack of information such as IP numbers, online time(s), and the number of downloaded files.

The complicated procedure of rogatory commission

Interpol London notified a criminal investigation in their country about hacking email accounts of nineteen females, some of whom were teenagers. Attracting them on MSN, an unidentified person insisted victims visit a web-site of his where he hacks MSN user names and passwords. He was blackmailing them to make a 20-minutes show before a web-cam. Otherwise, he would give these accounts to terrorists or other sexual

\(^{24}\) Each Interpol member declares which official language of the General Secretariat is/are accepted in its national bureau. Interpol Ankara accepts English and French.
criminals. Some of victims accepted the person's demands. In this way, the person could also access other friends of victims as if he is her and asked similar demands from them. Interpol London also submitted two pages of IP numbers and log details of these connections. Because this case was very broad and required an extensive investigation, Interpol Ankara requested from Interpol London to send a rogatory commission through diplomatic channels. The result of investigation is unknown (not reported) in its digital file.

Analysis of cases between 2005-2007

As seen in content analysis of digital files of 2005, 2006 and 2007 opened in Interpol Ankara, investigations of internet child pornography are significantly problematic for law enforcement agencies. Among the operational incoming messages of 86 cases in these years, only 18 of them could be considered as successfully solved, i.e. suspects are identified and/or brought before judicial authorities in Türkiye. This is about 20% of all the operational incoming messages.

In about 80% of all operational incoming messages, which is 14+54=68, investigations could not reach a significant end. While in fourteen files there were some kinds of technical, legal reasons known for not furthering investigations, 54 files are seen not be able to reach a significant end with no known reason given in the files.

As for outgoing investigations, among the 24 operational investigation requests from foreign Interpol departments, none of them shows that investigations abroad reveal a significant end, i.e. suspects are identified and/or are brought before judicial authorities. While four cases among them have some reasons for not being able to conduct
investigation in related countries, the other 20 files do not contain any information about the conclusion or progress in the countries requested.

This unpleasant situation for outgoing investigation request is also seen in Unveren’s study. Although he gives examples of some successful cases and investigations in Türkiye based on requests received from foreign Interpol Bureaus, no successful investigation is known abroad based on information and request by Interpol Ankara. Thus, prosecution efforts of authorities particularly in internet child pornography are not promising either as seen in this chapter.
CHAPTER VII
RESULTS, CONTRIBUTIONS, AND WEAKNESSES

RESULT OF EACH ANALYSIS

Research Question 1: To what extent do blocking measures on the Internet effectively prevent access to undesired websites and web content? As seen in previous sections, internet access blocking efforts by authorities are not very effective at preventing people access to undesired websites or web contents in Türkiye. The first pages of the all tested blocked websites are accessed by using one of three circumvention technics tested in this study, i.e. Tor, Ultrasurf and Ktunnel.\(^1\) Most of the blocked websites can be accessible through the circumvention methods tested here. The percentage of successful access to the blocked websites with the use of Tor is some 71% and this can reach up to 85%, if the results with “partly possible” are also considered as successful access. The percentage with the use of Ultrasurf is 69%. If the five websites for which the tool does not support are also excluded from the sample size for Ultrasurf, the percentage of successful access for this tool reaches 88%. The percentage of possible access with the use of Ktunnel is the lowest as 40%. If the ones which are evaluated as “access partly possible” are also considered satisfactory, this percentage reaches 72%. The numbers of websites which could not be accessed through each method are 2 sites for Ultrasurf, 6 webs for Ktunnel, and 3 for Ktunnel.

Second, there is always a risk of over blocking or under blocking error as explained in related sections. YouTube case shows both examples of over blocking as

\(^1\) If one circumvention tool tested in this study is not successful, any of the other is able to access for all blocked websites except from the three ones which are specified as excluded in the text.
seen in the errors of access blocking to some Google services like Google Translate, Google Analytic. This case also shows how this measure can be un-proportional by blocking access to the entire website because of a few undesired records although the website is hosting millions of video records and has millions of users for different purposes all over the world.

Finally, access blocking is not effective because of the fact that it does not remove the undesired website or web content from the internet. Blocked websites which have audience within the borders of blocking country can still be online outside national borders by changing their domain addresses with different extensions, suffixes, and/or by using different servers abroad.

Research Question 2: How effective are the police in identifying, tracing and bringing criminals involved in child pornography before judicial authorities? Like complications and gaps seen in blocking measures, significant problems are seen in investigations of child pornography on the Internet. Since Internet child pornography is very much a transnational crime, analyzing investigation files opened in an Interpol department, i.e. Interpol Ankara presents a good picture of transnational aspect of investigations regarding child pornography. The analysis of these files presents a clear picture about the research question since just focusing on data of a national unit for any cybercrime will give only one dimension of such a research question regarding prosecution. Analysis of transnational data as utilized in this study however covers both the efforts of national units in prosecution as well as those of foreign units. This coverage should be an ideal analysis since the internet is global and transnational in structure.

---

From this view, this study is unique to analyze a cybercrime like internet child pornography based on data of Interpol Ankara.

A number of international conventions by the United Nations and European Commission condemn different forms of child abuse along with child pornography, and recognize them as crime to be punished. Moreover, people's awareness and sensitivity on crimes against children is very high all over the world and authorities give special importance when a minor is the victim of such a crime. Thus, to enlighten this nasty crime and identify perpetrator, it is expected that each policing unit dealing with such kinds of investigations is more elaborative and cooperative with the investigating units, either at home or abroad.

However, as seen in section VI.B, most of the operational investigation requests about child pornography on the Internet end up without a significant result. Among the 86 operational incoming investigation requests came to Interpol Ankara in-between years of 2005 and 2007, in only 18 cases perpetrators are identified and/or transferred to the judicial authorities. In 68 cases, investigations reach no significant ends. This implies that among the reported operational incoming cases about child pornography, only 20% of them could be solved, whereas in 80% of the cases investigations reach no result.

Worse is seen for outgoing requests. Interpol Ankara conveyed 24 operational investigation requests to foreign Interpol Bureaus between 2005 and 2007. However, significant result could be achieved in none of them. Although in four cases, there are some extra message traffics between Interpol Ankara and other related Bureaus, these cases could not be solved either.

One of the important contributions of this study is the access and the analysis of

---

the files in Interpol Ankara. Examining the crime based on data of such an institution presents a broader perspective and covers all possible failures or incapability either at home or abroad. The result of this analysis confirms that the structure and characteristics of the internet complicates criminality in a significant way.

OVERALL ANALYSIS AND CONTRIBUTION

These findings, at least observed in two issue area are in parallel to the supporters of the independence claims of cyberspace, i.e. the internet is a new wine in a new bottle. Thus, traditional legal approaches and measures can become ineffective, and sometimes meaningless as seen in this study for Türkiye. There are a number of reasons which support such assumptions including the size and types of internet use and internet applications, the unique structure of the internet, the anonymity of the actor acting within the virtual platform and availability of variety methods to protect anonymity thorough covering, changing or manipulating.

The volume of the internet, the size and types of internet applications and internet activities cannot be compared with those of the previous media and communication devices. According to netcraft.com, the registered web-sites numbers in the most popular servers like Apache, Microsoft is 312,693,296 between August 1995- April 2011; and among them about 110,000,000 are considered active.4 Web-page numbers are more than billions. According to worldwidewebsize.com, at least 14.42 billion pages are known by The Indexed Web. While Google has indexed about 35 billion pages, 10.7 billion pages

---

are indexed by Yahoo. In some open resources, the number of webpages is estimated to exceed 600 billion.

In their diagram, The Intel Corporation shows that while 30 hours of video uploaded on YouTube, 1.3 million videos are being viewed in one minute on the same site. Over two million of search performed on Google and 204 million e-mails sent on the internet in sixty seconds. While 277,000 users are logins on Facebook, 6 million views are realized on the website. About 320 new accounts open on Twitter in one minute and users send about 100,000 tweeter messages. The number of networked devices is equal to the world population now (as of 2012) and will be double of the global population by 2015.

A website further notes that “60 new Blog account, 1500 new Blog post; 70 domain name registered in one minute.” A news indicate that “6150 hours of Skype conversation, 11 million having online chat, 2 million watch pornography, 12 website hacked among 416 attempt in 60 seconds.” Thus, it is very much complicated, difficult for nation states to control this huge size of image, data, record, link etc., though not all of them may concern them.

Looking at the blocking practices of Türkiye in the view of this enormous size of the internet, it can be seen that there is huge gaps between the number of available undesired websites on the internet and the number of similar websites blocked by Turkish authorities, particularly the TIB. The most internet blocking cases in the country based on

5 Maurice Kunder, "The Size of the World Wide Web (the Internet)," www.worldwidewebsize.com/.
6 Kevin Kelly, "We Are the Web," Wired, August 2005.
9 “İnternette 60 Saniyede Neler Oluyor?” Timeturk, 24 March 2012.
the law no: 5651 are seen against pornographic and obscenity. As cited in Atamer, pornographic and obscene websites on the Internet was estimated about 4-5 million which constituted 12% of the total websites of the internet. In 2003, it was estimated that such kinds of websites were about 1.3 million and web pages were about 260 million. However, as of March 2012, total blocked websites were about 16 thousands. Considering the size of these kinds of websites on the internet with the ones that are blocked by the TIB shows a lot about ineffectiveness of internet access blocking. Nor the size of the internet activities makes impossible to trace or prosecute every perpetrator involved cybercrime, as for an example stressed by Edwards in child pornography incidents on the internet.

The unique structure of the internet is another challenge either for regulation or prosecution. The internet is a global network of networks which make it naturally transnational. It exceeds national borders and does not belong to any authority. An online internet user is a citizen of cyberspace and can share whatever she wants with anyone online from anywhere on this platform. Having an internet access makes an individual to have a chance to amplify his voice to the world, to access foreign agents or institutions without travelling and a valid passport, or to have shopping in a foreign retailer.

The innovation mentality of the internet was essentially founded on a risk of a nuclear attack and ensuring communication when one or more central nodes are targeted. This idea created the medium on a network structure in a mesh typology and this

---

structure force itself to ensure communication in a shortest and efficient way within the available links of the network. "The Internet was originally designed based on a decentralized network architecture, resilient to failure and disruption, the Internet is resistant to external attempts at control."\textsuperscript{14} Thus, this unique structure is not very well appropriate for filtering or internet access blocking. And through any node which is weak and appropriate for misuse, it is open to criminality and manipulation.

Another important challenge for traditional approach and state policing is the constantly changing nature of the internet and internet technology. The internet today is totally different from the internet in the 1990s. While the internet was only World Wide Web, and email was the primary option in those years, today we have many other internet applications like VoIP, Instant Messengers, Blogging, TV, radio, and we have many other innovations today running over the internet like smart phones, 3G/4G technologies.\textsuperscript{15}

The technologic developments and changes occur very often before authorities to respond and before it is widely being used by people. Law comes after technology and the diffusion of the technology use. Once authorities decide to act, they may become late or it becomes very much expensive for them to control, regulate and prosecute the problems with the use of internet or new internet applications.

Rather than authorities try to force the internet to be bordered, regulated, nationalized, or territorialized, they need to adapt their traditional state mechanisms and tools in accordance with the realities of the internet. The Internet requires a different legal mentally, administrative approach, political perspective.

\textsuperscript{14} Cormac Callanan, Marco Gercke, Estelle De Marco, and Hein Dries-Ziekenheiner, "Internet Blocking: Balancing Cybercrime Responses in Democratic Societies," Open Society Institute, 2009.
WEAKNESS OF THE STUDY: LIMITATIONS AND FUTURE PROJECTIONS

The internet has both negative and positive sides for users as well as for national authorities. This study focuses on negative sides and problematic dimensions of internet use for authorities. Referring the negative situations in the two issue areas explored here, it is not possible to come a conclusion that authorities are powerless in controlling the internet. Still, many dimensions from user side as well as authority side need to be explored to see the complete picture about many questions arisen with the use of internet.

The test of internet blocking and pay-passing methods conducted for this study is not performed in a lab environment by technical experts. It is performed by the author of this study who had no professional training or education on blocking or filtering technology on the internet. This fact, however, is considered not a major issue to change the results of findings in this section in a significant degree. Even, this fact can be considered as positive effect on the results since the study aims to see the real situation for ordinary internet users who are using the internet in their daily life with medium level computer knowledge and skills.

This section of the study does not cover people perceptions about the internet blocking and their reactions to such measures. It is important for future studies to research sociological aspects of internet blocking, their tendency to use bypass methods, and reasons for using such methods. Making similar studies in other countries with different regime type and technical capacity will make significant contribution to understand the questions explored in this study.

New terms emerged with the internet like social media, citizen journalism have become very influential terms today. The uses of specific internet applications like Facebook, Twitter have significant socio political consequences around the globe. With
the use of smart phones and 3G technology, people access to the internet becomes easier and questions emerged with the internet use has gained new dimensions to be explored in future studies.

For the second dimension of the study, it is an advantage of the author to have worked before in an official department which was also dealing with child pornography investigation in the national Interpol department. This section is not a unit which is directly conducting such investigations but an intermediary unit between foreign and national expert units. This may have no or little effects on findings and conclusions of this section. However, making such a study based on data and files of a first unit which is directly conducting such investigations will better explain the reasons behind the unsolved investigations.

The internet is relatively a new technologic phenomenon. It is very often a surprise both for people as well as authorities to see a new innovation compatible with the internet. Law and preventive measures by authorities comes after the uses of such innovations are diffused among people, and after having face to their problems in legal and socio-political realm. Looking at the spread, type, and effective use of the internet in the past two decades and considering the capacity of this new phenomenon, show that the internet will have a bold signature in a variety of fields in this century and bears a huge area of immature research potential for future studies.
POLICY IMPLICATIONS

Despite such kinds of technical ineffectiveness, states tend to try to control this global network of networks with its traditional power tools, and they should do so. However, while these traditional tools are being considered for use in administering and legalizing, authorities should be aware of the unique structure of this medium. For instance, a court order called for termination of all the activities of the offending website. This is not possible, as Minister Binali Yıldırım explains, because Turkish law is valid within Turkish borders not in other countries.

Having shifting from the industry age to the information age, the Internet seems to be the engine of the new century. It has merged communication, media and information on the same platform, which are the essential constituents of the modern life. As a nation-state, Türkiye should understand this new medium well and try to develop policies to maximize its benefit from. Rather than blocking, filtering, monitoring or the like, the country should focus on developing a better Internet infrastructure and service standards, promoting enrichment of national Internet contents, encouraging the use of Internet in better serving to its people, and finding alternative ways to ensure its contribution to the economic development.

On the other hand, if regulation and law making is necessary in this field, applicability of the law should be prioritized. Ignoring enforcement aspects of the each provision will have negative impacts on the effectiveness of the law as seen in the case of
At this point, adaptation of technocracy into all levels of public administration seems to be inevitable.

The Internet itself, its infrastructure, and all kinds of hardware, and software that runs the Internet, are very much technical and require technical expertise. Bringing and adapting technical perspective to these fields will minimize unforeseen complications, possible gaps, failures and maximize the effectiveness of public services. While for some managerial, administrative and auditing departments and positions in this filed should handed over to technocracy; investigating units like police and even prosecutors should be specialized. Proficient police units and prosecutors who have expertise should deal with cybercrime investigations. Like the technocracy in these executive departments and specialization in investigative bodies, technical expertise should be invited to the law making committees and their hearings.

A special institution regarding cybercrime was finally founded in 2011 under the National Police Organization, General Directorate of Police. Separated from “Department of Struggling against Smuggling and Organized Crimes” under “General Directorate of Police”, a new department was established as “Department of Struggling against Information System Crimes.” The same department has changed its name as “Department of Struggling against Cyber-crimes” in 20013. The department is relatively a new department and should immediately develop its personnel regime, their training, and if necessary, should open hiring civilian experts in computer science and information systems. It should establish national standards for sections in cities and should immediately support these sections to achieve national standards in terms of technical and

---

1 For applicability challenges of criminal laws on cybercrimes, see Deb Shinder, "What Makes Cybercrime Laws So Difficult to Enforce," TechRepublic, 26 January 2011.

INTERNATIONAL COOPERATION

The main functions of a state are ensuring security, safety and justice within the country. For ensuring security and safety, state officials first implement preventive measures, tactics and policies in order to stop criminality. If a crime is already committed, the primary duty of state policing and prosecuting units is to identify perpetrator(s), collect forensic evidences against them, bring them before judicial authorities, and ensure they are being prosecuted and charged if found guilty. In a broader context, this is the policing functions of any governing state.

As Murray notes, “It is extremely difficult and costly to enforce traditional legal and regulatory control systems within cyberspace, due to a variety of factors including a relative degree of anonymity, lack of physicality, digitalization of content, environmental plasticity, and international or cross border nature of the network.” 3 The example of Türkiye in this study confirms this perspective that traditional response tools of the government to control the Internet suffer significant gaps, complications, and insufficiency. These situations can be observed in the two main functions of the country, both in preventing and in prosecution aspects.

In terms of blocking, for instance, the operation and network structure of the Internet make blocking and filtering attempts problematic, and enable users to bypass these barriers through variety of methods and ways. At this point, it is better to remember the famous saying of John Gilmore: “The net interprets censorship as damage, and routes

---

around it."\(^4\)

In terms of prosecution, for instance, uncertainty of identity and location complicate law enforcement.\(^5\) Most of the time, criminals use different tactics, methods to hide their IP,\(^6\) manipulate their location, or “manipulate the bits and bytes, making it harder for law enforcement to trace.”\(^7\) As seen in this study, many investigations of Internet child pornography reached no results either by Turkish authorities or by foreign authorities. In some cases, IP numbers were not enough for Turkish authorities to identify and find the location(s) of perpetrator(s).

Beside these technical challenges at home, the global and transnational network structure of the Internet make the situation further complicated with political challenges. For instance, a blocked website and its content can easily find a server and hosting abroad. Criminals may shift or direct their illegal activities to the countries where technical and legal capacity are relatively low.\(^8\) Keeping in mind that cybercrimes are very much transnational and that law enforcement agencies are having serious challenges at home, they will face more challenges when these crimes are committed abroad.

Callanan et al. stress that formal requirements and slow responses for legal assistance among states very often block investigations. This is one of the important reasons for states to develop their own controlling instruments, like Internet blocking.\(^9\)

The Internet Service Providers Association in Europe also notes that Internet blocking is

---


\(^5\) Shinder, ibid.


claimed to decrease “political pressure” within the state to seek for international cooperation.\textsuperscript{10}

As seen in section VI.B regarding investigations of Interpol cases on child pornography, many cases reached no results because of formal requirements among states. Judicial authorities tend not to prefer this non-routine way since preparing a formal letter, called a “Rogatory Commission”, its translation, and sending through diplomatic channels are very time consuming, also require further expertise. Even after these are fulfilled, it is no guarantee that the case will be admitted to be prosecuted by judicial authorities of the requested country. Last but not least, whether the case will be developed, criminals will be identified or arrested is not clear, very often not likely.

Comparing to other issue areas in international relations, which the literature very often compares to maritime and airspace to evaluate international cooperation, cyberspace is a new and immature issue area in terms of international law and international conventions. A quick search on the UN Convention database for the key words of each area as maritime, aviation and cyber reveals that while there are 357 international conventions about maritime and 392 conventions about aviation, only two conventions came into force about cyberspace.\textsuperscript{11}

States need to change this situation and develop effective ways of international cooperation since many issues on the Internet are transnational. Beside technological


\textsuperscript{11} United Nations Treaty Collection, http://treaties.un.org/Pages/UNTSOnline.aspx?id=2. Separate checks for each word (maritime, aviation, and cyber) reveals the following: Maritime: Title search (options for match any of these words and for any treaty type – bilateral, open multilateral etc.), record count 357 (the oldest multinational convention’s conclusion date seen on database 12 September 1923; Aviation: Title search (options for match any of these words and for any treaty type – bilateral, open multilateral etc.), record count 392 (the oldest multinational – open - convention is Interim Agreement on International Civil Aviation, entry force date 06 June 1945; Cyber: Title search (options for match any of these words and for any treaty type – bilateral, open multilateral etc.), record count 2 (both multilateral; one entry into force on 07 January 2004, the other on 3 January 2006. A search for the word “cyberspace” reveals no results. A search for the word “cyber” reveals 2 results. A search for the word “airspace” reveals 8 results.
barriers, inability and complications either seen during the administrative stage or during the judicial stage, states should not exacerbate problems with physical borders. Despite different political and legal approaches to administering and controlling the Internet among states, they should try to find issue areas to have consensus on.

Especially for judicial prosecution of cybercrimes, as seen in this study for child pornography investigations, states need to minimize and standardize formalities in legal assistance requests among each other. And they should take measures to accelerate procedures in these investigation requests. The Interpol General Secretariat should explore alternative ways to increase effectiveness of international investigations about cybercrimes and child pornography, either at police level or judicial level, and should strongly recommend member states to follow these advices.

The General Secretariat should develop standard form(s) for cybercrimes e.g. that can be used for child pornography investigations. Well organized, comprehensible and standard form(s) should include what technical details are necessary, in which format as well as other important information and requirements for an effective investigation that can be conducted in any country. States requesting legal assistance, their competent authorities can fill this standard form with available information and can send it to the related country through Interpol Bureaus.

Another important issue regarding criminal investigations about cybercrimes is the anonymous feature of Internet use. Users can hide who they are and often where they are in their Internet activities in a number of different ways. The IP number is the primary clue that investigators utilize to reach the Internet subscriber, if the user did not use alternative ways to manipulate its IP number. Very often, as seen in child pornography investigations in this study, an IP number belongs to a public network, like a commercial
Internet café which is open to public for their temporary use.

As seen in section IV of this study about the numbers of Internet cafés, there are thousands of cafés (excluding other places open to commercial public use) spread all cities and provinces of the country. Although these places have positive effects in spreading the Internet use to every part of the country, increasing the Internet use and minimizing the effects of the digital divide within the country; these places should not be a center for criminal activities. Therefore, the regulations of Internet commercial use in public places should be revised and tightened. Likewise, their supervision and controlling should be more systematic and effective in order to prevent these places from being misused by criminals.

In order to increase effective controlling functions on the Internet to some degree, nation-states should explore more the ways of international cooperation on the subject of the Internet which has started to erode their sovereignty, and has become an inducing center for criminals. They should take measures to ensure that cooperation is faster and operating effectively since it is relatively more difficult to have traces of Internet activities and criminals when authorities do not react in time. Other than cooperation, states will be alone to handle all the transnational externalities of the Internet along with other technical barriers either for prevention or prosecution.

CONCLUSION

One of the fundamental values of democratic states is the rule of law and this value is also a must for a Turkish Republic that defines itself in its Constitution as democratic, secular and social state of law. The country's political, economic and legal transformation, partly thanks to the influence of European Union, has developed the
standards of democracy and human rights, and further institutionalized the law in recent years.

However, Internet blocking has negatively affected these positive developments and progress in these fields, and received serious critics both from home and abroad against the country. Despite significant questions about the technical gaps and apparent doubts about the effectiveness of blocking, insisting on such policies; receiving such critics at home or abroad and being classified within the countries of censorship by independent unions and NGOs, all harm these democratic developments and the country’s image outside the world.

The issue of Internet blocking was not a subject of criticism in annual reports of EU access negotiations with Türkiye, for instance for the years of 2007 and 2008. However, it was later started to be criticized in the report of 2009 under the title of “freedom of expression”, and in the report of 2010 under the title of “civil and political rights”.\(^{12}\)

The country accepts its citizens to apply the European Court of Human Rights (ECHR) under certain conditions and some individuals applied to the court against such kinds of blocking verdicts by different authorities for certain websites like LastFm.com and some Google sites.\(^{13}\) Likewise, an international NGO that monitors press and Internet freedom in the world, the RSF, classified Türkiye within the second category as “countries under surveillance” along with 16 countries like Russia and Australia.\(^{14}\) Thus,


the issue of internet blocking has opened up a new issue area for critics aboard, either in the EU or other international NGOs.

Reports prepared for The OSCE (Organization for Security and Co-operation in Europe) by Akdeniz indicates that the number of blocked websites are increasing dramatically and blockings which were rationalized with moral, cultural reasons are now seen with other reasons such as political, and religious. Moreover, he claimed that the transparency of judicial and administrative decisions tends to be weakening.\textsuperscript{15}

The examples of internet access blocking and how such policies are implemented clearly violates a fundamental democratic value of “freedom of speech” in the country,\textsuperscript{16} and endangers other important freedoms like freedom of communication and freedom of press.\textsuperscript{17} Today, even some countries including Estonia, Finland and Spain have admitted that access to the Internet is a fundamental human right for their citizens.\textsuperscript{18} Thus, maintaining such policies bears significant political risks for the country to be misused by any national or international actor.

Being a lawyer specialized on Constitution, Gedik admits that it is necessary to take legal measures against crimes on the Internet like child pornography, violence and inducing crimes on the Internet, but he insists that there needs to be principles of limits and proportionality while taking these measures. Once these measures exceed the purpose

of these principles, then blocking measures become censorship, which is unacceptable. 19

The situation reminds us what Callanan et al. stress in their study:

“The inevitable circumvention possibilities, under-blocking, over-blocking, mission creep, conflicts of laws and the problem that blocking leaves material online all mean that the issue at stake is not simply ‘to block or not to block’ but rather what blocking measures can be introduced that are proportionate and acceptable in a democratic society. As a result, it is crucial to review the legal and democratic challenges that Internet blocking raises.” 20

Showing examples of YouTube and Geocities.com, Yaman Akdeniz notes that in some of blocking practices, particularly the ones which are taken directly and independently (ex-officio) by prosecutors, judges, courts or Telekomünikasyon İletişim Başkanlığı (the TIB), it is not always possible to understand the reason for blocking. 21

Google Transparency Report indicates global statistics of content removal requests from national governments and Türkiye is the first country both with 9,610 items requested for removal by court orders and with 2,552 items by executive, police authorities between January and June 2013. While the second country in terms of items removal requests by court orders is the United States with 3,415, it is India for item removal requests by executive, police authorities with 672 in the same period. 22

Criticizing the law no. 5651 on the Internet, Gedik notes that “this law does not struggle against crimes but struggle against the Internet.” 23 Likewise, TUSIAD, the Turkish Industry and Business Association, one of the most influential associations in the country, criticizes blocking policies as legal but not legitimate (i.e. applicable under

---

20 Callanan et al., ibid.
23 Gedik, ibid., 123.
current law but not appropriate under ideals of universal law).\textsuperscript{24}

Koc and Kaynak also indicates the dilemma in the law that, Article 4 finds content providers as responsible under some conditions for the links given within the websites. However, they believe that it is very much difficult always to follow up and monitor whether all these links are addressing a legal websites due to fast and constantly changing nature of the Internet. They believe that this is because that the Internet is not exactly understood by policy makers. Likewise, lawyer Atamer stresses a similar difficulty that the second generation websites are open to instant messages and posts which puts content providers in a difficult situation constantly to detect each of these inputs. This difficult situation can be misused by bad intendant users. It can cause one website to close for the purpose of unfair competition.

The law no. 5651 proposes to ensure a safe and secure Internet, and to protect physical and moral healthiness of children. Because of filtering and blocking policies known by the public can lead families to leave children unattended with computer online or lead families not to use any personal filtering program. As Assoc. Prof. Leyla Keser stresses, the most effective prevention on the Internet is the user herself, "No public institution or organization can protect persons' rights and benefits better than themselves."\textsuperscript{25}

Analyzing filtering software like AOL Parental Controls, Cyber Patrol, Cyber Sentinel etc.; children's ISPs like Planet Kids and Kidz.Net.; filtered search engines Alta Vista, UK Plus, Yahoo; and filter functions of Internet browsers Internet Explorer, and Netscape Navigator, a web based research by which.net reveals that although these kinds

\textsuperscript{24} "TÜSİAD: Türkiye'deki Internet Yasağı Hukuk'a Aykırıdır," Haber2000, 4 March 2011.
\textsuperscript{25} "Herkes Kendi Güvenliğini Kendi Sağlamalı!", Ibid.
of filtering system are effective to some degree, parental guidance and supervision should not be ignored to protect children from "the net nasties." 26

Moreover, measures such as blocking and censorship are believed to be increasing individuals interests in such censored objects. Karaca and Beyaznar give an example of two social networking websites used by gays and lesbians. Being hosted abroad, these websites were directly blocked by the TIB. The owners of websites opened a lawsuit against the TIB and were able to revoke the blocking measure. The number of members of the websites increased significantly just after they were online again. 27

The TIB is generally on the public agenda with its polemical filtering, and blocking policies. Rather, the organization should give priority on how the Internet and Internet contents within the country can be enriched and developed further, how the numbers of Internet use can further be increased. A study shows that the number of websites registered within the country is just above the half of the ones in Greece with a population five times less than Türkiye. 28 The TIB should organize meetings, and community-based workings to enlighten public. It should initiate projects and programs to develop contributions of the Internet within the economic development and the like.

Dealing with blocking and filtering should not be the issue or policy of a democratic state like Türkiye. Such measures can be an "exception" within democratic principles, but should not become a systematic, un-proportional "policy". These issues can be left to the preference of individuals, the private sector and of course judicial authorities. State organizations can give priority more on other kinds of education and

preventive activities and supervision. The default legal and political mentality should be liberty and freedom on the Internet rather than blocking, restriction or censorship.
REFERENCES


"Bu Protokol Hackeri Kişidir." Vatan, 15 February 2012.

Budakoğlu, Selahattin, and Bursa - Doğan Haber Ajansı (Dogan News Agency). "Bilgi İşlem Sorumlusundan Çocuklara Tuzak." Milliyet, 4 February 2011.


"Çocuk İstismarını Ve İhmalini Önleme Derneği." http://www.cocukistismari.org/.

"Çocuk Pornosuna Karşı Nasıl Savaş Verirsiniz?" SDN, 14 April 2011.

"Çocuk Ve Bilgi Güvenliği Derneği." cbgd.org.


"Darısı Diğerlerinin Başına!" NTVMSNBC, 30 October 2010.


HT. "Ve Youtube Sorunu için Harekete Geçildi." Aktif Haber, 13 August 2010.


"İnternette 60 Saniyede Neler Oluyor?" *Timeturk*, 24 March 2012.


74, no. 2 (Spring 2007).


"Ministry of Transportation (Türkiye Cumhuriyeti Ulaştırma)." www.ubak.gov.tr/.


"Number of Active Users at Facebook over the Years." *Associated Press*, 1 May 2013.


Tan, Zixiang (Alex), William Foster, and Seymour E. Goodman. "China's State-


"Tor: Overview." https://www.torproject.org/about/overview.html.en.


"Turkish Ministry of Education (Milli Eğitim Bakanlığı)." http://www.meb.gov.tr/.


"TÜSİAD: Türkiye'deki İnternet Yasağı Hukuk'a Aykırıdır." Haber2000, 4 March 2011.


"Ulaştırma Bakanlığı'ndan Sert Google Açıklaması." Chip Online, 8 June 2010.

"Ultrasurf." http://ultrasurf.us/.


"Yasaklı Youtube Nasıl Girilir?" Internethaber, 7 March 2007.


"Youtube'dan Şaşırtan Açıklama." BilisimLive, 31 October 2010.

"Youtube'u Kapatırın Savcı Konuştu." Hürriyet, 18 June 2008.

"Youtube Yasagının Ucu Google'a Dokundu." Akşam, 5 June 2010.

"Youtube Yasak Ama..." Aktifhaber, 17 June 2008.
VITA

Ersin Elibol
Graduate Program in International Studies
Old Dominion University
Batten Arts and Letters Bldg., Room 7045
Norfolk, VA 23529

Education

Virginia Commonwealth University, Richmond, Virginia
• M.P.A. International Studies May 2007
Turkish National Police Academy Faculty of Security Studies, Ankara, Türkiye
• B.A. Security Studies June 1995

Experience

Interpol Ankara, Ankara, Türkiye 1995-2005
United Nations, Mission in Bosnia and Herzegovina (UNBIH)
Chief of Police in Province of Hilvan, Sanliurfa, Türkiye 2012-2013